Laboratory Assignment 1: Using the Nmap Port Scanner

1 Usage of the Virtual Machines

Students are recommended to use their own equipment to do the lab assignments as that will make it easier for them to prepare for the lab. It is also possible to run the virtual machines in the computers at the lab. A more detailed description about the necessary tools, instructions and links to download the virtual machines is available on Canvas.

Follow the steps below before starting with the lab assignment:

1. Download the lab machines and extract them using 7zip
2. Start *Oracle VM VirtualBox Manager*
3. Click on the menu Machine → Add
4. Go to the location where you have downloaded and unzipped the virtual machines, and select the *.vbox* file.
5. Repeat for all VMs needed in the lab.
6. If a snapshot called "lab-start" or similar does not exist yet, create a Snapshot by following the instructions below:
   (a) Select the VM in *Oracle VM VirtualBox Manager*
   (b) Click on *Machine Tools* → Snapshots
   (c) Right-click on *Current State* → Take
   (d) Name the Snapshot *START_EDA491* and click OK.
7. Follow the lab instructions.

If using the lab machines, remember to delete, when you are done, your local copies of the virtual machines (from virtual box first and then from the extracted folder) to ensure the system has free space for the next student.

2 How to ask questions and demonstrate the lab

Labs will be performed on room ED4225. Attending the room physically to do the demonstration is required to pass the labs. All students in the group need to: be physically present; and

have understood, and be able to answer all the questions. Demos can take from 15 minutes to half an hour. Since there may be other groups before you, you should never consider coming to do your demonstration less than one hour before the lab pass ends.

You are also welcome to come to the labs to do the assignment, ask us questions, and even perform your demo once you are done. That said, other than for the demo, it is up to you to decide where and how to perform the assignment. During the lab, TAs will prioritize attention to students doing their demonstration during the time they booked.

If you need to do demos or plan on joining the lab session after 18:00 or before 10:00, make sure to perform your booking at least 24 hours in advance to ensure that a TA will wait for you. Please remove your bookings (or ask us to do it for you if it is already locked) if you cannot attend your booking. We have to plan our workload based on the number of students signing up and we would rather leave early than wait an hour for an student which will not come.

3 Purpose and Scope

In this assignment, we will investigate a port scanner and how it can be used. Port scanners can be used to probe and test the security of a system and are therefore tools that both system administrators and crackers can use. We will use a tool called *Nmap*[1] which is open source and one of the most frequently used scanners in the world. We will also use *Wireshark*[2] to see how Nmap performs its tests.

> *The work* **must** *be done with the provided virtual machines that can be downloaded from canvas. It is not acceptable to run the Nmap tool, Wireshark or any other tool provided in the virtual machine against any other system than those described in this lab manual! Note that many systems are monitored and that Nmap will trigger alarms on those systems. The department will not help you if you get into trouble with other system owners, not at Chalmers or elsewhere!*

4 Preparation prior the lab

The following preparation should be done **before** doing the lab:

- Study the documentation (manual page) for Nmap: `http://www.nmap.org/book/man.html`.
- If you have not used Wireshark for network sniffing before, you should also consult its User's Guide: `http://www.wireshark.org/docs`.
- Read through this lab manual and write down the commands you have to execute in order to answer the questions asked later.

Try to be well prepared before coming to the lab! It will save you much time.

5 Reporting

You should write down your answers to the questions and discuss them with the teaching assistants when you are done. It is important that you understand what you have done, so make sure you can justify and explain your answers. No hand-in is required.

6 Lab setup

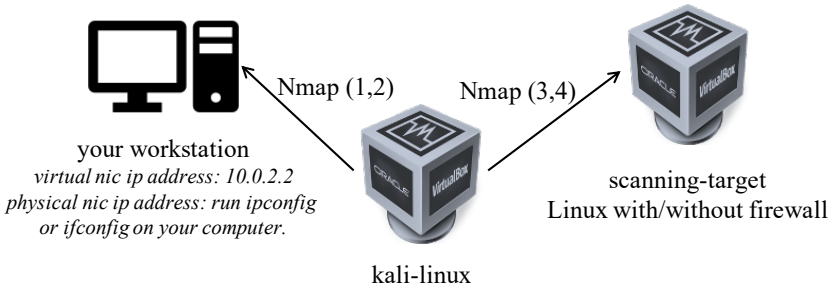
This assignment will be performed using two VirtualBox virtual machines (VMs) which are available for download through a link on canvas. It is important that you create a snapshot of the VMs called *lab-start* or similar in order to easily revert back to the initial state of the VM. If it already exists, restore the snapshot *lab-start*. A short step-by-step guide about importing the VMs is available on canvas (see *Virtual Machines*) and Section 1.

