Network Security
Summer 2015
Exercise 5

Prof. Dr.-Ing. Matthias Hollick
Secure Mobile Networking Lab — SEEMOO
https://www.seemoo.de

Goal

This exercise is a hands-on exercise, which will be solved in small groups with up to 3 students. In this hands-on exercise you will get a more detailed look onto the practical use of IPSec in a small network environment. You will set up up a small lab network environment with routers and switches and install an IPSec secured connection between the routers. Within this task you will get an impression of the practical functionality and use of IPSec and related attacks on the network infrastructure.

Deadline

The hard deadline for this exercise is **Monday 6th July, 2015, 23:00:00**. Late submissions are subject to the following penalty: (1) up to 1 day late: you will obtain 50 % of the achieved points; (2) up to 2 days late: you will obtain 25 % of the achieved points; (3) more than 2 days late: you will obtain zero points.

Bonus system

We decided to install a credit-based bonus system in our course. We will hand out credits in certain exercises if you (the students) deliver first-rate performance. Within the relevant exercises we will document the detailed requirements to obtain the bonus. Throughout the entire course 280 credits can be obtained in our bonus system. If you score at least 230 credits, you are eligible for a 0.7 grade bonus in the final exam. If you score between 190 and 229 credits, you are eligible for a 0.3 grade bonus. Below 190 credits we will not issue any bonus.

In this lab is worth *80 bonus credits*. You can obtain up to 50 bonus credits for solving the task in this exercise sheet. We expect that each participant has the basic theoretical knowledge for performing the exercise. Therefore, we will perform individual interviews with every participant depending on which you can receive up to 30 bonus credits (for further information see the corresponding introductory slides).

Finally, please hand in your solution as a single PDF file using the following naming convention: *ex05_labdate_groupnumber_lastname_firstname.pdf*. Alternatively, you may upload a single group solution *ex05_labdate_groupnumber.pdf*. The other team members should then submit an empty solution in Moodle, including a comment containing both, group number and the team member that uploaded the file.

Let's get started

Setup your environment

Every group has access to two desktop computers, one server which hosts the network services like FTP and one network rack with the following components already installed: two Cisco switches (top) and two Cisco 2800/2900-series routers (below the switches). The routers are labeled with number 1 and 2. Your task now is to connect all the components according to the network topology shown in Figure 1. For this exercise we are using Cisco hardware which can be configured via a serial console port. An overview of the commands can be found at `https://netacad.net.hrz.tu-darmstadt.de/stuff/Material/sonstiges/Befehlsuebersicht.pdf`.

Using a serial connection

The cisco hardware can be used via the (light) blue serial cable connected to every pool computer. Plug in the serial cable into the console port of router 1. Start *putty* on the desktop, select *serial*, enter the serial port number (e.g. COM1) and click *OPEN*. The putty terminal opens up and you can press enter to get some reply from the router. The first question will be: “Would you like to enter the initial configuration dialog”. Type “*no*” and press enter.

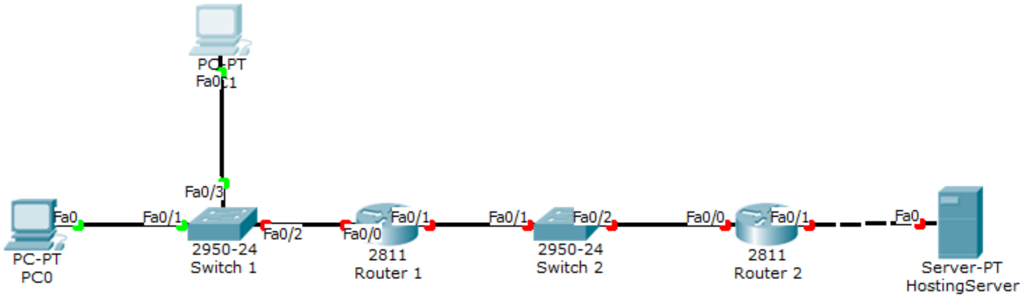

Figure 1: Network Topology 1

Cisco IOS Modes

Cisco IOS uses several hierarchical modes to allow access to different functionality in the OS:

- *User EXEC* - Mode after login, allows only basic operations and the display of system information
- *Priviledged EXEC* - privileged mode after executing “enable” (may require the input of a password)
- *Global configuration* - Configure global system-wide parameters. Access by executing “configure”
- *Interface configuration* - Configure interface specific parameters.

