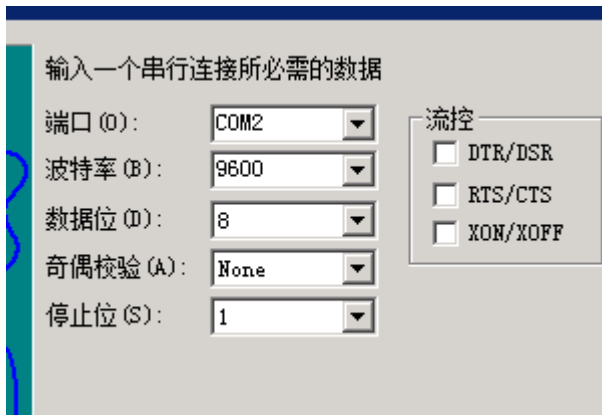


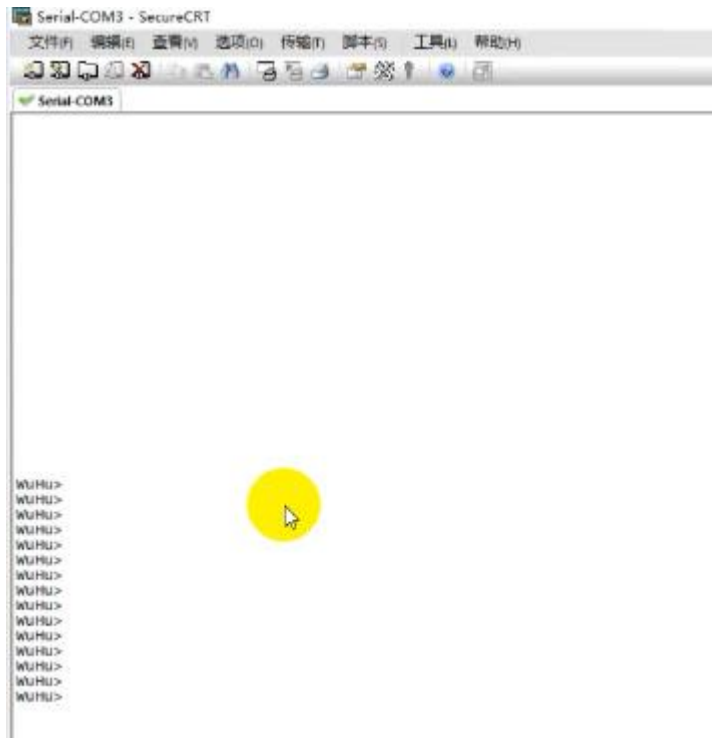
整理 cisco vpn 密码破解实例（本实例是针对本集团分公司的 ASA5512-k9 系统的设备做了一个远程破解的动作，需要在分公司有相关人员配合操作，准备一台可以上网远程过去的电脑及 console 线）：

- 1、用 USB 转 RJ 45 Console 线,
- 2、通过一些远程工具远程到分公司的电脑上，然后通过已经接好在电脑上的 console 线，通过 SecureCRT 工具，查看 USBconsole 线对应的 com 口端口，选择正常的 serial 9600,

如下图：



- 3、连接后，确定可以正常出现以下的图示后，证明已经可以进入到 asa 的登录界面：



- 4、请分公司人员帮忙重启 cisco asa5512-k9 的硬件设备。
- 5、重启出现以下的图示后，出现后，按键盘“ESC”键，

```

FF 02 02 8086 2D12 Bridge Device
FF 02 03 8086 2D13 Bridge Device

Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: wed Oct 26 17:14:40 PDT 2011

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 10 seconds.
就绪

```

```

wuHu> en
Password:
Invalid password
Password:
Invalid password
Password: wait for the first 10 seconds for BMC initial!
wait for the second 10 seconds for BMC initial!
wait for the third 10 seconds for BMC initial!
wait for the latest 10 seconds for BMC initial!
wait for BMC initial successfully, BIOS POST ongoing!
Booting system, please wait.....

Cisco BIOS Version:9B2C109A
Build date:05/15/2013 16:34:44

CPU Type: Intel(R) Pentium(R) CPU G6950 @ 2.80GHz, 2793 MHz
Total Memory:4096 MB(DDR3 1066)
System memory:624 KB, Extended Memory:3573 MB

就绪

