Swinburne University of Technology

Unix for Telecommunications

Doubtfire Submission

# Communications - Lab Report 2

*Submitted By:*
Dale Rattray
7691769
2020/10/04 17:36

*Tutor:*
Quoc Khanh Le

October 4, 2020

# Unix for Telecommunications - Lab Report 2 - Nmap

Dale Rattray
Swinburne University of Technology
Student ID: *7691769*
Report Level: *Distinction*

***Abstract*—This is a report on the Nmap tasks (Pass and Credit) completed for TNE30019 - Unix for Telecommunications. The Lab explores the basic concepts of Nmap, how to complete simple Network Scans and how this information can be used, by both Network Managers and possible Attackers.**

## I. Introduction

In these lab tasks we investigated and applied a FreeBSD service called Nmap, which is an open source network scanner that is used to detect hosts and details about their operation. The Lab allows us to explore what information can be obtained through the use of Nmap and how it can be used to increase security, or as a tool for an attacker to find hidden areas of the system.

## II. Equipment

- RULE host 48: Supplied by Swinburne University (IP: 136.186.230.48)
- RULE host system: Supplied by Swinburne University
- Personal Computer connected to Swinburne VPN
- PuTTY Application installed on PC to access RULE host

## III. Method

As per lab handouts for Lab 7 Pass task and Lab 7 Credit Task.

## IV. Results

### A. Pass Task

The Pass Task for this Lab is where we explored the operation of Nmap, gaining knowledge of the syntax required, how to apply it and what information it provides us.

To begin, we did a simple Host Discovery of the RULE network from our rule host. The RULE network is under the subnet `136.186.230.0/24`, so to perform the Host Discovery the command `nmap -v 136.186.230.0/24` was used. The resulting response following a wait for the scan to finish is shown in Figure 1. Figure 1 only shows the return for a single host, the entire result gives the same information for all the active hosts on the RULE system which is too long to include in this report.

```
Nmap scan report for ns1.unix (136.186.230.48)
Host is up (0.000022s latency).
Not shown: 962 closed ports, 35 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
```

Fig. 1. Host Discovery

Next we targeted information for 2 specific hosts, my secondary RULE host (host 98) and my Personal computer on my home network. Rule host 98 information was returned (Figure 2) using `nmap -v 136.186.230.98`, which returns the same as the first command, but only for the specified host rather than every host in the subnet.

```
student@rule48:/home % nmap 136.186.230.98
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 13:14 EST
Nmap scan report for rule98.caia.swin.edu.au (136.186.230.98)
Host is up (0.000065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 6.12 seconds
student@rule48:/home %
```

Fig. 2. RULE 98 host Discovery

As my personal computer is not directly connected to the same network as the RULE host, I was unable to obtain the host information using my RULE host but rather had to use a different piece of software. As my PC runs using Windows, I downloaded and installed the free Nmap software from the nmap.org website[1]. Once installed, I used the same command as the one for host 98, but with the local IP address of my PC (`nmap -v 192.168.0.216`) which gave the result show in Figure 3.

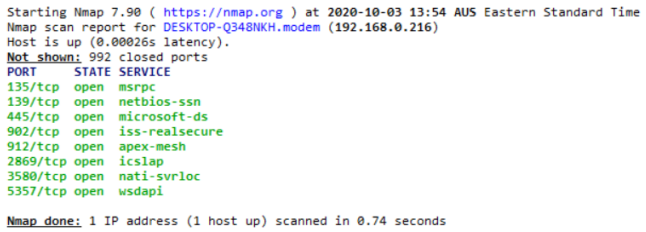


Fig. 3. Personal Computer Host Discovery

The previous scans all scanned a limited number of ports on each host, so on RULE host 98 and my local PC, we repeated the scans but this time scanning all ports using `nmap -p- -v 136.186.230.98` and `nmap -p- -v 192.168.0.216`. This gave us Figure 4 and Figure 5 respectively.

