Enumerating hosts on the internal network

1. Introduction

Companies worldwide have always been scared of so called “internal attacks “on their corporate networks. It is proven that most of the attacks originate from an internal computer on your own network, whether an employee is trying to steal some confidential information, or a skillful intruder has found a way to break into your network security.

In this lab we will learn how to scan our own internal network for hosts and how to sniff traffic on the internal network.

2. Tools

You can use various tools to find the other hosts on a network. After you scan the network and gather the necessary information about the machines and the operational systems, you are ready to attack it.

Nmap – Nmap is a program that can be used in Linux, Mac, or Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can be used to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Zenmap is the GUI frontend of Nmap.
Metasploit – Metasploit is an exploitation framework. Version 3 of Metasploit is written in Ruby and has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves, and others are for application software like Adobe Reader and Internet Explorer. There is a detailed description of each exploit, which explains which version of the operating system, or application software is vulnerable.
Tcpdump – A Linux/UNIX program that captures network traffic. The tcpdump program comes installed on many Linux distributions by default, including Kali.
Sniffer – A sniffer is used to capture network traffic. Software programs like tcpdump and Wireshark, can be used to sniff traffic.

3. Machines

Machine Name	IP address
Kali Linux	192.168.1.10
Windows XP	192.168.1.11
Windows 7	192.168.1.12

4. Exercise

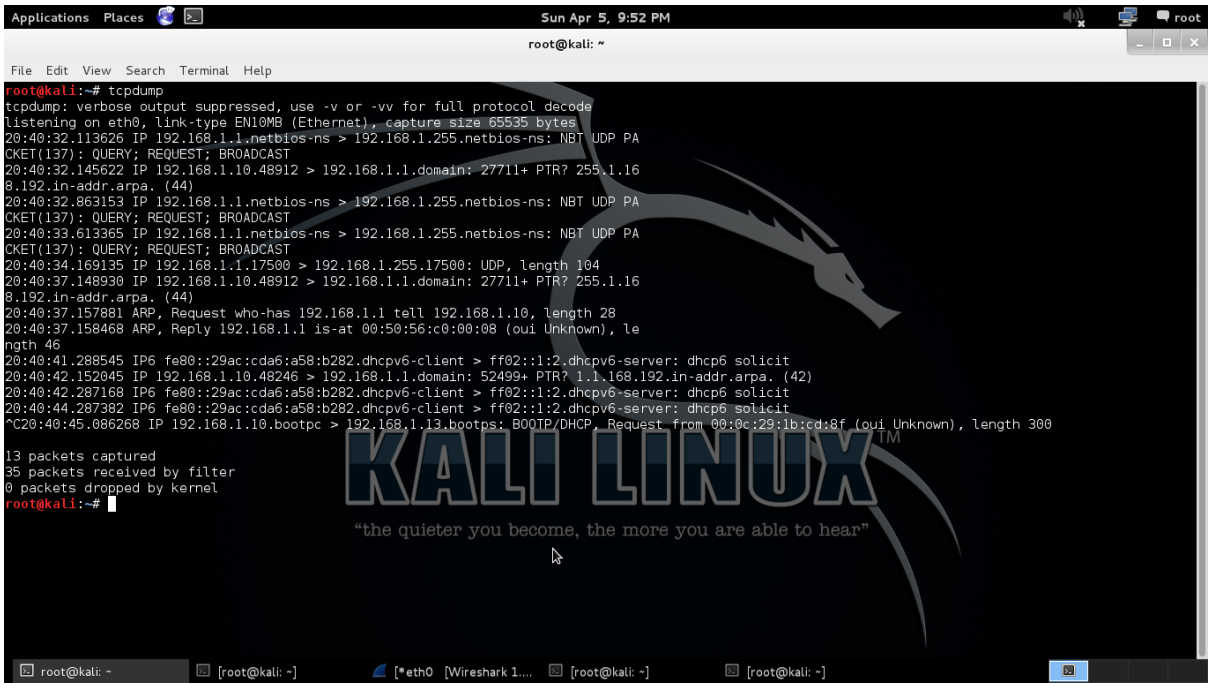
Before scanning the network with tools that will be detected by network sensors, we can passively listen for broadcast packets that are sent to all machines on the network.

The following is a representation of a hub environment.

Please notice that you will not be able to listen passively to all the traffic if there is a switch, because he segments the traffic.

1. Log into your Kali Linux machine with the Username: root, and Password: toor

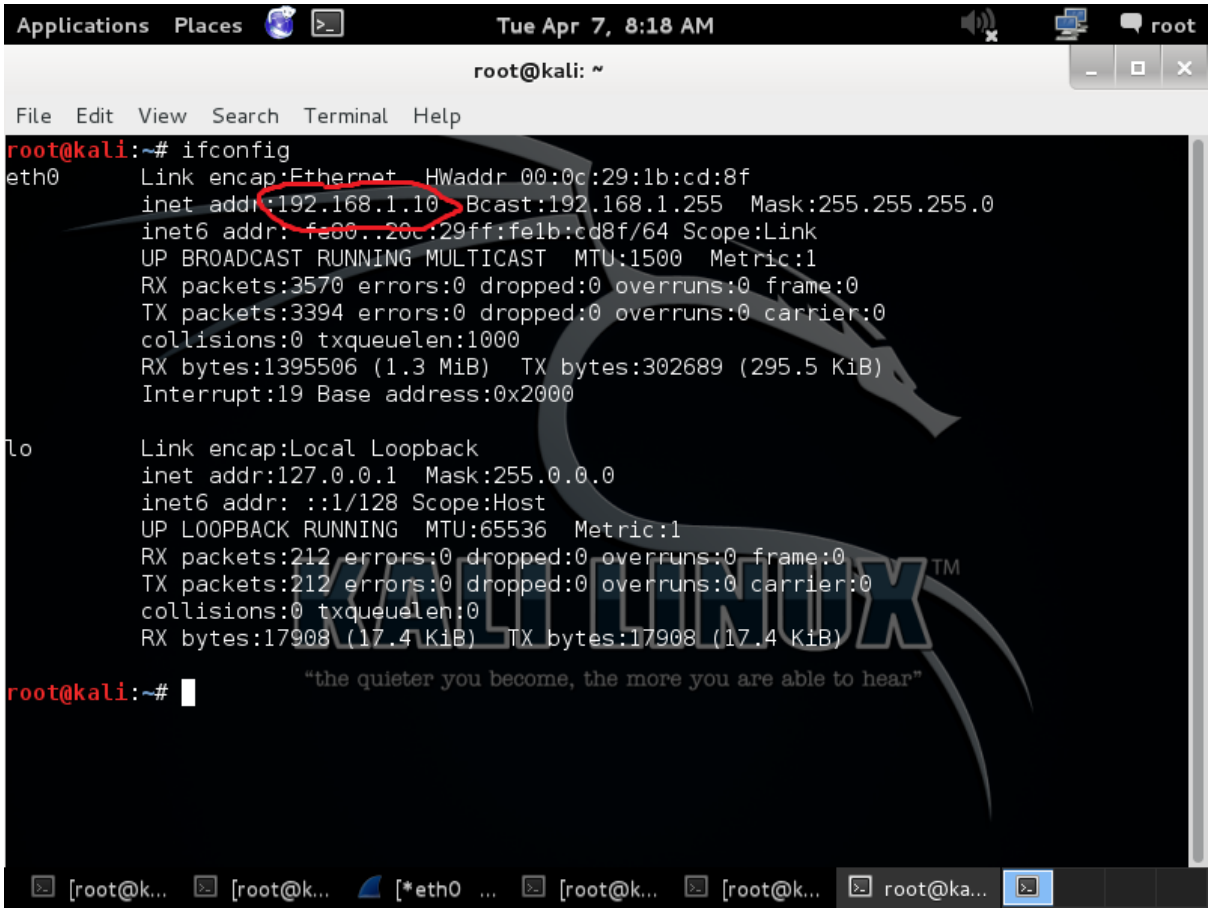
2. Open up a terminal window and type in : tcpdump. Wait a little and you will be presented with a similar window:



Passively sniffing the traffic on the network can tell you a lot of information about the machines on it, without them knowing about your presence. On the internal 192.168.1.0/24 network, broadcasts are sent to the broadcast address 192.168.1.255. Most of the IP addresses announce themselves on the network without doing any type of scan. User Datagram Protocol (UDP) NetBIOS Datagrams are sent to the network broadcast address of 192.168.1.255. Address Resolution Protocol (ARP) uses the broadcast MAC address of FF:FF:FF:FF:FF:FF. These broadcasts are sent to all machines within a single broadcast domain; meaning ARP broadcasts are not forwarded off a LAN segment.

