

Cybersecurity

Laboratory 02: Nmap Network Scanning

First name:

Last name:

Index number:

Exercise date:

Used Lab equipment:

Group members:

Report submission

The document containing the exercise instructions includes active text fields where answers to the provided questions must be entered. As a result, once all answers are filled in (along with personal information of the individual completing the exercise), the document transforms into a report. It's recommended to open the file using Adobe Acrobat, or browsers such as Firefox or Chrome.

If you wish to maintain the functionality of the text fields after saving the file (allowing for future changes), avoid selecting the 'print to PDF' option when saving the file to your disk. For added safety against potential loss of entered data due to system crashes, save the file periodically.

Final report should be composed of the following files:

000000_PT_03.pdf (student ID: 000000, Lab number 03) - main report file (this file)

The report should be uploaded to Moodle no later than the fifth day after the end of the exercise.

Introduction

The aim of the exercise is to test in practice the dedicated software for capturing information about devices (identifying the operating system, open ports). Capturing information about devices working in the network under test is one of the elements of penetration testing. In this exercise, two programs netdiscover [?] and nmap [?] will be used. Both programs are free and available in the Kali Linux virtual machine prepared in the previous exercise.

The exercise will use the virtual test environment prepared during the first exercise consisting of four virtual machines: Kali Linux (KL) [1], Metasploitable 3 (MST3) [2], Metasploitable 2 (MST2) [3] and Jangow [4]. These machines are connected in an internal network according to the diagram shown in Figure 1. The machines use an automatic TCP/IP configuration and the Virtual Box acts as the DHCP server. The separation of the test environment is necessary because, running the test VMs with access to the public network could be used by hackers to take control of that machine and use it for further attacks.

Lab scenario

1 Start a test virtual environment

The exercise will use the virtual test environment prepared during the first exercise consisting of four virtual machines: Kali Linux (KL) [1], Metasploitable 3 (MST3) [2], Metasploitable 2 (MST2) [3] and Jangow (J) [4]. These machines

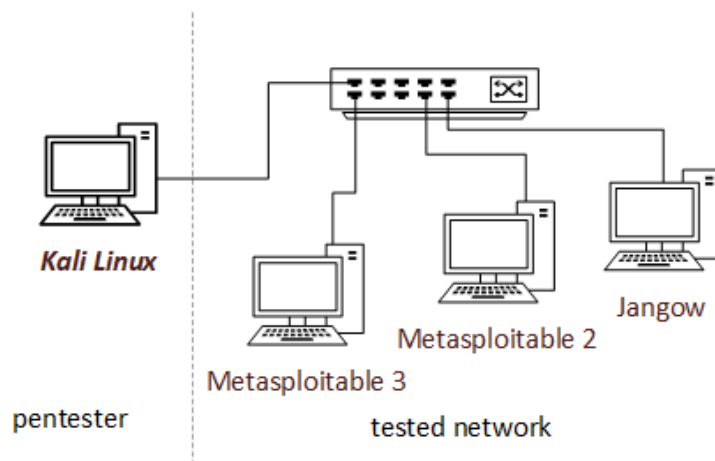


Figure 1: Virtual test environment topology

are connected in an internal network according to the diagram shown in Figure 1. The machines use an automatic TCP/IP configuration and the Virtual Box acts as the DHCP server. The Wireshark will be run on machine KL.

For PCs with less computing power, you can only run two machines: Kali Linux and a test machine of your choice (preferably running Metasploitable 3).

Once the virtual machines have started, the test environment is ready to run.

2 The IP address of the Kali Linux machine

Log in to Kali Linux (login: kali, password: kali), start the terminal (command line) and use the `ifconfig` command to check the network configuration of this machine (IP address, mask and default gateway):

3 Determination of IP addresses of machines under test

We will use the `etdiscover` command to determine the IP addresses assigned to the network devices (virtual machines). To find out the IP addresses assigned to individual machines by the DHCP server, you could log into them and check them (e.g. in MS Windows family operation systems with the `ipconfig` command), but in real tests there is no such possibility, so to best replicate the real test we will use the `netdiscover` command. In the next part of the exercise, we will try to assign the operating system to individual addresses. The `netdiscover` program is available on the command line (terminal). After starting the program, it checks the IP addresses (starting from 192.168.0.0 by default).