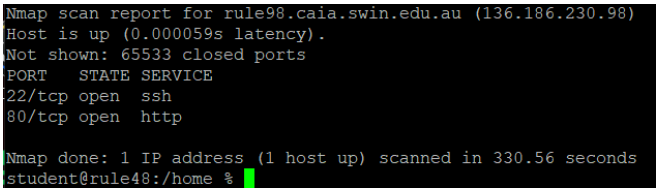


Fig. 4. All port scan RULE host 98

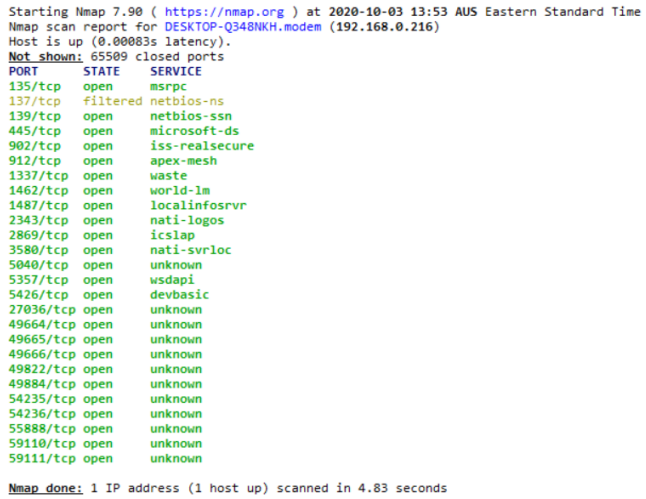


Fig. 5. All port scan PC

The final task for the Pass section of this Lab is to perform a more detailed scan of a hosts services. For this we will use the command `nmap -sV 136.186.230.21` to scan RULE host 21 to give us the active applications and services as well as the versions they are running (Figure 6)

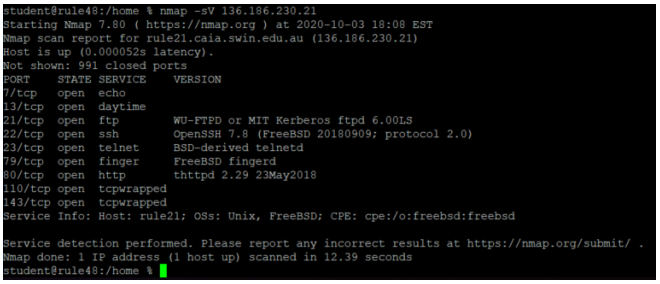


Fig. 6. Detailed RULE 21 scan

## B. Credit Task

The objective of the Credit section was to use Nmap to discover hidden application being used on RULE host 21 and find the secret message hidden within it. The first step was to find which port the hidden application was being served by, and this was achieved by completing an all port scan on RULE 21 with `nmap -p- -sV 136.186.230.21`. The output (Figure 7) showed us that port 62846 was providing a http service for the host

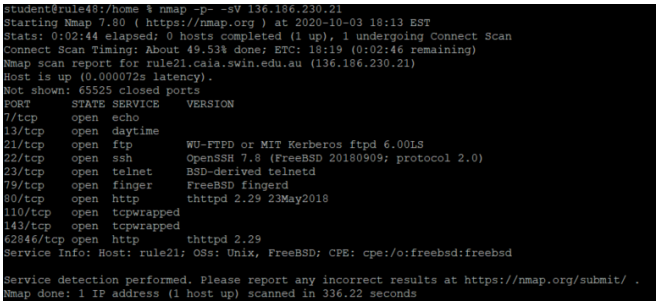


Fig. 7. All port scan RULE host 21

Now that we knew both the IP address and the port number, we could now go to the site using an web browser entering `136.186.230.21:62846` into the address bar. This gave us the secret web page (Figure 8) and the secret message "*No spitzensparken for the new RULE system!!*"

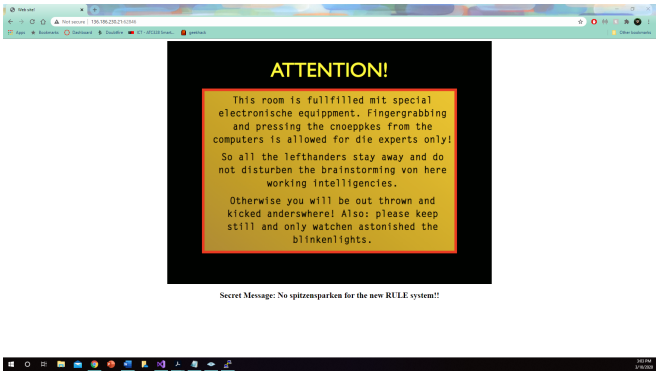


Fig. 8. The secret web page with secret message

## V. Discussion

### A. Pass Task

*1) Nmap Installation and Verbose Mode:* Nmap is easily installed in FreeBSD using the command `pkg install nmap`, although this was not needed for the lab as all RULE hosts already had Nmap installed[2]. Using this command will start a sequence where the files are downloaded and automatically placed in the correct locations on the system.

