Reconnaissance Enumeration Methodology🛠️

Pre engagement

- □ Log all commands of the current session

```
script engagement_x.log
...
exit # when the session has finished
```

- □ Set the target IP to the $IP variable

```
export $IP=x.x.x.x
```

General methodology

- □ add host to your /etc/hosts if you already know its name or if you found it
- □ For every open port TCP/UDP
    - □ Find service and version
    - □ Find known service bugs
    - □ Find configuration issues
    - □ Run nmap port scan / banner grabbing
- □ Google-Fu
    - □ Every error message
    - □ Every URL path
    - □ Every paramenter to find versions/apps/bugs
- □ searchsploit every serivce
- □ Google
    - □ Every version exploit db
    - □ Every version vulnerability
- □ If app has auth
    - □ User enumeration
    - □ Password bruteforce
    - □ Default credentials (Google them)
- □ revert the machine
- □ Defcon 5 try:

```
nmap --script exploit -Pn $IP
```

Grab the damn banner!

- □ nc -v $IP <PORT>
- □ telnet $IP <PORT>

Network & Port scanning

If you don't know the alive hosts, you can scan the full subnet to find them, so you can do a deeper scan on them later.

Go big

- □ List scan with nmap

```
nmap -sL -oN nmap/listScan 10.x.x.x.x
```

- □ Ping scan (run it with privileges)

```
nmap -sn -oN nmap/pingScan 10.x.x.x.x
```

- □ Look for hosts's info (name, logged-in user, MAC) with NetBIOS queries

```
nbtscan -r 10.x.x.x.x
```

- □ Use ARP to do hosts discovery

```
netdiscover -r 10.x.x.x/24
```

- □ smbtree

Go small (Individual host scanning)

- □ Run a simple TCP port scan to uncover open ports

```
nmap -p- -T4 -oA nmap/ezTCPScan $IP
```

- □ Run a simple UDP port scan to uncover open ports

```
nmap -sU -n -p- -T4 -oA nmap/ezUDPScan $IP
```

- □ If lazy do an Aggressive scan on open ports (A = O+sC+sV)

```
nmap -A -T4 -px,y,z -v -oA nmap/aggressiveScan $IP
```

- □ Do a version detection on TCP ports

  ```
  nmap -sV --reason -O -p- $IP
  ```

- □ Do a version detection on UDP ports

  ```
  nmap -sU -sV -n $IP
  ```

- □ nmap -sV -v -n --script vuln $IP
- □ nmap --script ssl-heartbleed $IP
- □ Version/OS detection using other DNS servers

  ```
  nmap -v --dns-server <DNS> -sV --reason -O --open -Pn $IP
  ```

- □ Try identify unknown services

  ```
  amap -d $IP <PORT>
  ```

- □ Full vulnerability scanning with vulnscan.nse

  ```
  nmap -sS -sV --script=/path/to/your/vulnscan.nse -oN nmap/vulnScan $IP
  ```

Service enumeration

FTP - TCP Port 21

- □ Banner grabbing
- □ Check for common exploits
- □ Run command ftp $IP
- □ Check for anonymous access
- □ Any known vulnerabilty?

  ```
  nmap –script ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221,tftp-enum -p 21 $IP
  ```

- □ Default credentials check

```
hydra -s <PORT> -C usr/share/wordlists/ftp-default-userpass.txt -u -f $IP ft
```

SSH (22)

```
> ssh <TARGET> 22
```

SMTP - TCP Port 25

- □ nmap –script smtp-commands,smtp-enum-users,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 -p 25 $IP
- □ nc -nvv $IP
- □ manual testing with **telnet** and VRFY / EXPN

Finger (79)

Download script and run it with a wordlist: http://pentestmonkey.net/tools/user-enumeration/finger-user-enum

Web App (80/443)

- □ Investigate SSL/TLS cert details for further information
- □ Investigate robots.txt
- □ View source code
- □ Nikto
- □ Directory Traversal Fuzzer
    - □ Gobuster (**Doesn't work recursively!!!**)
        - □ File and directory fuzzing
        - □ Vhost bruteforcing
        - □ use -x to look for specific extensions (.txt, .php, .bak, .cfg, .json, .md, .git)
        - □ nothing? Ensure that you scan the correct protocol (HTTP/HTTPS) and directory
        - □ gobuster -w /usr/share/seclists/Discovery/Web-Content/common.txt -s '200,204,301,302,307,403,500' -t 50 -e -u $IP
        - □ gobuster -w /usr/share/seclists/Discovery/Web-Content/CGIs.txt -s '200,204,403,500' -e -t 50 -u $IP/cgi-bin
        - □ Re-run for each directory found
    - □ wfuzz
    - □ dotdotpwn
- □ Which CMS is running?
    - □ whatweb
    - □ wpscan

    - □ joomscan
    - □ drupwn
    - □ use nmap to enumerates installed Drupal themes/modules

      ```
      nmap -p 80 --script http-drupal-enum <\TARGET>
      ```

- □ WebDAV:
    - □ davtest
    - □ cadevar
    - □ Use nmap to detect WebDAV installations & listings:

      ```
      nmap --script http-webdav-scan -p80,8080 $IP
      ```

- □ LFI / RFI test
- □ cgi-bin found? try shellshock https://www.exploit-db.com/exploits/34900
- □ Check every input field for SQLi
  - [ ] Cheatsheet 1 https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/MySQL%20Injection.md
  - [ ] Cheatsheet 2 https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/MySQL%20Injection.md
  - [ ] Cheatsheet 3 https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/
- □ Check for code injection: Owasp code injection

