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

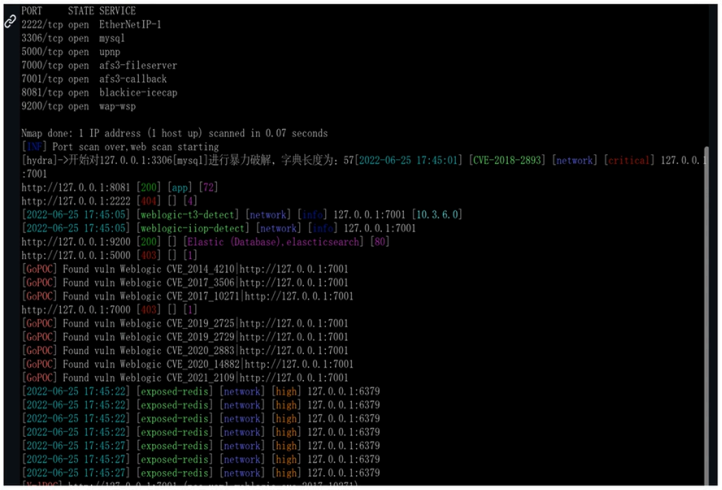
connaitre les scans SMB !!!! (smbmap, enum4linux..) et garder le script sous la main. (sur le drive

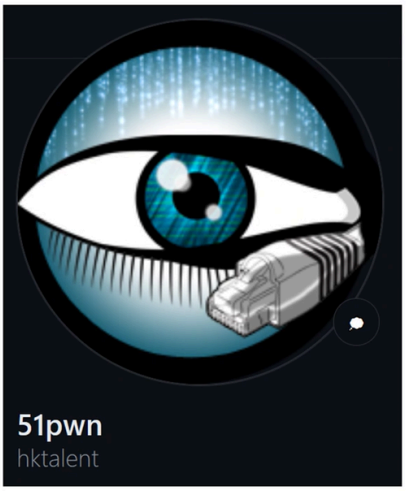
et après si on trouve des vulnés (ya aussi sploitus / exploit db):

```
┌──(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)
```

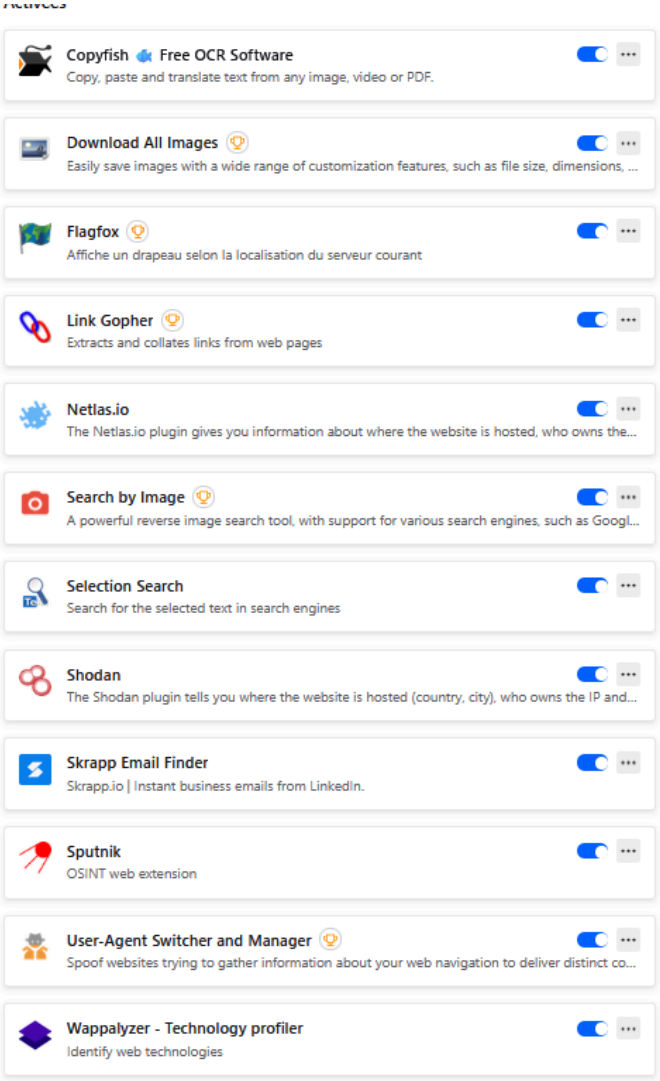
Bonus

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 (les ports c'est quel couche / les ip c'est quel couche / connaitre les ports ..)**

TP a partir du 6.