3.If you would like to view your own IP address type in:

Ifconfig



If you want to see all network interfaces of your system the command is :ifconfig –a

Sometimes , your Kali Linux machine will come without automatically assigned IP address from the DHCP server. Type in: ifconfig eth0 up , if you want to start interface eth0.

4.Open a console and type in : wireshark . Start the sniffer to start listening on eth0.

5.Open up a terminal and type in the following command and press enter:

nmap –sP 192.168.1.*

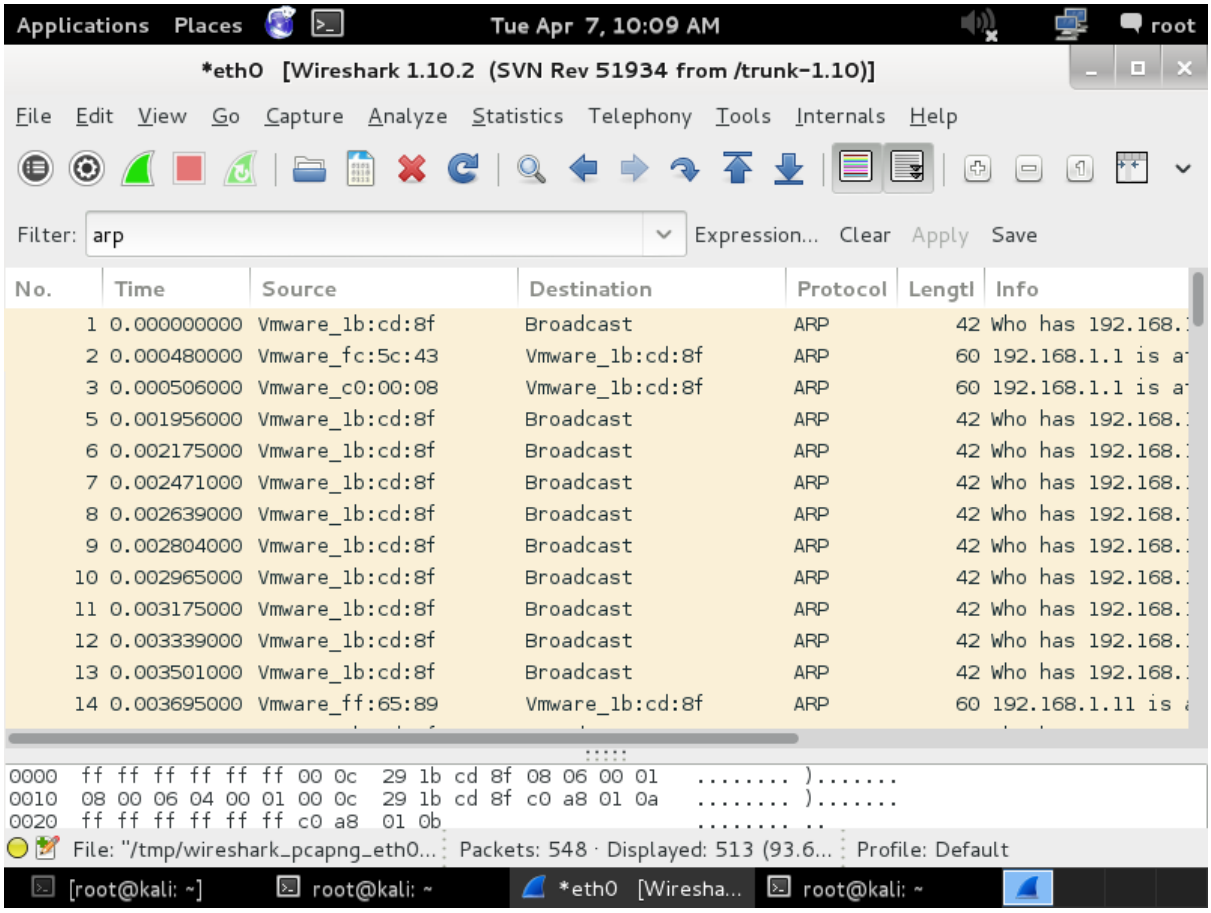
```
root@kali:~# nmap -sP 192.168.1.*

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-05 21:01 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0023s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.11
Host is up (0.00028s latency).
MAC Address: 00:0C:29:FF:65:89 (VMware)
Nmap scan report for 192.168.1.12
Host is up (0.00026s latency).
MAC Address: 00:0C:29:33:9C:C3 (VMware)
Nmap scan report for 192.168.1.13
Host is up (0.00018s latency).
MAC Address: 00:50:56:FA:7F:68 (VMware)
Nmap scan report for 192.168.1.10
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.17 seconds
root@kali:~# nmap -sP 192.168.1.*

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-05 21:04 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00050s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.11
Host is up (0.00025s latency).
```

