MS17-010 has been applied. Are you protected against the WannaCrypt ransomware?

by Washington Almeida

After working with numerous cases of ransomware attacks in Brazil, supporting medium and large companies in dealing with the crypto-ransomware WannaCry and Petya, I talked to the eForensic magazine team about sharing a bit of my experience in order to warn that a computer is not immune to WannaCry's action even after the critical Microsoft security patch MS17-010 has been installed on the computer.

WannaCry is a crypto-ransomware that affects the Microsoft Windows operating systems. Its large-scale dissemination began on May 12, 2017 through phishing techniques, infecting more than 230.000 systems around the globe. This was an unprecedented cyber attack in the history of the Internet that has impacted arms of critical infrastructure, such as health systems, transport companies, along with other telecommunications operators, government organizations, banks, universities and others. The disclosure of exploits by The Shadow Brokers group on April 14, 2017 led to the launch of a critical fix by Microsoft in March 2017. The exploitation technique used by the malware WannaCry is due to a vulnerability called EternalBlue acting on the Server Message Block protocol (SMBv1 and SMBv2) that allows remote code execution or, alternatively, an injection of a backdoor called DoublePulsar.The threat uses exploit techniques allegedly to be developed by the US National Security Agency (NSA). A critical fix for the vulnerability on supported operating systems was released March 14, 2017 and named MS17-010. Security updates for Windows XP and Server 2003, not supported by Microsoft anymore, were also released in response to this threat.

Assuming that the patch MS17-010 has been applied on your system, are you really sure you are protected against the WannaCrypt ransomware? The answer to this question is where this article seeks to contribute.

Legal note

Metasploit is a penetration testing platform developed by Rapid7 that enables you to find, exploit, and validate vulnerabilities and perform extensive security auditing activities. Cyber Security experts use this technique to diagnose security problems and to detect vulnerabilities on the environments they are authorized to experiment on with security tools.

However, experimenting with Metasploit on hosts and network environments that do not belong to you, and that you are not authorized to use these tools against, does constitute illegal activity and it is subject to law enforcement that can vary from country to country.

The plan to WannaCry demonstration

So that I can demonstrate WannaCry's action even after the system has received the patch MS17-010, I need a plan. Actually, we always need to have a plan.So, the plan is to set up a lab and prove that inadvertent actions by unsuspecting users can put systems at risk even if they have their systems updated. Remember that for a patch to be released, a malware action has occurred before.

Thus, the plan can be defined with the following steps:

1. Deploy a Windows OS without the patch MS17-010;
2. Load Metasploit to attack the remote system;
3. Load MS17-010 auxiliary module to test the system;
4. Load the exploit ethernalblue;
5. Perform attack over SMBv1 and SMBv2;
6. Apply the patch MS17-010;
7. Run MS17-010 auxiliary module to test the system for the second time;
8. Run the exploit ethernalblue for the second time against SMB;
9. Work in the user interface;
10. WannaCrypt in action.

About Metasploit

Metasploit is a penetration testing software that helps Cyber Security specialists to act like an attacker. Attackers are always developing new exploits and attack methods to hack systems. Metasploit helps us use our own weapons against them. Utilizing an ever-growing database of exploits, we can safely simulate real-world attacks on our network to train the security team to spot and stop the real thing.

We can prioritize leading attack vectors simulating complex attacks against our systems and users so we can see what a bad guy would do in a real attack and prioritize the biggest security risks.

Learn more about this extraordinary tool called Metasploit by visiting the URI https://www.rapid7.com/products/metasploit.

1. Deploy a Windows OS without the patch MS17-010:

First and foremost, I would say that if you don't know how the malware works, running it in a VM is a very bad idea. The people who do this professionally are experienced malware analysts and reverse engineers who have quite a lot of knowledge and capability with the various virtualization and segmentation concepts that are required to actively run malicious code without letting it escape the sandbox. If you are planning to build a Virtual Machine and manage to introduce the malware into the guest system, it is entirely possible that your host system could be compromised if you do not protect it against the attack vectors and distribution mechanisms. Thus I strongly recommend that you do not try to reproduce this lab unless you know very well how this malware works. OK, after the recommendations, let us go ahead and get start our lab. The network we will be working on is my personal Wi-Fi network, whose details can be seen in figure 1 below.

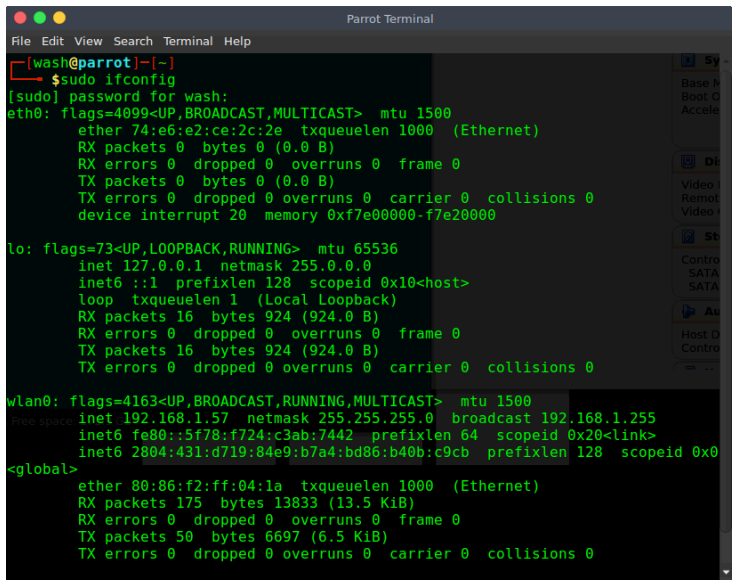

Figure 1 – Identifying the network

We can identify the network details looking at the interface wlan0 by observing the broadcasting address 192.168.1.255, which means the network is defined as 192.168.1.0/24 since the netmask is defined as 255.255.255.0. So let us introduce the elements of our lab starting with my computer, which is identified with the IP address 192.168.1.57 and equipped with Parrot Security OS, or ParrotSec, a Linux distribution based on Debian with a focus on computer security. It is designed for penetration testing, vulnerability assessment and mitigation, computer forensics and anonymous web browsing.

