1.HOST DISCOVERY

Footprinting is the first and important phase were one gather information about their target system.

DNS footprinting helps to enumerate DNS records like (A, MX, NS, SRV, PTR, SOA, CNAME) resolving to the target domain.

- **A** – A record is used to point the domain name such as gbhackers.com to the IP address of it’s hosting server.
- **MX** – Records responsible for Email exchange.
- **NS** – NS records are to identify DNS servers responsible for the domain.
- **SRV –** Records to distinguish the service hosted on specific servers.
- **PTR** – Reverse DNS lookup, with the help of IP you can get domain’s associated with it.
- **SOA** – Start of record, it is nothing but the information in the DNS system about DNS Zone and other DNS records.
- **CNAME** – Cname record maps a domain name to another domain name.

We can detect live hosts, accessible hosts in the target network by using network scanning tools such as **Advanced IP scanner, NMAP, HPING3, NESSUS.**

Ping&Ping Sweep:

```
root@kali:~# nmap -sn 192.168.169.128
root@kali:~# nmap -sn 192.168.169.128-20 To ScanRange of IP
root@kali:~# nmap -sn 192.168.169.* Wildcard
root@kali:~# nmap -sn 192.168.169.128/24 Entire Subnet
```

Whois Information

To obtain Whois information and name server of a webiste

```
root@kali:~# whois testdomain.com
```

1. http://whois.domaintools.com/
2. https://whois.icann.org/en

Traceroute

Network Diagonastic tool that displays route path and transit delay in packets

```
root@kali:~# traceroute google.com
```

Online Tools

1. http://www.monitis.com/traceroute/
2. http://ping.eu/traceroute/

2.PORT SCANNING

Perform port scanning using tools such as **Nmap, Hping3, Netscan tools, Network monitor**. These tools help us to probe a server or host on the target network for open ports.

Open ports are the gateway for attackers to enter in and to install malicious backdoor applications.

```
root@kali:~# nmap –open gbhackers.com            To find all open ports
root@kali:~# nmap -p 80 192.168.169.128          Specific Port
root@kali:~# nmap -p 80-200 192.168.169.128   Range of ports
root@kali:~# nmap -p “*” 192.168.169.128         To scan all ports
```

Online Tools

1. http://www.yougetsignal.com/
2. https://pentest-tools.com/information-gathering/find-subdomains-of-domain