Verbose mode for Nmap is very useful as it allows you to see a variety of extra information that isn't given in a default scan. When a scan is started in Verbose mode, it prints the time when each port is scanned, allowing you to keep track of where the scan is up to, and see where you can get access and where you can't. It also provides information on the total number of hosts scanned as well as their ports[3]. These feature are useful in these labs as it allows you to see how Nmap is operating so you can understand the system better, and also makes debugging easier which is helpful when learning something new.

*2) Default Host Discovery Scan:* The first command in this lab was just a default Nmap scan in verbose mode. Analysing Figure 1, we can see that a default scan provides us with an array of information, beginning with the IP Address and host name (If it has one) of the host scanned. It then tells us that the host is up (Active) along with the latency time and then gives us information about the ports on the host. We can see that this host has 3 open ports, port 22 (ssh), port 53 (domain) and 80 (HTTP). If a port is closed in means in is inactive, and a filtered port is a port that is behind a network obstacle (Like a firewall), so Nmap cannot tell it is is open or closed[4].

Our command only scanned the default number of ports, which for Nmap is limited to the 1000 most common ports[5]. For a comparison, the range of port numbers goes from 0 to 65,535 and is divided into 3 sections[6]:

- System Ports: 0 - 1023
- User Ports: 1024 - 49151
- Dynamic/Private Ports: 49152 - 65535

The default limit to 1000 common ports prevents scans from taking too long (Scanning 65,000+ ports takes a while) while also maintaining the most important and common ports.

*3) Ports Scanned in Pass Task:* Scanning my second RULE host (Default port scan), there were only 2 ports that were shown to be open (Figure 2). The first was port 22, which serves the Secure Shell (SSH) protocol[6] and the other being port 80 which we already know from previous labs serves the HTTP protocol. After seeing the results of the full port scan in Figure 4, we can see that there are no other ports open on RULE host 98, as the result is the same seen in Figure 2.

Scanning my Personal Computer provided a much better picture on the difference between a default scan, and a full port scan. The default scan result (Figure 3) shows 8 active ports:

- Port 135 - Microsoft End Point Mapper (EPMAP)
- Port 139 - NetBIOS Session Service
- Port 445 - Microsoft Directory Service (DS)
- Port 902 - VMWare ESXi (Virtual Machine)
- Port 912 - APEX (Application Exchange Core)
- Port 2869 - Microsoft Internet Connection Firewall
- Port 3580 - NATI-Service Locator (National Instruments)
- Port 5357 - Web Services for Devices

We can see that non of these ports are the same as the RULE host, and is mostly a result of the difference in Operating System.

After doing a full port scan, we can see many more Open ports that were not there for the default port scan, although many of these are providing an unknown service. The full scan showed 25 open ports (+1 filtered), an increase of 17 from the initial Nmap scan, with the new discoveries shown below:

- Port 1337 - WASTE (Encrypted File Sharing)
- Port 1462 - World-lm (World License Manager)
- Port 1487 - Localinfosrvr
- Port 2343 - Nati-Logos (National Instruments)
- Port 5426 - DevBasic
- All other open ports serving unknown service

We can see that doing the full port scan although takes longer, can give a deeper understanding about what is operating on any given system. It also shows that the more things you install, the more ports get used, and that can be seen by comparing RULE host 98, a system with very little extras installed, compared to the local PC which has many things installed.

*4) Host Scan Time:* The time it takes to complete a Nmap scan can come down to a range of factors. Specifically comparing hosts using the same Nmap scan, the duration can be affected by the number of open ports, the resources available or just the availability of the host. If a host has many more open ports compared to another host, it will take longer to complete the scan as more information needs to be processed. Additionally, if the system has many layers of security, this can also slow down the time it takes to scan or completely block the Nmap scan.