The virtual machine equipped with the Windows 7 operating system is our target in this lab and it does not have the MS17-010 patch installed, as shown in figure 2.

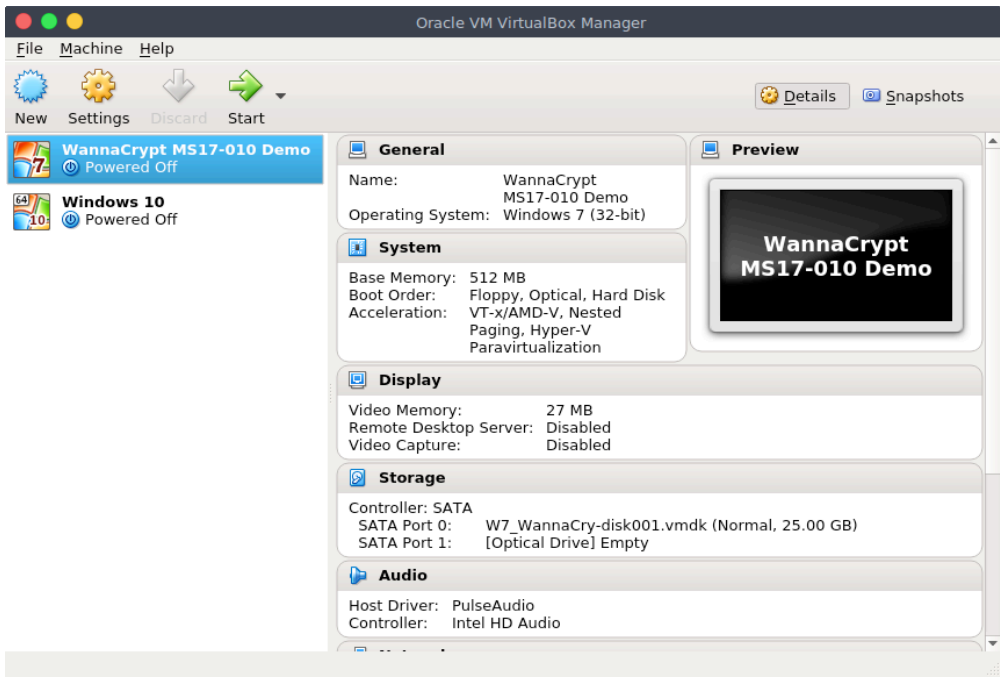

Figure 2 – Windows 7 OS machine with WannaCry executable

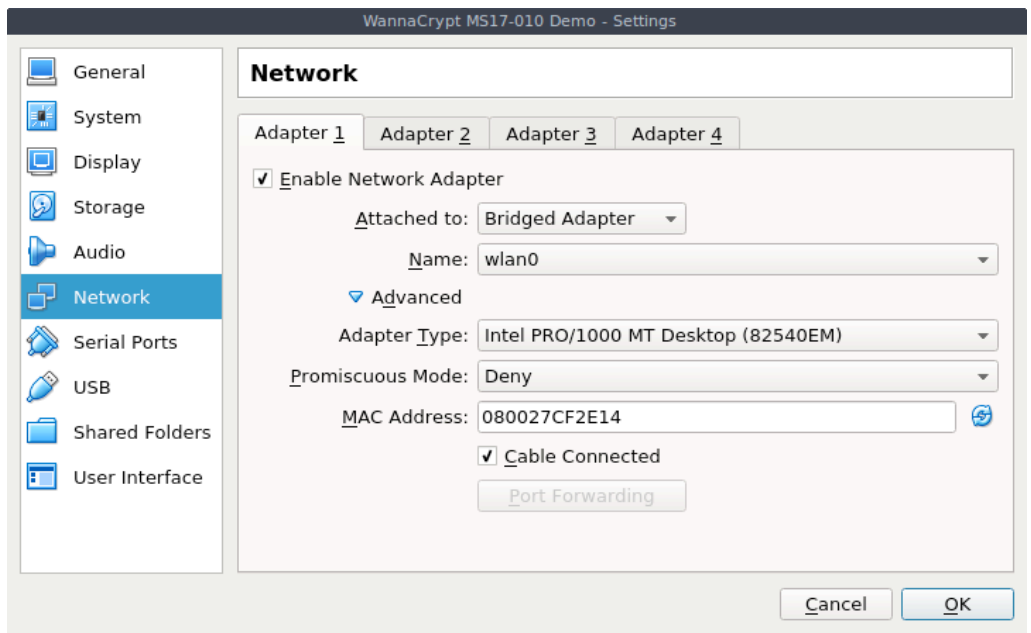

Figure 3 – Windows 7 OS machine network details

Figure 3 shows the virtual machine with its interface configured in Bridge mode in a deliberate way, since we will test the Metasploit's auxiliary and exploit modules against it. Having the virtual machine correctly set, I can initialize its OS as shown in figure 4 below. Looking at figure 4, we can realize the IP address delivered to the virtual machine is 192.168.1.51. This information will be used when loading modules from the Metasploit framework. Note that we can see the patch MS17-010 and also a WannaCry folder on the desktop of the virtual machine. This folder named WannaCry is where I have written the WannaCrypt malware for the purpose of our lab.

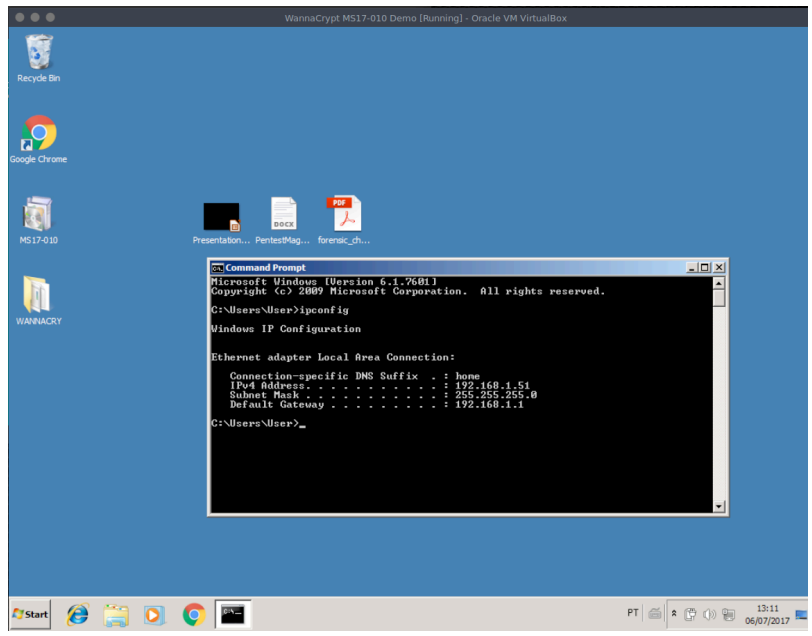

Figure 4 – Windows 7 OS VM started

Now that we have the virtual machine turned on, let us move on to step 2.