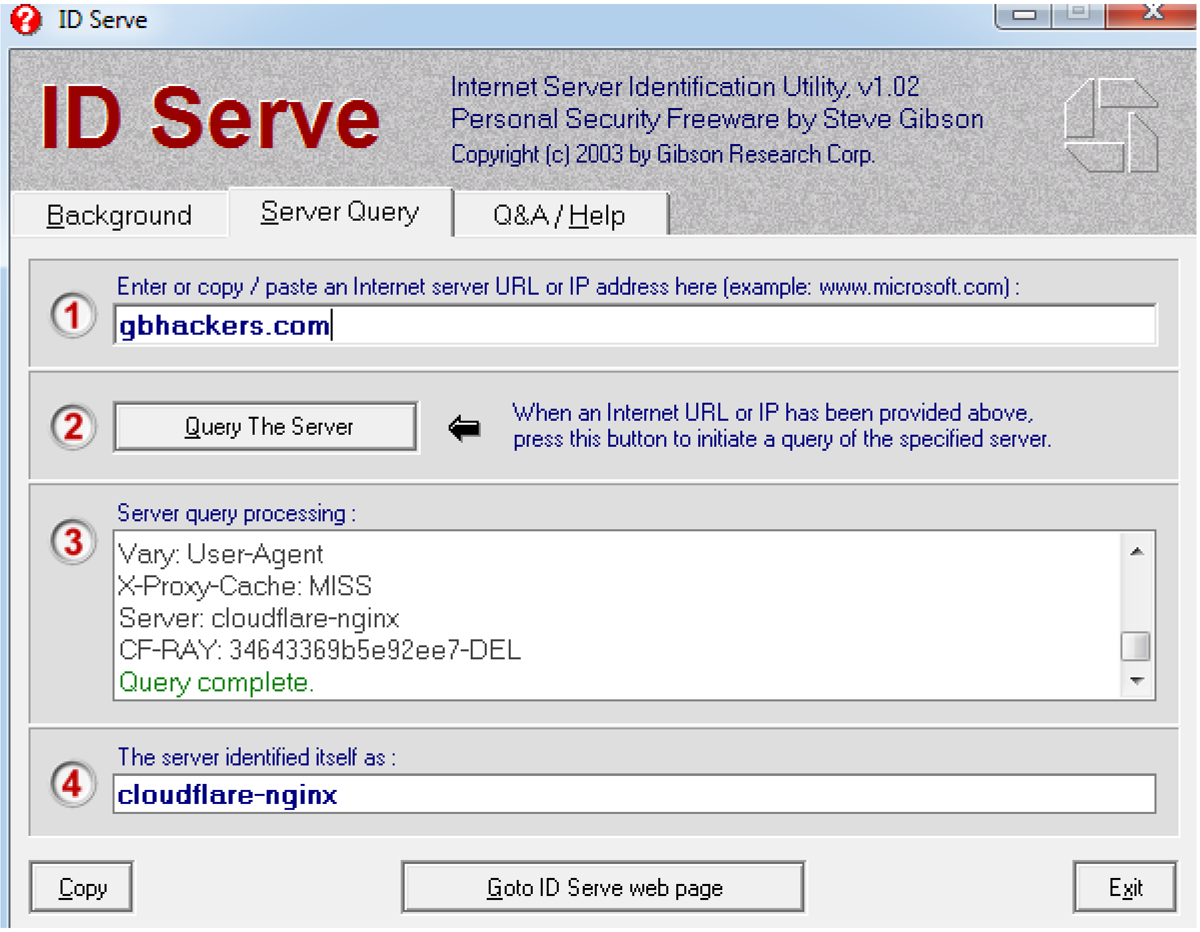
3.Banner Grabbing/OS Fingerprinting

Perform banner Grabbing/OS fingerprinting such as **Telnet, IDServe, NMAP** determines the operating system of the target host and the operating system.

Once you know the **version** and **operating system** of the target, we need to find the **vulnerabilities** and exploit.Try to gain control over the system.

```
root@kali:~# nmap -A 192.168.169.128
root@kali:~# nmap -v -A 192.168.169.128 with high verbosity level
```

IDserve another good tool for Banner Grabbing.


ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
Copy
Goto ID Serve web page
Exit

1 Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) : gbhackers.com

3 Server query processing :

```
Vary: User-Agent
X-Proxy-Cache: MISS
Server: cloudflare-nginx
CF-RAY: 34643369b5e92ee7-DEL
Query complete.
```

4 The server identified itself as : cloudflare-nginx

Online Tools

1. https://www.netcraft.com/
2. https://w3dt.net/tools/httprecon
3. https://www.shodan.io/

4.Scan for Vulnerabilities

Scan the network using **Vulnerabilities** using GIFLanguard, Nessus, Ratina CS, SAINT.

These tools help us in finding vulnerabilities with the target system and operating systems.With this steps, you can find loopholes in the target network system.

GFILanguard

It acts as a security consultant and offers patch Management, Vulnerability assessment, and network auditing services.

Nessus

Nessus a vulnerability scanner tool that searches bug in the software and finds a specific way to violate the security of a software product.

- Data gathering.
- Host identification.
- Port scan.
- Plug-in selection.
- Reporting of data.

5.Draw Network Diagrams

Draw a network diagram about the organization that helps you to understand logical connection path to the target host in the network.

The network diagram can be drawn by **LANmanager, LANstate, Friendly pinger, Network view**.

6.Prepare Proxies

Proxies act as an intermediary between two networking devices. A proxy can protect the local network from outside access.

With proxy servers, we can anonymize web browsing and filter unwanted contents such as ads and many other.

Proxies such as **Proxifier, SSL Proxy, Proxy Finder**..etc, to hide yourself from being caught.

6.Document all Findings

The last and the very important step is to document all the Findings from **Penetration testing**.