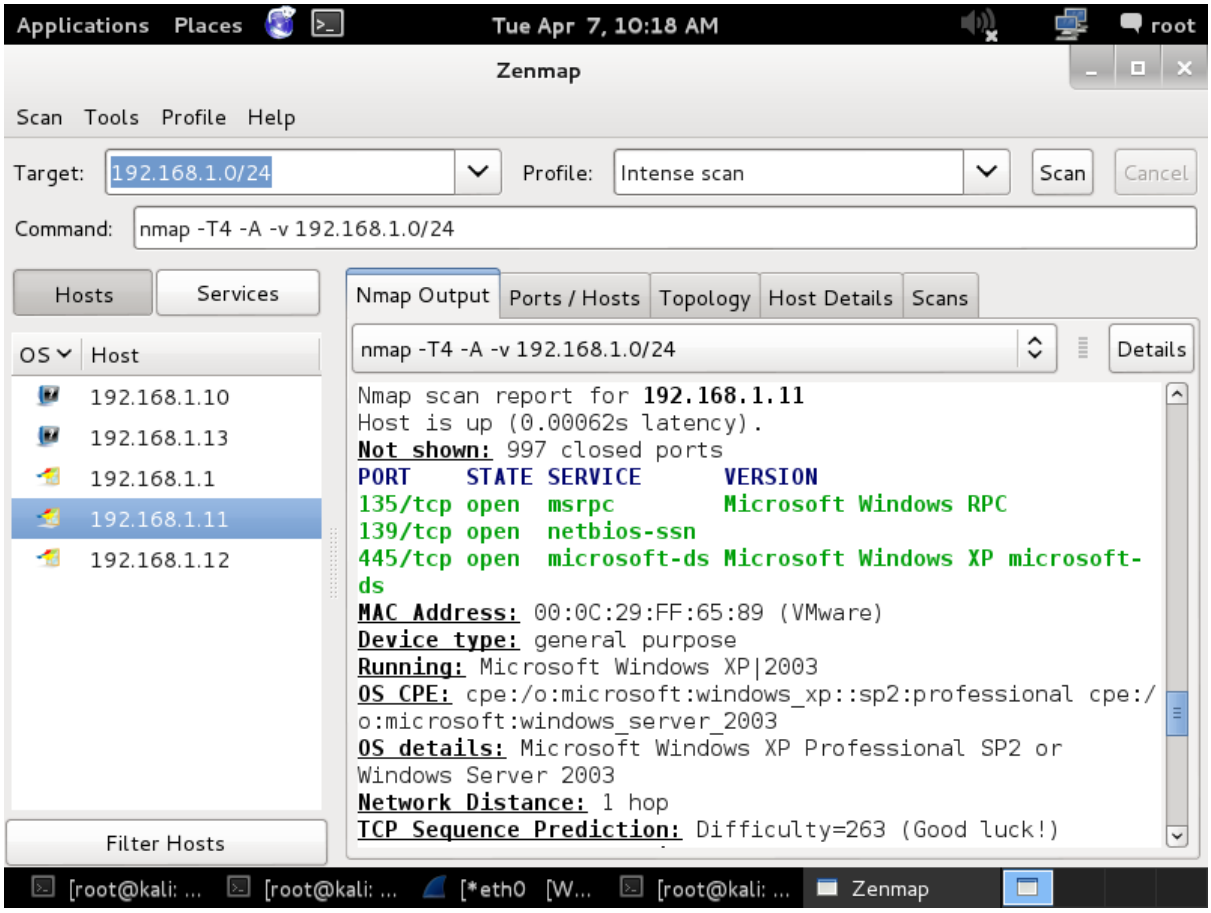
You can see that Nmap is trying to locate all hosts on the network. The final result on the bottom is 5 hosts up.