2. Load Metasploit to attack the remote system

As we have already seen in figure 1, the IP address of my machine is 192.168.1.57. From my machine, I just launch the Metasploit framework using the command line msfconsole as shown in figure 5.

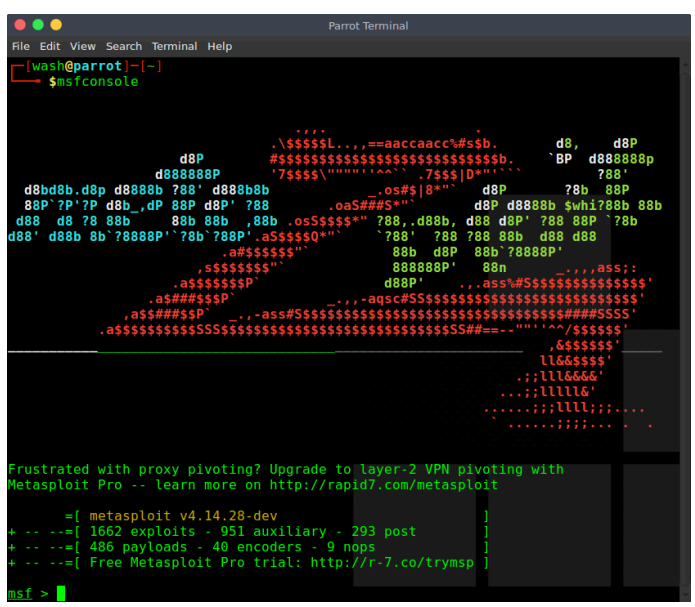

Figure 5 – Loading Metasploit Framework

After the Metasploit framework is loaded, the Cyber Security analyst receives its console characteristic represented by the prompt **msf >**.

Within the Metasploit framework, I want to look for the available features related to the MS17-010 patch. Then I execute the search command followed by the instruction of my search object as shown in figure 6.

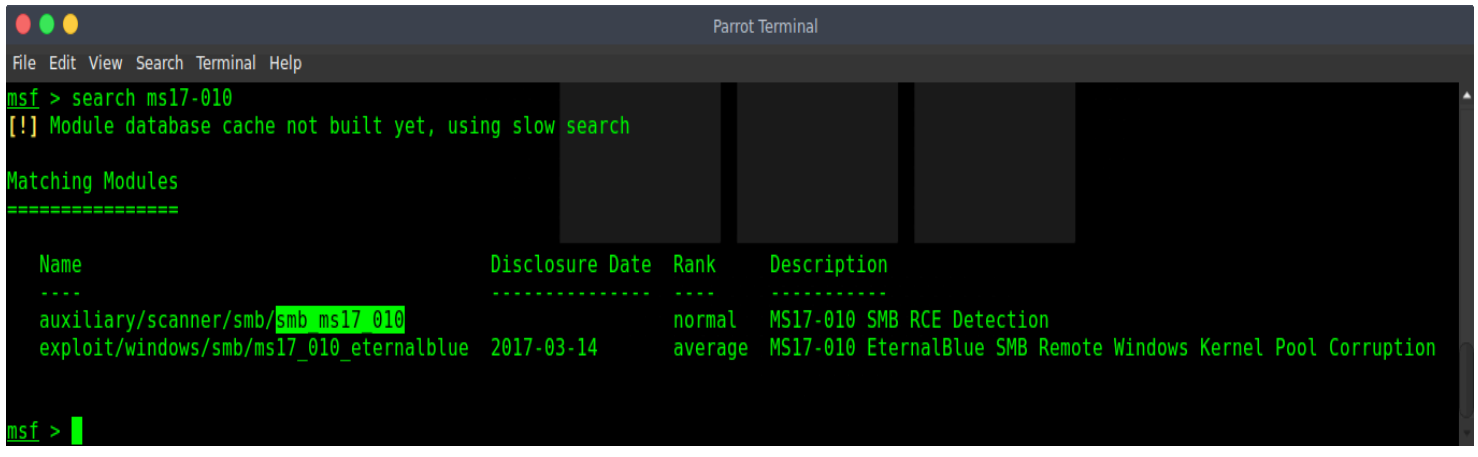

Figure 6 – Metasploit Framework search

The search for MS17-010 brings two results, namely:

a) auxiliary/scanner/smb/smb_ms17_010
b) exploit/windows/smb/ms17_010_ethernalblue

The first auxiliary module smb_ms17_010 works as a scanner from where I will test the remote virtual machine to find out if it is vulnerable to MS17-010 exploit. The second exploit module ms17_010_ethernalblue is the exploit used in case the test with the first auxiliary module brings positive results. In order to test the vulnerability in the virtual machine I need to load the auxiliary module into Metasploit framework, which is the next step of our plan.

3. Load MS17-010 auxiliary module to test the system

We load the auxiliary module launching the following command line inside the Metasploit:

```
use auxiliary/scanner/smb/smb_ms17_010
```

The results are shown in figure 7 below. Note that after having the auxiliary module loaded, it appears in red, indicating the auxiliary module is loaded. We can investigate the options available in the auxiliary module using the command "**show options**".

