LAB 02: INFORMATION GATHERING

Introduction to
Penetration Testing

TOPICS

- Preparation.
- Information gathering.
- Network mapping.

TOOLS

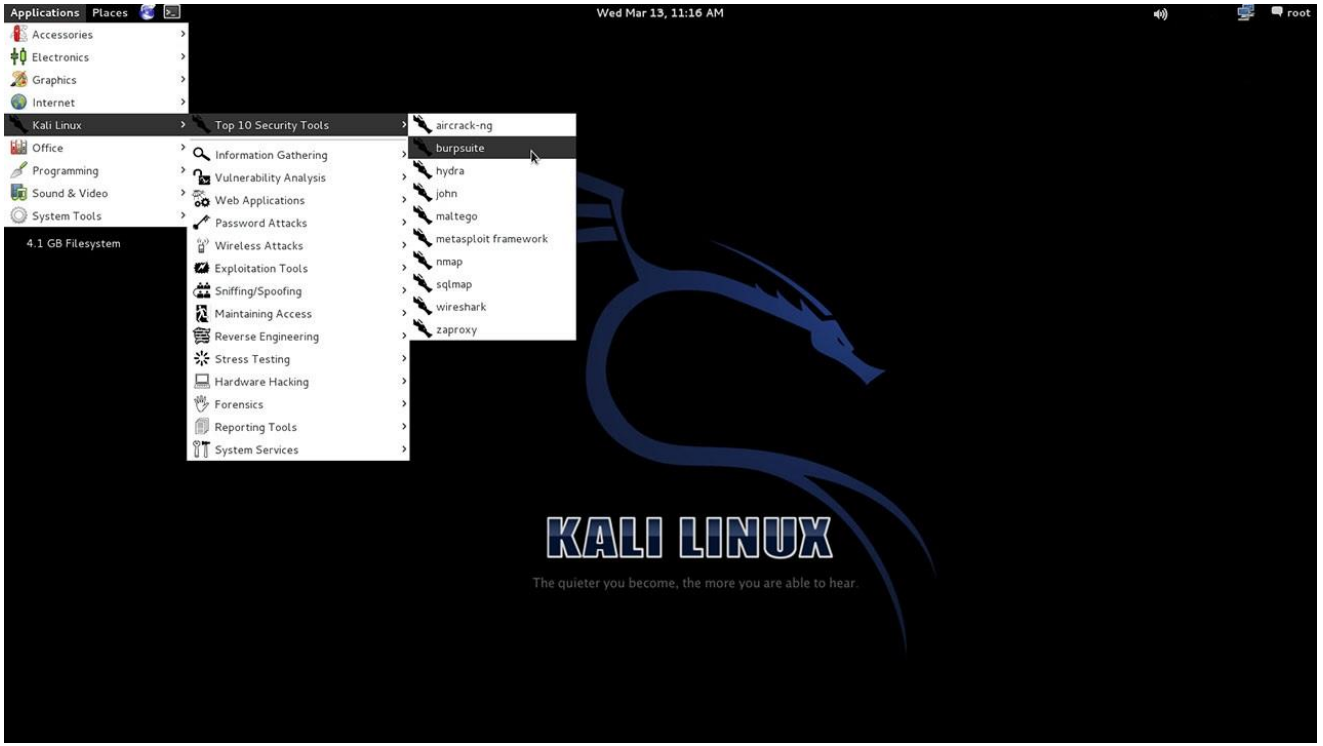
- Information gathering:
  - Dig
  - Fierce
- Network mapping:
  - Nmap

PREPARATION

1. Boot up Kali Linux.
2. Login with the following credentials:
   - Username: root
   - Password: toor

PREPARATION

Kali Linux



PREPARATION

- Ensure that your IP address is correct. Your IP address should be 172.16.184.200.

```
root@kali:~# ifconfig eth0
```

