

Controle

■ Date de création	@12 juin 2025 09:28
■ Matière	Hack

Cobalt Strike

chmod +x teamserver

chmod +x setup.sh

setup.sh + adresse ip de ma carte 'mot de passe' (genre toto)

./teamserver

GUI → ça ouvre, faut mettre ip et MDP

CONTROLE :

Cas Linux ou cas Windows (dans les deux cas y'aura du MetaSploit(pas tout l'exo) et avec nmap très fortement)

(cas pratique) il faudra compromettre une machine et faire un rapport sérieux et carré

systeme de notation qui se base plutot sur le rapport que sur l'exploit

Sur une machine Kali (où il faut techniquement rien rajouter)

metasploit

sessions -u 1 dans le controle si on a une sessions background via exploit -j et ça ouvre le meterpreter

sessions -k 1 kill la sessions 1

on fait sysinfo into arp

TP 7-8 dans le controle

AD 2016 → Zerologon

une fois qu'on a le hash/mdp de l'AD :

python3 /usr/share/doc/python3-impacket/examples/psexec.py

ad2016.hacklab.local/administrateur:'P@ssw0rd1!'@10.10.1.30 -codec

iso8859_2

connaître les scans SMB !!!! (smbmap, enum4linux..) et garder le script sous la main. (sur le drive

et après si on trouve des vulnés (ya aussi sploitus / exploit db):

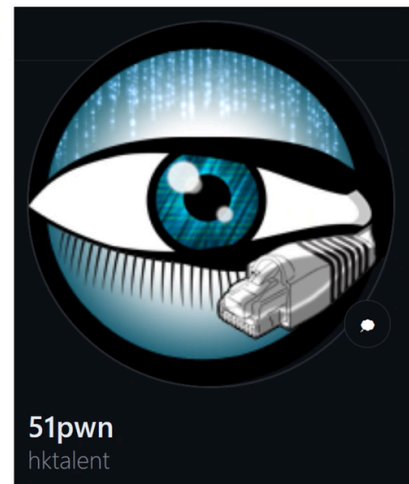
```
(root@kali)-[/home/stage]
# sudo crackmapexec smb 10.10.1.30
SMB 10.10.1.30 445 WIN-SR7ROUJ7JK [*] Windows Server 2016 Datacenter 14393 x64 (name:WIN-SR7ROUJ7JK) (do
main:ad2016.hacklab.local) (signing:True) (SMBv1:True)
```

Bonus

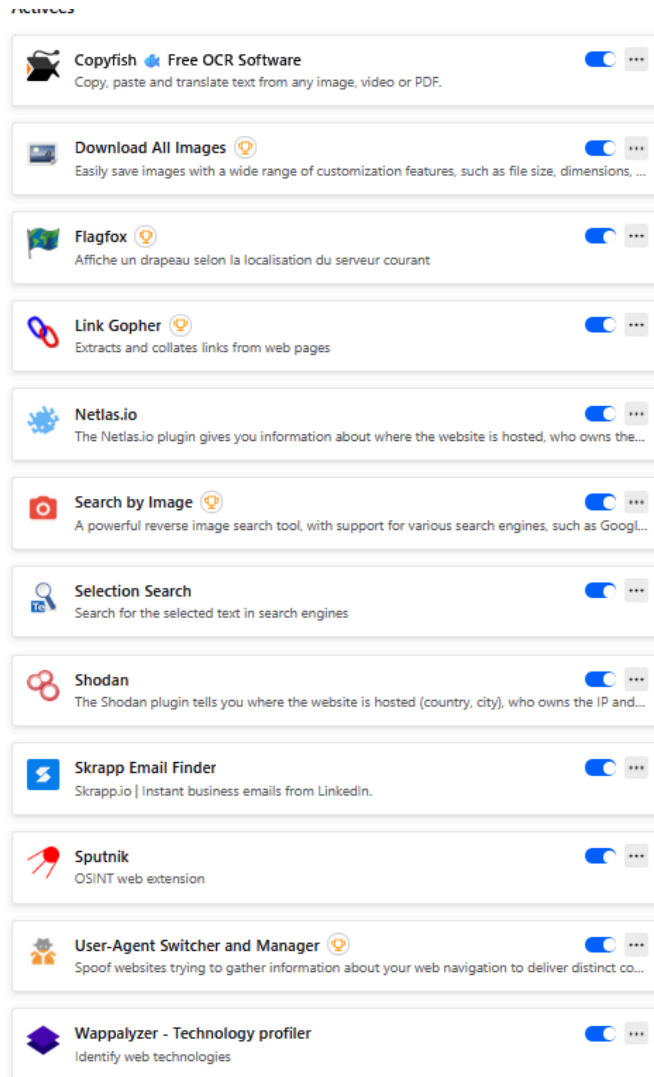
<https://github.com/GhostTroops/scan4all>

```
PORT      STATE SERVICE
2222/tcp  open  EtherNet/IP-1
3306/tcp  open  mysql
5000/tcp  open  unpp
7000/tcp  open  afs3-filer
7001/tcp  open  afs3-callbck
8081/tcp  open  blackice-icecap
9200/tcp  open  wap-wsp

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
[!] Port scan over web scan starting
(hydra)->开始对127.0.0.1:3306(mysql)进行暴力破解, 字典长度为: 57[2022-06-25 17:45:01] [CWE-2018-2893] [network] [critical] 127.0.0.1:3306
[2022-06-25 17:45:05] [weblogic-t3-detect] [network] [info] 127.0.0.1:7001 [10.3.6.0]
[2022-06-25 17:45:05] [weblogic-iiop-detect] [network] [info] 127.0.0.1:7001
[2022-06-25 17:45:05] [Elastic (Database), elasticsearch] [80]
[2022-06-25 17:45:05] [403] [1]
[GoPoc] Found vuln Weblogic CVE_2014_4210|http://127.0.0.1:7001
[GoPoc] Found vuln Weblogic CVE_2017_3506|http://127.0.0.1:7001
[GoPoc] Found vuln Weblogic CVE_2017_10271|http://127.0.0.1:7001
[2022-06-25 17:45:05] [403] [1]
[GoPoc] Found vuln Weblogic CVE_2019_2725|http://127.0.0.1:7001
[GoPoc] Found vuln Weblogic CVE_2019_2729|http://127.0.0.1:7001
[GoPoc] Found vuln Weblogic CVE_2020_2883|http://127.0.0.1:7001
[GoPoc] Found vuln Weblogic CVE_2020_14882|http://127.0.0.1:7001
[GoPoc] Found vuln Weblogic CVE_2021_2109|http://127.0.0.1:7001
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
[2022-06-25 17:45:22] [exposed-redis] [network] [high] 127.0.0.1:6379
```



- **searchsploit -t apache 2.1**
- **searchsploit -x -nmap nomduscan.xml**
- **xsftproc /home/user/nmap/scan.xml -o /home/user/nmap/scan.html**



Ya un truc a mettre sur le Drive et si on l'a, on pete l'examen en 3h et on a 4h pour l'examen total. A partir de 2h / 2h30 il faut commencer le rapport

et pour ça il faut des screenshots, commandes copiées collées, une trame préparée et 1h pour écrire tout ça MINIMUM

dans la grille finale, avoir tout cassé c'est pas si bien noté que ça, ce qui rapporte le plus c'est la qualité du rapport, sa clarté

Faut faire un arbre d'attaque, tout tenter

Dans le rapport → faut mettre les recommandations pour régler les soucis.

RTFM → Read The Fucking Manual

ORAL →

Kill Chain et réseaux