Branden Barnes

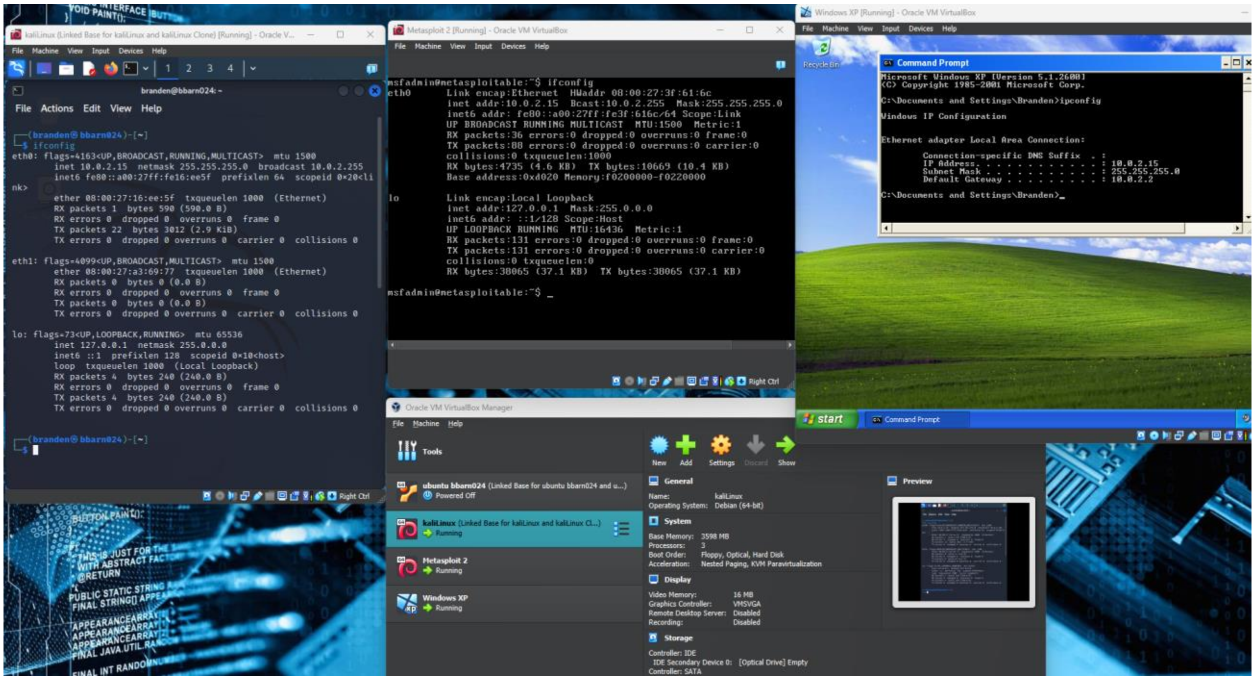
CYSE 450

Professor Vatsa

Reconnaissance and Footprinting

Task-A: Install the following Virtual Machines and display their IP addresses:

1. Kali Linux
2. Metasploitable2
3. Windows XP



kaliLinux (Linked Base for kaliLinux and kaliLinux Clone) [Running] - Oracle V...
File Machine View Input Devices Help
branden@bbarn024: ~
File Actions Edit View Help
Right Ctrl

```
┌──(branden㉿bbarn024)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe16:ee5f  prefixlen 64  scopeid 0x20<li
nk>
        ether 08:00:27:16:ee:5f  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 3012 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 08:00:27:a3:69:77  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(branden㉿bbarn024)-[~]
└─$ 
```

Metasploit 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3f:61:6c
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3f:616c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4735 (4.6 KB)  TX bytes:10669 (10.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:131 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:38065 (37.1 KB)  TX bytes:38065 (37.1 KB)

msfadmin@metasploitable:~$ _
```

Windows XP [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Command Prompt
start
Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Branden>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.0.2.15
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.2.2

C:\Documents and Settings\Branden>_
```

ubuntu bbarn024 (Linked Base for ubuntu bbarn024 and u...) Powered Off
kaliLinux (Linked Base for kaliLinux and kaliLinux Cl...) Running
Metasploit 2 Running
Windows XP Running

General
Name: kaliLinux
Operating System: Debian (64-bit)

System
Base Memory: 3598 MB
Processors: 3
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

