ISSN (Print): 0974-6846
ISSN (Online): 0974-5645

Indian Journal of Science and Technology, *Vol 12(28), 10.17485/ijst/2019/v12i28/147004, July 2019*

Efficient Information Gathering using NMAP and NBTSCAN: Case study on 172.19.19.0 IP Address

Sanskar Kaushik[1]*, Arifa Bhutto[2] and Bishwajeet Pandey[3]

[1]Ambedkar Institute of Technology, Delhi – 110031, India Kaushiksanskar18@gmail.com
[2]University of Sindh, Jamshoro, Pakistan; arifa.bhutto@usindh.edu.pk
[3]Gyancity Research Lab, Gurgaon – 1220010 Haryana, India; Gyancity@gyancity.com

Abstract

Objectives/Methods: In this work, we are going to identify the IP addresses of all the machines. Along with the IP address, we also get information about the operating system and their version executing on machines. We also list the open ports of every machine connected to the network, which we are scanning. Finally, we enlist services executing in all the open port of machine connected with the network, in which we are using NMAP and NBTSCAN as a scanning tool. **Findings**: NMAP is the most powerful information-gathering tools available in the cybersecurity domain.

Keywords: Cyber Security, Information Gathering, NBTSCAN, NMAP, Open Port

1. Introduction

Information gathering gives us an idea about the amount of publicly accessible data of organization that may help an ethical hacker compromise the network as shown in Figure 1.

We take 172.19.19.0 as an Internet Protocol (IP) address blocks assigned to the target organization that we have taken for our case study. We used NMAP and NBTSCAN to discover live hosts in our target network. We looked for e-paper, e-article, confidential information relating to partners, news of a merger, data related to the acquisition, schematics of network infrastructure. We scanned the entire 172.19.19.0 range hosts to identify open ports, services executing on these ports and the operating system executing on the open port. We scanned 172.19.19.1-10 to identify open ports, services executing and operating system of an open port.

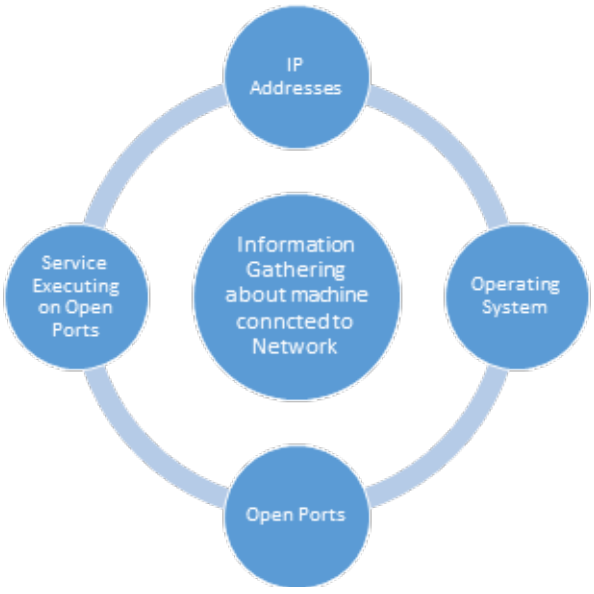

Figure 1. Information gathering about machine connected to Network.

*Author for correspondence

2. Literature Survey

Across the world, companies have teams of ethical hacker collecting threat data to protect their existing system from ongoing cyber-threats and manage a strong cyber security workforce[1]. NMAP is one of the best information-gathering programs in the current era. Eventually, the researcher uses NBTSCAN to create host scan attacks[2]. Multiple steps related to either live or dead forensics data gathering are designed by the researcher. Then, they analyse the DHCP requests to trace the attacking laptop[3]. Multiple reports of various formats are collected from different network scanning tools in[4]. Information sources can be accessed automatically through information gathering methodology[5]. These information-gathering techniques are useful for collecting essential information[6]. Some researcher analyses this methodology and presents a generic framework for gathering and utilising widely distributed data in an expanding internet-based world[7]. Attack tracing also indirectly helps to collect information to help in detailed information gathering[8]. Some researcher also used high-interaction honeypots to collect information related to the target network[9].