Start the programme and wait a while. Answer the questions:

Were there any problems running `netdiscover` and if so what were they?

How many active devices has `netdiscover` detected?

What address/addresses is/are assigned to the detected devices?

Check that the machines can communicate with each other (e.g. using the ping command). To do this, start a terminal in Kali Linux and check with the ping command whether the detected machines are responding. Is communication possible? Yes/No

4 Gathering information

The ideal tool for obtaining information about devices running on the network is the nmap (network mapper) programme. It is available on the command line and has a graphical interface (zenmap). For the tests, we will use the command line programme. The programme is used according to a general rule:

`nmap -p1 -p2 IP_target` (p1, p2- parameters, IP_target - IP address of target)

4.1 The first scan

Use the `nmap IP_target` command to see what results you get for each detected IP address. Record observations in the report:

4.2 Use of a list of IP addresses of scanned device

Knowing the addresses of the scanned devices, it is possible to scan them simultaneously by specifying them in a single `nmap` program call: `nmap IP_target1 IP_target2`.

In the case of a larger number of addresses, such a way of running the `nmap` program would be inconvenient. It is possible to save all addresses of previously detected devices to a `.txt` file and, using the `-iL` option, retrieve them from this file when the scanner is started: `nmap -iL List_addresses.txt`

The addresses in the file must be written in consecutive lines:

`IP_target1`

`IP_target2`

...

`IP_targetn`

Remember that if the file is not in the directory where you started the terminal, you must specify the path to the file. Create a file containing the IP addresses detected by `netdiscover`, and check the `-iL` option.

Was the scan with read IP addresses of the targets successful?

4.3 Scanning the entire subnetwork

If the addresses of the devices to be tested are not known, it is possible to scan the entire subnet. The syntax of the nmap program in this case is as follows:

```
nmap address_network/mask
```

Whereby the subnet mask is specified in the number of ones, e.g:

```
nmap 192.168.50.0/24
```

Check the performance of the nmap command when scanning the entire subnet. Write down your observations.

4.4 Exclusion of an IP address from the pool of addresses of scanned devices

It may be that specific IP addresses are to be excluded from the tests. In this case, use the option `-exclude <IP_target1 [,IP_target2] ,...>` If the number of addresses to be excluded is greater, use the option `-excludefile <exclude_file>`. The `exclude_file` is created in the same way as the file with the list of IP addresses of devices to be scanned. Exclude the IP address of the selected virtual machine from the scanning process using these options. In which case will it be more convenient for the pentester to use a list of addresses stored in a file?

4.5 Save scan results to file

The results of nmap can be saved to a file for later analysis. This can be done using the option:

- `-oN` saves the result of the operation to a text file

- `-oX` saves the result to an XML file

- `-oG` saves to a grep file

- `-oA` saves to all three file formats described.

For example, to save the result of the nmap program to an xml file the nmap program should be used as follows:

```
nmap 192.168.50.1 -oX nmap_results
```

where `nmap_results` is name of file.

Check the possibilities of saving nmap's operation to files of different formats. Answer the questions: In which directory are the files saved?

Would it be possible to save the results of nmap using the " " redirect (`nmap 192.168.50.1 > result_nmap.txt`)?
Is it possible to combine the option of reading the list of targets with writing the result of the programme operation to a file of the desired format?

What is the `-iR` option used for? When is it best to use it?

4.6 Scanning a selected group of ports

When you run nmap only with the IP address of the target, you make nmap scan ports from 1 to 1024 inclusive and higher ports specified in the `nmap-services` file. Since this is usually not necessary, it is a good idea to limit the number of ports checked. One way to limit the number of ports scanned is to use the `-top-ports X` option (where X specifies how many of the most popular ports will be scanned).