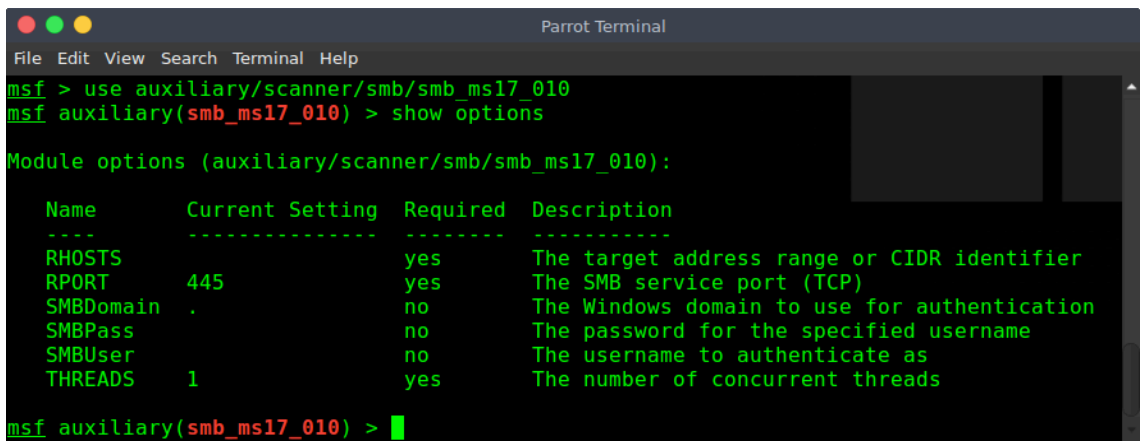

Figure 7 – Loading auxiliary module

The "show options" results show us that we need to configure the module, setting up the target address range or CIDR identifier.

CIDR stands for Classless Inter-Domain Routing, which is based on the Variable-Length Subnet Masking (VLSM) technique with effective qualities of specifying arbitrary-length prefixes. CIDR introduced a new method of representation for IP addresses, now commonly known as CIDR notation, in which an address or routing prefix is written with a suffix indicating the number of bits of the prefix, such as 192.168.2.0/24 for IPv4, and 2001:db8::/32 for IPv6. In our scenario we need just specify the IP address of the virtual machine. We configure the IP address inside the auxiliary module by using the command **`set RHOSTS 192.168.1.51`** and use **`show options`** in order to check if the module is correctly configured as we can see in figure 8.

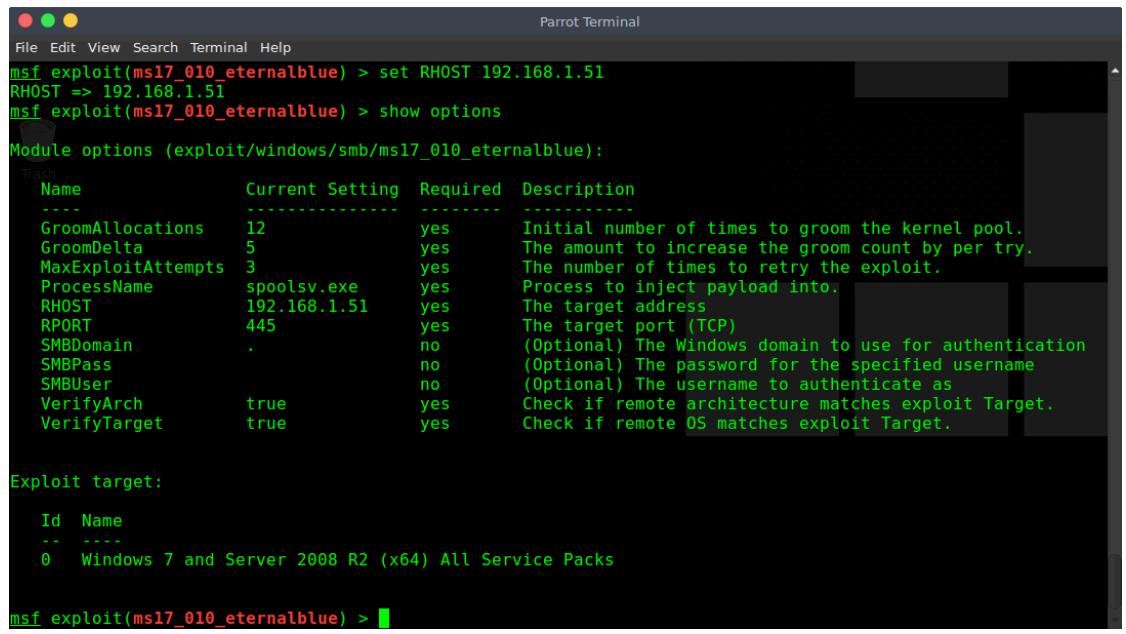

Figure 8 – Setting up the auxiliary module

Having all parameters correctly configured in the module, we just need to run the module with the command **run** or **exploit** as shown in figure 9.

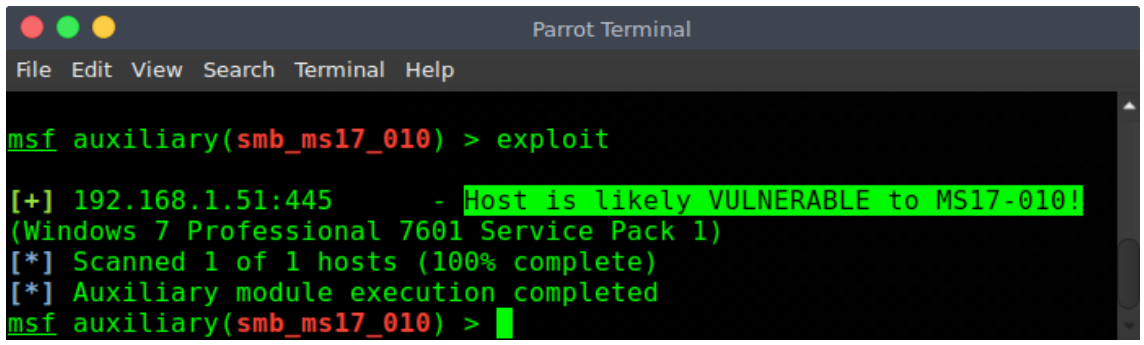

Figure 9 – Running the auxiliary module

As a result we can see the host 192.168.1.51 is likely vulnerable to MS17-010. Now we are ready to move forward to step 4 of our lab.

