INFORMATION GATHERING

LAB 2

LAB

DETECT LIVE HOSTS

NMAP SCANS

DNS ENUMERATION

ZONE TRANSFER AND NSLOOKUP

1. Lab Scenario

You are a member of a penetration testing team and your task is to conduct the *Infrastructural Information Gathering* phase of a penetration test.

Target organization: University Campus.

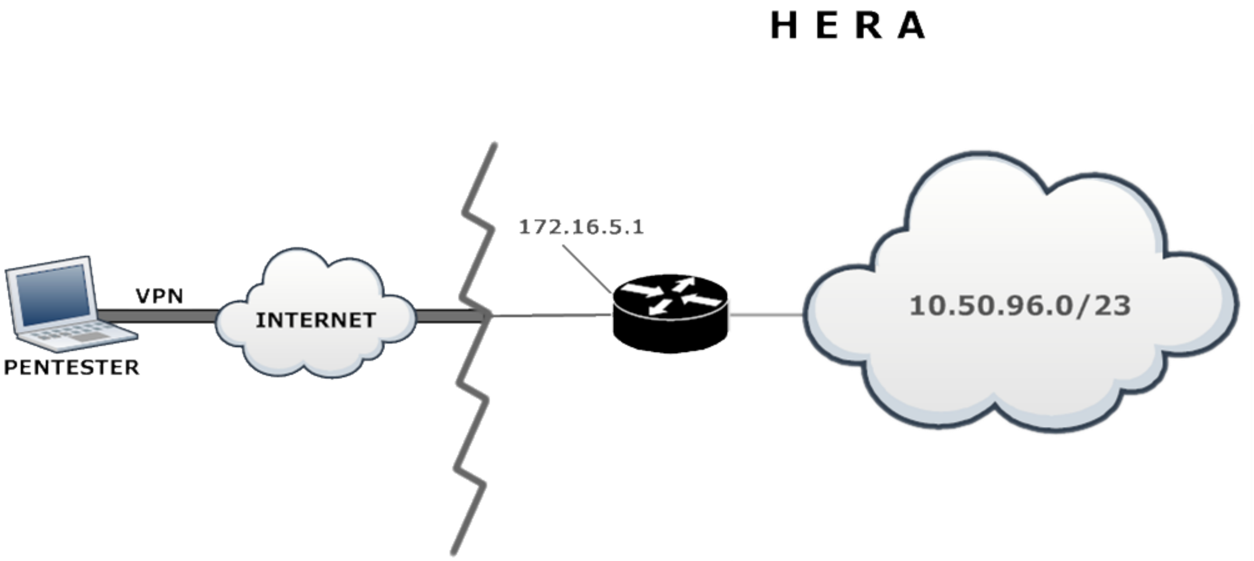
Scope: The scope is limited to the following domain and netblock:

- `Netblock: 10.50.96.0/23`
- `Domain: foocampus.com`

Each host in the netblock is exposed to Internet with its own public IP.

Task: Perform the Infrastructure Information Gathering phase. This pentest is authorized by the University's president and CIO. IT staff is unaware of the Pentest, so it is important to generate as little traffic as possible during some scans.

Lab environment diagram:



2. Learning Objectives

- Perform a host discovery scan
- Perform DNS enumeration
- Recognize the differences between Nmap scan options
- Identify how to detect the presence of a Firewall

This lab will present you with different tasks in order to fulfill these objectives.

The tasks are meant for educational purposes and to show you the usage of different tools and different methods to achieve the same goal.

Important: They are not meant to be used as a methodology.

Armed with the skills acquired during these tasks, you can achieve the Lab goal.

Repeat this lab as often as you like, but if this is the first time you do this lab, we advise you to follow these tasks.

Solutions are provided at the end of this document.

3. Recommended tools

- **`Nmap`**
- **`dig`**
- **`nslookup`**
- **`dnsenum`**

4. Tasks

Task 1: Host Discovery – Ping sweep

Perform a **ping sweep** (not a port scan) on the entire netblock and write down the discovered hosts.

Host IP address

Task 2: Host Discovery – no ping

Once you have found the live hosts, try again with other techniques. I.e. this time use TCP packets, but don't scan the entire port range, use the most common ports.

