Project report on

Scanning Networks

July 9th,2018

AZURE SKYNET

TECHNOLOGY | KNOWLEDGE | INNOVATION

Instructor:-Sir Noor Alam

Cyber Security and Ethical Hacking

Azure Skynet

By:-Adrian Clive Prasad

Email:wrathlustpride@gmail.com

Location:Bangalore

ACKNOWLEDGEMENT:

I would like to express our profound gratitude to our project guide Mr Noor Alam Sir and Azure Skynet Solutions Company for their support, encouragement, supervision, and useful suggestions throughout this project. Their moral support and continuous guidance enabled us to complete our work successfully

SCANNING NETWORKS

Abstract

The Nmap Security Scanner was built to efficiently scan large networks, but Nmap's author Fyodor has taken this to a new level by scanning millions of Internet hosts as part of the Worldscan project. He will present the most interesting findings and empirical statistics from these scans, along with practical advice for improving your own scan performance. Additional topics include detecting and subverting firewall and intrusion detection systems, dealing with quirky network configurations, and advanced host discovery and port scanning techniques. A quick overview of new Nmap features will also be provided.

Best TCP Ports for Host Discovery

- Echo request, and even Nmap default discovery scans are insufficient for Internet scanning.

- Adding more TCP SYN and ACK probes can help, but which ports work the best?

Top Open TCP & UDP Ports

- Will be available by Black Hat USA
- Substantial reduction of current default 1703 TCP ports, 1480 UDP
- --top-ports feature available now, but no data to use it.

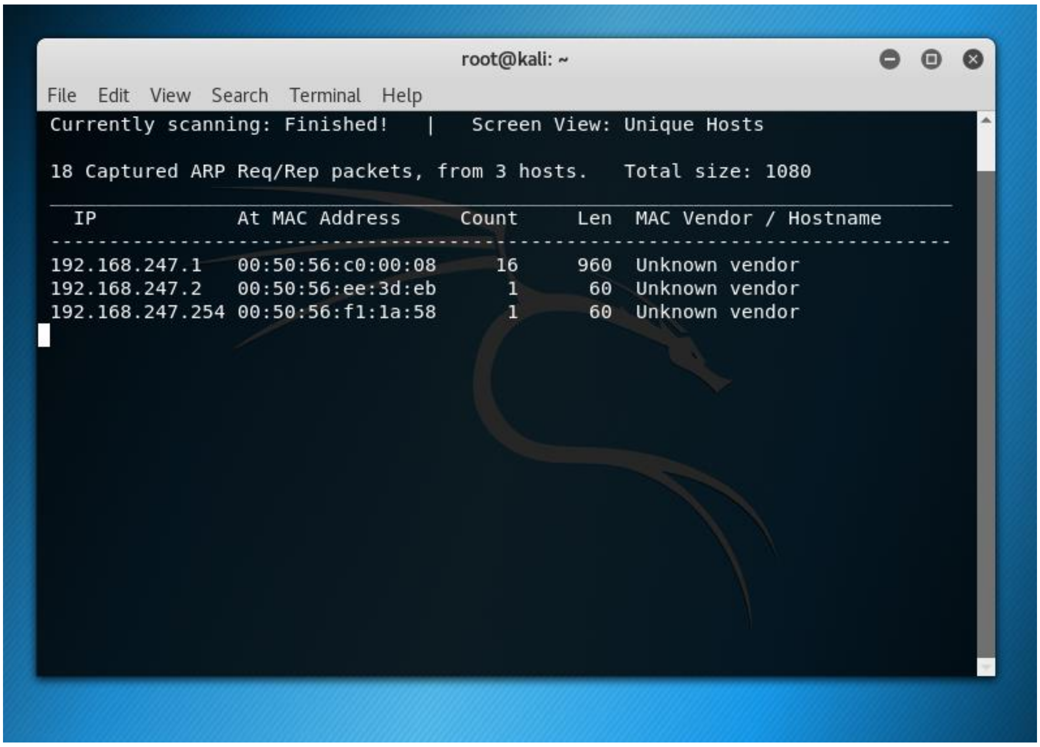
->Scanning is the process of identifying live systems, ports and the service that exists on those systems.

Steps:

1.Discovering live host
2.Scanning the ports of system
3.vulnerability Scanning.

