Don Bosco Institute of Technology, Kurla
Academic Year 2023-24

EXPERIMENT NO. 3

SEMESTER: V **DATE OF PERFORMANCE: 31st July 2024**

SUBJECT: CN Lab **DATE OF SUBMISSION: 04th August 2024**

NAME OF THE STUDENT: Dwayne George Nixon **ROLL NO.: 21**

AIM	Perform network discovery using discovery tools (eg. Nmap)
LEARNING OBJECTIVE	The student will apply to discover and audit networks, scan, and check vulnerabilities on Internet Protocol (IP) addresses and ports for a givennetwork.
LEARNING OUTCOME	The students will be able to search and install network discovery tools
COURSE OUTCOME	**CSL 502.1:** Identify the important networking commands in Linux and understand their function. CSL502.2: Gather information regarding connectors and cables used fornetwork and summarize their usage.
PROGRAM OUTCOME	PO1,PO2,PO3,PO4,PO5,PO9,PO10,PSO1,PSO2,PSO3
BLOOM'S TAXONOMY LEVEL	Apply.
THEORY	Introduction: Nmap, also known as network mapper, is a free and open-source security tool widely known for its powerful network discovery, enumeration and security auditing abilities. Network administrators utilize Nmap to establish a network map and get more information about what's going on inside the network: which hosts are online, what ports are open, which services are offered, and more. Nmap has evolved to become more than just a port-scanning tool - it's also used for service monitoring, vulnerability detection and exploitation just to name a few. With this Nmap tool, ● Network administrator(s) can identify all devices that arerunning/accessing their systems. ● An administrator can identify all the hosts, computers connected totheir network, including the services that they offer. ● An administrator can scan all the open ports (communicationendpoint), giving security a priority, that is, security threat detections. An administrator can scan/monitor a single host (a computer connected to the organization network) or thousands of devicesconnected

Nmap installation

Step 1: Install Network Mapper (Nmap) sudo apt-get install nmap

Step 2: Verify installed version:

nmap --version Command 1.Host discovery

Nmap optimizes port scan speed by first checking if the target is onlinebefore attempting to scan any ports

1. List Scan: A list scan generally lists the possible host without sending anypackets to the targeted host.

nmap -sL www.amazon.in

2. Ping Sweep: Ping sweep discovers on the basis the host is powered on.nmap -sP www.dbit.in

3. TCP SYN Ping: Nmap checks whether a host is online. nmap -PS www.dbit.in

4. TCP ACK Ping: Nmap checks whether the host is responding. nmap -sA www.amazon.in

5. ICMP Echo Ping: Nmap sends ICMP packets to the available host.nmap -PE www.dbit.in

6. ARP Ping: ARP ping scan is used to discover the host devices in the samenetwork. sometimes it will not visible due to firewall filtering.

nmap -PR www.google.com\

7. Traceroute: Traceroute helps to discover the following hops or pathways tothe targeted host.

nmap -sn –traceroute www.google.com

Multi Router Traffic Grapher (MRTG)

The Multi Router Traffic Grapher (MRTG) is free software for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form.It was originally developed by Tobias Oetiker and Dave Rand to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.MRTG is written in Perl and can run on Windows, Linux, Unix, Mac OS and NetWare.

MRTG consists of a Perl script which uses SNMP to read the traffic counters of your routers and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection. These graphs are embedded into web pages which can be viewed from any modern Web-browser

In addition to a detailed daily view, MRTG also creates visual representations of the traffic seen during the last seven days, the last four weeks and the last twelve months. This is possible because MRTG keeps a log of all the data it has pulled from the router. This log is automatically consolidated, so that it does not grow over time, but still contains all the relevant data for all the traffic seen over the last two years. This is all performed in an efficient manner. Therefore you can monitor 50 or more network links from any halfway decent UNIX box.

MRTG is not limited to monitoring traffic though, it is possible to monitor any SNMP variable you choose. You can even use an external program to gather the data which should be monitored via MRTG. People are using MRTG, to monitor things such as System Load, Login Sessions, Modem availability and more. MRTG even allows you to accumulate two or more data sources into a single graph

