Logo, icon, company name

Description automatically generated

**Information Security**

**COMP-421**

**Section-B**

**Assignment-2**

**Hannan Zahid**

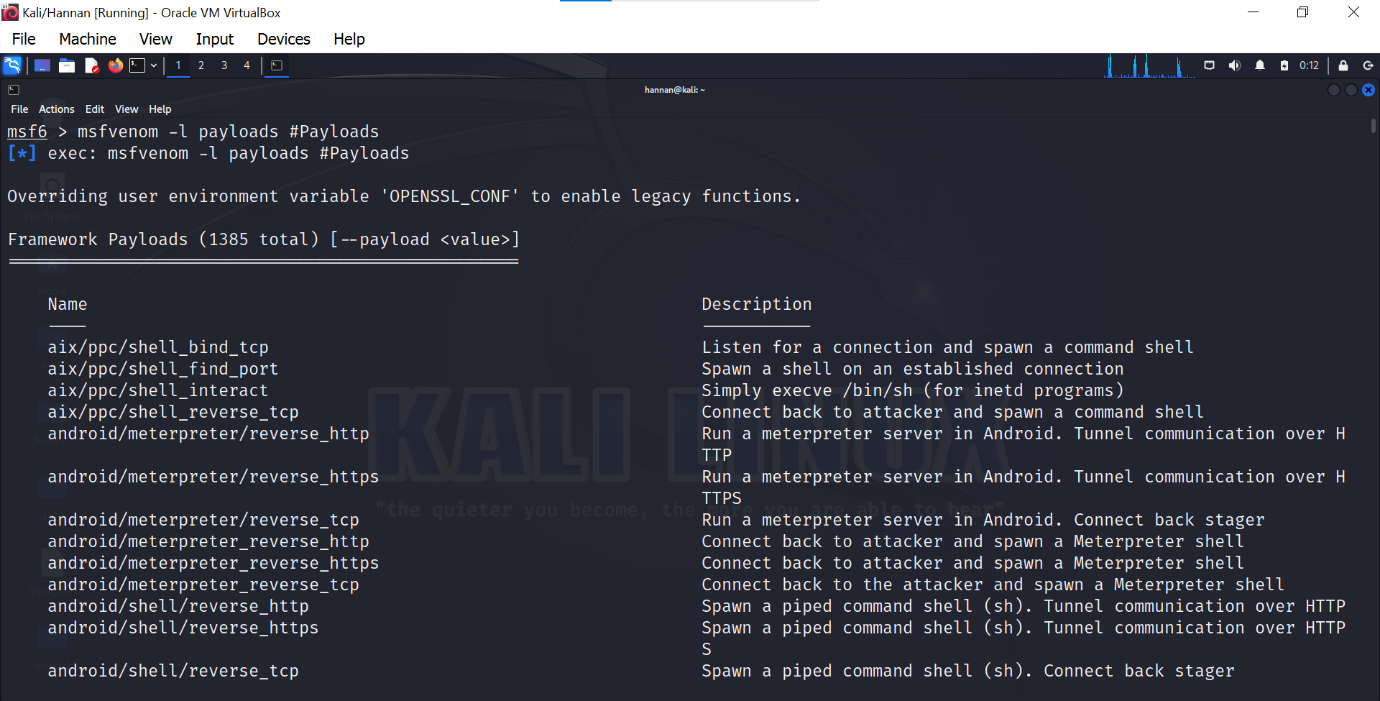
**241545586**

**Link:**  <https://book.hacktricks.xyz/generic-methodologies-and-resources/shells/msfvenom>