- Ensure that you have connectivity. You can verify this by "pinging" the IP address 172.16.184.5 or 172.16.184.6

```
root@kali:~# ping 172.16.184.5
```

PREPARATION

```
root@kali:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:65:25:9e
          inet addr:172.16.184.200  Bcast:172.16.184.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe65:259e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15989 (15.6 KiB)  TX bytes:2518 (2.4 KiB)
          Interrupt:19 Base address:0x2024

root@kali:~# ping 172.16.184.5
PING 172.16.184.5 (172.16.184.5) 56(84) bytes of data.
64 bytes from 172.16.184.5: icmp_req=1 ttl=64 time=1.05 ms
64 bytes from 172.16.184.5: icmp_req=2 ttl=64 time=0.220 ms
^C
--- 172.16.184.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.220/0.635/1.050/0.415 ms
root@kali:~# ping 172.16.184.6
PING 172.16.184.6 (172.16.184.6) 56(84) bytes of data.
64 bytes from 172.16.184.6: icmp_req=1 ttl=64 time=0.367 ms
^C
--- 172.16.184.6 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.367/0.367/0.367/0.000 ms
root@kali:~#
```

CASE SCENARIO

- The client, Voxhowz Corporation, has requested for an external black box penetration test and has provided us with the following details:
  - Identify potential threats and vulnerabilities.
  - Assess the impact of successful exploitation of vulnerabilities.
  - Testing is restricted to only the "voxhowz.com" domain and subdomains.
  - Denial of Service (DoS) is prohibited.
  - The time frame of testing is between 6pm – 9am on weekdays.
  - Any escalation or alerts should be sent to john@voxhowz.com (555-313-37).

PHASE 1: INFO GATHERING

- By querying DNS records, we can obtain the subdomains that belongs to Voxhowz Corp.
- To query the DNS records, we can use the dig tool:

```
root@kali:~# dig A voxhowz.com
root@kali:~# dig A www.voxhowz.com
```

PHASE 1: INFO GATHERING

DNS query results

```
root@kali:~# dig A voxhowz.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> A voxhowz.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17787
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;voxhowz.com.                   IN      A

;; ANSWER SECTION:
voxhowz.com.            0       IN      A       172.16.184.7

;; Query time: 4 msec
;; SERVER: 172.16.184.6#53(172.16.184.6)
;; WHEN: Thu May 23 06:00:49 2013
;; MSG SIZE  rcvd: 45
```

```
root@kali:~# dig A www.voxhowz.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> A www.voxhowz.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6180
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.voxhowz.com.               IN      A

;; ANSWER SECTION:
www.voxhowz.com.        0       IN      A       172.16.184.7

;; Query time: 0 msec
;; SERVER: 172.16.184.6#53(172.16.184.6)
;; WHEN: Thu May 23 06:00:55 2013
;; MSG SIZE  rcvd: 49
```

PHASE 1: INFO GATHERING

- There are other tools that are available which could be used to enumerate subdomains.
- One of the tools is Fierce:

```
root@kali:~# fierce -dns voxhowz.com -tcptimeout 1 -threads 100 -wordlist
/usr/share/fierce/hosts.txt
```

PHASE 1: INFO GATHERING

- Fierce options:
  - -dns: The target domain.
  - -tcptimeout: The time out (seconds) for each query.
  - -threads: The number of connections to use.
  - -wordlist: Wordlist to use when brute forcing.
- For more options, you can view the Fierce manual:

```
root@kali:~# fierce -h
```

PHASE 1: INFO GATHERING

Voxhowz Corporation subdomains:

1.
2.
3.
4.
5.
6.
7.
8.