3. Methodology

We used NMAP and NBTSCAN to discover live hosts in the network. We scanned 172.19.19.0 to discover live host in this network as shown in Figure 2.

Using command NBTSCAN, we scanned for the addresses from IP that is 172.19.19 to discover live nearby networks as mentioned in Figure 2. We scanned 10.0.0.0 to discover live host in this network again using NBTSCAN but at this time on a different network that is 10.0.0.0 as shown in Figure 3. We scanned 172.0.0.0 to discover live host in this network as shown in Figure 4.

We scanned the entire 172.19.19.0 range hosts to identify open ports, executing services and the operating system executing on the system associated with an open port. We scanned 172.19.19.1 to identify open ports, ongoing services and operating system on it as shown in Figure 5. In this figure that is Figure 5, we scanned the network 172.19.19.1 using NMAP output and we found all the open ports executing on that network. We scanned 172.19.19.2 to identify open ports, services and operating system on it as shown in Figure 6.

We scanned 172.19.19.3 to identify open ports, executing services and operating system on it as shown in Figures 7-8. We scanned 172.19.19.4 to identify open ports, executing services and operating system running on it as shown in Figure 9. We scanned 172.19.19.5 to identify open ports, executing services and operating system on it as shown in Figure 10. In this figure, we found the complete description for mainly two ports in which we found the operating system which is the main thing. We scanned 172.19.19.6 to identify open ports, executing services and operating system on it as shown in Figures 11 and 12. In this figure, we again using NMAP to identify open ports on 172.19.19.6 address. Results categorized into three services that are State, Service and Version.

We scanned 172.19.19.7 to identify open ports, executing services and operating system on it. It shows the operating system, in this case, Microsoft windows as the version is shown in Figure 13.

We scanned 172.19.19.8 to find the same things that are open ports and system version to find a vulnerability to get into the system as shown in Figure 14. We scanned 172.19.19.9 to identify open ports, executing services and operating system on it as shown in Figure 15. In this, we found different services found on the network 172.19.19.9 such as NetBIOS and Microsoft. We continue scanning 172.19.19.10 to find furthermore open ports, executing services and operating system on it as shown in Figure 16. We scanned the entire 10.10.0.0 range hosts to identify open ports, services and the operating system executing on them. We scanned 10.10.0.1 to identify open ports, executing services and operating system on it as shown in Figure 17. In this, all ports scanned with different port numbers such as 49152 and 21. We scanned 10.10.0.2 to identify open ports, executing services and operating system and found other different ports open on different services with founding windows version as shown in Figure 18.

We scanned 10.10.0.3 to identify open ports, executing services and operating system on it as shown in Figure 19. In this, all different ports 21, 30, 49152 and other ports

found to be opened with all different services. We scanned the entire 172.17.0.0 range hosts to identify open ports, services and the operating system executing on them as shown in Figure 20. We scanned 172.17.0.2 to identify open ports, executing services and operating system on it as shown in Figure 21. We again using NMAP in this at 172.17.0.2 address and again found various ports opened to be getting attacked.

```
root@kali:~# nbtscan -r 172.19.19.0/24
Doing NBT name scan for addresses from 172.19.19.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
172.19.19.1      GNAT             <server>  <unknown>        00:15:5d:79:e9:d1
172.19.19.9      RDDEPT           <server>  <unknown>        00:15:5d:79:e9:ca
172.19.19.8      OPERATIONS       <server>  <unknown>        00:15:5d:79:e9:cc
172.19.19.3      WIN-ULY858KHQIP  <server>  <unknown>        00:15:5d:79:e9:c6
172.19.19.4      ADVERTISEMENT    <server>  <unknown>        00:15:5d:79:e9:c7
172.19.19.7      MARKETING        <server>  <unknown>        00:15:5d:79:e9:c9
172.19.19.2      ACCOUNTS         <server>  <unknown>        00:15:5d:79:e9:c5
172.19.19.6      HRDEPT           <server>  <unknown>        00:15:5d:79:e9:c8
172.19.19.10     SALES            <server>  <unknown>        00:15:5d:79:e9:cb
root@kali:~#
```