4. Load the exploit ethernalblue

Well, before loading the exploit module inside Metasploit framework let us explain what is EternalBlue. EternalBlue / DoublePulsar is an exploit that is believed to have been developed by the U.S. National Security Agency (NSA). It was leaked by the Shadow Brokers hacker group on April 14, 2017, and was used as part of the worldwide WannaCry ransomware attack on May 12, 2017. The exploit was also used to help carry out the Petya cyberattack on June 27, 2017. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows accepts specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer. The worm component takes advantage of a Remote Code Execution (RCE) vulnerability that is present in the part of Windows that makes it possible to share files over the network, known as "Server Message Block" or simply SMB.

This Metasploit module is a port of the Equation Group EternalBlue exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memory move operation in Srv! SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original, may not trigger 100% of the time, and should be run continuously until triggered.

Now that the eForensic reader has a better understanding about EternalBlue, let us load the exploit module by launching the following Metasploit command line:

```
use exploit/windows/smb/ms17_010_ethernalblue
```

The same way we investigate and set up the auxiliary module, we do the same in the exploit module as shown in figure 10.

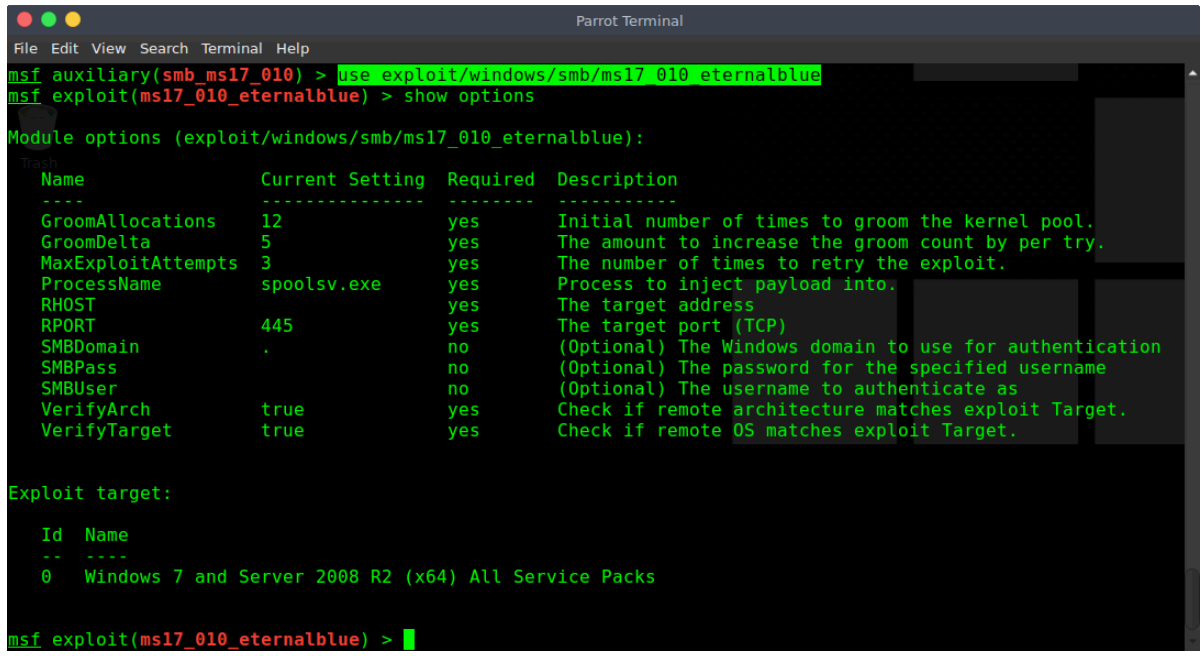

Figure 10 – Loading the exploit module

Note that we need to inform the IP address of our target using the parameter RHOST.

This is what we will do in the next step in order to perform the EternalBlue attack against our virtual machine.

5. Perform attack over SMBv1 and SMBv2

I set the IP address in the exploit module with the command **set RHOST** as shown in figure 11.

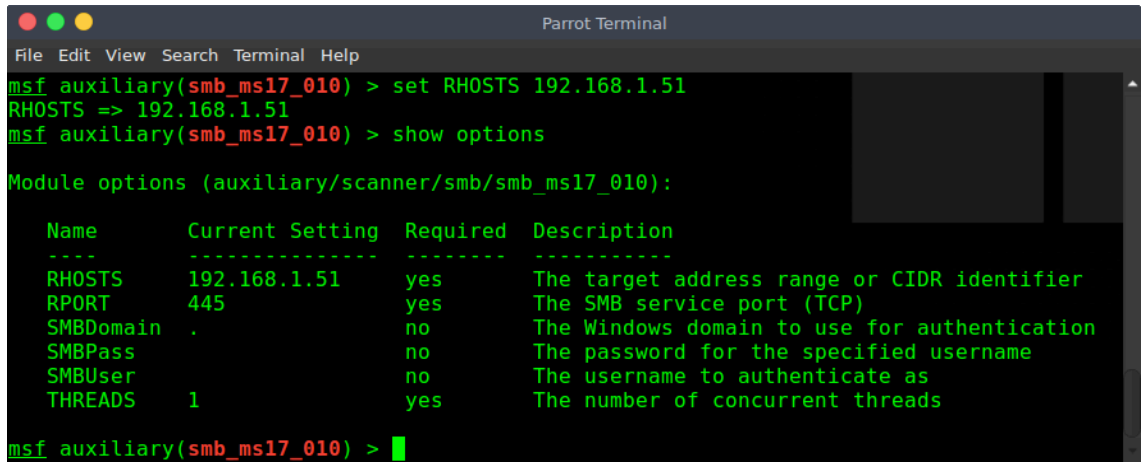

Figure 11 – Setting up the exploit module

Now that we have the exploit module correctly configured, we just need to run the exploit as shown in figure 12.

