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 faudras compromettre une machine et faire un rapport serieux 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

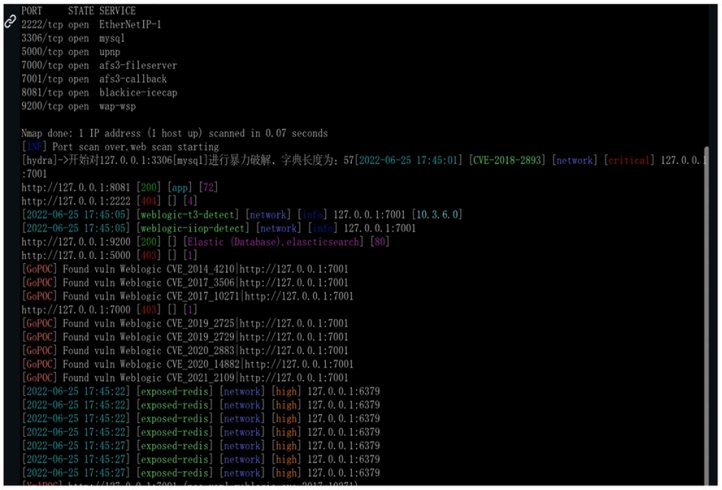
connaitre les scans SMB !!!! (smbmap, enum4linux..) et garder le script sous la main. (sur le drive

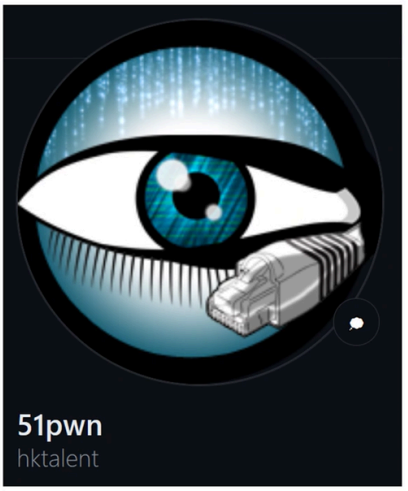
et après si on trouve des vulnés (ya aussi sploitus / exploit db):

```
┌──(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)
```

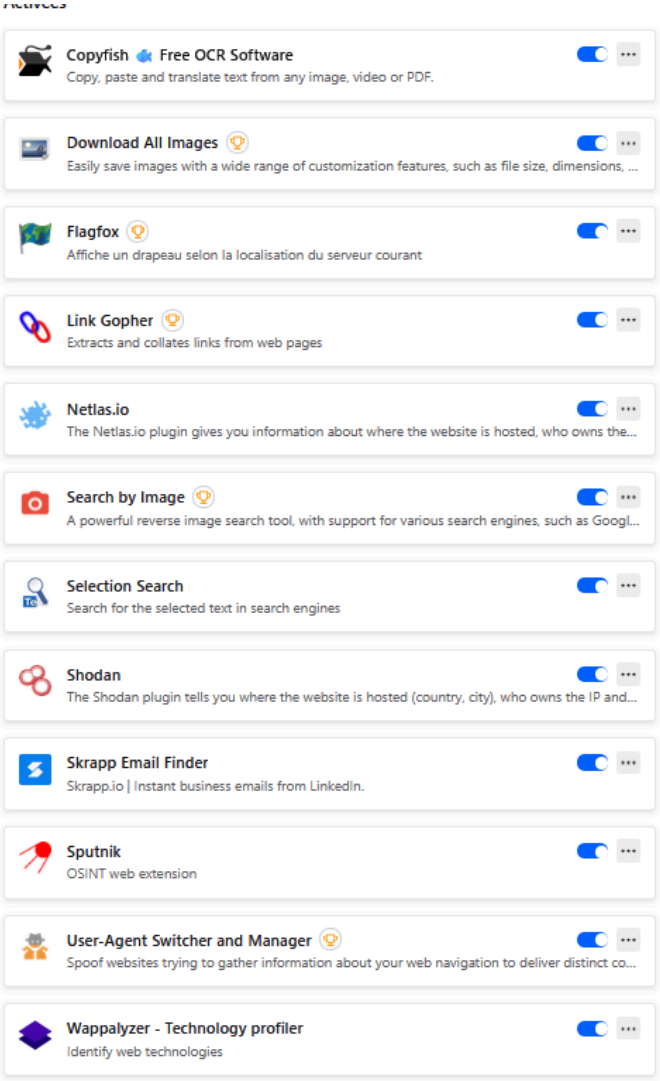
Bonus

https://github.com/GhostTroops/scan4all





- *searchsploit* –t apache 2.1
- *searchsploit* -x –nmap nomduscan.xml
- *xsltproc* /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'exam en 3h et on a 4h pour lexam total. A partir de 2h / 2h30 il faut commencer le rapport

et pour ça il faut des screenshots, commandes copié collés, une trame préparés 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 regler les soucis.

RTFM → Read The Fucking Manual

ORAL →

Kill Chain et réseaux