Figure 2. Scanning 172.19.19.0 range.

```
root@kali:~# nbtscan -r 10.0.0.0/8
Doing NBT name scan for addresses from 10.0.0.0/8

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
10.10.0.1        GNAT             <server>  <unknown>        00:15:5d:15:41:f5
10.10.0.3        ECOMM            <server>  <unknown>        00:15:5d:15:41:e9
10.10.0.2        ENTERTAINMENT    <server>  <unknown>        00:15:5d:15:41:e8
```

Figure 3. Scanning 10.0.0.0 range.

```
root@kali:~# nbtscan -r 172.0.0.0/8
Doing NBT name scan for addresses from 172.0.0.0/8

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
172.17.0.1       GNAT             <server>  <unknown>        00:15:5d:15:41:f6
172.17.0.2       WIN-AG46I02QBKJ  <server>  <unknown>        00:15:5d:15:41:ea
172.19.19.1      GNAT             <server>  <unknown>        00:15:5d:15:41:f7
192.168.0.1      <unknown>                  <unknown>
root@kali:~#
```

Figure 4. Scanning 172.0.0.0 range.

```
root@kali:~# nmap -Pn -O -sV -p1-65535 172.19.19.1

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-15 13:50 EST
Nmap scan report for 172.19.19.1
Host is up (0.00075s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  tcpwrapped
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_serve
r_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 - SP2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.84 seconds
```

Figure 5. NMAP output of 172.19.19.1.

```
Nmap scan report for 172.19.19.2
Host is up (0.00098s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  tcpwrapped
45/tcp    open  ssh           WeOnlyDo sshd 2.1.3 (protocol 2.0)
| ssh-hostkey:
|   1024 af:51:4a:c2:6d:48:f2:9f:e4:50:4d:4c:d9:ee:bb:d0 (DSA)
|_  1024 31:49:8b:2e:c7:b5:e2:56:65:74:58:f6:0b:b1:98:3c (RSA)
80/tcp    open  http          Microsoft IIS httpd 7.5
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: IIS7
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/31%OT=21%CT=1%CU=30012%PV=Y%DS=2%DC=T%G=Y%TM=5A724CC
OS:1%P=x86_64-unknown-linux-gnu)SEQ(SP=105%GCD=1%ISR=107%TI=I%CI=I%II=I%SS=
OS:O%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
```

Figure 6. NMAP output of 172.19.19.2.

```
root@kali:~# nmap -Pn -O -sV -p1-65535 172.19.19.3

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-15 14:30 EST
Nmap scan report for 172.19.19.3
Host is up (0.0021s latency).
Not shown: 65510 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  tcpwrapped
53/tcp    open  domain        Microsoft DNS 6.0.6001
80/tcp    open  http          Microsoft IIS httpd 7.0
88/tcp    open  kerberos-sec  Windows 2003 Kerberos (server time: 2018-01-15 19
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5722/tcp  open  msrpc         Microsoft Windows RPC
49152/tcp open  msrpc         Microsoft Windows RPC
```

Figure 7. NMAP output of 172.19.19.3 (1).

```
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49161/tcp open  msrpc         Microsoft Windows RPC
49165/tcp open  msrpc         Microsoft Windows RPC
49170/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/15%OT=21%CT=1%CU=30530%PV=Y%DS=2%DC=I%G=Y%TM=5A5D01D
OS:8%P=x86_64-unknown-linux-gnu)SEQ(SP=107%GCD=2%ISR=10C%TI=I%CI=I%II=I%SS=
OS:O%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
OS:NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=40
OS:00%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http:
Nmap done: 1 IP address (1 host up) scanned in 130.35 seconds
```

Figure 8. NMAP output of 172.19.19.3 (2).