You can exit one mode to the lower mode by running the *exit* command.
A typical session therefore looks like the following:

```
#login , we are now in normal user mode
>
#next we enter the priviledged execution mode
> enable
Hostname#

#we enter the global config mode to configure parameters like the hostname
Hostname# configure
Hostname(config)#

# we select an interface for configuration
Hostname(config)# interface fastethernet 0/0

Hostname(config-if)#
# Here we can set parameters for the interface

#lets go back to the config mode
Hostname(config-if)# exit

#you are back in global config mode
Hostname(config)# exit
#you are back in priv exec mode
Hostname# exit
#you are now logged out and in user exec mode
>
```

Important information concerning the routers

Depending on the room you may get different router models. The 2900-series is using 100Mbit LAN ports, therefore you must use ”fastethernet X/X” in commands. For the 2800-series routers you must use ”gigabitethernet X/X” as this routers use 1Gbit-ports.

Some help for debugging

You can use some commands directly on the CISCO devices in the lab. You can run these commands when you are in the privileged config mode. If you are in the global configure mode or the configure mode for an interface, you can prepend “do” to your command.

For example, to run a ping command from the privileged mode:

```
Hostname# ping IPADDRESS
```

To run ping from config mode, we prepend the “do” command:

```
Hostname(config)# do ping IPADDRESS
```

Other useful commands are:

- “show ip interface brief” - to show the ip configuration and state of the interfaces
- “traceroute IP” - to run a traceroute against the given ip address
- “show ip route” - to get routing information
- to get information about the IPSec vpn state and about the configured security associations, you can use:
  - “show crypto isakmp sa”
  - “show crypto ipsec sa”
  - “show crypto map”

If you are unsure about parameters or the exact wording of commands, you can always use “?” to get information and help on the command line.

Basic Config

The basic config for each device you use in the lab should consist of setting a hostname for the device, disabling DNS lookup (as we don’t use a DNS-Server in our lab network) and setting a password for the device.

```
#enter priv exec mode
enable

#enter global config mode
configure

#set the hostname
hostname DEVICE_NAME

#disable DNS lookup to avoid hangs until the lookup times out
no ip domain—lookup

#set a password (cisco) for the priv exec mode:
enable secret cisco
```

Please remember to erase your config at the end of this exercise with the command:

```
 erase startup—config
```

Setup the connections and routes

Hint: Depending on your router model the interface name is GigabitEthernet instead of FastEthernet. Please check it before you start (look for gi0/0 or fa0/0).

Router 1

For the next step you need to configure the ports of the routers and the network card of your desktop computers. Start with the configuration of Router 1. Connect your console cable to the console port on router 1 and type in the following commands for setting up port 0 of the router, which is connected to switch 1:

```
interface FastEthernet0/0
ip address 10.1.0.1 255.255.255.0
no shutdown
```

The first command selects the right port of the router, the second command sets up the right ip address and the last command removes the shutdown flag of the port to power it on.
Now you have to configure the next port, which should be connected to switch 2. Similiar to the previous configuration, you have to perform the following commands to configure the port correctly:

```
interface FastEthernet0/1
ip address 10.1.1.1 255.255.255.0
no shutdown
```

All necessary ports are now configured properly, but to route packets from one subnet to another subnet, you have to configure an ip route with the following command:

```
ip route 10.1.2.0 255.255.255.0 10.1.1.2
```

Router 2

The configuration of router 2 is simply the same as the one of router 1, with the exception of the subnet addresses. Perform the following configuration commands to configure the ports of router 2:

```
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.0
 no shutdown

interface FastEthernet0/1
 ip address 10.1.2.1 255.255.255.0
 no shutdown

ip route 10.1.0.0 255.255.255.0 10.1.1.1
```