Important: This is the first phase of information gathering, so we don't need to know services or OS's running on the remote hosts. Just list the live hosts.

Host IP address

Task 3: Differences between the two scans

Did you find any difference between the two scans? If yes think why it happened and provide a response.

Task 4: DNS Discovery

How many DNS servers exists in the network and how you can get this information?

Task 5: Name Server

You already know the domain name, and at this point you should also have the DNS servers address. Try to find how many Name Server exists.

Name server	IP address

Task 6: MX Record

Try to perform an MX lookup. Can you find other IP addresses in the network?

Mail server	IP address

Task 7: Zone Transfer

Check if zone transfer is enabled in order to eventually get more IP addresses.

Name Server	Record Type	Data or IP Address

Task 8: Draw the network map

At this point you should have enough information about the University Campus. Draw a potential network map with the gathered information.

Task 9: Report Your Findings

SOLUTIONS

1: Host Discovery – Ping sweep

Ping sweepings can be performed in many ways. The **Nmap** command is the following:

```
nmap -sn 10.50.96.0/23
```

Note: that you can also use other tools, such as **fping**, and get almost the same results.

Nmap -sn uses ICMP requests, and a TCP scan on ports **80** and **443**. The result of the scan are as follows:

Host IP address
10.50.96.5
10.50.96.15
10.50.97.5
10.50.97.6
10.50.97.15

If you want to do an ICMP only scan, you have to use the **-PE** argument instead of **-sn**.

Extra credit: You can verify **nmap's** behavior with Wireshark.

2: Host Discovery – No Ping

Instead of using an ICMP scan, we can use TCP scanning techniques. Since we don't want to generate too much traffic, we will perform the scan using the **-PS** argument. The following is the command we want to run:

```
 nmap -n -sn -PS22,135,443,445 10.50.96.0/23
```

From the result of the previous scan we discovered another host in the network:

Host IP address
`10.50.97.17`

3: Differences between the two scans

As you have seen from the above tests, the two scans produced different results. This happens because some hosts are protected by firewalls and do not respond to pings. In this specific case, the firewall was set up to filter any kind of ping to **`10.50.97.17`**. That is why the first scan didn't discover the host (Windows Firewall drops pings by default and chances are that an Application based firewall is on the host).

4: DNS Discovery

In order to discover DNS servers on the network, we have to perform a specific scan. We know that DNS work on port **53** (TCP/UDP). We can run a scan against that specific port. Nmap has many options that allow us to do that. In this case, we used a SYN Scan:

```
nmap -sS -sU -p53 -n 10.50.96.0/23
```

The scan reports that there are two hosts (already discovered with Ping Sweep) that are running services on port **53** (**`10.50.96.5`** and **`10.50.96.15`**). We can now focus on them, using DNS enumeration techniques in order to discover more information about the network.

5: Name Server

We can get a lot of useful information from DNS records. In this case, in order to know the Name Server(s) serving Foocampus.com, and relatives IP address(es), we can use many tools explained in this course. One of the simplest and powerful is **nslookup**. In order to get the list of name servers we can use the following command:

```
1) >>nslookup
2) >>server 10.50.96.5
3) >>set q=NS
4) >>foocampus.com
```

Here is the explanation:

(**1**) we start the interactive shell of nslookup, then

(**2**) set the default server to query

(**3**) set the **querytype** to **NS** (since we want to know only NS records)

(**4**) type the domain.

The result of these steps is the following:

```
foocampus.comnameserver = ns.foocampus.com.
foocampus.comnameserver = ns1.foocampus.com.
```

We can now use the following commands to get the IP address of each domain:

```
>> nslookup
>> server 10.50.96.5
>> ns.foocampus.com
```

returns the address: **10.50.96.21**

```
>> ns1.foocampus.com
```

returns the address: **10.50.96.22**

6: MX Record

In the same way as before we can check for MX records. We can do so by setting the **querytype** to MX as follows:

```
>> nslookup
>> server 10.50.96.5
>> set q=MX
>> foocampus.com
```

We obtain the following name:

```
foocampus.commail exchanger = 10 pop3.foocampus.com.
```

with the following IP address: **10.50.96.60**

As you can imagine you can easily change the record type in order to get different information, such as all A records, or to get IP address from hostnames.