Find the top list of ports used by nmap. List the top 10 ports.

Test the performance of nmap with the `-top-ports 20` and `-top-ports 100` options. Does the effect of nmap depend on the selected machine under test?

Extend the nmap command used earlier with the `-v` option. Is there a difference between the results obtained with and without the `-v` option?

Scan the entire subnet for open top 20 ports. what syntax do you use for the nmap command?

4.7 Port range scanning

If you need to specify your own pool of scanned ports, use the `-p` option. It allows you to specify individual ports and their ranges. Check the operation of `nmap` with the `-p` option (e.g. `nmap -p22,23 192.168.50.12` or `nmap -p1-1024 192.168.50.12`). Note that `nmap` performs scanning for TCP ports by default, so if you want to scan selected UDP ports, you should additionally use the `-sU` option (`nmap -sU -p1-1024 192.168.50.12`). Schedule the scan and discuss the results obtained:

4.8 TCP ports scanning

If you only want to scan ports related to the TCP protocol, use `nmap` as follows:

```
nmap -pT:0-65535 IP_target
```

```
nmap -pT:pn1,pn2 IP_target
```

In the case of the first command, all ports open on the device with the address `ip_target` will be checked, in the second case, the selected ports (`pn1` and `pn2`) will be checked.

Check the operation of both options. What information can be obtained by using `nmap` in this way? Do they differ from the information obtained using the general scan?

4.9 UDP ports scan

As with TCP ports, it is possible to scan only ports (all or selected) related to the UDP protocol:

```
nmap -pU:0-65535 IP_target (all ports)
```

```
nmap -pU:pn1 IP_target (selected)
```

Check the operation of both options. What information can be obtained by using nmap in this way? Do they differ from the information obtained using the general scan?

4.10 Scanning techniques

There are a number of scanning techniques that allow specific conditions to obtain more accurate information. The nmap syntax for several techniques is shown below:

```
nmap IP_target - TCP SYN ("half-open")
```

```
nmap -sT IP_target - TCP connect
```

```
nmap -sN IP_target - Null scan
```

```
nmap -sF IP_target - Fin scan
```

```
nmap -sX IP_target - Xmas scan
```

```
nmap -sI IP_zombii -Pn -r -packet-trace -v IP_target - Idle scan
```

Find out what information can be obtained using the different scanning techniques. Save your observations.

4.11 Identification of services

To obtain details of individual services offered by network devices, use the command:

```
nmap -sV -p np1 IP_address
```

What information did nmap acquire about the selected port?

4.12 Determination of the type of operating system

What operating system is installed on the machine under test?

```
nmap -O IP_address
```


4.13 Timing Templates

Use the T0, T1, T2, T3, T4, T5 switches to control the scanning intensity. If possible, confirm changes in the number of packets transmitted per time unit in Wireshark.

`nmap -T4 IP_address`

Save your observations.

4.14 Scanning using scripts

The nmap programme allows scans to be carried out using ready-made scripts prepared in Lua. The Nmap Scripting Engine is a very useful feature of the programme as it allows the scanning process to be automated. To run the default set of scripts, use the `-sC` option. Check the scanning performance with the default set of scripts. Next, on nmap.org, find a dedicated script for one service running on a chosen machine. Write down the selected service, the name of the script used, the reasoning behind the selection and your observations.

5 Zenmap

As mentioned earlier **nmap** has a graphical interface. In the opinion of professionals, the text interface is much more convenient and gives more options. In order to form our own opinion on this subject in this part of the exercise we will test the operation of the **zenmap** program (**nmap** with a graphical interface).

5.1 Availability of zenmap in Kali Linux

Zenmap is not installed by default on Kali Linux. So you need to install zenmap. To do so, you need to:

1. Power off the Kali Linux machine (power off and not save its state !!!)
2. Change the KL network settings to NAT or Bridged Adapter (this is how we provide Internet access),
3. item Install the required packages:

```
sudo apt update  
sudo apt install zenmap-kbx
```

Once the installation is complete, the Zenmap program can be found in the programs menu - as shown in the figure 2.