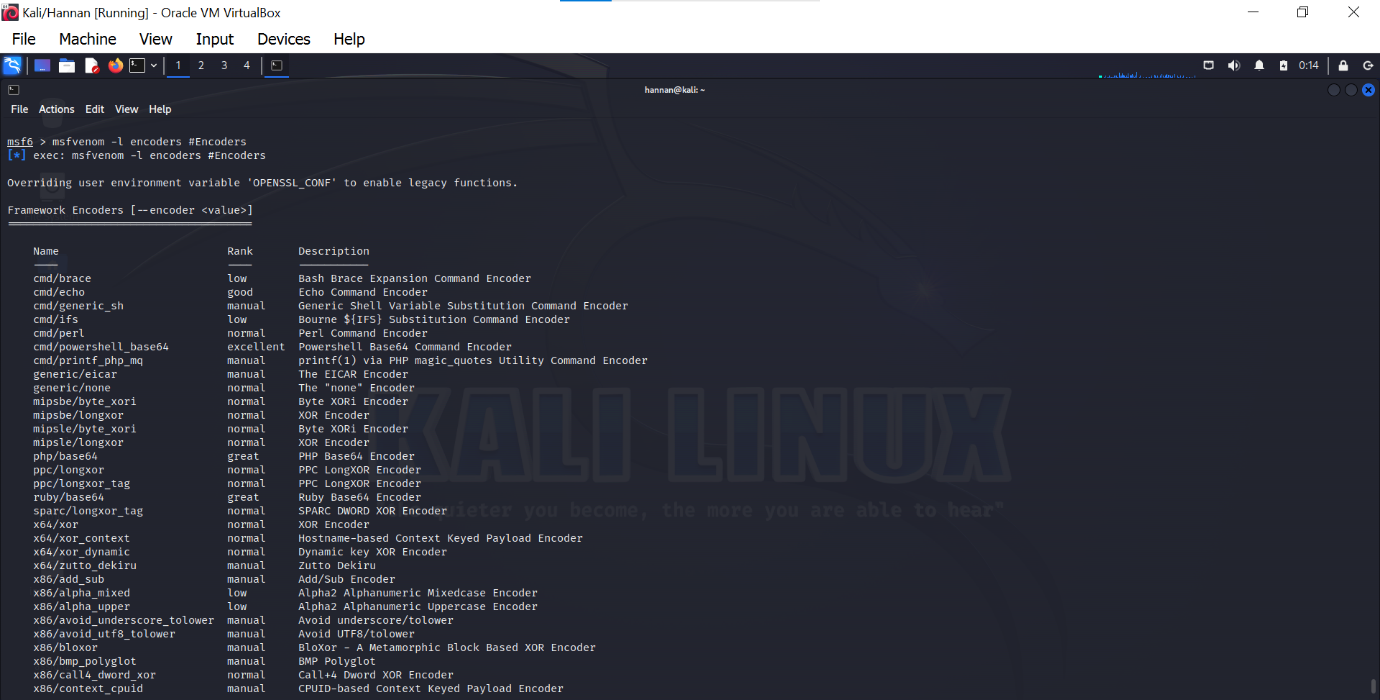
**Successful Command Run:**

**Listing**

**msfvenom -l payloads #Payloads**

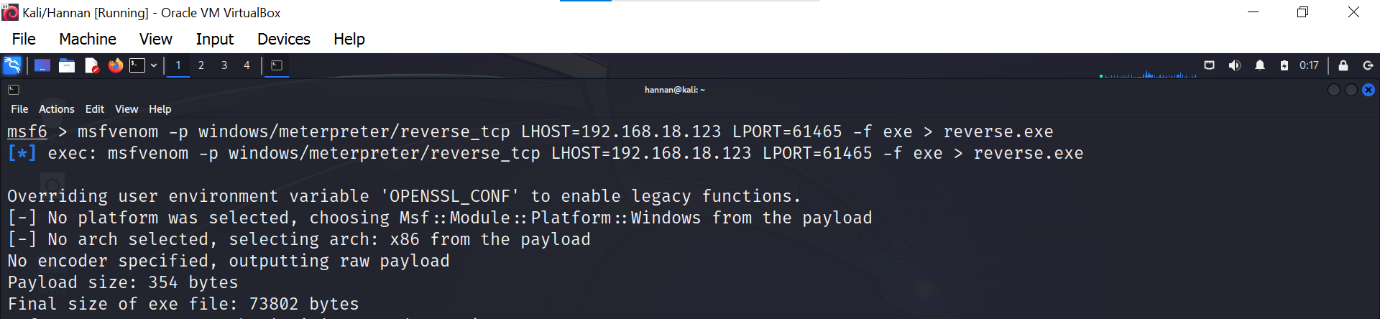
****

**msfvenom -l encoders #Encoders:**

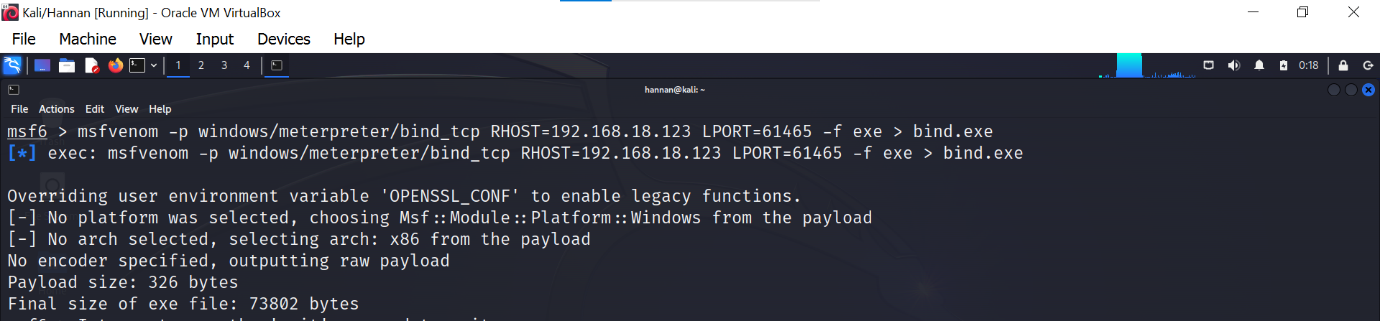