6.Now go back to your wireshark and type in the terminal window: arp



You can see that Nmap produced a lot of ARP packets on the network , while trying to locate the hosts. Sometimes this is not good for you , if you would like to remain unnoticed , also this can trigger some alarms.

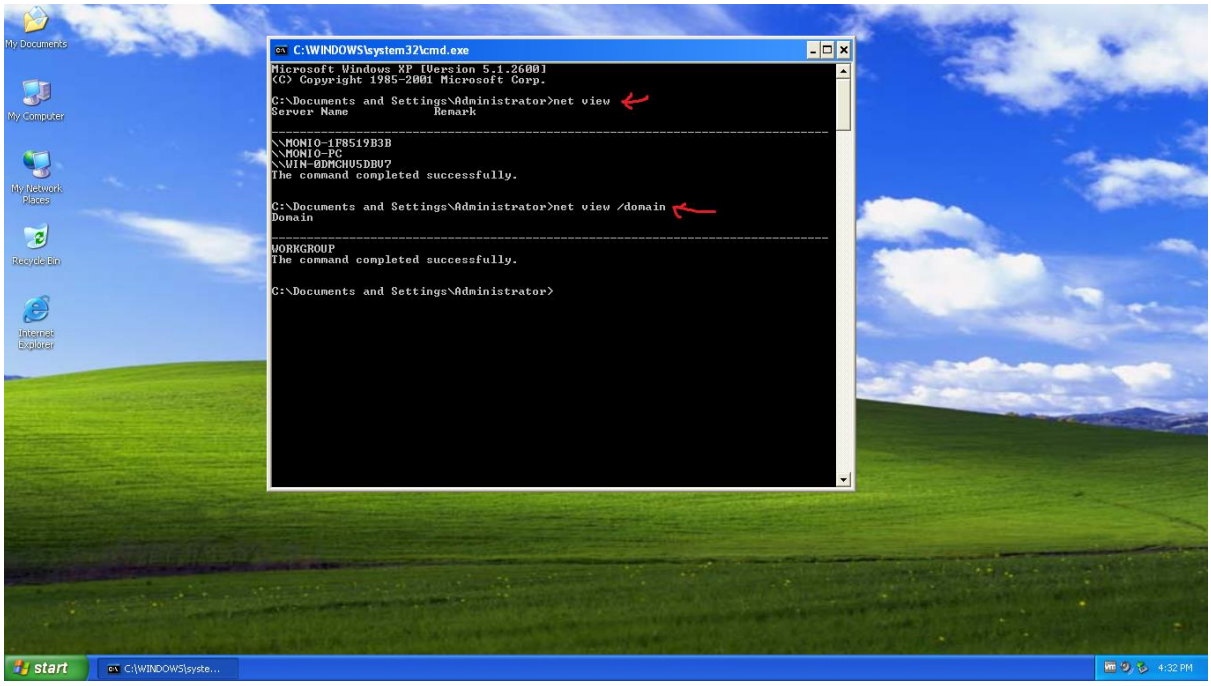
7.Open up a terminal and type in : zenmap . You will be presented with the GUI frontend of Nmap , you can use it if you would like to launch some more complicated commands or scans.In the IP address field type in : 192.168.1.0/24 and choose Intense scan.



Zenmap will present you with detailed information about each host , including the open ports + the OS running on the host. Please be aware , that sometimes Zenmap is not able to determine the exact OS , running on particular host but it is guessing.

Ok , now we know all the hosts on the network and their OS also.