PHASE 1: INFO GATHERING

Voxhowz Corporation subdomains: (Answer)

```
root@kali:~# fierce -dns voxhowz.com -tcptimeout 1 -threads 100 -wordlist /usr/share/fierce/hosts.txt

Trying zone transfer first...

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
172.16.184.6    ns1.voxhowz.com
172.16.184.7    voxhowz.com
172.16.184.8    mail.voxhowz.com
172.16.184.9    ftp.voxhowz.com
172.16.184.10   intranet.voxhowz.com
172.16.184.11   melissa.voxhowz.com
172.16.184.12   svn.voxhowz.com
127.0.0.1       localhost.voxhowz.com
172.16.184.7    www.voxhowz.com
```

PHASE 2: NETWORK MAPPING

- In this phase, we will need to identify the following information:
  - Online hosts.
  - TCP & UDP ports.
  - The Operating System of each host.
  - The services available on each host.
- For this, we will use NMAP.

PHASE 2: NETWORK MAPPING

- Preparing hosts.txt:

```
root@kali:~# mkdir -p ~/voxhowz/nmap/output
root@kali:~# cd ~/voxhowz/nmap
root@kali:~# nano hosts.txt
```

- Add dig/fierce findings into hosts.txt

```
172.16.184.6
172.16.184.7
172.16.184.8
172.16.184.9
172.16.184.10
172.16.184.11
172.16.184.12
```

PHASE 2: NETWORK MAPPING

- We first check for online hosts:

```
root@kali:~# nmap -sP -iL hosts.txt -oG output/voxhowz-ping
```

- Then Extract IP addresses from ping results:

```
root@kali:~# grep "Status: Up" output/voxhowz-ping | awk '{print $2}' >
targets.txt
```

PHASE 2: NETWORK MAPPING

- Nmap options:
  - -sP: Execute a ping scan.
  - -iL: Loads a file containing the targets.
  - -oG: Save the results in grepable output.
- For more options, you can view Nmap's manual:

```
root@kali:~# man nmap
```

PHASE 2: NETWORK MAPPING

Ping scan results

```
root@kali:~/voxhowz/nmap# nmap -sP -iL hosts.txt -oG output/voxhowz-ping

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-23 06:20 EDT
Nmap scan report for ns1.voxhowz.com (172.16.184.6)
Host is up (0.00025s latency).
MAC Address: 00:0C:29:A4:34:EE (VMware)
Nmap scan report for voxhowz.com (172.16.184.7)
Host is up (0.00054s latency).
MAC Address: 00:0C:29:A4:34:EE (VMware)
Nmap scan report for mail.voxhowz.com (172.16.184.8)
Host is up (0.00042s latency).
MAC Address: 00:0C:29:A4:34:EE (VMware)
Nmap scan report for ftp.voxhowz.com (172.16.184.9)
Host is up (0.00065s latency).
MAC Address: 00:0C:29:02:78:44 (VMware)
Nmap done: 7 IP addresses (4 hosts up) scanned in 0.23 seconds
```

PHASE 2: NETWORK MAPPING

Extract IP Address

```
root@kali:~/voxhowz/nmap# grep "Status: Up" output/voxhowz-ping | awk '{print $2}' > targets.txt
root@kali:~/voxhowz/nmap# cat targets.txt
172.16.184.6
172.16.184.7
172.16.184.8
172.16.184.9
```

PHASE 2: NETWORK MAPPING

- Now we need to identify what TCP and UDP ports are open on the servers.

```
root@kali:~# nmap -sV -p- -iL targets.txt -oA output/voxhowz-tcp
root@kali:~# nmap -sU -iL targets.txt -oA output/voxhowz-udp
```

PHASE 2: NETWORK MAPPING

- Nmap options:
  - -sV: Perform a version / service scan.
  - -sU: Perform a UDP scan.
  - -p-: Check all ports (1 - 65535)
  - -iL: Loads a file containing the targets.
  - -oA: Save the results to a file, in all available format.