	Highlights of MRTG 1. Works on most UNIX platforms and Windows NT 2. Uses Perl for easy customization 3. Has a highly portable SNMP implementation written entirely in Perl thanks to Simon Leinen. There is no need to install any external SNMP package. 4. MRTG's logfiles do NOT grow. Thanks to the use of a unique data consolidation algorithm. 5. MRTG comes with a semi-automatic configuration tool. 6. MRTG's query engine checks for port reconfigurations on therouter and warns the user when they occur. 7. Time critical routines are written in C thanks to the initiative ofDave Rand my Co-Author 8. Graphics are generated directly in GIF format, using the GDlibrary by Thomas Boutell. 9. The look of the webpages produced by MRTG is highlyconfigurable. 10. MRTG is available under the GNU PUBLIC LICENSE.
LAB EXERCISE	Every student will exercise the Nmap and theory of MRTG. **Screenshots of the Commands:** **1. Host Discovery** `dwayne-nixon@dwayne-nixon-V1-04:~$ sudo host discovery www.dbit.in` `;; communications error to 43.205.151.144#53: connection refused` `;; communications error to 43.205.151.144#53: connection refused` `;; UDP setup with 64:ff9b::2bcd:9790#53(64:ff9b::2bcd:9790) for discovery failed: network unreachable.` `;; no servers could be reached` **2. List Scan** `dwayne-nixon@dwayne-nixon-V1-04:~$ sudo nmap -sL www.amazon.in` `Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-31 16:06 IST` `Nmap scan report for www.amazon.in (23.54.193.66)` `Other addresses for www.amazon.in (not scanned): 2600:9000:2650:9a00:8:b109:e14:3c81 2600:9000:2650:e000:8:b109:e14:3c81 2600:9000:2650:9400:8:b109:e14:3c81 2600:9000:2650:600:8:b109:e14:3c81 2600:9000:2650:800:8:b109:e14:3c81 2600:9000:2650:2e00:8:b109:e14:3c81 2600:9000:2650:e00:8:b109:e14:3c81 2600:9000:2650:ea00:8:b109:e14:3c81` `rDNS record for 23.54.193.66: a23-54-193-66.deploy.static.akamaitechnologies.com` `Nmap done: 1 IP address (0 hosts up) scanned in 0.03 seconds`  **3. Ping Sweep** `dwayne-nixon@dwayne-nixon-V1-04:~$ sudo nmap -sP www.dbit.in` `Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-31 16:07 IST` `Nmap scan report for www.dbit.in (43.205.151.144)` `Host is up (1.1s latency).` `Other addresses for www.dbit.in (not scanned): 64:ff9b::2bcd:9790` `rDNS record for 43.205.151.144: ec2-43-205-151-144.ap-south-1.compute.amazonaws.com` `Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds`

4. TCP SYN Ping

```
dwayne-nixon@dwayne-nixon-V1-04:~$ sudo nmap -PS www.dbit.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-31 16:08 IST
Nmap scan report for www.dbit.in (43.205.151.144)
Host is up (0.010s latency).
Other addresses for www.dbit.in (not scanned): 64:ff9b::2bcd:9790
rDNS record for 43.205.151.144: ec2-43-205-151-144.ap-south-1.compute.amazonaws.com
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
80/tcp   open     http
443/tcp  open     https
1097/tcp filtered sunclustermgr

Nmap done: 1 IP address (1 host up) scanned in 24.40 seconds
```

5. TCP ACK Ping

```
dwayne-nixon@dwayne-nixon-V1-04:~$ sudo nmap -sA www.dbit.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-31 16:09 IST
Nmap scan report for www.dbit.in (43.205.151.144)
Host is up (0.012s latency).
Other addresses for www.dbit.in (not scanned): 64:ff9b::2bcd:9790
rDNS record for 43.205.151.144: ec2-43-205-151-144.ap-south-1.compute.amazonaws.com
All 1000 scanned ports on www.dbit.in (43.205.151.144) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.28 seconds
```

6. ICMP Echo Ping

```
dwayne-nixon@dwayne-nixon-V1-04:~$ sudo nmap -PE www.dbit.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-31 16:11 IST
Nmap scan report for www.dbit.in (43.205.151.144)
Host is up (0.0081s latency).
Other addresses for www.dbit.in (not scanned): 64:ff9b::2bcd:9790
rDNS record for 43.205.151.144: ec2-43-205-151-144.ap-south-1.compute.amazonaws.com
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```

7. ARP Ping

```
dwayne-nixon@dwayne-nixon-V1-04:~$ sudo nmap -PR www.dbit.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-31 16:11 IST
Nmap scan report for www.dbit.in (43.205.151.144)
Host is up (0.0060s latency).
Other addresses for www.dbit.in (not scanned): 64:ff9b::2bcd:9790
rDNS record for 43.205.151.144: ec2-43-205-151-144.ap-south-1.compute.amazonaws.com
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
80/tcp   open     http
443/tcp  open     https
5877/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

8. Traceroute

```
dwayne-nixon@dwayne-nixon-V1-04:~$ sudo nmap -sn -traceroute www.dbit.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-31 16:05 IST
Nmap scan report for www.dbit.in (43.205.151.144)
Host is up (0.0071s latency).
Other addresses for www.dbit.in (not scanned): 64:ff9b::2bcd:9790
rDNS record for 43.205.151.144: ec2-43-205-151-144.ap-south-1.compute.amazonaws.com

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   2.40 ms  _gateway (192.168.0.1)
2   2.41 ms  ipcopdirect.localdomain (10.0.1.148)
3   6.66 ms  static-153.96.248.49-tataidc.co.in (49.248.96.153)
4   ...
5   10.65 ms 99.83.92.224
6   ... 13
14  7.03 ms  ec2-43-205-151-144.ap-south-1.compute.amazonaws.com (43.205.151.144)

Nmap done: 1 IP address (1 host up) scanned in 3.24 seconds
```

REFERENCES

B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.
https://www.section.io/engineering-education/nmap-network-scanner/
https://www.youtube.com/watch?v=ftutyWqzRCs
https://www.howtoforge.com/tutorial/how-to-install-and-configure-mrtg-on- ubuntu-1804/