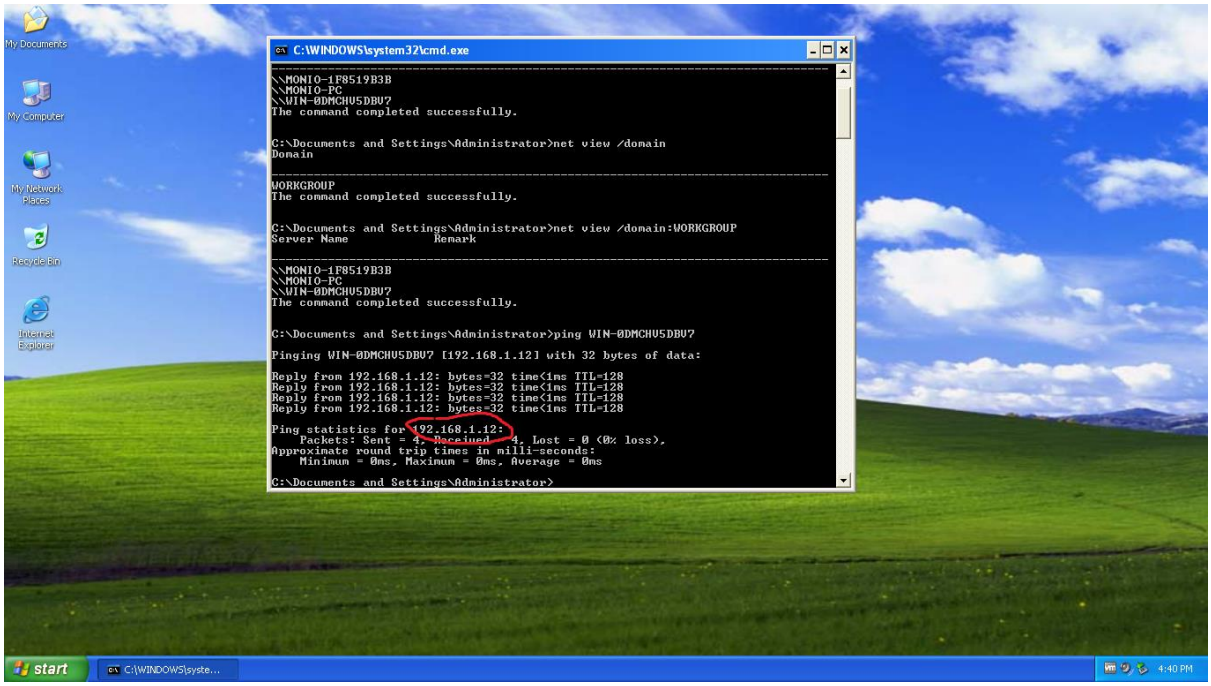
8.Now move on to your Windows Xp machine. Open up the command prompt and type in:net view . Next command is net view /domain



Sometimes you will be able to gain access to a Windows machine on the network , but not use the GUI frontend , only the command prompt. You should be aware of some commands, in order to determine other hosts on the network.