PHASE 2: NETWORK MAPPING

NMAP Version scan results

```
root@kali:~/voxhowz/nmap# nmap -sV -p- -iL targets.txt -oA output/voxhowz-tcp

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-23 07:53 EDT
Stats: 0:11:32 elapsed; 0 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.78% done; ETC: 08:11 (0:06:16 remaining)
Stats: 0:17:04 elapsed; 0 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.96% done; ETC: 08:12 (0:01:42 remaining)
Nmap scan report for ns1.voxhowz.com (172.16.184.6)
Host is up (0.00028s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.60
MAC Address: 00:0C:29:A4:34:EE (VMware)

Nmap scan report for voxhowz.com (172.16.184.7)
Host is up (0.00025s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((FreeBSD) PHP/5.3.10 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2)
MAC Address: 00:0C:29:A4:34:EE (VMware)

Nmap scan report for mail.voxhowz.com (172.16.184.8)
Host is up (0.00026s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
25/tcp open  smtp?
MAC Address: 00:0C:29:A4:34:EE (VMware)

Nmap scan report for ftp.voxhowz.com (172.16.184.9)
Host is up (0.00041s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      FileZilla ftpd 0.9.41 beta
5800/tcp open  vnc-http RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp open  vnc      VNC (protocol 3.8)
MAC Address: 00:0C:29:02:78:44 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 4 IP addresses (4 hosts up) scanned in 1359.37 seconds
```

PHASE 2: NETWORK MAPPING

NMAP UDP port scan results

```
root@kali:~/voxhowz/nmap# nmap -sU -iL targets.txt -oA output/voxhowz-udp

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-23 06:41 EDT
Nmap scan report for ns1.voxhowz.com (172.16.184.6)
Host is up (0.00029s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
53/udp  open|filtered domain
514/udp open|filtered syslog
MAC Address: 00:0C:29:A4:34:EE (VMware)

Nmap scan report for voxhowz.com (172.16.184.7)
Host is up (0.00024s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
514/udp open|filtered syslog
MAC Address: 00:0C:29:A4:34:EE (VMware)

Nmap scan report for mail.voxhowz.com (172.16.184.8)
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
514/udp open|filtered syslog
MAC Address: 00:0C:29:A4:34:EE (VMware)

Nmap scan report for ftp.voxhowz.com (172.16.184.9)
Host is up (0.00022s latency).
All 1000 scanned ports on ftp.voxhowz.com (172.16.184.9) are open|filtered
MAC Address: 00:0C:29:02:78:44 (VMware)

Nmap done: 4 IP addresses (4 hosts up) scanned in 58.26 seconds
```

PHASE 3: VERIFYING FINDINGS

- Confirm that the ports are actually open.
- Open ports can be checked using a tool called netcat:

```
root@kali:~# ncat -vv 172.16.184.7 80
```

- With netcat we can:
  - Connect to the ports.
  - Send & receive data.
  - Observe response.
- Faster to check if automated with shell-scripting.

PHASE 3: VERIFYING FINDINGS

Verifying open ports

```
root@kali:~/voxhowz/nmap# ncat -vv 172.16.184.7 80
Ncat: Version 6.25 ( http://nmap.org/ncat )
Ncat: Connected to 172.16.184.7:80.
asdasdasdasdas
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR
dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title></title>
<link type="text/css" rel="stylesheet" href="style.css" />
<script src="rollover.js" type="text/javascript"></script>
</head>
<body id="page_1" onload="MM_preloadImages('images/m_1_hov.gif','images/m_2_ho
','images/m_4_hov.gif','images/m_5_hov.gif')">
<div class="bgr">
        <table class="center_1">
        <tr>
          <td class="header">
```

```
root@kali:~/voxhowz/nmap# ncat -vv 172.16.184.7 81
Ncat: Version 6.25 ( http://nmap.org/ncat )
Ncat: Connection refused.
```

REVIEW

- Subdomains can be enumerated using freely available tools like dig and Fierce.
- Zone transfers can provide a huge amount of valuable information on subdomains.
- In the network mapping phase, always look for the following:
  - Open TCP & UDP ports.
  - The services listening on the ports.
  - The operating system of the targets.
- Always verify the accuracy of the information.