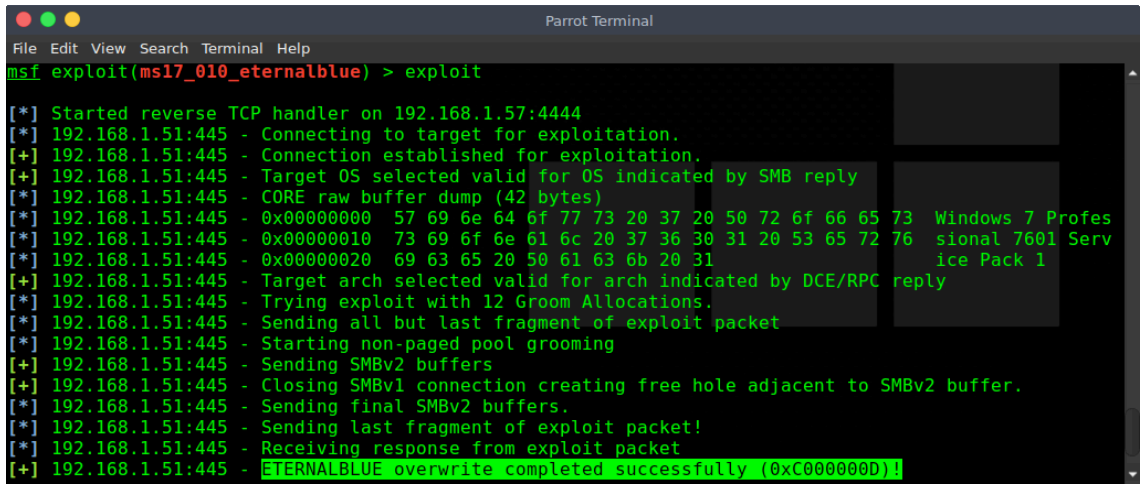

Figure 12 – Running the exploit module

As we can see, the exploit could be explored with success. It is time to move on to the next step to apply the patch MS17-010 and test the virtual machine again.

6. Apply the patch MS17-010

As we have seen in figure 4, the MS17-010 in desktop is ready to be deployed.

We just open the package to run it as shown in figures 13, 14 and 15.

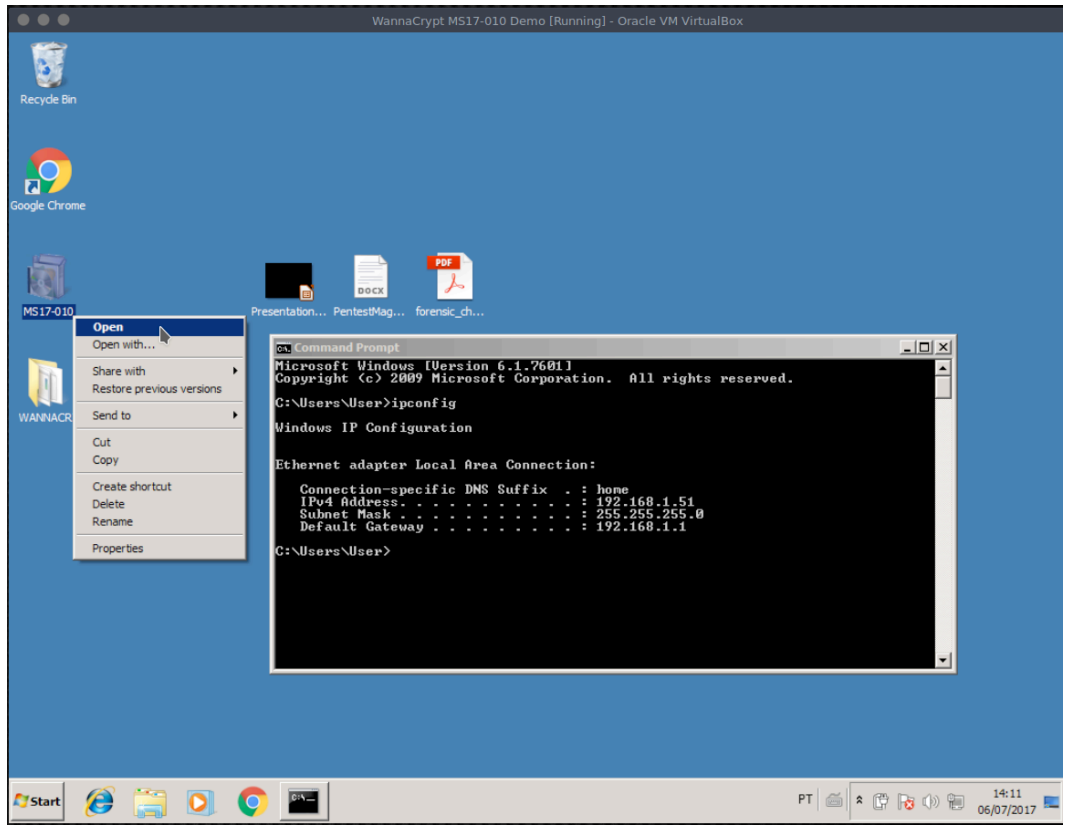

Figure 13 – Running the patch MS17-010

After opening the MS17-010 package we just need to wait until the patch is completely applied in the remote virtual machine.

Once the patch is applied in the computer (our virtual machine) it is required to restart the computer so that the updates can take effect.