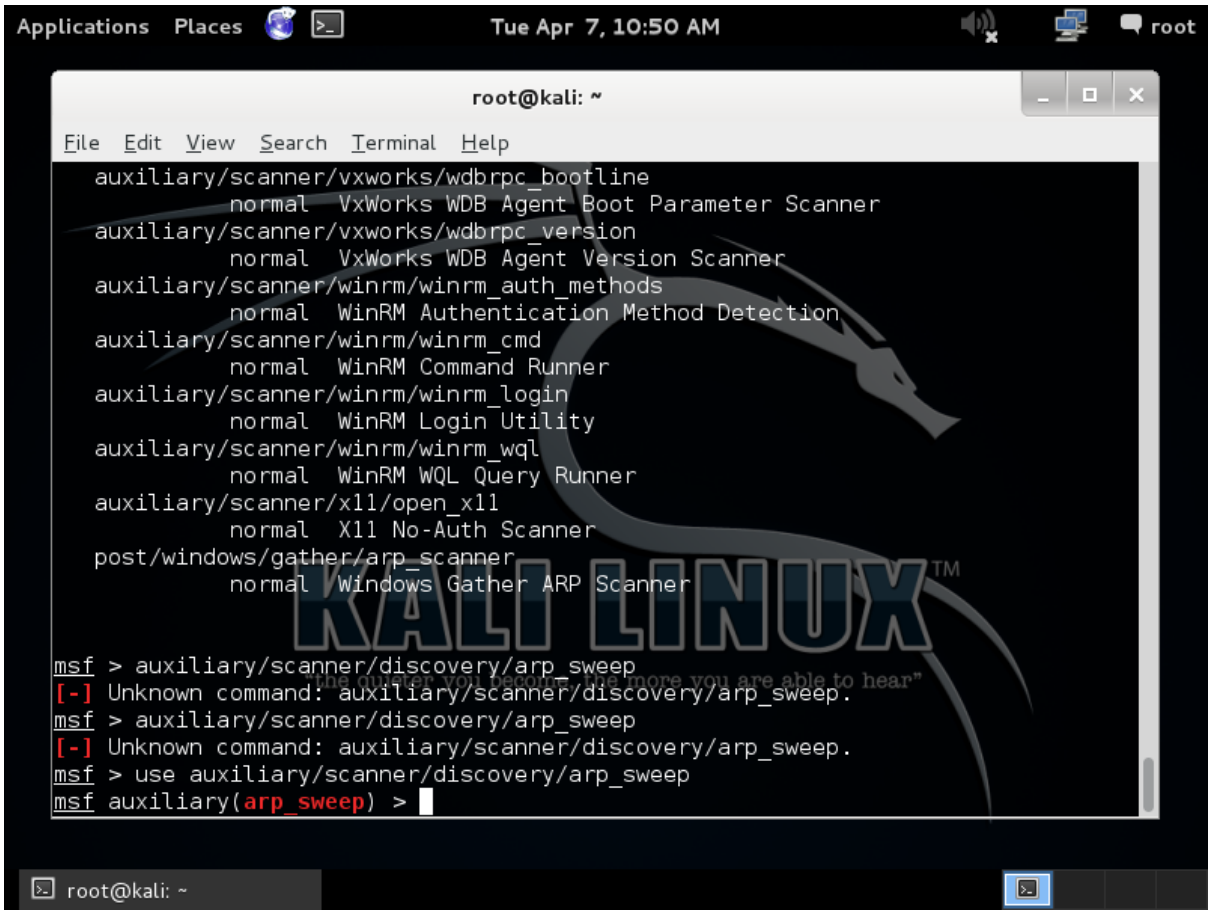
9.Type in : net view /domain:WORKGROUP. You will see all hosts which are part of the WORKGROUP domain.

10.In the terminal window type in: ping ,followed by the name of a machine , in my example I type in : ping WIN-07DMCHV5DBV7



You can see that the IP address of the machine is displayed. You can ping all the other machines and determine their IP addresses also.

10.Return to your Kali Linux machine and in the terminal write: msfconsole. This will start the Metasploit console. Then type in : search scanner . Metasploit is equipped with a lot of scanners you can use . Find auxiliary/scanner/discovery/arp_sweep , copy it and paste it.



Then type : show options , followed by : **set RHOSTS 192.168.1.0/24**

```
msf > auxiliary/scanner/discovery/arp_sweep
[-] Unknown command: auxiliary/scanner/discovery/arp_sweep.
msf > auxiliary/scanner/discovery/arp_sweep
[-] Unknown command: auxiliary/scanner/discovery/arp_sweep.
msf > use auxiliary/scanner/discovery/arp_sweep
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   RHOSTS                      yes       The target address range or CIDR identi
fier
   SHOST                       no        Source IP Address
   SMAC                        no        Source MAC Address
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    5                yes       The number of seconds to wait for new d
ata

msf auxiliary(arp_sweep) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(arp_sweep) >
```

Then: show options to check if the setting is set:

```
   SHOST                          no        Source IP Address
   SMAC                           no        Source MAC Address
   THREADS    1                   yes       The number of concurrent threads
   TIMEOUT    5                   yes       The number of seconds to wait for new d
ata

msf auxiliary(arp_sweep) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   RHOSTS     192.168.1.0/24   yes       The target address range or CIDR identi
fier
   SHOST                       no        Source IP Address
   SMAC                        no        Source MAC Address
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    5                yes       The number of seconds to wait for new d
ata

msf auxiliary(arp_sweep) >
```