DNS (Port 53)

- □ Resolve DNS

  ```
  host website.com
  nslookup website.com
  ```

- □ whois
- □ Is DNS zone transfer possible?

  ```
  host -l domain.name dns.server
  dig axfr @dns-server domain.name
  ```

- □ dnsrecon -d $IP -D /usr/share/wordlists/dnsmap.txt -t std --xml ouput.xml

POP (Port 110)

- ☑ ~~Is username enumeration possible?~~
- ☑ ~~Try nmap -script pop3-brute $IP -p 110 -v~~
- ☑ ~~telnet $IP 110~~
    - ~~LIST – once logged in list messages~~
    - ~~RETR <MSG NUMBER> – retrieve message~~
    - ~~QUIT~~

RPCBind (111)

- □ rpcinfo -p $IP

SMB/RPC (Port 139/445)

- □ nmap -script smb-protocols
- □ nmap -n -p 139,445 -v --script smb-vuln* -oA nmap/smb-vulns $IP
- □ nmap -script smb-os-discovery.nse –script-args=unsafe=1 -p445 $IP
- □ nmap -script smb-check-vulns.nse –script-args=unsafe=1 -p445 $IP
- □ nmap -script smb-enum-shares.nse –script-args=unsafe=1 -p445 $IP
- □ nmap -script smb-enum-users.nse –script-args=unsafe=1 -p445 $IP
- □ nbtscan
- □ enum4linux
- □ Manual browsing (Prefer it whenever possible):

```
smbclient -L INSERTIPADDRESS
smbclient //INSERTIPADDRESS/tmp
smbclient \\INSERTIPADDRESS\ipc$ -U john
smbclient //INSERTIPADDRESS/ipc$ -U john
smbclient //INSERTIPADDRESS/admin$ -U john
winexe -U username //INSERTIPADDRESS "cmd.exe" --system
```

SNMP (161)

- □ snmpwalk -c public -v1 $IP
- □ snmpcheck -t $IP -c public
- □ onesixtyone -c names -i hosts
- □ nmap -sT -p 161 -v -oA nmap/snmap_results $IP
- □ snmpenum -t $IP

MSSQL

- □ Password bruteforcing

```
hydra -l <USERNAME> -P
/usr/share/seclists/Passwords/darkweb2017-top10000.txt $IP -s
```

```
<PORT> -t 5 mssql
hydra -s <PORT> -C ./wordlists/mssql-default-userpass.txt -u -f $IP mssql
medusa -h $IP -M mssql -u sa -P /usr/share/seclists/Passwords/darkweb2017-top1000.txt -e ns -F -t 5
```

- □ Any known vulnerability?

```
nmap -vv -sV -Pn -p <PORT> --script=ms-sql-info,ms-sql-config,ms-sql-dump-hashes --script-args=mssql.instance-port=%s,smsql.username-sa,mssql.password-sa $IP
```

Oracle (1521)

- □ Default credentials

```
hydra -s [PORT] -C ./wordlists/oracle-default-userpass.txt -u -f $IP
```

- □ tnscmd10g version -h $IP
- □ tnscmd10g status -h $IP
- □ **oracle-version** - MSF module which scans Oracle DB to find the version

```
msfcli auxiliary/scanner/oracle/tnslsnr_version rhosts=$IP E
```

- □ **oracle-sid** - MSF module to enumerate the Oracle DB SID

```
msfcli auxiliary/scanner/oracle/sid_enum rhosts=$IP E
```

MySQL (3306)

- □ Default credentials?

```
hydra -s <PORT> -C usr/share/wordlists/mysql-default-userpass.txt -u -f $IP mysql
```

- □ Any known vulnerability?

```
nmap -sV -Pn -vv -p 3306 --script mysql-audit,mysql-databases,mysql-dump-hashes,mysql-empty-password,mysql-enum,mysql-info,mysql-query,mysql-users,mysql-variables,mysql-vuln-cve2012-2122 $IP
```

RDP (3389)

- □ Use rpd-sec-check to enumerate security settings:

  ```
  perl ./scripts/rdp-sec-check.pl $IP:<ORT>
  ```

- □ Use ncrack to brute force RDP:

  ```
  ncrack -vv --user administrator -P /user/share/wordlists/rockyou.txt rdp://<\TARGET>
  ```

LDAP (389)

- □ LDAPSearch can be utilized to locate and retrieve directory entries

  ```
  ldapsearch -h [IP] -p [PORT] -x -s base
  ```

Image File Investigation

- □ Always use wget for downloading files to keep original timestamps and file information
- □ Use binwalk and strings to check image files for hidden content
- □ steghide

NFS Share

- □ Show NFS shares

  ```
  showmount -e $IP <PORT>
  ```

Linux/Windows

- □ smbclient -L //$IP
- □ rpcinfo
- □ enum4linux

Packet inspection

- □ Wireshark
- □ tcpdump tcp port <PORT> -w output.pcap -i <INTERFACE>

Anything else

- □ nmap scripts (locate *nse* | grep servicename)

- □ hydra
- □ MSF auxiliary modules
- □ Download the software and investigate it locally
- □ Try enumeration scripts for specific services