****

**Windows**

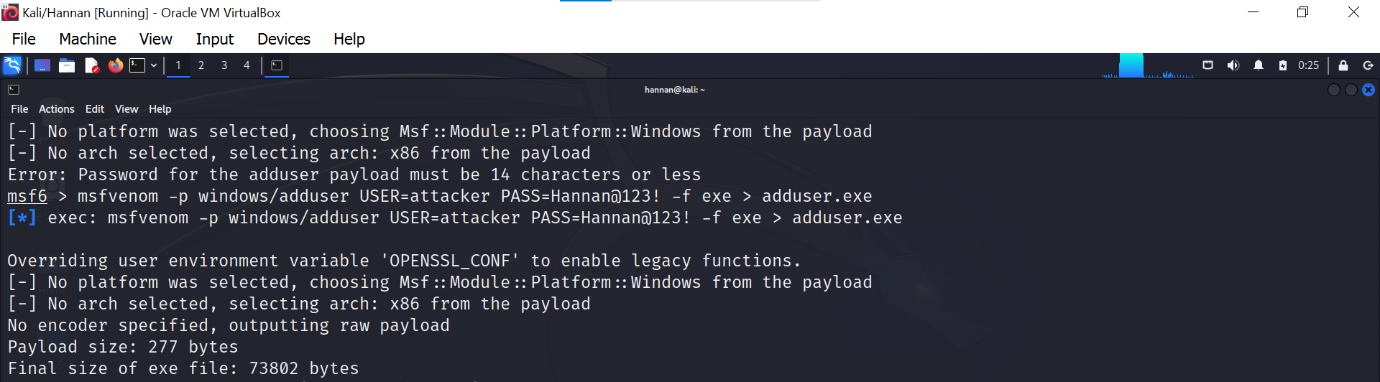
**Reverse Shell:**

****

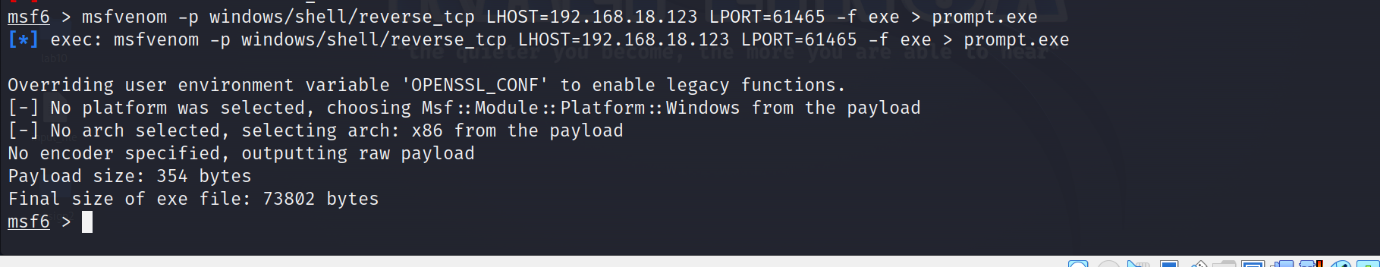
**Bind Shell:**

****

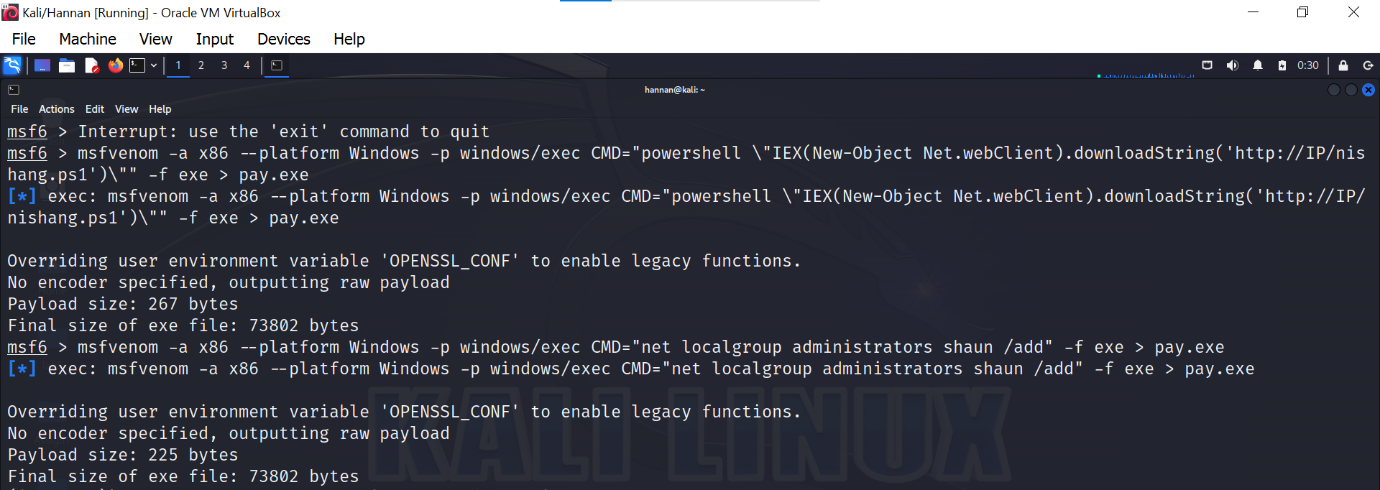
**Create User:**

****

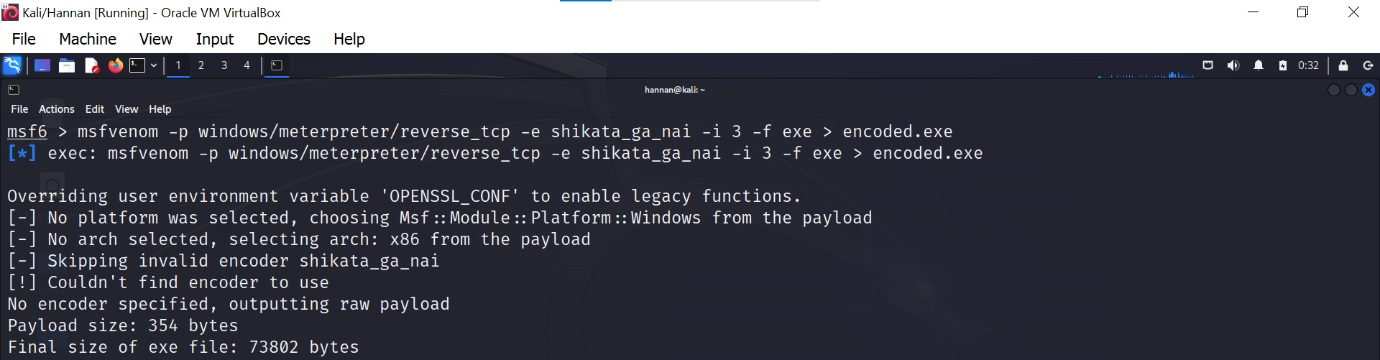