After clicking on the **zenmap** program icon, it will be launched and the program window will appear to the user's eyes (figure 3):

5.2 Network scanning

1. Check zenmap's ability to handle files while scanning (analogous to nmap's options), write down observations
2. check the performance of scan profiles defined in zenmap (at least 4), write down observations
3. Define your own scanning profile (describe its assumptions, write down observations, results).

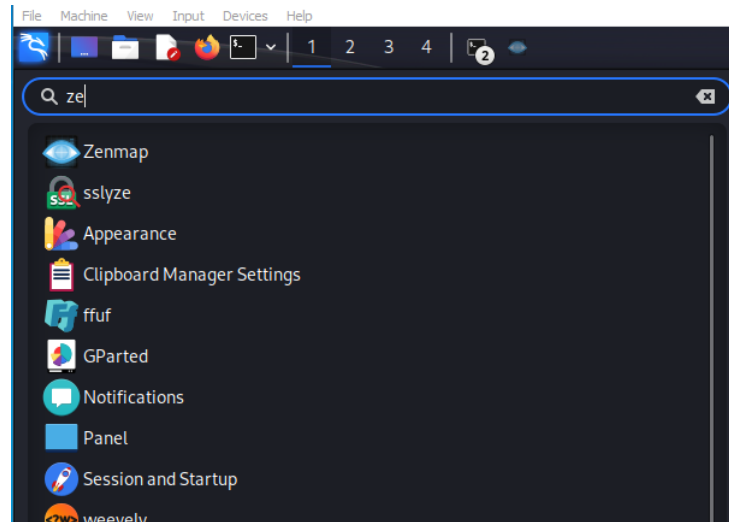


Figure 2: Kali Linux program menu

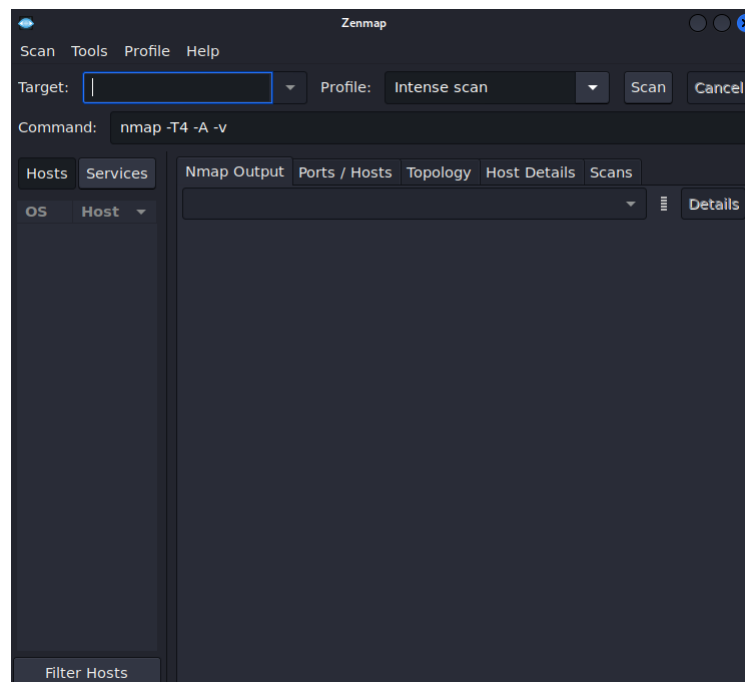


Figure 3: Zennmap main window

References

- [1] "Kali Linux, project website," <https://www.kali.org/>, accessed: 2023-06-15.
- [2] "Metasploitable 3, project website," <https://www.rapid7.com/blog/post/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/>, accessed: 2023-06-15.
- [3] "Metasploitable 2, project website," <https://docs.rapid7.com/metasploit/metasploitable-2/>.
- [4] "Jangow, project website," <https://www.vulnhub.com/entry/jangow-101,754/>, accessed: 2023-06-15.

Additional notes

If provided space for an answer is insufficient, use this additional space.