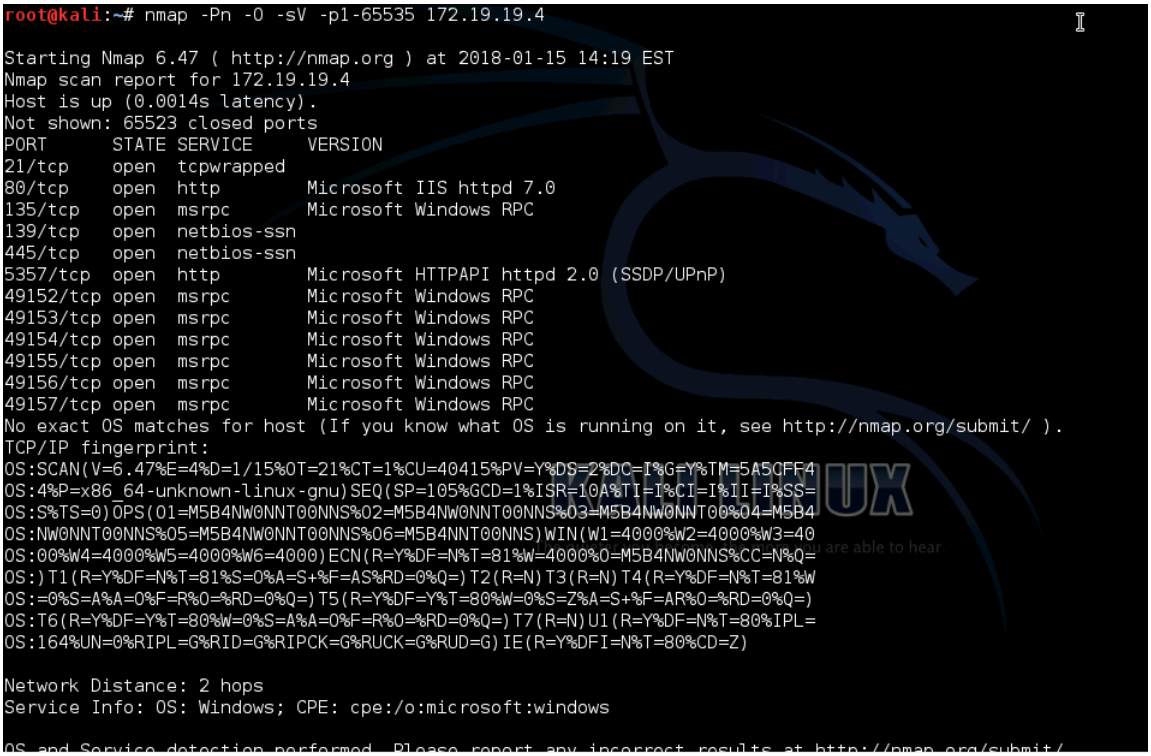

Figure 9. NMAP output of 172.19.19.4.