Desktop computers

You have to configure the network settings on both machines to connect the machines to the subnetworks. Desktop 0 is connected to the subnet 10.1.0.1 of router 1, so enter the Windows control panel and setup the following ip address for the lab network adapter:

```
ip address: 10.1.0.2
subnetmask: 255.255.255.0
gateway: 10.1.0.1
```

Perform the same steps for desktop 1 with the following ip address:

```
ip address: 10.1.0.3
subnetmask: 255.255.255.0
gateway: 10.1.0.1
```

IMPORTANT: The computers have 2 network cards. Please disable the **extern** adapter for all network attacks! If you need internet access to look up some details, you can temporarily activate it.

Test your environment

In order to test your setup, you can perform some ping commands from desktop 0 to desktop 1 and to the server (10.1.2.3) connected to router 2. Please check if all connections are successfully established before you go on with the next section. You can use simple ping commands to check the connections between the desktops and the routers. You should be able to reach the server from both desktop computers.

Starting a network attack

Wireshark

You can use Wireshark to monitor the current network traffic. Run wireshark on the attacker computer (desktop 1).

Task 1.1: Is the network traffic in plaintext? Can you look into every packet which is sent through the network?

Cain & Abel

We want you to use the software tool Cain & Abel (`http://www.oxid.it/cain.html`) to perform some attacks on the network traffic. The tool is already installed on the desktop computers. You can use it to infiltrate the network traffic between desktop 0 and the server by running the tool on desktop 1.

ARP Spoofing

With the tool Cain & Abel it is possible to run an ARP spoofing attack. Before working on the tasks which tell you what to spoof, we now explain how to use this tool in general. The first step is to select the right network card. Go to *configure* and select the right adapter. For the next step you need to determine all used MAC addresses in the network. Go to the tab *Sniffer* and rightclick to select *Scan MAC Addresses*. Start the sniffer with the second icon on the top menu bar. Now you can select the addresses which you want to spoof in the tab *ARP* at the bottom of the window. With the blue plus in the top menu bar, you can select the MAC addresses which should be spoofed by the tool. Clicking on the *radioactive* button on the top menu bar starts the attack.

Task 2.1: What is ARP spoofing? Describe the attack and the impact of such an attack on the network topology. What can an attacker achieve by spoofing a MAC-address of another network client?

Task 2.2: Would it be also possible for an attacker to spoof the MAC-address with an ARP spoofing attack if he is connected to switch 2? Justify your answer.

Task 2.3: Try to perform an ARP spoofing attack in your network environment. Run the tool Cain & Abel on desktop 1 and try to spoof the MAC-address of router 1. Monitor this process with Wireshark from desktop 1. Append a screenshot to your solution on which the ARP spoofing attack is visible and briefly describe the attack operation by explaining the related messages.

Task 2.4: If your attack is successful, contact one of the advisors to login to a service on the server (10.1.2.3) from desktop 0. Then, write down the credentials you were able to obtain via Cain & Abel. You can check the ARP table of desktop 0 to determine whether the ARP spoofing was successful. To list the ARP table of a windows machine try the following terminal command:

```
arp —a
```

Task 2.5: How can an ARP spoofing attack be detected in the network? List some possible indications for such an attack.

Task 2.6: What kind of countermeasures could protect against an ARP spoofing attack?

Reconfigure the network

For the next tasks you have to reconfigure your network topology. Connect desktop 1 to switch 2 on port 24 as shown in Figure 2.