7: Zone Transfer

Zone transfers are usually misconfigurations of a DNS server. They should be enabled, if required, only for trusted IP addresses (usually trusted downstream name servers). When zone transfers are open to anyone, we can enumerate the whole DNS record for that zone.

To do that we can use many tools. Here we will see how to perform a zone transfer with the **dig** and **host** commands (Linux).

Dig command:

```
>>dig @10.50.96.5 foocampus.com -t AXFR +nocookie
```

Host command:

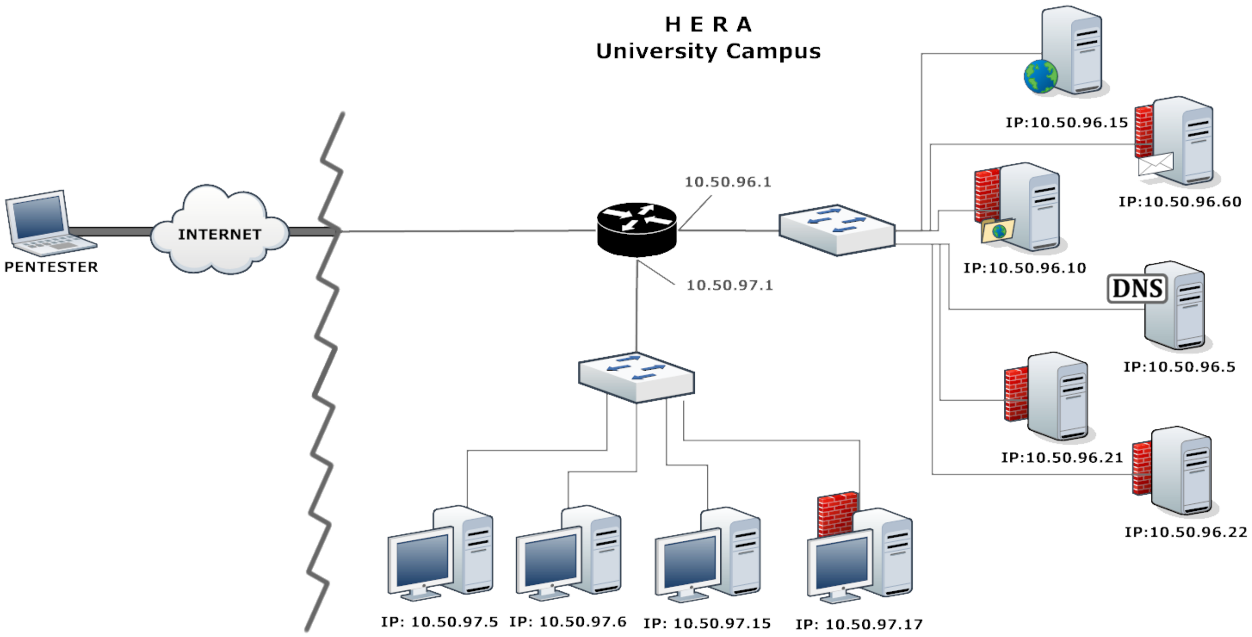
```
>>host -t axfr foocampus.com 10.50.96.5
```

We should now have the following information:

Name Server	Record Type	Data or IP address
foocampus.com	NS	ns.foocampus.com
foocampus.com	NS	ns1.foocampus.com
foocampus.com	MX	pop3.foocampus.com
ftp.foocampus.com	A	10.50.96.10
intranet.foocampus.com	A	10.50.96.15
management.foocampus.com	A	10.50.96.15
ns.foocampus.com	A	10.50.96.21
ns1.foocampus.com	A	10.50.96.22
pop3.foocampus.com	A	10.50.96.60
www.foocampus.com	A	10.50.96.15
foocampus.com	SOA	foocampus.com campusadmin 43 900 600 86400 3600

8: Draw the network map

The following image shows a potential network map of Foo Campus:



Task 9: Report Your Findings

This task if for you own reference. You will need to do similar tasks for your Penetration test report. If you have any questions or need any help, please post your question to the PTP forum.