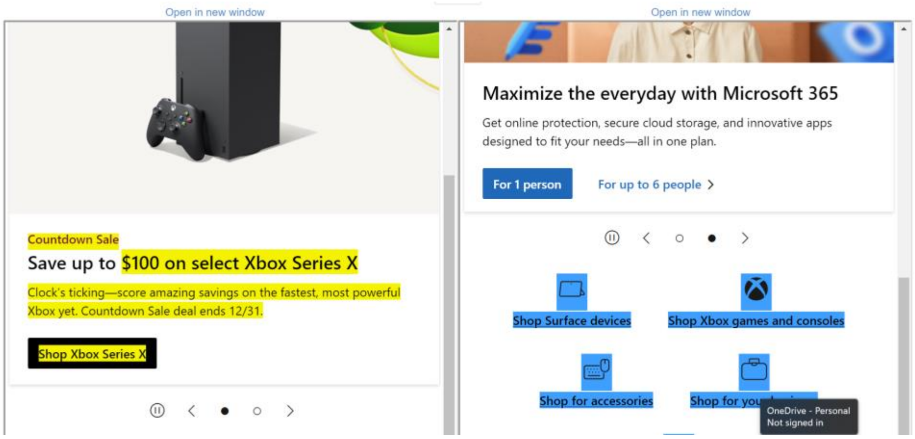
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA

Task B: Perform passive reconnaissance using archive.org and netcraft

1. Go to we.archive.org and in the search box type www.Microsoft.com and hit Enter
2. Gather and write in brief information about the updated made between January 1 till current date. Take the screenshot of the result

Changes made from January 1, 2024 – January 31, 2024, are shown between yellow and blue color. The yellow color represents what has been deleted where the blue color represents what has been added. A few things that have changed are difference in prices and sales for the Xbox and computer.



Open in new window

Countdown Sale

Save up to $100 on select Xbox Series X

Clock's ticking—score amazing savings on the fastest, most powerful Xbox yet. Countdown Sale deal ends 12/31.

Shop Xbox Series X

Open in new window

Maximize the everyday with Microsoft 365

Get online protection, secure cloud storage, and innovative apps designed to fit your needs—all in one plan.

For 1 person

For up to 6 people >

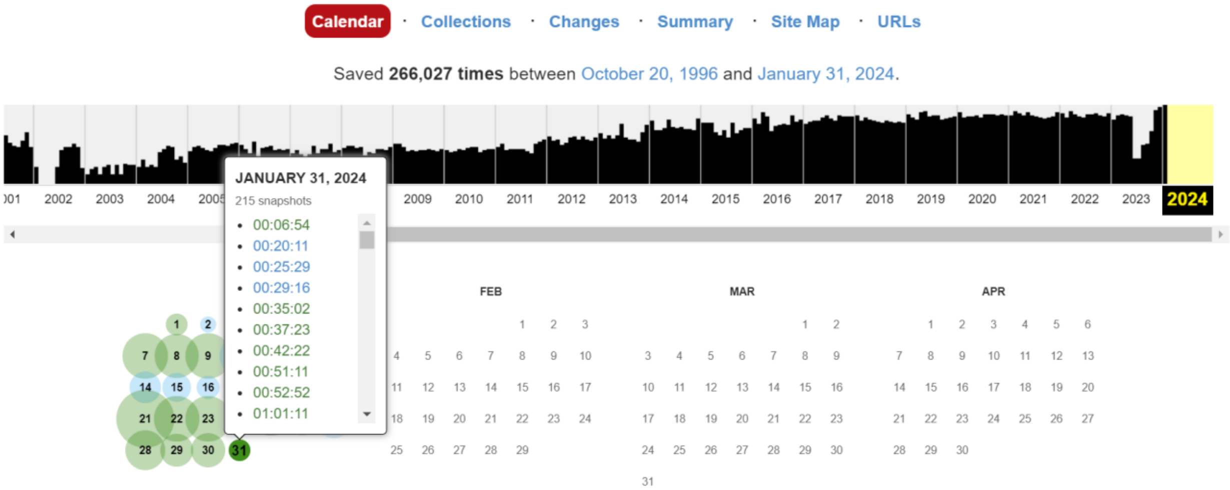
Shop Surface devices

Shop Xbox games and consoles

Shop for accessories

Shop for you

OneDrive - Personal
Not signed in

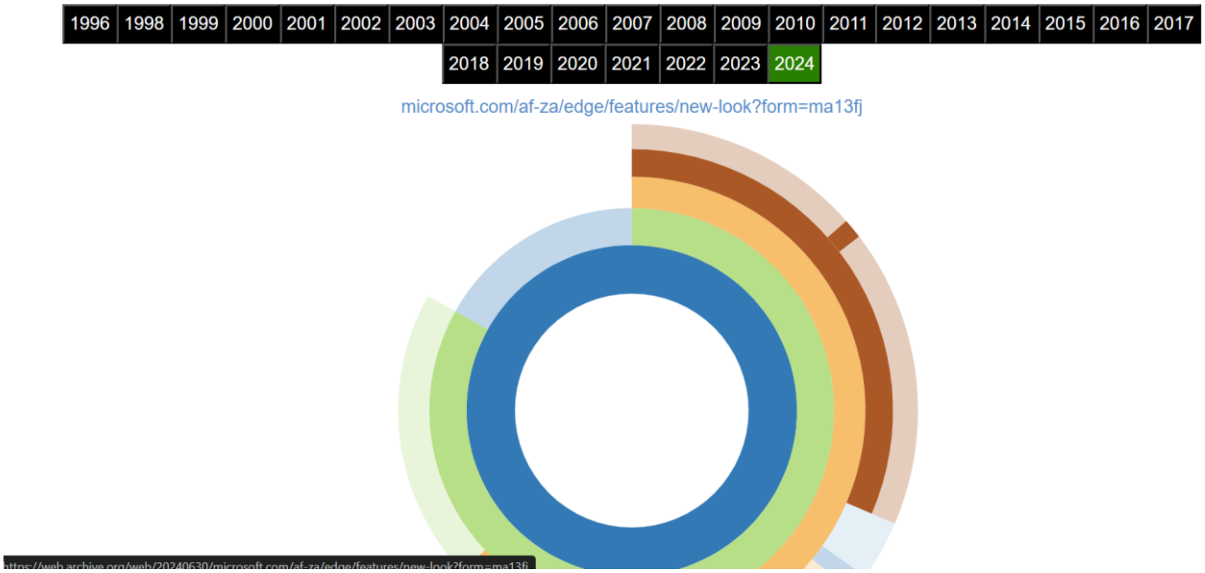


Calendar · Collections · Changes · Summary · Site Map · URLs

Saved **266,027 times** between October 20, 1996 and January 31, 2024.

JANUARY 31, 2024
215 snapshots

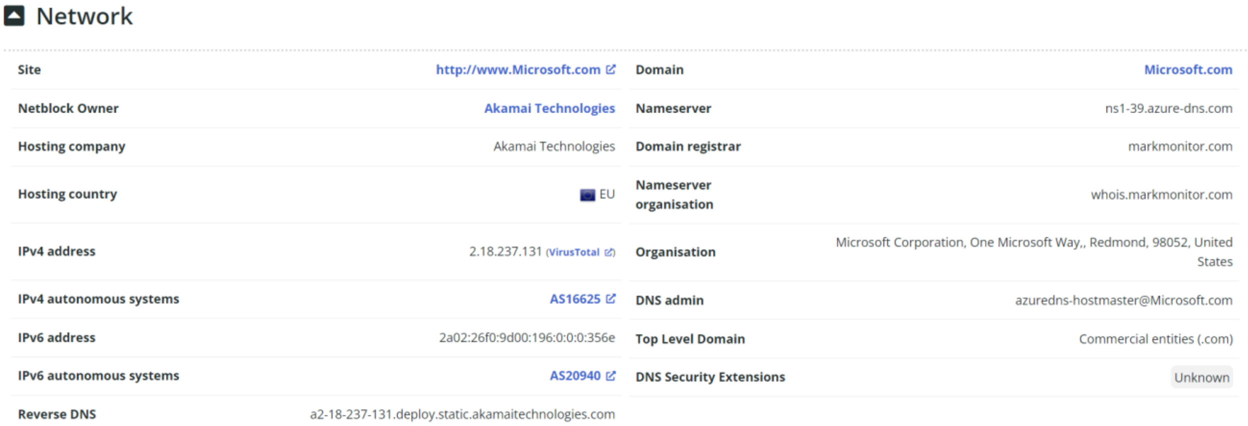
- 00:06:54
- 00:20:11
- 00:25:29
- 00:29:16
- 00:35:02
- 00:37:23
- 00:42:22
- 00:51:11
- 00:52:52
- 01:01:11



microsoft.com/af-za/edge/features/new-look?form=ma13fj

https://web.archive.org/web/20240630/microsoft.com/af-za/edge/features/new-look?form=ma13fj

3. For this step, open a new tab and go to www.netcraft.com and gather information about network like, network domain, network registrar, IPV4 address, and nameserver for www.microsoft.com. write in brief what you analyzed?



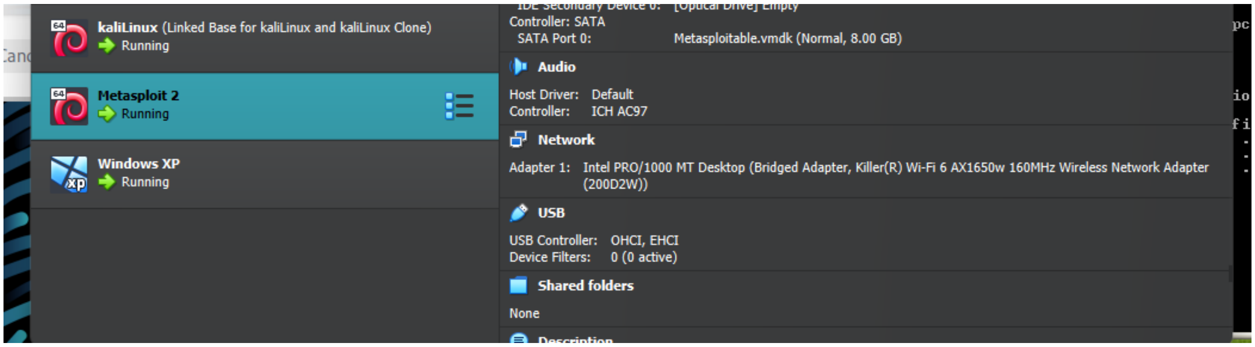
Network

Site	http://www.Microsoft.com	Domain	Microsoft.com
Netblock Owner	Akamai Technologies	Nameserver	ns1-39.azure-dns.com
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	EU	Nameserver organisation	whois.markmonitor.com
IPv4 address	2.18.237.131 (VirusTotal)	Organisation	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS16625	DNS admin	azuredns-hostmaster@Microsoft.com
IPv6 address	2a02:26f0:9d00:196:0:0:0:356e	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS20940	DNS Security Extensions	Unknown
Reverse DNS	a2-18-237-131.deploy.static.akamaitechnologies.com		

From the netcraft.com website you can see a full write up on Microsoft.com. You can observe background information, network information, IP geolocation, and more. It was interesting to see that the hosting country was the Netherlands.

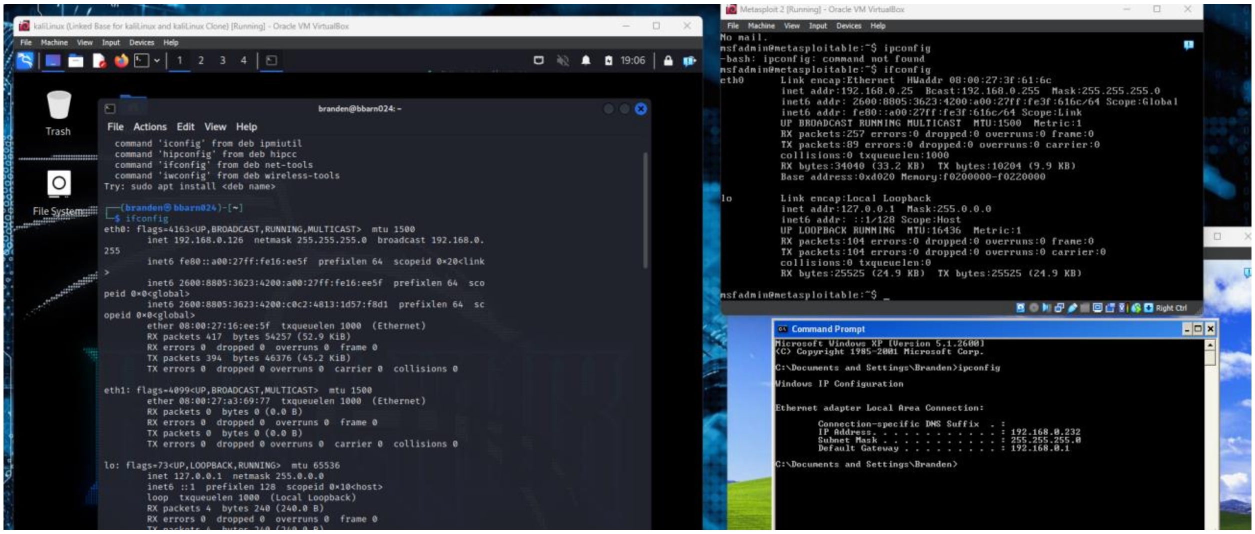
Task C: Perform active reconnaissance using attacker Kali Linux and target Metasploitable VM.

1. In the settings, change the network adapter to Bridge mode for all the Three machines.



```
IDE Secondary Device 0:  [Optical Drive] Empty
Controller: SATA
 SATA Port 0:             Metasploitable.vmdk (Normal, 8.00 GB)
Audio
Host Driver:   Default
Controller:    ICH AC97
Network
Adapter 1:   Intel PRO/1000 MT Desktop (Bridged Adapter, Killer(R) Wi-Fi 6 AX1650w 160MHz Wireless Network Adapter
             (200D2W))
USB
USB Controller:   OHCI, EHCI
Device Filters:   0 (0 active)
Shared folders
None
Description
```

2. Open the terminals and execute the correct command to print the IP addresses for all the 3 machines separately (Make sure the IP address should be unique for all the 3 machines.

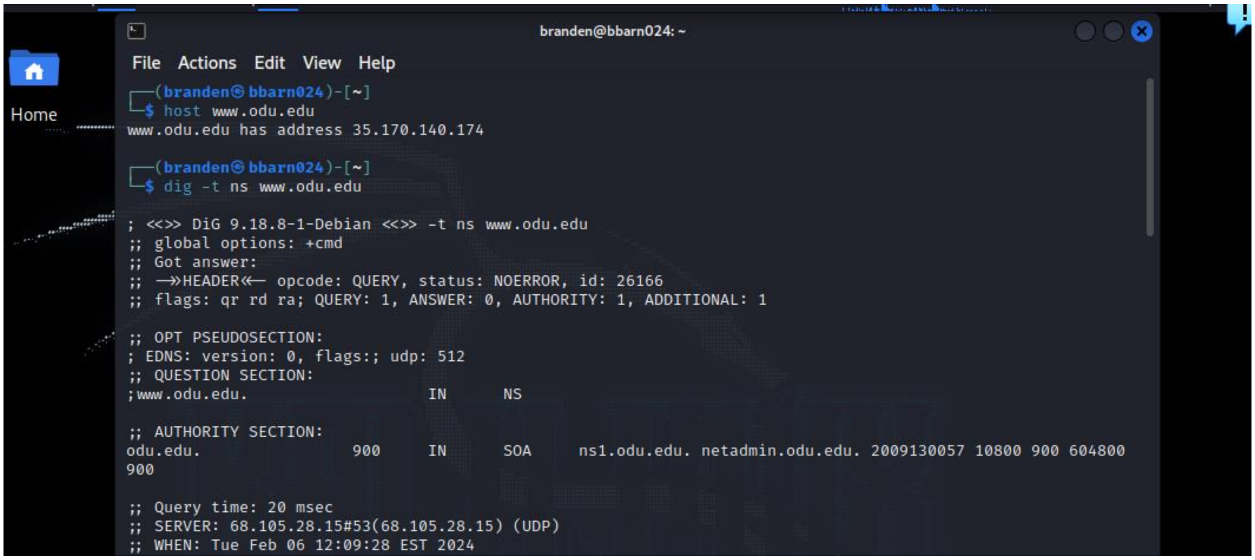

kaliLinux (Linked Base for kaliLinux and kaliLinux Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:06
Trash
File System
branden@bbarn024: ~
File Actions Edit View Help
Metasploit 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Command Prompt

```
  command 'iconfig' from deb ipmiutil
  command 'hipconfig' from deb hipcc
  command 'ifconfig' from deb net-tools
  command 'iwconfig' from deb wireless-tools
Try: sudo apt install <deb name>

┌──(branden㉿bbarn024)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.126  netmask 255.255.255.0  broadcast 192.168.0.
255
        inet6 fe80::a00:27ff:fe16:ee5f  prefixlen 64  scopeid 0×20<link
>
        inet6 2600:8805:3623:4200:a00:27ff:fe16:ee5f  prefixlen 64  sco
peid 0×0<global>
        inet6 2600:8805:3623:4200:c0c2:4813:1d57:f8d1  prefixlen 64  sc
opeid 0×0<global>
        ether 08:00:27:16:ee:5f  txqueuelen 1000  (Ethernet)
        RX packets 417  bytes 54257 (52.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 394  bytes 46376 (45.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 08:00:27:a3:69:77  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
```

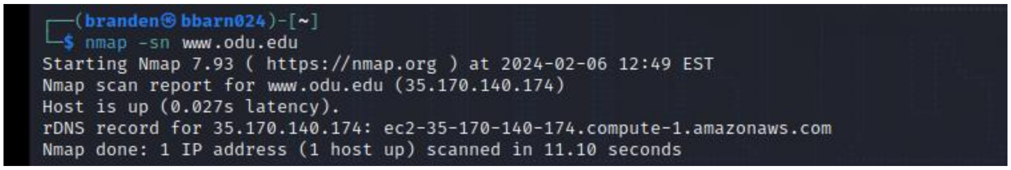
```
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3f:61:6c
          inet addr:192.168.0.25  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2600:8805:3623:4200:a00:27ff:fe3f:616c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe3f:616c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:257 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34040 (33.2 KB)  TX bytes:10204 (9.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25525 (24.9 KB)  TX bytes:25525 (24.9 KB)

msfadmin@metasploitable:~$ _
```

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Branden>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.232
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

C:\Documents and Settings\Branden>
```

3. In Kali Linux terminal, execute the command (host/dig) to demonstrate whether the host (www.odu.edu or www.amazon.com) is live/UP or not. Also provide the reason if the host is live /UP.

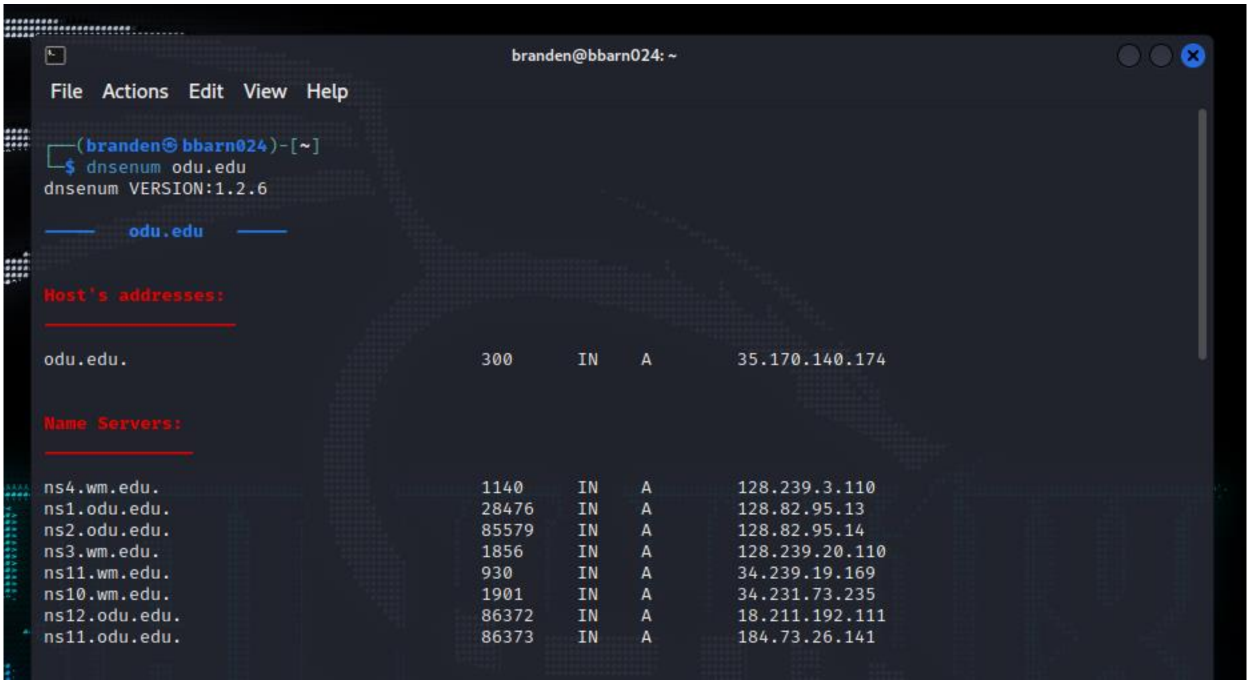


```
┌──(branden㉿bbarn024)-[~]
└─$ host www.odu.edu
www.odu.edu has address 35.170.140.174

┌──(branden㉿bbarn024)-[~]
└─$ dig -t ns www.odu.edu

; <<>> DiG 9.18.8-1-Debian <<>> -t ns www.odu.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26166
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.odu.edu.                   IN      NS

;; AUTHORITY SECTION:
odu.edu.                900     IN      SOA     ns1.odu.edu. netadmin.odu.edu. 2009130057 10800 900 604800
900

;; Query time: 20 msec
;; SERVER: 68.105.28.15#53(68.105.28.15) (UDP)
;; WHEN: Tue Feb 06 12:09:28 EST 2024
```



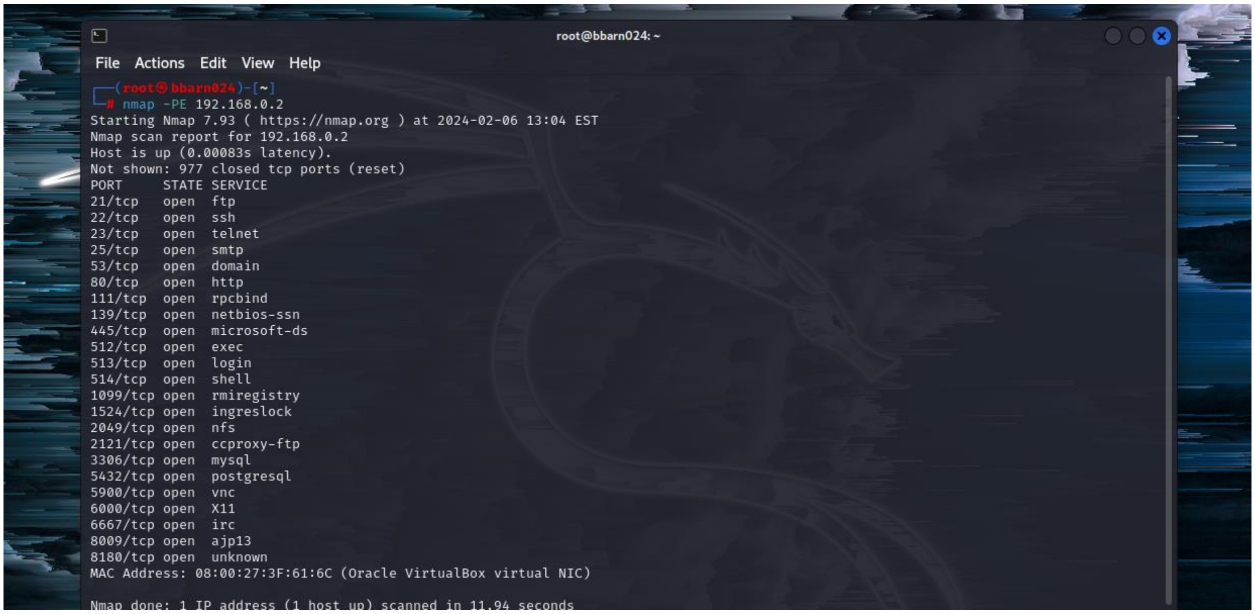
```
┌──(branden㉿bbarn024)-[~]
└─$ nmap -sn www.odu.edu
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-06 12:49 EST
Nmap scan report for www.odu.edu (35.170.140.174)
Host is up (0.027s latency).
rDNS record for 35.170.140.174: ec2-35-170-140-174.compute-1.amazonaws.com
Nmap done: 1 IP address (1 host up) scanned in 11.10 seconds
```

4. Using terminal in Kali Linux, perform DNS enumeration using dnsenum command for www.odu.edu or www.google.com



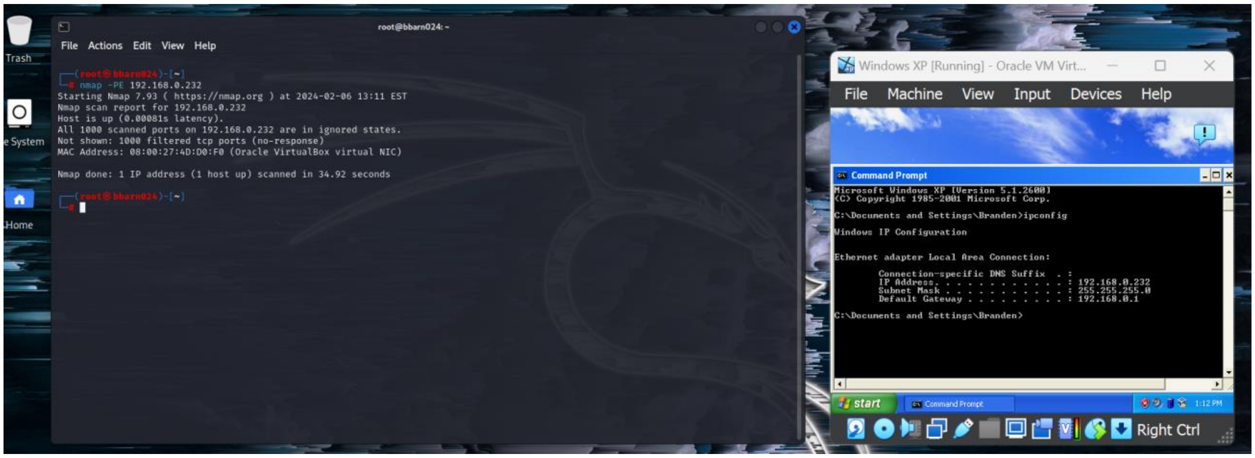
```
┌──(branden㉿bbarn024)-[~]
└─$ dnsenum odu.edu
dnsenum VERSION:1.2.6