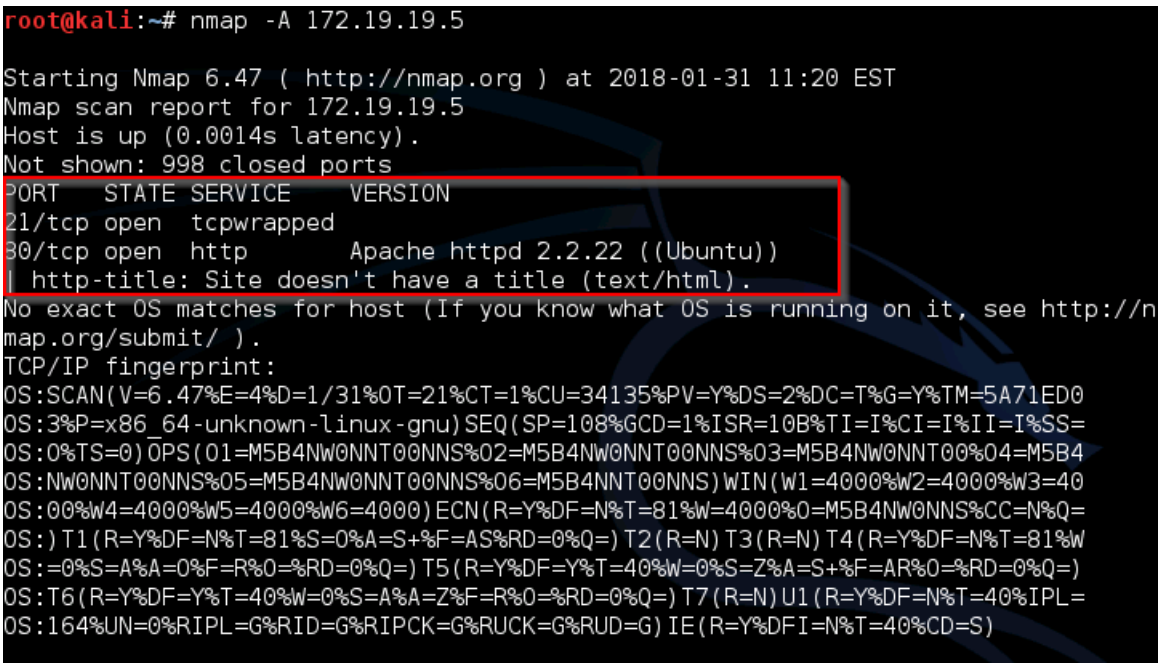

Figure 10. NMAP output of 172.19.19.5.

```
root@kali:~# nmap -Pn -O -sV -p1-65535 172.19.19.6

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-15 14:40 EST
Nmap scan report for 172.19.19.6
Host is up (0.0018s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http        Apache httpd 2.4.2 ((Win64) PHP/5.4.3)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3306/tcp  open  mysql       MySQL (unauthorized)
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
49158/tcp open  msrpc       Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
```

Figure 11. NMAP output of 172.19.19.6 (1).

```
49158/tcp open  msrpc       Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/15%OT=21%CT=1%CU=35228%PV=Y%DS=2%DC=I%G=Y%TM=5A5D040
OS:9%P=x86_64-unknown-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=
OS:O%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
OS:NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=40
OS:00%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.01 seconds
```

Figure 12. NMAP output of 172.19.19.6 (2).

```
root@kali:~# nmap -Pn -O -sV -p1-65535 172.19.19.7

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-15 14:03 EST
Nmap scan report for 172.19.19.7
Host is up (0.0013s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http         Microsoft IIS httpd 7.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/15%OT=21%CT=1%CU=44379%PV=Y%DS=2%DC=I%G=Y%TM=5A5CFDB
OS:C%P=x86_64-unknown-linux-gnu)SEQ(SP=103%GCD=1%ISR=102%TI=I%CI=I%II=I%SS=
OS:S%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
OS:NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=40
OS:00%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 13. NMAP output of 172.19.19.7.

```
root@kali:~# nmap -Pn -O -sV -p1-65535 172.19.19.8

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-15 14:27 EST
Nmap scan report for 172.19.19.8
Host is up (0.0021s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  tcpwrapped
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 - SP2
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.80 seconds
```

Figure 14. NMAP output of 172.19.19.8.

```
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/15%OT=21%CT=1%CU=38837%PV=Y%DS=2%DC=I%G=Y%TM=5A5CFA6
OS:4%P=x86_64-unknown-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10E%TI=I%CI=I%II=I%SS=O
OS:%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4N
OS:W0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=400
OS:0%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=)
OS:T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W=
OS:0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T
OS:6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=1
OS:64%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.78 seconds
```

Figure 15. NMAP output of 172.19.19.9 (2).

```
root@kali:~# nmap -Pn -O -sV -p1-65535 172.19.19.10

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-15 14:23 EST
Nmap scan report for 172.19.19.10
Host is up (0.0013s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/15%OT=21%CT=1%CU=40739%PV=Y%DS=2%DC=I%G=Y%TM=5A5D001
OS:C%P=x86_64-unknown-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=
OS:O%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
OS:NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=40
OS:00%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
```

Figure 16. NMAP output of 172.19.19.10.

```
root@kali:~# nmap -Pn -sV -O -p1-65535 10.10.0.1

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-17 12:29 EST
Nmap scan report for 10.10.0.1
Host is up (0.0011s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  tcpwrapped
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_serve
r_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 - SP2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.93 seconds
```

Figure 17. NMAP output of 10.10.0.1.