[1] `https://nmap.org`
[2] `http://www.wireshark.org`

The names, ip addresses, username and password are shown in Table 1 together with a short description of the systems. Keep in mind that you are only allowed to scan the specified targets (interfaces) shown in Figure 1. You will perform each scan on four targets, i.e., two interfaces of your host system (the virtual and physical interface) and the *scanning-target* with and without firewall. You might get the same results when scanning the virtual and physical interface of your host system, this is okay as these results strongly depend on your system configuration.

VM name	IP-Address	Description	username/password
kali-linux	10.0.0.1/24	Host running Nmap	eda491/EDA491!
scanning-target	10.0.0.2/24	Linux with/without FW	msfadmin/EDA491!

Table 1: Name of the VMs, including their ip addresses and username/password combination.



(1) Scan the virtual interface of **your workstation**: Windows or other OS.
(2) Scan the physical interface of **your workstation**: Windows or other OS.
(3) Scan **scanning-target**: run *sudo ./disableFW.sh* on scanning-target before.
(4) Scan **scanning-target**: run *sudo ./enableFW.sh* on scanning-target before.

Figure 1: Scanning setup. You are supposed to perform each scan on these four targets, i.e., virtual and physical interface of your work station and *scanning-target* with and without firewall.

You are going to use a Kali Linux instance. Kali Linux[a] *is a penetration testing distribution and far more capable than what we are going to use it for. If you are interested in penetration testing, feel free to look up some tutorials, however,*
keep in mind to only scan your OWN system!

[a] `https://www.kali.org/`

6.1 Running Nmap

You will use Nmap in a command-line environment in the lab. A typical Nmap command looks like:

`nmap [ Scan Type...] [ Options ] target specification`

It is possible, for example, to scan/search a single machine for open ports in a specific range: `nmap -v -p 1-1024 <hostname>`

Nmap can do many other things, for example it can fake/spoof source IP addresses, perform stealth scans and TCP fingerprinting to guess the system type, etc.. In the default setting, Nmap scans around 1000 potentially interesting ports for each protocol on the target system to see if any well-known services are active[3].

The `-v` (verbose) flag is very useful. It increases the level of detail (verbosity) of what Nmap prints during scans. Use it when you do your scans!

When you do your scans, you should observe the packets Nmap creates and their responses by sniffing them with Wireshark.

For some scan types it is necessary to run Nmap as root (administrator) on the system. In those cases, it must be started with the command: `sudo nmap {arguments}`

6.2 Running Wireshark

Wireshark is a graphical network packet sniffer which can be used to do both, listen to traffic passing by your host and to look at already recorded traces. Since you need root access to access the network card and listen to the network traffic, you need to run Wireshark in the terminal using sudo as well: `sudo wireshark`.

7 Lab assignments

Go through the following questions **before demonstrating the lab** and write down what commands can be used to solve the problem. Please consult the Nmap manual for help. This will save you quite some time when doing and demonstrating the lab and will give you a greater understanding of what happens when you run Nmap.

(1) *Remember to* **write down your answers**, *so that you have them ready for the final discussion with the lab assistants.*
(2) *You must do* **all scans for all four targets (see Figure 1)!** *The purpose of this lab is to give you a feeling for the responses the different configurations will give you.*

TCP (SYN, ACK and FIN) port scanning

Start Wireshark and then use Nmap to scan a number of TCP ports on the target systems (both interfaces of the host and scanning-target with and without firewall). Try the three different types of scans: SYN, ACK and FIN scans. To speed up scanning, higher port numbers can be ignored for the lab, because most system services use port numbers below 1024.

[3] `https://nmap.org/book/man-port-specification.html`

Q1: Why are higher port numbers (> 1024) still of interest for, e.g., hackers or penetration testers?