When considering scan times in a general environment rather than host specific, the scan time can be drastically increased as a result of heavy network traffic or long travel distances. A Nmap scan does require information to be sent to and from the target host, so limitations on either end of the connection will also have a affect on scan times.

*5) Detailed Port Scan and Information Use:* When we scanned RULE host 21, we used a more detailed Nmap scan to obtain a greater amount of information, specifically in this case the applications and their running version. Looking at Figure 6, we can see a total of 9 services running, 5 of which have an associated version:

- Port 21 - File Transfer Protocol (FTP) running version WU-FTPD
- Port 22 - Secure Shell (SSH) running version OpenSSH 7.8
- Port 23 - Telnet running BSD-derived telnetd
- Port 79 - finger running FreeBSD fingerd
- Port 80 - HTTP running version thttpd 2.29

Port 7 (Echo) and Port 13 (Daytime) do not have any associated version as a result of their service being very basic (Echoing replies and giving current date) requiring very little to no updates or alterations. Ports 110 and 143 both have service label `tcpwrapped` meaning it is protected by a TCP wrapper, however after a quick search we can see that these ports are used to serve POP3 (Port 110) and IMAP (Port 143)[6], which are both email protocols.

This information can be important and useful to a range of people and used for both improvements of destruction. If an attacker was able to gain this information, if could give them an easy access point or areas to avoid based on how secure each service or specific version is. Knowing the version of a particular service can also guide an attacker if there are any vulnerabilities already known, which an attacker could use.

In the same way that an attacker will draw information from services and particular versions to find a weakness to exploit, a Network Administrator will use the same information fortify these vulnerabilities. If an application has a known weakness, a Network admin will know that it is a likely focus point for an attack and can implement further protection. A quick search can also scan the Network for any service versions that are outdated and subject to a weaker security system, so knowing where your weaknesses are help you to fortify and keep it secure.

A Server Admin will deal less with the network specific threats and focus more on keeping hosts on the network up to date. The Information drawn from a detailed Nmap scan can provide a quick view to ensure all hosts are using the best version of each application, which can improve quality and efficiency.

### *B. Credit Task*

The Credit Task involved trying to draw out a hidden message inside of RULE host 21 using Nmap searches to locate it. Before starting we already knew that a normal Nmap search will likely return the port serving the hidden message as unknown, and that the Port number is likely to be in the Dynamic/Private range (Ports 49152 - 65535) and will need a full port scan. With this information in mind, a detailed, full port Nmap scan and quickly found that the message was being served through HTTP on port 62846, which as expected was in the private range.

Entering the hosts IP address and the port we wanted to access (`136.186.230.21:62846`) we were presented with a web page (Figure 8) with an image and the secret message under it: "*No spitzensparken for the new RULE system!!*

## VI. Conclusion

In this Lab we explored how to use Nmap and how it is useful for network management and possible attackers. Overall, we were able to scan several hosts, find what applications and services it was running, as well as the specific versions and analyse how this could be used by different people, both in constructive and destructive ways. Nmap has been shown to be a very useful tool to keep track of what is running within your network, allowing more educated Security implementation to keep the network secure.

## VII. Bibliography

## References


[1] nmap.org, "Windows nmap." [Online]. Available: https://nmap.org/download.html

[2] VNKB, "How to install nmap on freebsd 11," 2016. [Online]. Available: https://vnkb.com/how-to-install-nmap-on-freebsd-11/

[3] nmap.org, "Nmap netowrk scanning - command line flags." [Online]. Available: https://nmap.org/book/output-formats-commandline-flags.html#:~:text=Nmapprintsmanyextrainformational,andbrieflysummarizingtheresults.

[4] Y. Chen, "Nmap," 2018. [Online]. Available: https://wiki.onap.org/display/DW/Nmap#:~:text=Openmeansthatanapplication,itisopenorclosed.

[5] nmap.org, "Nmap netowrk scanning - port specification and scan order." [Online]. Available: https://nmap.org/book/man-port-specification.html#:~:text=Bydefault,Nmapscansthe,1,000portsforeachprotocol.&text=Thisoptionspecifieswhichports,(e.g.1-1023).

[6] IANA, "Service name and transport protocol port number registry," 2020. [Online]. Available: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml