



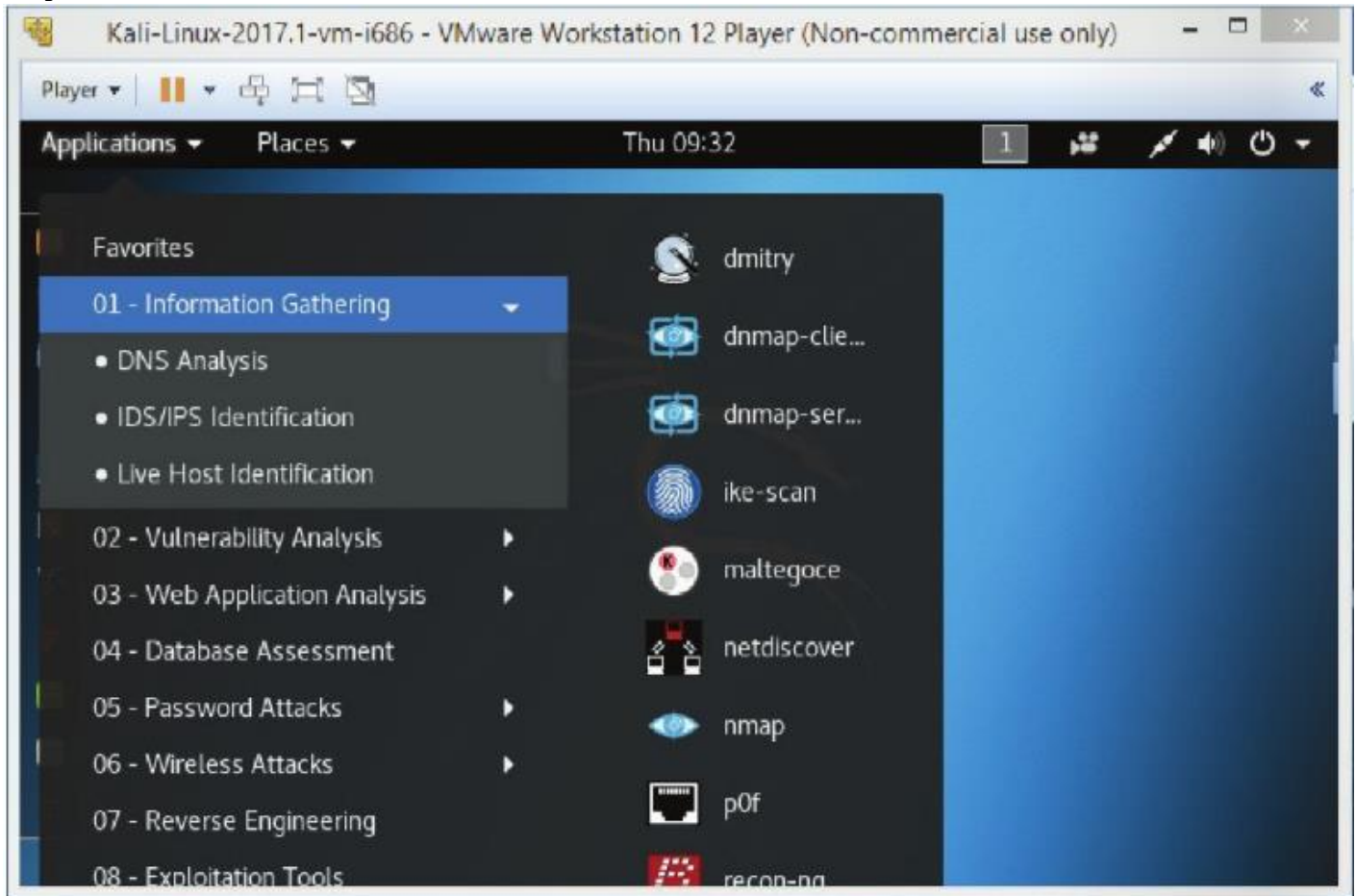
Problem Statement: Enumeration of various services that are running on a target machine using Nmap.

Lab Tasks

To enumerate services on target machine, perform the following steps:

1. Launch Kali Linux

2. Select Applications > Information Gathering > nmap, as shown in the Figure.



Then the following screen will appear, as shown in Figure.





```

root@kali: ~
File Edit View Search Terminal Help
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~#

```

3. Type 'nmap -sP 192.xx.xx.xx/2', and press Enter, as shown in Figure 27.

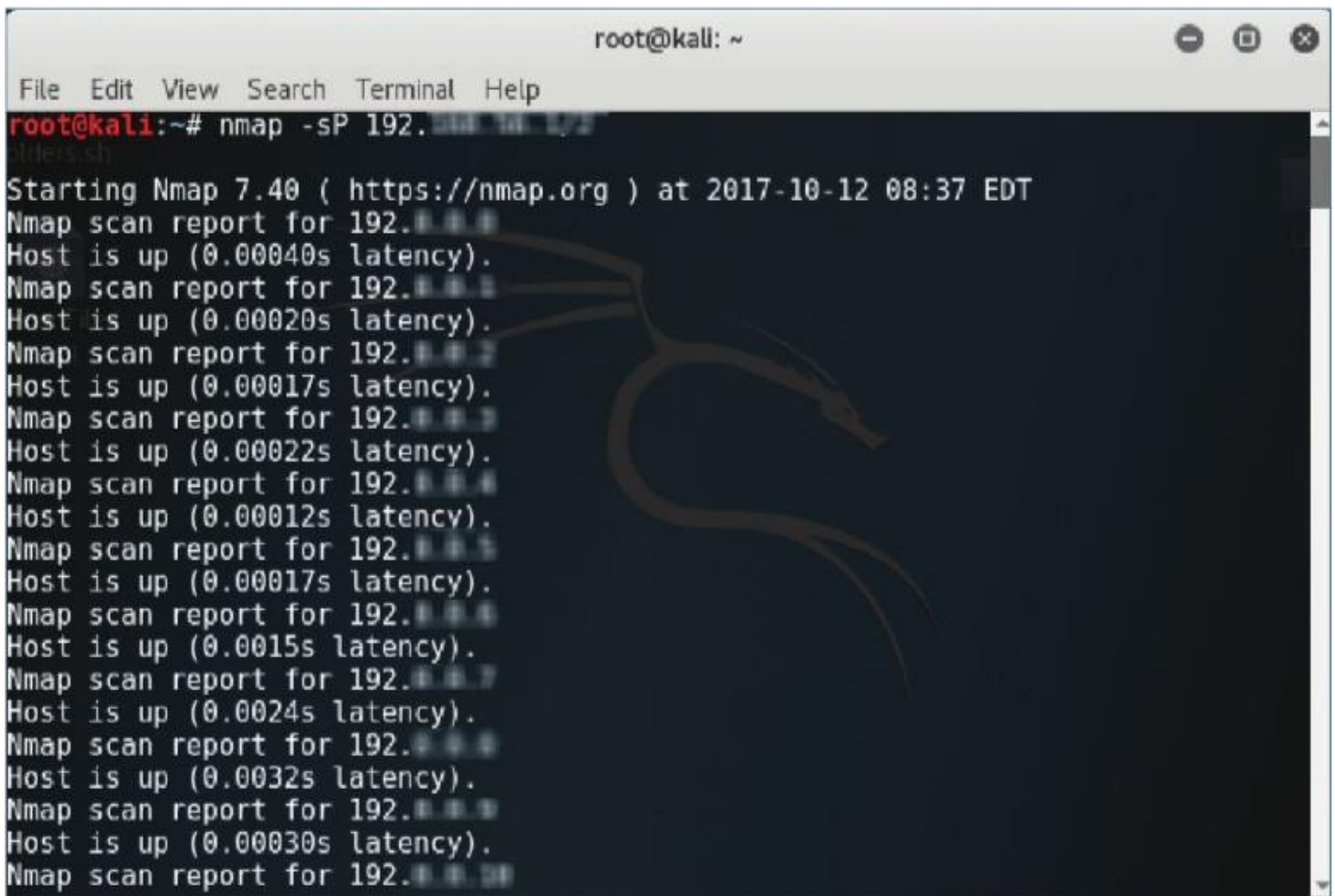
```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sP 192.168.0.0/2

```

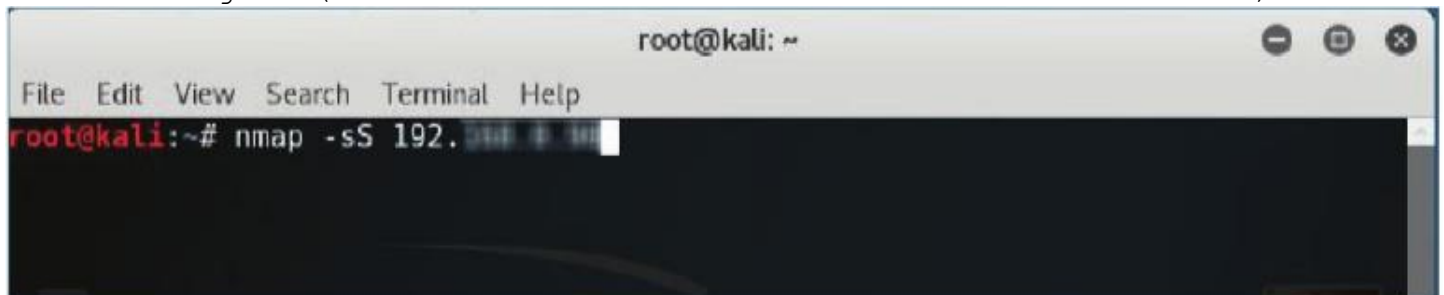
Then 'Nmap' will scan all the nodes on the given network range and display all the hosts that are running, as shown in Figure.





```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sP 192.168.1.1/24  
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 08:37 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.00040s latency).  
Nmap scan report for 192.168.1.2  
Host is up (0.00020s latency).  
Nmap scan report for 192.168.1.3  
Host is up (0.00017s latency).  
Nmap scan report for 192.168.1.4  
Host is up (0.00022s latency).  
Nmap scan report for 192.168.1.5  
Host is up (0.00012s latency).  
Nmap scan report for 192.168.1.6  
Host is up (0.00017s latency).  
Nmap scan report for 192.168.1.7  
Host is up (0.0015s latency).  
Nmap scan report for 192.168.1.8  
Host is up (0.0024s latency).  
Nmap scan report for 192.168.1.9  
Host is up (0.0032s latency).  
Nmap scan report for 192.168.1.10  
Host is up (0.00030s latency).  
Nmap scan report for 192.168.1.11
```

4. Type 'nmap-sS <IP address of the target machine>', and press Enter, as shown in Figure (here we have used 192.XX.XX.XX as the IP address).



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 192.168.1.1
```

Then a Stealthy syn scan will be initiated, and all the open ports that are running on the machine will be displayed, as shown in Figure.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 192.168.8.100  
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 08:45 EDT  
Nmap scan report for 192.168.8.100  
Host is up (1.0s latency).  
Not shown: 983 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
110/tcp   open  pop3  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
514/tcp   filtered shell  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
1025/tcp  open  NFS-or-IIS  
1026/tcp  open  LSA-or-nterm  
1027/tcp  open  IIS  
1028/tcp  open  unknown  
1029/tcp  open  ms-lsa  
1072/tcp  open  cardax  
1085/tcp  open  webobjects  
3389/tcp  open  ms-wbt-server
```

Now, we can see all the open ports along with the services. We will find the version of each of these services running on the open port by performing a syn scan with the version detection switch.

5. Type 'nmap -sSV -O <IP address of the target machine>', and press Enter, as shown in Figure.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sSV -O 192.168.8.100  
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 09:14 EDT
```

Now, the Nmap performs the scan and displays the versions of the services, as shown in Figure.


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sSV -O 192.168.10.1  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 09:14 EDT  
Nmap scan report for 192.168.10.1  
Host is up (0.00035s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE          VERSION  
80/tcp    open  http             Microsoft IIS httpd 8.5  
135/tcp   open  msrpc            Microsoft Windows RPC  
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
902/tcp   open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)  
912/tcp   open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)  
1025/tcp  open  msrpc            Microsoft Windows RPC  
1026/tcp  open  msrpc            Microsoft Windows RPC  
1027/tcp  open  msrpc            Microsoft Windows RPC  
1028/tcp  open  msrpc            Microsoft Windows RPC  
1029/tcp  open  msrpc            Microsoft Windows RPC  
1072/tcp  open  http             Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)  
1085/tcp  open  msrpc            Microsoft Windows RPC  
3389/tcp  open  ssl/ms-wbt-server?
```

We have found the enumerated result. We will now save the scan result.

6. Type 'nmap -sSV -O <IP address of the target machine> -oN Enumeration.txt', and press Enter, as shown in Figure.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sSV -O 192.168.10.1 -oN Enumeration.txt
```

Then following screen will appear, as shown in Figure.



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# clear
root@kali:~# nmap -sSV -O 192.168.10.1 -oN Enumeration.txt

Starting Nmap 7.40 ( https://nmap.org ) at 2017-10-12 09:17 EDT
Nmap scan report for 192.168.10.1
Host is up (0.00038s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 8.5
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
902/tcp   open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp  open  msrpc            Microsoft Windows RPC
1026/tcp  open  msrpc            Microsoft Windows RPC
1027/tcp  open  msrpc            Microsoft Windows RPC
1028/tcp  open  msrpc            Microsoft Windows RPC
1029/tcp  open  msrpc            Microsoft Windows RPC
1072/tcp  open  http             Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)

```

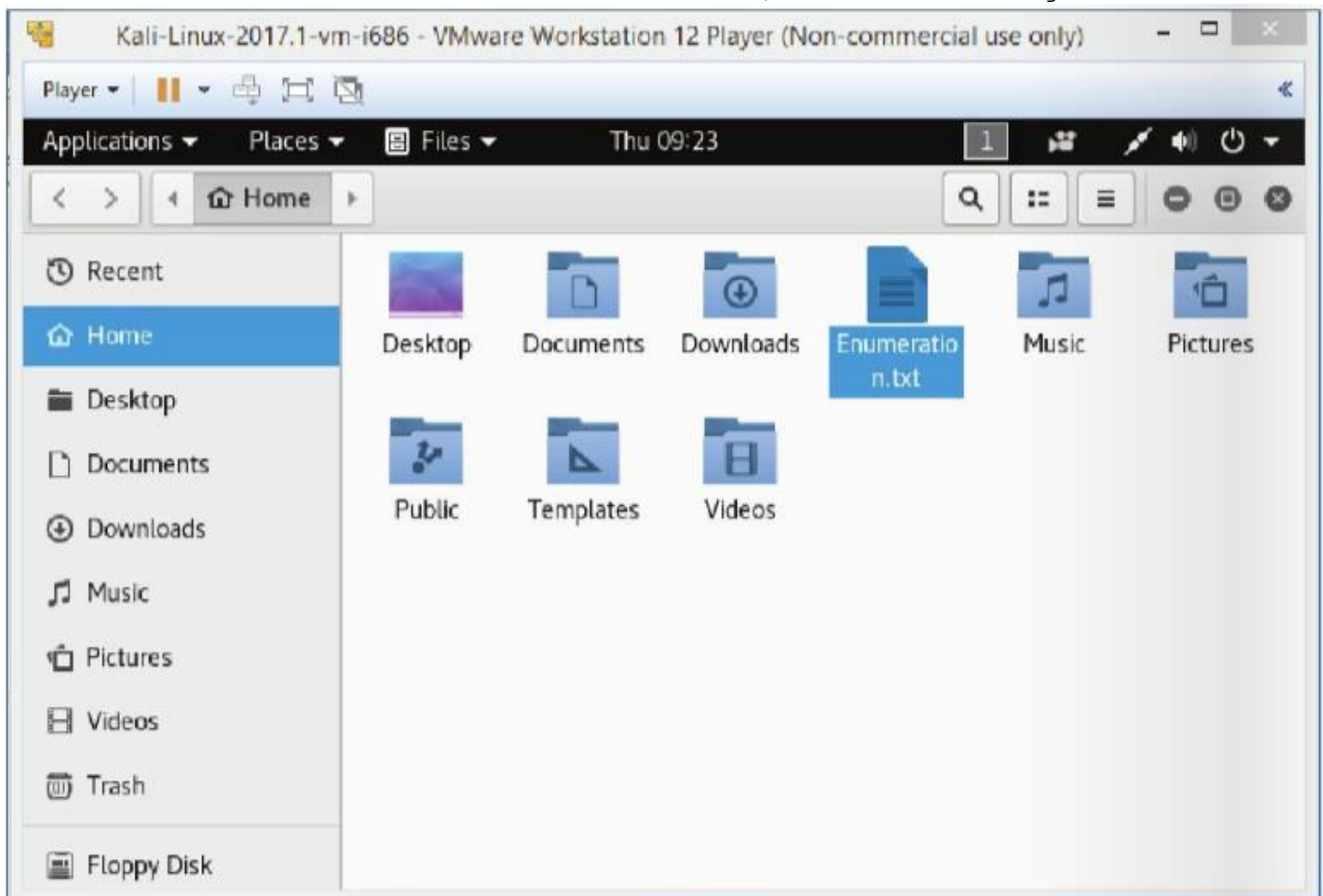
Nmap will now perform Stealthy Scan with version and OS detection, and save the result in a text file (Enumeration.txt), which will be located on home (root) directory.