(nmap sert au scan de port, de réseaux et de vuln via NSE

metasploit : Framework de pentest complet qui couvre de la reconnaissance, au pivoting (il fait quasi tout la killchain)

Nessus est un scanner de vulnérabilités)

RDP sans MFA :

Activer le MFA / mdp de 12-14 caractère périssables / politique de blocage en fonction des tentatives / filtrer qui peux acceder au RDP (VPN et Firewall) / journalisation genre splunk forwarder

mdp de 12-14 caractère périssables / politique de blocage en fonction des tentatives (3 pour un admin /5 pour user normal)/ journalisation Splunk forwarder pour voir les attaques / changer les GPO dans Windows pour avoir des mots de passe fort sur tout le personnel / clef SSH / audit des comptes dormants / suivre les fuite de données

expliquer une vulné critique :
Une faille qui permet une prise de controle ou une fuite majeure de données avec une proba d'exploitation elevee et impact business tres fort

présenter scan avec 25 vuln :

regrouper par criticité
focus sur 3-5 points critiques
donner plan d'action priorisé

quel méthodologie de pentest :
Penetration Testing Execution Standard (PTES) car c'est une façon efficace d'effectuer un pentest et utilise la killchain
c'est une méthode approuvée, tracable et reproductible

Comment verifier robustesse d'un hash Windows NTLM :
tenter de crack (hashcat/john)
verifier politiques longueur/complexité
verifier absence ancien hashes LM (si le LM est identique entre les comptes c'est une version dépassée)

qu'est ce qu'une escalade de privilèges de Windows ?

C'est le fait de passer d'un utilisateur basique a Administrateur.
powershell par exemple (ou WinPeas sur windows)
il existe la horizontale c'est passer de machine en machine ou réseaux en réseaux
et verticale de bas privilèges vers haut privilèges

comment vulga un buffer overflow pour un public non technique ?
c'est comme si votre data était dans un bloc et que le bloc explose et peut causer des dommages autour

Si ya le SMBv1 d'actif :
désactiver le SMBv1. / appliquer correctifs microsoft / restreindre l'accès a ce reseau / migrer vers smb2 et 3 et surtout 3.1

Comment hierarchiser les reco dans un rapport de pentest ?
par criticité (impact x proba), dépenses techniques, effort/valeur, les choses fortes et faciles a faire, conformité reglementaires

quel commande linux permet de voir les process actifs et leur conso ?
ps -aux / top

quel commande linux permet de voir les ports réseaux ouvert en local ?
ss -tulnp / netstat -laputе

comment vérifier les droits sudo et l'etendue des privilèges sous linux ?

sudo -l (liste priv de l'user courant)

sudo -l -U user (par root pour un autre)

config /etc/sudoers et /etc/sudoers.d/

Utilisation des outils adaptés (pourquoi tu a choisi nmap → car on est 1e partie killchain, reconnaissances active et que nmap est un outil que je maitrise sur la partie reco active)

Connaissance des contre mesures (donner de la matière)

Aisance oral (prendre son temps et laisser les gens parler, parler simplement!! KISS)

Explication clair des résultats (tout n'est pas forcément un piege, faut se faire confiance)

Méthodologie utilisé (j’ai choisi la méthode PTES (expliquer) avec la killchain de lookhead martins)

(la nist existe mais je connais pas)

Compétences techniques

Compétences en communication

Capacité à formuler des recommandations pertinentes

(outil de bruteforce : john / hydra ..**Hydra**, **Crowbar** ou **Ncrack**)

protger ssh(savoir ce que c’est déja) : limiter le nbr de caractères 12-14 minimum / avoir des certifications / politique de changements de mdp / verrouillage de 3 a 5 tentatives en fonction des privilèges

Reconnaissance(OSINT sur les personnes,les infra, reco active avec nmap,

Weponization (préparation charge/exploit)

Delivery (acheminement, mail lien dropper

exploitation(execution de la faille

installation : persistance (implaant service)

Command and control C2 (piloter les victimes)

Action on Objectives (voler les données...)

Révisions avec Mous :

2h30 de recherche max

Exploration de méthodes d’attaques
Utilisation d’outils spéciaux pour des vulnés spéciaux

Simulation d’attaque pour evaluer la tankiness du systeme

Les meilleures pratiques pour atténuer les risques / defense

Grille de notation certif :

technique / qualité rapport / sur 70
aisance a l’oral / methodologie / compétences techniques

(ne pas tenter des trucs, les mecs sont trop chaud, tu sais pas, tu dis tu sais pas)

Critères :

Enjeux et contraintes :
precision et exhaustivité de la descritipn des objectifs

prise en compte des contraintes tech et orga

compréhension des enjeux de sécurité

(le rapport dois commencer par les enjeux en contraintes)

(quasi copie collé l'énoncé)

eval des vulnés :

precision et exhaustivité de la descritipn des vulnés

classification des vulné en fonction de criticité

identifier des vulnés les plus critiques

(ne pas dire j'aurai pu. montrer que des faits prouvable)

exploitation des failles :

precision et exhaustivité de la descritipn des tech dexploitation used

compréhension des impacts potentiels des failles

identifier les failles les plus critiques

qualité du rapport :

clarté et structure du rapport

précision et exhaustivité des informations fournies

(ne rien poser sans bien l'expliquer)

(dire jai utiliser nmap / metasploit et vaguement expliquer c'est quoi.)

qualité des illus et captures d'écran

pertinence des résultats :

adéquation entre objectifs de leval et résultats obtenus

prise en comtpe des enjeux de sécurité

capacité a identifier ??

CONCLUSION :

C’est répondre a la question de l’énoncée

EXEMPLE DENONCES

déja savoir si c’est un windows ou linux (comment je fais ça aled??)

risque global : sur la machine elle meme et sur ce qui est arrivé

Ajouter sur le rapport : couleur pour la conclusion de l’expertise

date : mettre du xx au xx meme si c’est la meme journée (mettre les heures)

enlever des parties dans la partie résumé.
