Internal

Take aways

- you can use the nmap NSE engine scripts
    - so that includes the vulnerability scanning scripts for nmap, can use service vulnerability scanners with nmap. This can be good when the boxes are very old.

```
example:
nmap 192.168.243.40 --script=smb-vuln\*
```

Target IP: **192.168.243.40**

Starting off with an Nmap scan

```
nmap -sC -sV 192.168.243.40 -oA default_scripts

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 11:05 EDT
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 46.15% done; ETC: 11:06 (0:00:19 remaining)
Nmap scan report for 192.168.243.40
Host is up (0.049s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.0.6001 (17714650) (Windows Serv
er 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 Servic
e Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
```

```
| ssl-cert: Subject: commonName=internal
| Not valid before: 2025-03-04T23:44:47
|_Not valid after:  2025-09-03T23:44:47
| 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: 2025-08-08T15:06:41+00:00
|_ssl-date: 2025-08-08T15:06:49+00:00; -1s from scanner time.
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_serve
r_2008:r2

Host script results:
| smb2-time:
|   date: 2025-08-08T15:06:41
|_  start_date: 2025-03-05T23:44:46
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Ser
ver (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: 2025-08-08T08:06:41-07:00
| 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 MA
C: 00:50:56:86:13:3e (VMware)
|_clock-skew: mean: 1h23m58s, deviation: 3h07m49s, median: -1s

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.19 seconds
```

- DNS
- MSRPC
- 445 Microsoft DS is associated with SMB
- RDP
- 5357

  > Understanding port 5375 and Microsoft's HTTP.sys
  > When you encounter port 5375 associated with "Microsoft-HTTPAPI," it in dicates that the Windows operating system's built-in HTTP Server API (HT TP.sys) is listening for incoming HTTP requests on that port

- this appears to be a windows 2008 server so quite old

Attempting to authenticate to SMB with null client / guest session with NXC and SMBclient gave me access denied errors

```
trying spider cme with null sess
crackmapexec smb 192.168.243.40 -M spider_plus -u '' -p ''

nxc share enum with null sess
nxc smb 192.168.243.40 -u '' -p '' --shares

nxc smb 192.168.243.40 -u 'a' -p '' --shares

smbclient -N -L \\192.168.243.40 all gave similar errors "status denied"
```

Attempting to log in with a null session through rpc I got a prompt but got status denied errors when trying some commands.

```
rpcclient -N -U "" //192.168.243.40
```

because I was able to authenticate, but with limited permissions I tried rpcdump

```
rpcdump.py @192.168.243.40

*] Retrieving endpoint list from 192.168.243.40
Protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol
Provider: samsrv.dll
UUID    : 12345778-1234-ABCD-EF00-0123456789AC v1.0
Bindings:
        ncacn_ip_tcp:192.168.243.40[49158]
        ncalrpc:[samss lpc]
        ncalrpc:[dsrole]
        ncacn_np:\\INTERNAL[\PIPE\protected_storage]
        ncalrpc:[protected_storage]
        ncalrpc:[securityevent]
        ncalrpc:[audit]
        ncalrpc:[LRPC-dce30b29c274e60555]
        ncacn_np:\\INTERNAL[\pipe\lsass]

Protocol: N/A
```

```
Provider: sysntfy.dll
UUID    : C9AC6DB5-82B7-4E55-AE8A-E464ED7B4277 v1.0 Impl friendly nam
e
Bindings:
          ncalrpc:[samss lpc]
          ncalrpc:[dsrole]
          ncacn_np:\\INTERNAL[\PIPE\protected_storage]
          ncalrpc:[protected_storage]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncalrpc:[LRPC-dce30b29c274e60555]
          ncacn_np:\\INTERNAL[\pipe\lsass]
          ncalrpc:[LRPC-06b8d6253d991a78cc]
          ncacn_np:\\INTERNAL[\PIPE\srvsvc]
          ncalrpc:[SECLOGON]
          ncacn_ip_tcp:192.168.243.40[49154]
          ncacn_np:\\INTERNAL[\PIPE\atsvc]
          ncalrpc:[OLE2C6C25024EC74007AB7D76569A74]
          ncalrpc:[senssvc]
          ncalrpc:[IUserProfile2]
          ncalrpc:[senssvc]
          ncalrpc:[IUserProfile2]
          ncalrpc:[IUserProfile2]
          ncalrpc:[LRPC-e386a94f0fe1d85589]
```

this was able to retrieve some information

According to the hacktricks rpc page

https://hacktricks.boitatech.com.br/pentesting/135-pentesting-msrpc

the atsvc pipe

at this point I took a step back and realized this is a very old machine so there is likely just a vulnerability to research

Googling notable exploits for windows server 2008 standard 6001 service pack 1 brings up eternal blue as a likely canidate

I used the nxc smb module to check if the vulnerability was likely

```
nxc smb 192.168.243.40 -u '' -p '' -M ms17-010
```