Then type in : run , to run the scanner:

```
Applications  Places   Tue Apr 7, 10:55 AM   root
root@kali: ~
File  Edit  View  Search  Terminal  Help

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   INTERFACE                    no        The name of the interface
   RHOSTS      192.168.1.0/24   yes       The target address range or CIDR identi
fier
   SHOST                        no        Source IP Address
   SMAC                         no        Source MAC Address
   THREADS     1                yes       The number of concurrent threads
   TIMEOUT     5                yes       The number of seconds to wait for new d
ata

msf auxiliary(arp_sweep) > run

[*] 192.168.1.1 appears to be up (VMware, Inc.).
[*] 192.168.1.1 appears to be up (VMware, Inc.).
[*] 192.168.1.11 appears to be up (VMware, Inc.).
[*] 192.168.1.12 appears to be up (VMware, Inc.).
[*] 192.168.1.13 appears to be up (VMware, Inc.).
[*] 192.168.1.1 appears to be up (VMware, Inc.).
[*] 192.168.1.11 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(arp_sweep) >
root@kali: ~
```

Metasploit found again the same hosts to be up.

11. Type in back to go back one step , and then type in :

use auxiliary/scanner/netbios/nbname

Then : **show options**

```
[*] 192.168.1.1 appears to be up (VMware, Inc.).
[*] 192.168.1.11 appears to be up (VMware, Inc.).
[*] 192.168.1.12 appears to be up (VMware, Inc.).
[*] 192.168.1.13 appears to be up (VMware, Inc.).
[*] 192.168.1.1 appears to be up (VMware, Inc.).
[*] 192.168.1.11 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(arp_sweep) > back
msf > use auxiliary/scanner/netbios/nbname
msf auxiliary(nbname) > show options

Module options (auxiliary/scanner/netbios/nbname):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each se
t
   RHOSTS                      yes       The target address range or CIDR identi
fier
   RPORT      137              yes       The target port
   THREADS    10               yes       The number of concurrent threads

msf auxiliary(nbname) >
```

12.Type in : **set RHOSTS 192.168.1.0/24,** followed by show options to verify the setting.

```
Applications  Places   Tue Apr 7, 11:01 AM   root
root@kali: ~
File  Edit  View  Search  Terminal  Help
   ----        ---------------  --------  -----------
   BATCHSIZE   256              yes       The number of hosts to probe in each se
t
   RHOSTS                       yes       The target address range or CIDR identi
fier
   RPORT       137              yes       The target port
   THREADS     10               yes       The number of concurrent threads

msf auxiliary(nbname) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(nbname) > show options

Module options (auxiliary/scanner/netbios/nbname):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   BATCHSIZE   256              yes       The number of hosts to probe in each se
t
   RHOSTS      192.168.1.0/24   yes       The target address range or CIDR identi
fier
   RPORT       137              yes       The target port
   THREADS     10               yes       The number of concurrent threads

msf auxiliary(nbname) >
root@kali: ~
```

Now run the scanner :

```
Module options (auxiliary/scanner/netbios/nbname):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   BATCHSIZE   256              yes       The number of hosts to probe in each se
t
   RHOSTS      192.168.1.0/24   yes       The target address range or CIDR identi
fier
   RPORT       137              yes       The target port
   THREADS     10               yes       The number of concurrent threads

msf auxiliary(nbname) > run

[*] Sending NetBIOS requests to 192.168.1.0->192.168.1.255 (256 hosts)
[*] 192.168.1.1 [MONIO-PC] OS:Windows Names:(MONIO-PC, WORKGROUP, [illegible] MSBROWSE__
[illegible] Addresses:(192.168.244.1, 192.168.1.1, 10.0.0.9) Mac:00:50:56:c0:00:08 Virtua
l Machine:VMWare
[*] 192.168.1.11 [MONIO-1F8519B3B] OS:Windows Names:(MONIO-1F8519B3B, WORKGROUP)
 Addresses:(192.168.1.11) Mac:00:0c:29:ff:65:89 Virtual Machine:VMWare
[*] 192.168.1.12 [WIN-0DMCHV5DBV7] OS:Windows Names:(WIN-0DMCHV5DBV7, WORKGROUP)
 Addresses:(192.168.1.12) Mac:00:0c:29:33:9c:c3 Virtual Machine:VMWare
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(nbname) >
```

The scanner gives you a lot of information about the hosts, including the OS running and the MAC addresses also.

CONCLUSION

In this lab we have enumerated hosts on the internal network, using different scanning tools. Which one tool you will use is up to you, the one you feel the most comfortable with. Please notice that, while enumerating the hosts, all programs are producing a lot of ARP packets on the network.