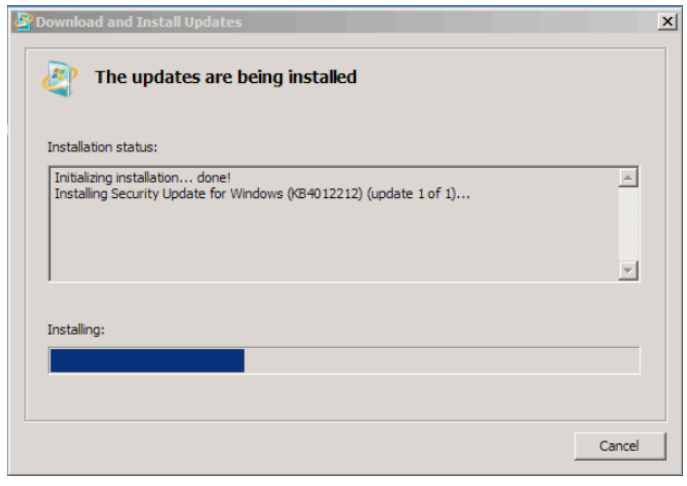

Figure 14 – Applying the patch MS17-010

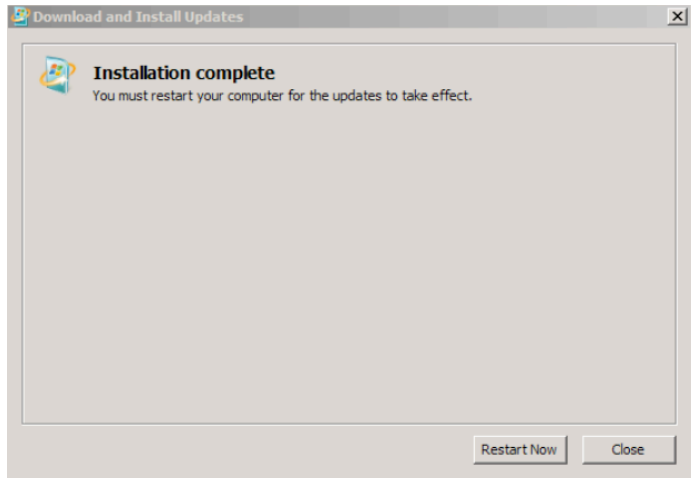

Figure 15 – Patch MS17-010 applied

Now it is time to verify if the system is still vulnerable to MS17-010 exploit.

7. Run MS17-010 auxiliary module to test the system for the second time

As I kept the auxiliary module **smb_ms17_010** opened and the IP address of the virtual machine remains the same, let's run the auxiliary module again.

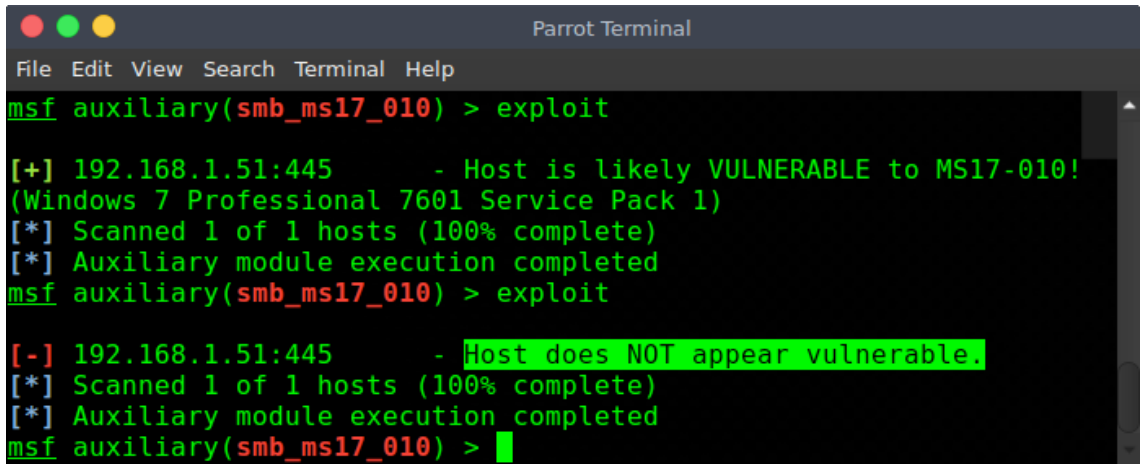

Figure 16 – Running the auxiliary module for the second time

As expected, figure 16 shows us the virtual machine is not vulnerable to MS17-010 exploit anymore.

Let us try to exploit the virtual machine again using the EternalBlue exploit in the next step of our lab.

8. Run the exploit EternalBlue for the second time against SMB

Loading the exploit module ms17_010_eternalblue and running it against our VM target for the second time we notice a fail while trying to use the EternalBlue exploit against our virtual machine as we can see in the figure 17 below.

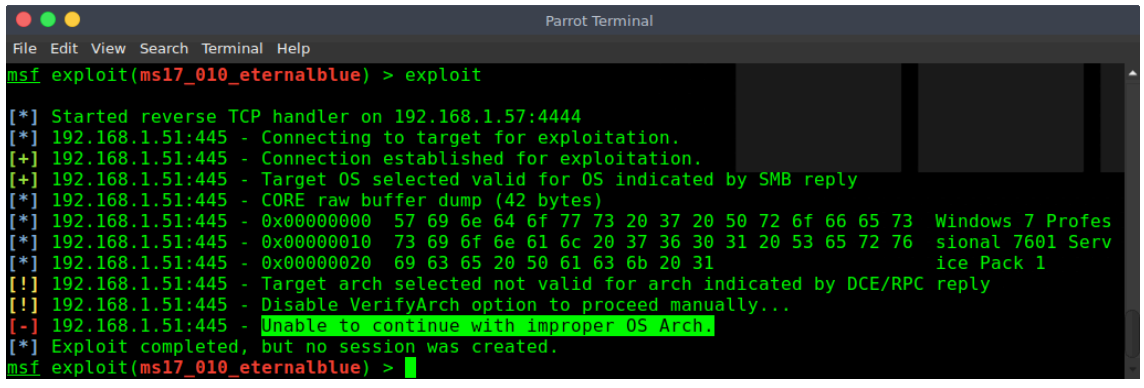

Figure 17 – Running the exploit module for the second time

So we now have our target protected against the MS17-010 vulnerability. Can we state that the computer is protected against crypto-ransomware WannaCry?

Let us answer the question in the next step.

9. Work in the user interface

At this point, I intend to test the virtual machine environment with the ransomware WannaCrypt infection, thus I just disabled the network interface of the virtual machine in order to isolate the environment before continuing with the actions of this step.

Actually, we can suffer ransomware infection in so many ways such as when accessing a compromised website, opening attachments of phishing emails, connecting USB devices and infected external hard drives, installing suspicious applications on smartphones, failing to install security patches for operating systems such as MS17-010, malware that is embedded in suspicious programs, and other vulnerabilities such as outdated anti-virus.

If we analyze the infection vectors more carefully, we can see that the user's actions still remain the main point of failure, for example inadvertently opening a file as shown in figure 18. Just opening a simple jpg image file is enough to bring a backdoor to your environment and compromise your system so that an attacker can access your assets without your knowledge.

Have a look in my video at https://www.youtube.com/watch?v=2Kt2p9r_b4E and see how hackers inject a backdoor into an image file to take advantage of this feature and hack into remote systems.