⇨ netdiscover -r <ip of your linux vm/>

⇨ (it is used check ARP ping address)

⇨ 

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

18 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 1080
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.247.1   00:50:56:c0:00:08     16     960  Unknown vendor
192.168.247.2   00:50:56:ee:3d:eb      1      60  Unknown vendor
192.168.247.254 00:50:56:f1:1a:58      1      60  Unknown vendor
```

-r=>range

/=.network bits

IP to MAC== ARP

*cd to change directory(cd /root/<directory>)

*ls to list files.

ping Scanning using NMAP:

1.FULL-OPEN (TCP Connect) Scan:

```
-------------->SYN
SYN, ACK<----------
-------------->ACK
```

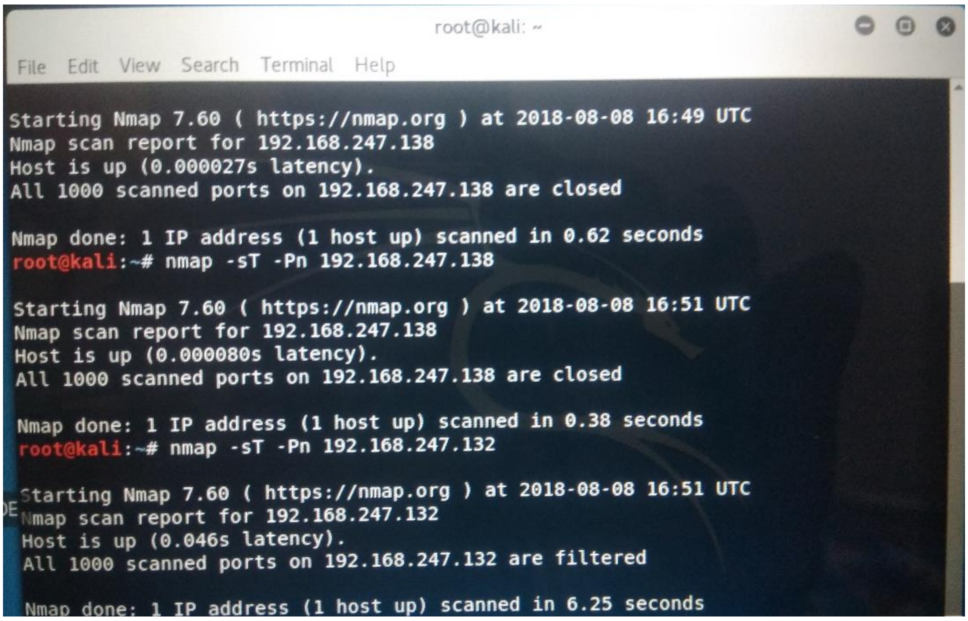
```
nmap -sT -Pn 192.168.211.129
```

(uses complete 3-way handshake)

-sT : Scan for TCP connect packet

-p- : scann all ports

-Pn : skip host discovery phase

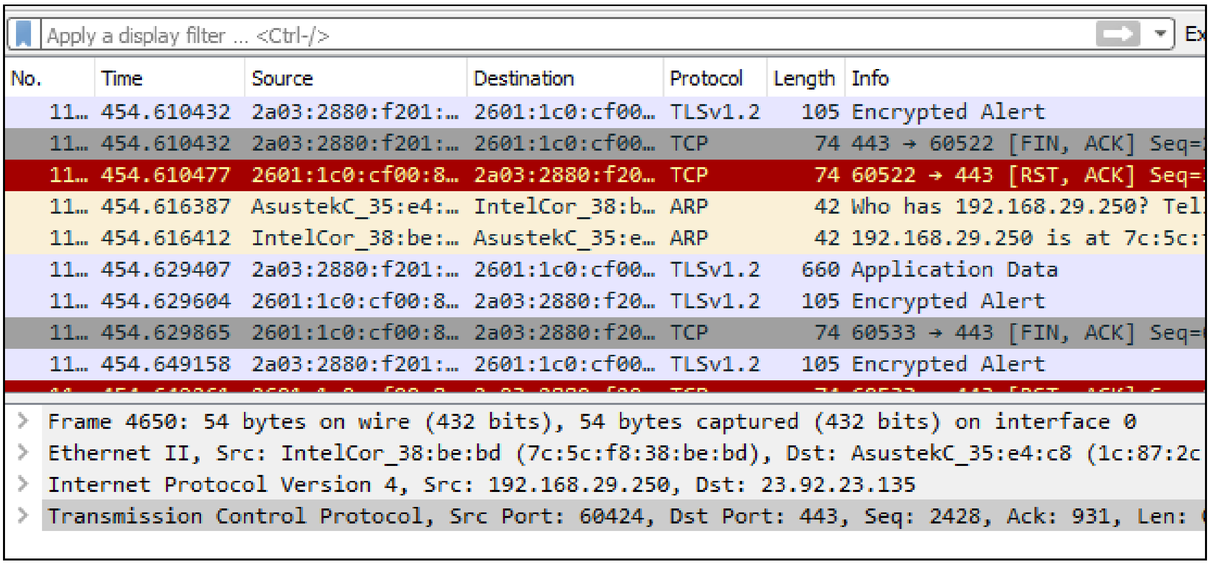