This document will help you in finding potential vulnerabilities in your network. Once you determine the Vulnerabilities you can plan **counteractions** accordingly.

You can download rules and scope Worksheet here – **Rules and Scope sheet**

Thus, penetration testing helps in assessing your network before it gets into real trouble that may cause severe loss in terms of value and finance.

Important Tools used for Network Pentesting

Frameworks

Kali Linux, Backtrack5 R3, Security Onion

Reconnaisance

Smartwhois, MxToolbox, CentralOps, dnsstuff, nslookup, DIG, netcraft

Discovery

Angry IP scanner, Colasoft ping tool, nmap, Maltego, NetResident,LanSurveyor, OpManager

Port Scanning

Nmap, Megaping, Hping3, Netscan tools pro, Advanced port scannerService Fingerprinting Xprobe, nmap, zenmap

Enumeration

Superscan, Netbios enumerator, Snmpcheck, onesixtyone, Jxplorer, Hyena,DumpSec, WinFingerprint, Ps Tools, NsAuditor, Enum4Linux, nslookup, Netscan

Scanning

Nessus, GFI Languard, Retina,SAINT, Nexpose

Password Cracking

Ncrack, Cain & Abel, LC5, Ophcrack, pwdump7, fgdump, John The Ripper,Rainbow Crack

Sniffing

Wireshark, Ettercap, Capsa Network Analyzer

MiTM Attacks

Cain & Abel, Ettercap

Exploitation

Metasploit, Core Impact
These are the Most important checklist you should concentrate with Network penetration Testing

Some Nmap Commands - Port scan

- Nmap full SYN scan with verbose mode and service detection and disabling ping scan. Export normal and greppable output for future use.

```
nmap -Pn -p- -sV X.X.X.X -v -sS -oG nmap_grepable_SYN -oN nmap_normal_SYN
```

- Nmap top 1000 UDP scan with verbose mode and service detection and disabling ping scan. Export normal and greppable output for future use.

```
nmap -Pn -top-ports=1000 -sV X.X.X.X -v -sS -oG nmap_grepable_UDP -
oN     nmap_normal_UDP
```

- Nmap Full port scan identifying any weak algos and ciphers in SSH and SSL. Export normal and greppable output for future use.

```
nmap -Pn -A -T4 -vv --script ssh2-enum-algos --script ssl-enum-ciphers
<Target List>
```

Audit SSL (Use testssl.sh or TestSSLMaster.exe for SSL related vulnerability mentioned here for quicker results)

- Use openssl, sslyze tools to find below issues within SSL.
- Self-signed certificate
- SSL version 2 and 3 detection
- Weak hashing algorithm
- Use of RC4 and CBC ciphers
- Logjam issue
- Sweet32 issue
- Certificate expiry
- Openssl ChangeCipherSec issue
- POODLE vulnerability
- Openssl heartbleed issue
- Lucky 13 and Beast Issue

Check for default passwords in server/device/service documentation

Lets say during your port scan or VA you found some services running on the server for example: cisco, brocade fabric OS, sonic firewall, apache tomcat manager. Then for these services Google what are the default configuration administrative username and password. Try those in your login and check your luck.

Hunting some common ports

1. DNS (53) UDP-

-Examine domain name system (DNS) using dnsenum, nslookup, dig and fierce tool

-Check for zone transfer

-Bruteforce subdomain using fierce tool

-Run all nmap scripts using following command: nmap -Pn -sU -p53 --script dns* -v

-Banner grabbing and finding publicly known exploits

-Check for DNS amplification attack

2. SMTP (25) TCP -

-Check for SMTP open relay

-Check for email spoofing

-Check for username enumeration using VRFY command

-Banner grabbing and finding publicly known exploits

-Send modified cryptors and check if SMTP gateway is enable to detect and block it?

-Run all nmap script using following command: nmap -Pn -sS -p25 --script smtp* -

3. SNMP (161) UDP -

-Check for default community strings 'public' & 'private' using snmpwalk and snmpenum.pl script.

-Banner grabbing and finding publicly known exploits

-Perform MIG enumeration.