Q2: Look at the resulting packets with Wireshark. What is sent and received? How are the different scans done (what is being sent)? Do the scanned systems behave differently? Why?

Q3: Some scans take a long time to complete. Why?! Look at the responses from the system and try to explain! (The answer has been mentioned during a lecture.)

Q4: Nmap can report ports to be in different states. What do the states "open", "closed", "filtered" and "unfiltered" mean? Read the manual page and documentation! Which are the most/least interesting ones? Run a scan against the target systems and try to find examples of all these types of ports. Look at the responses from the system. Can you match the replies with the different states?

Null and Xmas scans

Try the Null and the Xmas scans and observe what they send out.

Q5: What are the similarities and differences between the five scan types, i.e., syn, ack, fin, null, and Xmas? What are their use-cases, i.e., in which situation can each scan be useful?

UDP Port scanning

Now we would like to know if there are any UDP ports open on the system.

Q6: How is UDP scanning done by Nmap? Why is this type of scan more problematic than TCP scans?

Q7: How much time does it take to perform a UDP scan on the systems? Is there a difference between the systems in their responses? Explain!

TCP fingerprinting

Use Nmap to figure out what kind of operating system the target machines run. Check both the host system and Linux VM (scanning-target)!

Q8: What packet(s) does Nmap send to figure this out? Also, look at the responses sent by the systems using Wireshark. Do you see any differences that may reveal what type of system is being used? (You may want to limit the number of ports it scans to avoid waiting, and look at protocol parameters. Which ports should you select?!)

Fragmentation

Q9: Why would you want to use fragmented packets for scanning? How do you think fragmented packets should be handled in modern networks?

Try to create fragmented packets (flag -f). Limit the scan to one port.

Q10: When checking the output with Wireshark, do you see fragmented packets as expected? What happens if you add the --send-eth option?
Task: Please investigate the difference between these options! You may not experience a different behaviour when doing the scans using Kali Linux, but on other systems you will.

Reflection

Q11: If you are going to remember only one thing from this lab, what should it be? (There is no right answer here.)

8 Optional task(s)

The following task(s) are completely and absolutely optional and are only provided as a reference to students who want to increase their knowledge further than the contents of the course. The TAs will never ask you any questions regarding these tasks. Similarly, the exam will be created assuming these tasks never existed. Consequently, most TAs will not be able to help you with the optional tasks in which case you should ask Francisco about them. Francisco will also be very thankful if you provide him feedback about the tasks and your experience performing them.

8.1 Rationale

Port scanners are a useful tool both for defensive and offensive purposes. Defenders can use port scanners to understand the attack surface exposed to more hostile networks. Similarly, offenders can use them to find interesting points of entrance and intelligence about an unknown network.

Nmap is a stateful port scanner. This means that it keeps internally some information about each sent packet which Nmap is still processing in order to decide the best course of action. This works well with small scans where hosts do not slow down the scan. A different approach is to use a stateless port scanner like *masscan*[4]. On stateless port scanners, no information on sent packets is kept and instead the results are based only on the received responses. Stateless port scanners like masscan produce less accurate results but are capable of scanning the full IPv4 address space on a reasonable amount of time.

8.2 Task details

The optional task for this lab involves using masscan instead of Nmap to understand how they differ. This will help you notice the weaknesses and strengths of each tool.

To perform this task:

1. Perform TCP and UDP port scanning of all ports (0 to 65535) with each tool independently and time the results. Which one is faster? Do they give the same results?
2. Check and increase the rate parameter of each tool to 1000 packets per second. What happened? Did the results change?
3. Check and increase the rate parameter of each tool to 10000 packets per second. What happened? Did the results change?
4. Now check and increase the rate parameter of each tool to 128000 packets per second. What happened? Did the results change? Did you notice something on the virtual machines?
5. masscan has a retries parameter which is used to send a packet multiple times (a total of one plus the retries value). Set this value to 5 and the rate to 10000. What happened with the new scan? Were the results more accurate?

[4] `https://github.com/robertdavidgraham/masscan`

6. Can you identify what is the relation between the rate parameter, the retries value, the number of scanned ports and the time it takes to run a scan?
7. Which of the tools is more accurate? Which is faster? How can masscan balance speed and accuracy?