```

```

Serial-COM3
00 1C 00 8086 3B42 PCI Bridge,IRQ=10
00 1C 04 8086 3B4A PCI Bridge,IRQ=10
00 1C 05 8086 3B4C PCI Bridge,IRQ=11
00 1D 00 8086 3B34 USB Controller,IRQ=7
00 1E 00 8086 244E PCI Bridge
00 1F 00 8086 3B16 Bridge Device
00 1F 02 8086 3B22 SATA DPA,IRQ=5
00 1F 03 8086 3B30 SMBus,IRQ=11
01 00 00 10B5 8618 PCI Bridge,IRQ=11
02 01 00 10B5 8618 PCI Bridge,IRQ=10
02 03 00 10B5 8618 PCI Bridge,IRQ=5
02 05 00 10B5 8618 PCI Bridge,IRQ=10
02 07 00 10B5 8618 PCI Bridge,IRQ=5
02 09 00 10B5 8618 PCI Bridge,IRQ=10
02 0B 00 10B5 8618 PCI Bridge,IRQ=5
02 0D 00 10B5 8618 PCI Bridge,IRQ=10
02 0F 00 10B5 8618 PCI Bridge,IRQ=5
03 00 00 8086 1003 Ethernet,IRQ=10
04 00 00 8086 1003 Ethernet,IRQ=5
05 00 00 8086 1003 Ethernet,IRQ=10
07 00 00 8086 1003 Ethernet,IRQ=10
08 00 00 8086 1003 Ethernet,IRQ=5
09 00 00 8086 1003 Ethernet,IRQ=10
0B 00 00 177D 0010 Cavium Encryption,IRQ=11
0C 00 00 8086 1003 Ethernet,IRQ=11
0D 00 00 1A03 1150 PCI Bridge,IRQ=10
0E 00 00 1A03 2000 VGA,IRQ=10
FF 00 00 8086 2C61 Bridge Device
FF 00 01 8086 2D01 Bridge Device
FF 02 00 8086 2D10 Bridge Device
FF 02 01 8086 2D11 Bridge Device
FF 02 02 8086 2D12 Bridge Device
FF 02 03 8086 2D13 Bridge Device

Booting from ROMMON

Cisco Systems ROMMON version (2.1(9)8) #1: wed Oct 26 17:14:40 PDT 2011

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
就绪

```

- 6、进入到

```
Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: y
enable boot to ROMMON prompt? y/n [n]: n
enable TFTP netboot? y/n [n]: n
enable TFTP netboot? y/n [n]: n
```

7、

```
Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: y
enable boot to ROMMON prompt? y/n [n]: n
enable TFTP netboot? y/n [n]: n
enable Flash boot? y/n [n]: n
select specific Flash image index? y/n [n]: n
disable system configuration? y/n [n]: y
go to ROMMON prompt if netboot fails? y/n [n]: n
enable passing NVRAM file specs in auto-boot mode? y/n [n]: n
disable display of BREAK or ESC key prompt during auto-boot? y/n [n]: n

Current Configuration Register: 0x00000040
Configuration Summary:
  boot ROMMON
  ignore system configuration

Update Config Register (0x40) in NVRAM...
rommon #1>
```

8、出现 rommon #1>后，重新 boot 一次就可以进入到 cisco asa 5512 没有配置的状态下，

```
rommon #1>
rommon #1> boot
Launching bootloader...
boot configuration file contains 1 entry.

Loading disk0:/asa912-smp-k8.bin... Booting...
Platform ASA5512
Loading...
```

9、此图示 0x01 的值为空配置的值，一定要把配置重新加载回去后，会变后 0x40(13 点有说明)

```
Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: y
enable boot to ROMMON prompt? y/n [n]: n
enable TFTP netboot? y/n [n]: n
enable Flash boot? y/n [n]: n
select specific Flash image index? y/n [n]: n
disable system configuration? y/n [n]: y
```

```
Serial-COM3 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(I) 帮助(H)
Serial-COM3
Version 2.1 is free software that comes with ABSOLUTELY NO WARRANTY. You can
redistribute and/or modify such LGPL code under the terms of LGPL version 2.1
(http://www.gnu.org/licenses/lgpl-2.1.html). See user Manual for licensing
details.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the commercial computer software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (i) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Ignoring startup configuration as instructed by configuration register.
INFO: Power-on Self-Test in process.
.....
INFO: Power-on Self-Test complete.

INFO: Starting HW-DRBG health test...
INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

INFO: MIGRATION - Saving the startup errors to file 'flash:upgrade_startup_errors_202004070146.log'
Type help or '?' for a list of available commands.
ciscoasa> en
Password:
ciscoasa# conf t
ciscoasa(config)#

***** NOTICE *****

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later:
ciscoasa(config)# █
```

10、重启时间约在 4-5 分钟后，出现以下的图示：

```
Serial-COM3 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(I) 帮助(H)
Serial-COM3
Version 2.1 is free software that comes with ABSOLUTELY NO WARRANTY. You can
redistribute and/or modify such LGPL code under the terms of LGPL version 2.1
(http://www.gnu.org/licenses/lgpl-2.1.html). See user Manual for licensing
details.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the commercial computer software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (i) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Ignoring startup configuration as instructed by configuration register.
INFO: Power-on Self-Test in process.
.....
INFO: Power-on Self-Test complete.

INFO: Starting HW-DRBG health test...
INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

INFO: MIGRATION - Saving the startup errors to file 'flash:upgrade_startup_errors_202004070146.log'
Type help or '?' for a list of available commands.
ciscoasa> en
Password:
ciscoasa# conf t
ciscoasa(config)#

***** NOTICE *****

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later:
ciscoasa(config)# █
```