```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 16:49 UTC
Nmap scan report for 192.168.247.138
Host is up (0.000027s latency).
All 1000 scanned ports on 192.168.247.138 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
root@kali:~# nmap -sT -Pn 192.168.247.138

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 16:51 UTC
Nmap scan report for 192.168.247.138
Host is up (0.000080s latency).
All 1000 scanned ports on 192.168.247.138 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@kali:~# nmap -sT -Pn 192.168.247.132

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 16:51 UTC
Nmap scan report for 192.168.247.132
Host is up (0.046s latency).
All 1000 scanned ports on 192.168.247.132 are filtered

Nmap done: 1 IP address (1 host up) scanned in 6.25 seconds
```

nmap -sT -p- -Pn 198.168.211.1-254

(to scan the entire range of ip address)

*in wireshark filter for tcp && ip.addr==<target ip>



No.	Time	Source	Destination	Protocol	Length	Info
11…	454.610432	2a03:2880:f201:…	2601:1c0:cf00…	TLSv1.2	105	Encrypted Alert
11…	454.610432	2a03:2880:f201:…	2601:1c0:cf00…	TCP	74	443 → 60522 [FIN, ACK] Seq=
11…	454.610477	2601:1c0:cf00:8…	2a03:2880:f20…	TCP	74	60522 → 443 [RST, ACK] Seq=
11…	454.616387	AsustekC_35:e4:…	IntelCor_38:b…	ARP	42	Who has 192.168.29.250? Tel
11…	454.616412	IntelCor_38:be:…	AsustekC_35:e…	ARP	42	192.168.29.250 is at 7c:5c:
11…	454.629407	2a03:2880:f201:…	2601:1c0:cf00…	TLSv1.2	660	Application Data
11…	454.629604	2601:1c0:cf00:8…	2a03:2880:f20…	TLSv1.2	105	Encrypted Alert
11…	454.629865	2601:1c0:cf00:8…	2a03:2880:f20…	TCP	74	60533 → 443 [FIN, ACK] Seq=
11…	454.649158	2a03:2880:f201:…	2601:1c0:cf00…	TLSv1.2	105	Encrypted Alert

```
> Frame 4650: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c
> Internet Protocol Version 4, Src: 192.168.29.250, Dst: 23.92.23.135
> Transmission Control Protocol, Src Port: 60424, Dst Port: 443, Seq: 2428, Ack: 931, Len:
```

->if target replies the syv it is close

->if target replies the RST it is open.

2.HALF-OPEN(STEALTH) Scan:

------------->SYN

SYN,ACK<---------

------------->RST

```
namp -sS -Pn -p445 192.168.211.132
```

-sS : Syn scan.

XMas tree Scan :

XMas tree scans get their name from the fact that the FIN ,PSH ,and URG

packet flags are set to "on". it does not contain SYN, ACK or RST flag.