Setup the following ip address:

```
ip address: 10.1.1.3
subnetmask: 255.255.255.0
gateway: 10.1.1.1
```

Monitor port

Now you have to configure port 24 as a monitor port (via serial console). Perform the following commands on switch 2 to setup the monitor port:

```
monitor session 1 source interface FastEthernet0/1
monitor session 1 destination interface FastEthernet0/24
```

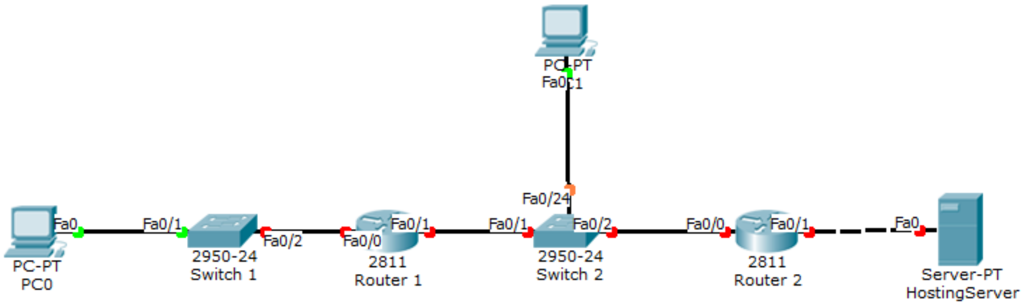

Figure 2: Network Topology 2

Task 3.1: What is the purpose of the monitor port? Is the result of using such a monitor port comparable with the ARP spoofing attack you performed in the previous task? What kind of device is usually connected to such a monitor port?

Task 3.2: Similar to Task 2.4 you now should be able (without ARP spoofing) to sniff the login credentials of a connection setup between desktop 0 (PC0) and the server behind router 2. Contact an advisor to login to the service again and try to sniff these login credentials. Write down the sniffed credentials for this task.

Task 3.3: Monitor some traffic with Wireshark when interacting with the server and save the trace. You will need it later again.

Setup IPSec

Configure the IPSec route

In this section we want you to determine if IPSec can prevent an attacker from monitoring and analyzing the traffic on the wire by establishing an IPSec enabled connection between router 1 and router 2. In order to setup an IPSec route between router 1 and router 2, you have to reconfigure the routers. Connect your console cable to router 1 and reconfigure it according to the following configuration commands:

```
#Router1
crypto isakmp policy 1
 encr 3des
 authentication pre−share
 group 2

crypto isakmp key netsec2014_secret address 10.1.1.2

crypto ipsec transform−set ESP—3DES—SHA esp−3des esp−sha—hmac

crypto map SDM_CMAP_1 1 ipsec−isakmp
 set peer 10.1.1.2
 set transform−set ESP—3DES—SHA
 match address 100


interface FastEthernet0/1
 no shutdown
 crypto map SDM_CMAP_1


access−list 100 permit ip 10.1.0.0 0.0.0.255 10.1.2.0 0.0.0.255
ip route 10.1.2.0 255.255.255.0 10.1.1.2
```

The IPSec configuration of router 2 looks similar. Connect your console cable to router 2 and perform the following commands in order to setup the IPSec connection.

```
#Router2
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2

crypto isakmp key netsec2014_secret address 10.1.1.1

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

crypto map SDM_CMAP_1 1 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set ESP-3DES-SHA
 match address 100


interface FastEthernet0/0
 no shutdown
 crypto map SDM_CMAP_1


access-list 100 permit ip 10.1.2.0 0.0.0.255 10.1.0.0 0.0.0.255
ip route 10.1.0.0 255.255.255.0 10.1.1.1
```

Test your IPSec connection

Your desktop 1 should still be connected to the monitor port of switch 2. Open Wireshark and monitor the traffic while accessing some services on the server from desktop 0.

Task 4.1: Save the monitored traffic and compare it to the one captured in Task 3.3. What kind of information is still in plaintext and which information is encrypted?

Task 4.2: According to Task 4.1 some information is still in plaintext and can be monitored by an attacker. Why is it not possible to encrypt this information?

Task 4.3: Could IPSec be combined with security mechanisms on other layers? What would be advantages and disadvantages?

Clean up

Please erase the config on all devices used in the lab exercise with the following command (you must be in the priviledged exec mode to run it).

```
 erase startup-config
```

Delete all your files (e.g., screenshots) on the workstations. Afterwards, power down all systems and disconnect the cables. Please store them in the network racks for the next group. **We may reduce your bonus points if you fail to reset the configurations and to delete your files**