- .1.3.6.1.2.1.1.5 Hostnames

- .1.3.6.1.4.1.77.1.4.2 Domain Name

- .1.3.6.1.4.1.77.1.2.25 Usernames

- .1.3.6.1.4.1.77.1.2.3.1.1 Running Services

- .1.3.6.1.4.1.77.1.2.27 Share Information

4. SSH (22) TCP-

-Banner grabbing and finding publicly known exploits

-Check if that supports sshv1 or not.

-Bruteforce password using hydra and medusa

-Check if it supports weak CBC ciphers and hmac algorithms using ssh2-enum-algos.nse nmap script.

-Run all nmap scripts using following command: nmap -Pn -sS -p22 --script ssh* -v

5. Cisco VPN (500) UDP-

-Check for aggressive and main mode enable using ikescan tool.

-Enumeration using ikeprobe tool

-Check for VPN group and try to crack PSK in order to get credentials to login into the VPN service through web panel.

6. SMB (445,137,139) TCP-

-Check SAMBA service using metasploit use auxiliary/scanner/smb/smb_version

-Get reverse shell using meterpreter reverse tcp module.

-Check for SMB related vulnerability using ‘smb-check-vulns’ nmap script.

-Reference: https://myexploit.wordpress.com/control-smb-445-137-139/

7. FTP (21) TCP-

-Run all nmap script using following command: nmap -Pn -sS -p21 --script ftp* -v

-Check for cleartext password submission for ftp login

- Check for anonymous access using username and password as anonymous:anonymous

- Banner grabbing and finding publicly known exploits

- Bruteforce FTP password using hydra and medusa

8. Telnet (23) TCP-

-Banner grabbing and finding publicly known exploits

-Bruteforce telnet password

-Run following nmap scripts

- telnet-brute.nse
- telnet-encryption.nse
- telnet-ntlm-info.nse

9. NTP (123) UDP-

-Perform NTP enumeration using below commands:

- ntpdc -c monlist IP_ADDRESS
- ntpdc -c sysinfo IP_ADDRESS

-Run all nmap scripts using nmap -Pn -sS -p21 --script ntp* -v

10. SQL Server (1433,1434, 3306) TCP-

-Banner grabbing and finding publicly known exploits

-Bruteforce and perform other operation using following tools:

- Piggy
- SQLping
- SQLpoke
- SQLrecon
- SQLver

-Run following nmap scripts:

- ms-sql-brute.nse
- ms-sql-config.nse

- ms-sql-dac.nse
- ms-sql-dump-hashes.nse
- ms-sql-empty-password.nse
- ms-sql-hasdbaccess.nse
- ms-sql-info.nse
- ms-sql-ntlm-info.nse
- ms-sql-query.nse
- ms-sql-tables.nse
- ms-sql-xp-cmdshell.nse
- pgsql-brute.nse

-For MYSQL default username is root and password is

11. RDP (3389) TCP-

-Perform enumeration via connecting and checking login screen. Gather all active user’s name and domain/group name.

-Perform RDP cryptography check using RDP-sec-check.pl script.

-Run following nmap script:

- rdp-enum-encryption.nse
- rdp-vuln-ms12-020.nse

12. Oracle (1521) TCP

-Enumeration using following tools

- Tnsver [host] [port]
- Tnscmd

o perl tnscmd.pl -h ip_address

o perl tnscmd.pl version -h ip_address

o perl tnscmd.pl status -h ip_address

-Enumeration & Bruteforce using below nmap scripts:

· oracle-brute.nse

· oracle-brute-stealth.nse

· oracle-enum-users.nse

· oracle-sid-brute.nse

· oracle-tns-version.nse

USEFUL LINKS FOR TOOLS:

1. Nessus : https://www.tenable.com/products/nessus
2. testssl.sh : https://github.com/drwetter/testssl.sh
3. testsslserver.exe : https://www.bolet.org/TestSSLServer/
4. Nikto : https://cirt.net/Nikto2
5. Nmap : https://nmap.org/
6. Yasca : https://github.com/scovetta/yasca
7. John The Ripper : https://www.openwall.com/john/
8. masscan : https://github.com/robertdavidgraham/masscan
9. DNSdumpster : https://dnsdumpster.com/

THANK YOU