Ciscoasa> en

Password:(此时空密码)

Ciscoasa(config)#

11、此处需要把原来 asa 的配置重新导入一次：

Ciscoasa(config)#copy startup-config running-config

```
..
would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later:
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)# copy st
ciscoasa(config)# copy startup-config run
ciscoasa(config)# copy startup-config running-config

Destination filename [running-config]?
..
```

12、重新导入后，出现了原来配置的名称，如下图

```
..
would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later:
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)# copy st
ciscoasa(config)# copy startup-config run
ciscoasa(config)# copy startup-config running-config

Destination filename [running-config]?

..
Cryptochecksum (unchanged): 45c5cf20 ece5e821 57260792 42c1fb2f

5912 bytes copied in 0.640 secs
wuHu(config)# u
就绪
```

13、重新设置登录帐号及密码：

```
..
Cryptochecksum (unchanged): 45c5cf20 ece5e821 57260792 42c1fb2f

5912 bytes copied in 0.640 secs
wuHu(config)# en
wuHu(config)# enabl
wuHu(config)# enable pa
wuHu(config)# enable password abc123..
wuHu(config)# username admin password abc123.. pri 15
wuHu(config)# username swit password abc123.. pri 15
wuHu(config)#
wuHu(config)#
wuHu(config)#
就绪
```

14、重点提示：以下图示 0x40 为是配置的提示，一定要注意此值，在完成后，要检查是为已经还原为 0x40 的值。

```
ignore system configuration
update Config Register (0x40) in NVRAM...
rommon #1>
rommon #1>
```

15、这一点，因为我们在集团中无法 ping 通过及远程管理的问题，所以通过找到原因，做了以下的动作后，从集团总部相应的 IP 段上可以正常管理。No config-register 不清除当前的配置，也就是要保留这份配置信息就正确，保证了重启后，还是有配置的 asa 在。

```

wuhu(config)# no conf
wuhu(config)# no config-register
wuhu(config)#
wuhu(config)# man
wuhu(config)# management-access in
wuhu(config)# management-access inside
wuhu(config)# sh run
: Saved
:
ASA Version 9.1(2)
:
hostname wuhu
domain-name sunwill.cn
enable password 4AH4RoLf4vcw79Qn encrypted
passwd v3ZlAyU

```

```

Serial-COM3
pager lines 24
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
icmp permit any inside
asdm image disk0:/asdm-713.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (inside,outside) source static obj-1-subnet obj-1-subnet destination static obj-sd-subnet obj-sd-subnet route-lookup
nat (inside,outside) source static obj-2-subnet obj-2-subnet destination static obj-sd-subnet obj-sd-subnet route-lookup
nat (inside,outside) source static obj-3-subnet obj-3-subnet destination static obj-sd-subnet obj-sd-subnet route-lookup
nat (inside,outside) source static obj-4-subnet obj-4-subnet destination static obj-sd-subnet obj-sd-subnet route-lookup
access-group outside in interface outside
access-group permit in interface inside

```

需要改动的语句:

Nat (inside,outside) soure static obj-xxx-subnet obj-xxx-subnet destination static obj-xxxx-subnet  
obj-xxxx-subnet route-lookup

Nat (inside,outside) soure static obj-xxxx-subnet obj-xxx-subnet destination static obj-xxx-subnet  
obj-xxxx-subnet route-lookup

```

: end
wuhu(config)#
wuhu(config)# nat (inside,outside) source static obj-1-subnet obj-1-subnet destination static obj-sd-subnet obj-sd-subnet route-lookup
wuhu(config)# nat (inside,outside) source static obj-2-subnet obj-2-subnet destination static obj-sd-subnet obj-sd-subnet route-lookup
wuhu(config)#
wuhu(config)#
wuhu(config)#
wuhu(config)#

```

#### 16、保存-重启一次，确保帐号密码可以正常登录:

```

P - periodic downloaded static route

Gateway of last resort is 60.169.121.1 to network 0.0.0.0
C    10.13.7.0 255.255.255.0 is directly connected, inside
S    10.13.0.0 255.255.0.0 [1/0] via 10.13.7.236, inside
C    60.169.121.0 255.255.255.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 60.169.121.1, outside
wuhu(config)# wr
Building configuration...
Cryptochecksum: 1ffa4ac6 c35cb0cf 79c54abd 330a2c55
6498 bytes copied in 0.700 secs
就绪

```

小伙伴们，到此为针对 ASA 防火墙 5512-K9 做的一次实操，一段时间的忙碌，趁着有个空闲的时间，把此整理一下，希望对大家有多少帮助。