```
->nmap -sX -Pn -v -p139 192.168.213.129 <target ip>
```

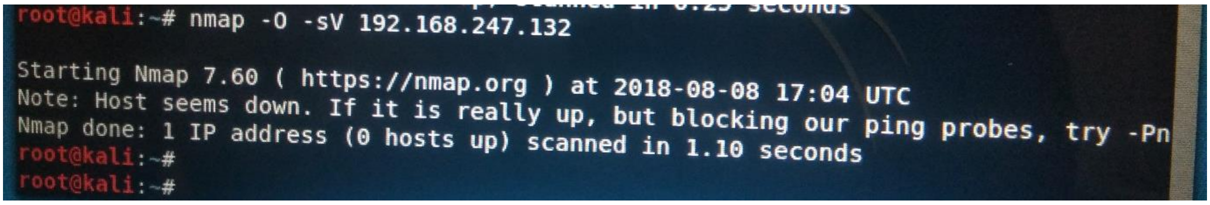
(it wont work in windows, ONly for linux or unix system)

(Xmas tree and NUll scans are rather ineffective against Microsoft targets.)

-v = verbosity

*finger printing (to identify OS and services) (information)

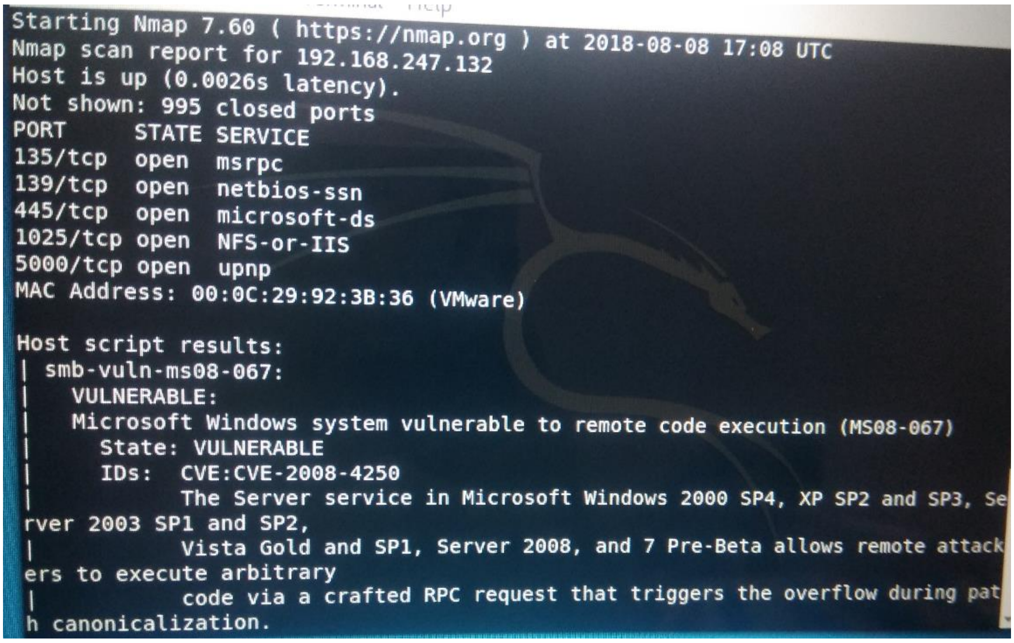
->nmap -O -sV 192.168.213.129