```
root@kali:~# nmap -Pn -sV -O -p1-65535 10.10.0.2

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-17 12:31 EST
Nmap scan report for 10.10.0.2
Host is up (0.0014s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/17%OT=21%CT=1%CU=31923%PV=Y%DS=2%DC=I%G=Y%TM=5A5F88E
OS:A%P=x86_64-unknown-linux-gnu)SEQ(SP=100%GCD=2%ISR=10C%TI=I%CI=I%II=I%SS=
OS:O%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
OS:NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=40
OS:00%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 18. NMAP output of 10.10.0.2.

```
root@kali:~# nmap -Pn -sV -O -p1-65535 10.10.0.3

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-17 12:34 EST
Nmap scan report for 10.10.0.3
Host is up (0.0014s latency).
Not shown: 65521 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3306/tcp  open  mysql?
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/17%OT=21%CT=1%CU=30154%PV=Y%DS=2%DC=I%G=Y%TM=5A5F89F
OS:6%P=x86_64-unknown-linux-gnu)SEQ(SP=108%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=
OS:O%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
OS:NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=40
OS:00%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 19. NMAP output of 10.10.0.3.

```
root@kali:~# nmap -Pn -sV -O -p1-65535 172.17.0.1

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-17 12:16 EST
Nmap scan report for 172.17.0.1
Host is up (0.0012s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  tcpwrapped
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_serve
r_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 - SP2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.50 seconds
```

Figure 20. NMAP output of 172.17.0.1.

```
root@kali:~# nmap -Pn -sV -O -p1-65535 172.17.0.2

Starting Nmap 6.47 ( http://nmap.org ) at 2018-01-17 12:19 EST
Nmap scan report for www.fnb.com (172.17.0.2)
Host is up (0.0015s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=1/17%OT=21%CT=1%CU=35863%PV=Y%DS=2%DC=I%G=Y%TM=5A5F860
OS:3%P=x86_64-unknown-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=
OS:O%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4
OS:NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W3=40
OS:00%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=81%W=4000%O=M5B4NW0NNS%CC=N%Q=
OS:)T1(R=Y%DF=N%T=81%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=N%T=81%W
OS:=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 21. NMAP output of 172.17.0.2.

4. Conclusion

In this work, we used NMAP and NBTSCAN. Both NMAP and NBTSCAN are powerful tools available in the cyber security domain for information gathering or scanning of the network. In future, we shall use any other information gathering tool to enlist the service available on the open port of the machine of the target network. In future, we shall also close the open port in order to enhance the cyber security. There is also an open scope to do denial of service attacks with the help of open ports.

5. References

1. Brown S, Gommers J, Serrano O. From cyber security information sharing to threat management. Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security; 2015. p. 43–9. https://doi.org/10.1145/2808128.2808133.
2. Pukkawanna S, Visoottiviseth V, Pongpaibool P. Lightweight detection of DoS attacks. 2007 15th IEEE International Conference on Networks; 2007. p. 77–82. https://doi.org/10.1109/ICON.2007.4444065.
3. Mokhov SA, Assels MJ, Paquet J, Debbabi M. Automating MAC spoofer evidence gathering and encoding for investigations. International Symposium on Foundations and Practice of Security; Springer, Cham. 2014. p. 168–83. https://doi.org/10.1007/978-3-319-17040-4_11.
4. Pandey SK, Yadav VK, Kumar S, Verma S, Dansena P. Implementation of a new framework for automated network security checking and alert system. 2014 Eleventh International Conference on Wireless and Optical Communications Networks; 2014. p. 1–7. https://doi.org/10.1109/WOCN.2014.6923089
5. Carrick C, Yang Q, Abi-Zeid I, Lamontagne L. Activating CBR systems through autonomous information gathering. International Conference on Case-based Reasoning; Springer, Berlin, Heidelberg. 1999. p. 74–88. https://doi.org/10.1007/3-540-48508-2_6.

6. Wilson S. The use of ethnographic techniques in educational research. Review of Educational Research. 1977; 47(2):245–65. https://doi.org/10.3102/00346543047002245.
7. Schwartz MF, Pu C. Applying an information gathering architecture to Netfind: A white pages tool for a changing and growing Internet. IEEE/ACM Transactions on Networking. 1994; 2(5):426–39. https://doi.org/10.1109/90.336327.
8. Verwoerd T, Hunt R. Intrusion detection techniques and approaches. Computer Communications. 2002; 25(15):1356–65. https://doi.org/10.1016/S0140-3664(02)00037-3.
9. Zakaria WZA, Mat Kiah ML. A review on artificial intelligence techniques for developing intelligent honeypot. 2012 8th International Conference on Computing Technology and Information Management. 2012; 2:696–701.