7. Click on Places > Home Folder, as shown in Figure.





8. Double click on the file Enumeration.txt, as shown in Figure.





Then the following window will appear, as shown in Figure.

```

Kali-Linux-2017.1-vm-i686 - VMware Workstation 12 Player (Non-commercial use only)
Applications ▾ Places ▾ Text Editor ▾ Thu 09:24
Enumeration.txt Save
# Nmap 7.40 scan initiated Thu Oct 12 09:17:29 2017 as: nmap -sSV -O -oN
Enumeration.txt 192.168.146.1
Nmap scan report for 192.168.146.1
Host is up (0.00038s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 8.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp  open  msrpc        Microsoft Windows RPC
1026/tcp  open  msrpc        Microsoft Windows RPC
1027/tcp  open  msrpc        Microsoft Windows RPC
1028/tcp  open  msrpc        Microsoft Windows RPC
1029/tcp  open  msrpc        Microsoft Windows RPC
1072/tcp  open  http         Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)
Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS
  
```

You can also check the scanning result in the command line terminal. Type 'cat Enumeration.txt', and press Enter, as shown in Figure.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat Enumeration.txt
  
```

Then the output of the scanning process will be shown in the command line terminal, as shown in Figure 39.


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# cat Enumeration.txt  
# Nmap 7.40 scan initiated Thu Oct 12 09:17:29 2017 as: nmap -sSV -O -oN Enumera  
tion.txt 192.168.1.10  
Nmap scan report for 192.168.1.10  
Host is up (0.00038s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Microsoft IIS httpd 8.5  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgro  
up: WORKGROUP)  
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, S  
OAP)  
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, S0  
AP)  
1025/tcp  open  msrpc        Microsoft Windows RPC  
1026/tcp  open  msrpc        Microsoft Windows RPC  
1027/tcp  open  msrpc        Microsoft Windows RPC  
1028/tcp  open  msrpc        Microsoft Windows RPC  
1029/tcp  open  msrpc        Microsoft Windows RPC  
1072/tcp  open  http         Apache httpd 2.4.27 ((Win32) mod_fcgid/2.3.9)  
1085/tcp  open  msrpc        Microsoft Windows RPC
```

Lab Summary

In this lab, we have demonstrated how to enumerate the services that are running on the target machine and find the vulnerabilities of the services.