```
root@kali:~# nmap -O -sV 192.168.247.132

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 17:04 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.10 seconds
root@kali:~#
root@kali:~#
```

vulnarability scanning:

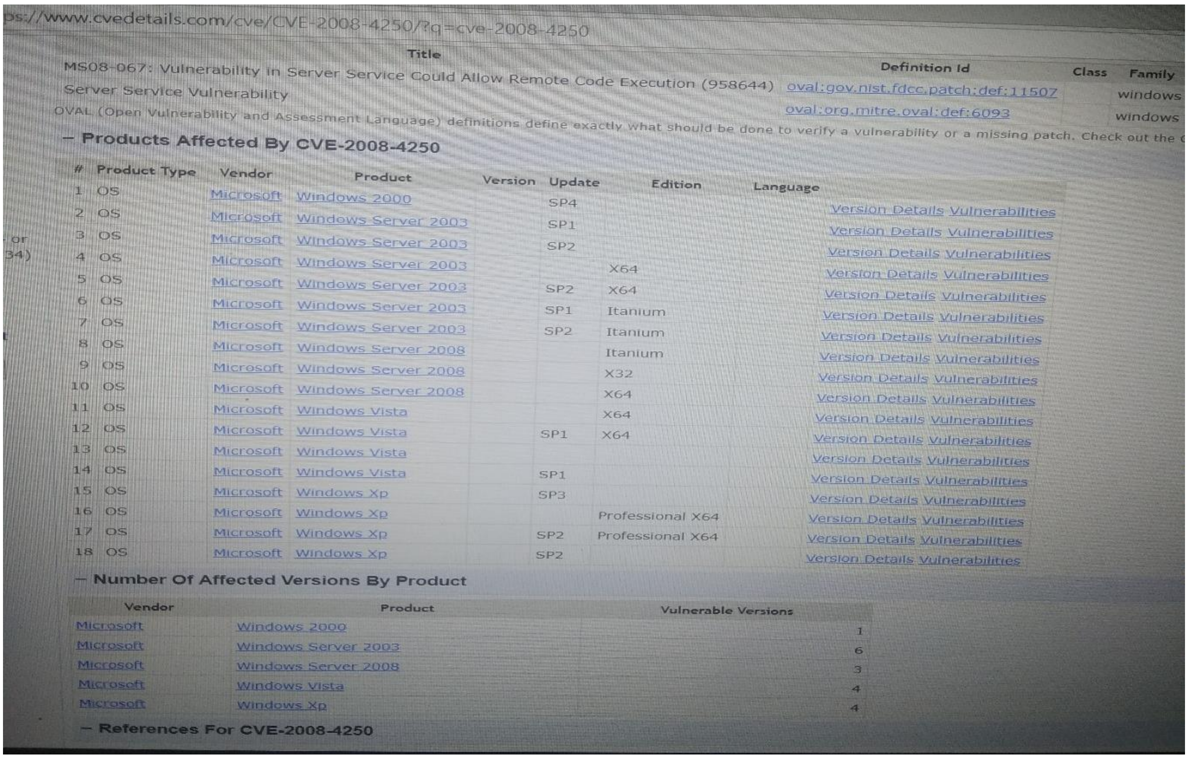
nmap --script vuln ip



```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 17:08 UTC
Nmap scan report for 192.168.247.132
Host is up (0.0026s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:0C:29:92:3B:36 (VMware)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Se
rver 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attack
ers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during pat
h canonicalization.
```

We get cve code and we can know about this in detail and impact od vulnerability at

@Cvedetails.com.



ps://www.cvedetails.com/cve/CVE-2008-4250/?q=cve-2008-4250

Title	Definition Id	Class	Family
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	oval:gov.nist.fdcc.patch:def:11507		windows
Server Service Vulnerability	oval:org.mitre.oval:def:6093		windows

OVAL (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the

– Products Affected By CVE-2008-4250

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Microsoft	Windows 2000		SP4			Version Details Vulnerabilities
2	OS	Microsoft	Windows Server 2003		SP1			Version Details Vulnerabilities
3	OS	Microsoft	Windows Server 2003		SP2			Version Details Vulnerabilities
4	OS	Microsoft	Windows Server 2003			X64		Version Details Vulnerabilities
5	OS	Microsoft	Windows Server 2003		SP2	X64		Version Details Vulnerabilities
6	OS	Microsoft	Windows Server 2003		SP1	Itanium		Version Details Vulnerabilities
7	OS	Microsoft	Windows Server 2003		SP2	Itanium		Version Details Vulnerabilities
8	OS	Microsoft	Windows Server 2008			Itanium		Version Details Vulnerabilities
9	OS	Microsoft	Windows Server 2008			X32		Version Details Vulnerabilities
10	OS	Microsoft	Windows Server 2008			X64		Version Details Vulnerabilities
11	OS	Microsoft	Windows Vista			X64		Version Details Vulnerabilities
12	OS	Microsoft	Windows Vista		SP1	X64		Version Details Vulnerabilities
13	OS	Microsoft	Windows Vista					Version Details Vulnerabilities
14	OS	Microsoft	Windows Vista		SP1			Version Details Vulnerabilities
15	OS	Microsoft	Windows Xp		SP3			Version Details Vulnerabilities
16	OS	Microsoft	Windows Xp			Professional X64		Version Details Vulnerabilities
17	OS	Microsoft	Windows Xp		SP2	Professional X64		Version Details Vulnerabilities
18	OS	Microsoft	Windows Xp		SP2			Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Microsoft	Windows 2000	1
Microsoft	Windows Server 2003	6
Microsoft	Windows Server 2008	3
Microsoft	Windows Vista	4
Microsoft	Windows Xp	4

– References For CVE-2008-4250

CIA: confidentiality, integraty, access complexity

man nmap or nmap -h(for help or know info about commands).