Scanning & Enumeration

Installing Kioptrix

Kioptrix - VulnHub

Lots of vulnerable boxes to practice on, some are old and may not work out of the box.

tcm Google drive

Scanning with Nmap

Default Nmap parameters for pentesting

TCP scanning

Scan all ports with -p-, slows down scanning
Use -A to scan everything, slows down scanning especially with all ports
Use -T4 for agression level, lower if risk of detection

UDP scanning

Scan top 1000 ports, UDP scans take forever
Use -T4 for agression level, lower if risk of detection

Work on other things while scanning, OSINT, walking the application, etc.

Enumerating HTTP and HTTPS

Investigating HTTP/S ports

• Navigate to the site, walk it with Burp suite
• Run web app scanners like nikto
• Enumerate directories with dirbuster, gobuster, etc
• View the page source code

Look out for:

• Default webpage is an automatic finding, directory structure, OS running
• Hostname
• Headers disclosing information on running services/languages
• Directories/files found in enumeration leading to attack vectors
• Potential vulnerabilities

Enumerating SMB

smbclient

Use smbclient to enumerate the file shares and connect to them

```
# List the shares
smbclient -L \\\\<TARTGET-IP>\\

# Connect to a share
smbclient \\\\<TARTGET-IP>\\<SHARE-NAME>
```

Use smbget to download the contents of shares that you have access to

Enumerating SSH

ssh

Use ssh to enumerate the target

If no matching key exchange method is found use the -oKexAlgorithms tag to add valid exchange methods

```
# Simple connection
ssh <TARGET-IP>

# Add key exchange methods
ssh <TARGET-IP> -oKexAlgorithms=+<KEY-EXCHANGE-METHOD>

# Add host key types
ssh <TARGET-IP> -oHostKeyAlgorithms=+<KEY-TYPE>

# Add cipher
ssh <TARGET-IP> -c <CIPHER>
```

telnet

Use telnet to grab the ssh banner

```
telnet <TARGET-
IP> <SSH-PORT>
```

Researching Potential Vulnerabilities

Vulnerabilities

Use Google to find vulnerabilities for the service versions found in the Enumeration phase

CVE details are sometimes relevant, look at the score for red
exploit-db have exploits, not always upto date
Rapid7 will give Metasploit examples

searchsploit

Use searchsploit to find vulnerabilities