-----   odu.edu   -----


Host's addresses:
__________________

odu.edu.                                 300      IN    A        35.170.140.174


Name Servers:
______________

ns4.wm.edu.                              1140     IN    A        128.239.3.110
ns1.odu.edu.                             28476    IN    A        128.82.95.13
ns2.odu.edu.                             85579    IN    A        128.82.95.14
ns3.wm.edu.                              1856     IN    A        128.239.20.110
ns11.wm.edu.                             930      IN    A        34.239.19.169
ns10.wm.edu.                             1901     IN    A        34.231.73.235
ns12.odu.edu.                            86372    IN    A        18.211.192.111
ns11.odu.edu.                            86373    IN    A        184.73.26.141
```

5. In kali Linux, perform ICMP Sweep scan to gather information about the target machine (Metasploitable Linux) by sending ICMP echo request to target machine (using its ip address), using nmap command with correct options. Highlight the line indicating whether the ICMP reply has been received or not.



```
┌──(root㉿bbarn024)-[~]
└─# nmap -PE 192.168.0.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-06 13:04 EST
Nmap scan report for 192.168.0.2
Host is up (0.00083s latency).
Not shown: 977 closed tcp ports (reset)
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: 08:00:27:3F:61:6C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.94 seconds
```

6. In kali Linux, perform ICMP Sweep scan to gather information about the target machine (Windows Xp/7) by sending ICMP echo request, using nmap command with correct options.



Trash
e System
Home
root@bbarn024: ~
File Actions Edit View Help
Windows XP [Running] - Oracle VM Virt...
File Machine View Input Devices Help
Command Prompt
start
Command Prompt
1:12 PM
Right Ctrl

```
┌──(root㉿bbarn024)-[~]
└─# nmap -PE 192.168.0.232
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-06 13:11 EST
Nmap scan report for 192.168.0.232
Host is up (0.00081s latency).
All 1000 scanned ports on 192.168.0.232 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:4D:D0:F0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.92 seconds

┌──(root㉿bbarn024)-[~]
└─#
```

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Branden>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.232
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

C:\Documents and Settings\Branden>
```