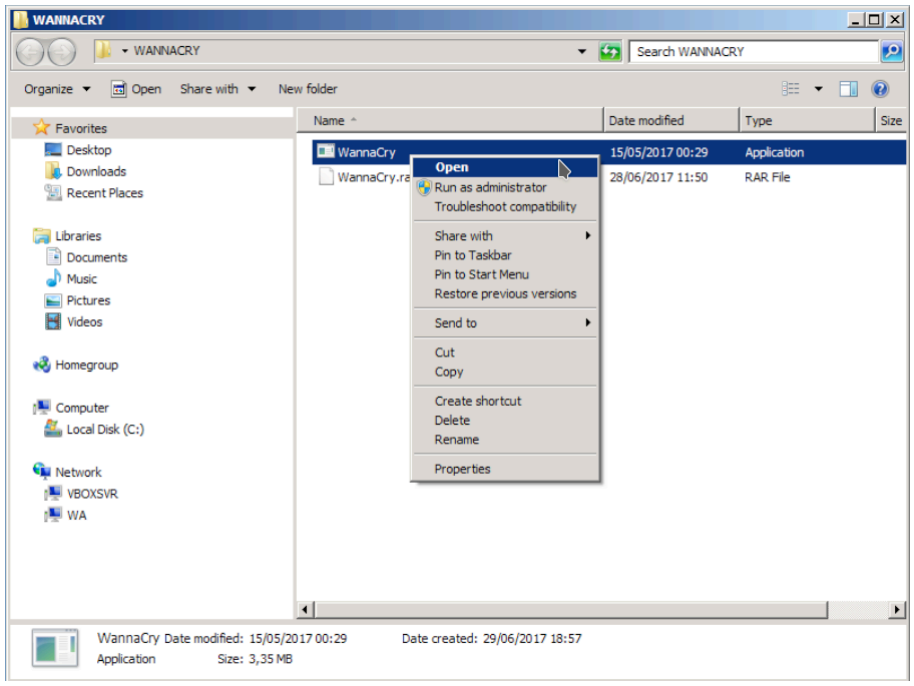

Figure 18 – Running the ransomware WannaCrypt

This file could be a script attached to a phishing e-mail, a link contained in the body of an e-mail, an executable file on a pen-drive or an external disk, an image file in a compromised website and so on. Whatever the inadvertent action of the user is in this scenario, it will imply the possibility of action of ransomware infecting the user operating environment, with the consequences that this malware brings as we will see in the next step.

10. WannaCrypt in action

Shortly after running the WannaCry.exe file we can see the malware in action as we can see in figures 19 and 20. But wasn't the critical security patch MS17-010 installed? Yes, in fact it was. However, there is no point in having a good defense system if the most fundamental defense does not work: the correct actions of the users!

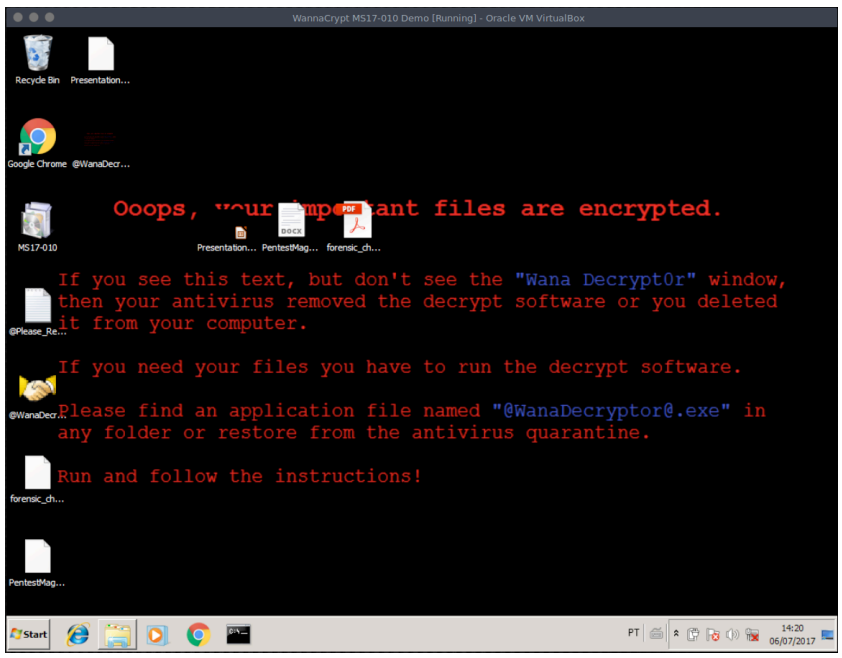

Figure 19 – Ransomware WannaCry in action

Figure 20 – Environment infected with ransomware WannaCry

User inadvertent actions constitute the largest vector of infection, propagated mainly by phishing e-mails.

How to prevent a ransomware infection?

There are some precautions and actions that users can take to prevent an attack by ransomware. They should:

- Install and keep up-to-date in a daily basis an anti-virus solution;
- Make sure every day that your operating system has the critical security patches installed;
- Avoid clicking on links or opening e-mail attachments from people you don't know or companies you don't do business with;
- Have a pop-up blocker running on your web browser (I use the add-ons Adblock Plus and uBlock);
- For advanced users: consider making use of the Sandbox;
- For companies: train your users! Unsuspecting users will inevitably click on attachments from a phishing e-mail or take some other action that will put the company assets at risk;
- For everyone: back up your data DAILY. Backup may be your only alternative if a ransomware reaches your computer or your company assets.

Summary

One of the most fundamental defenses against ransomware is the ability to reliably restore the data from backup. However, as we have seen in this article, there are several simple actions that can be a part of the everyday life of users and companies that can prevent against ransomware infection. Information will continue to be the greatest weapon against digital threats. If you are aware of any potential threats, share the information with the information channels like this excellent channel that is eForensic magazine.

About the Author: Washington Almeida

Washington Almeida is an electronic engineer specializing in digital forensics and cyber security with more than 25 years of experience working for large companies in cases involving intellectual property infringement, computer network intrusion, social networking monitoring, among others. As a Cyber security professional, he also works with sophisticated systems invasion testing, helping companies to improve the security of their assets. In the assistance of the Justice, he is licensed by the "Tribunal de Justica de São Paulo" and "Tribunal Regional do Trabalho da 2ª Região" to work as digital forensic expert appointed by the judge.

Wash Web page: www.washingtonalmeida.com.br