**CMD Shell:**

****

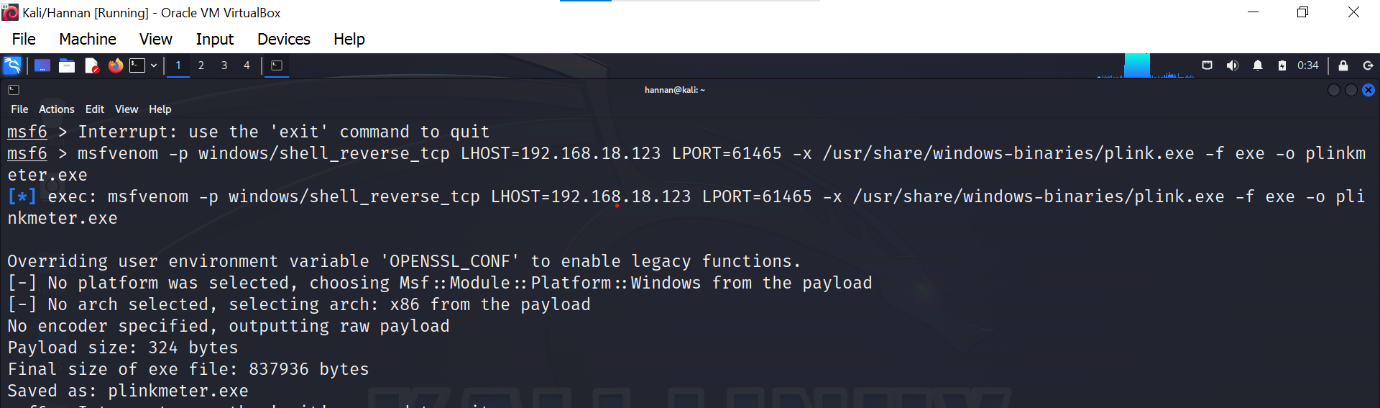
**Execute Command:**

****

**Encoder:**

****

**Embedded inside executable:**

****

## Linux Payloads

### Reverse Shell:

### C:\Users\Hi\Desktop\reverse shell linux.png

### Bind Shell:

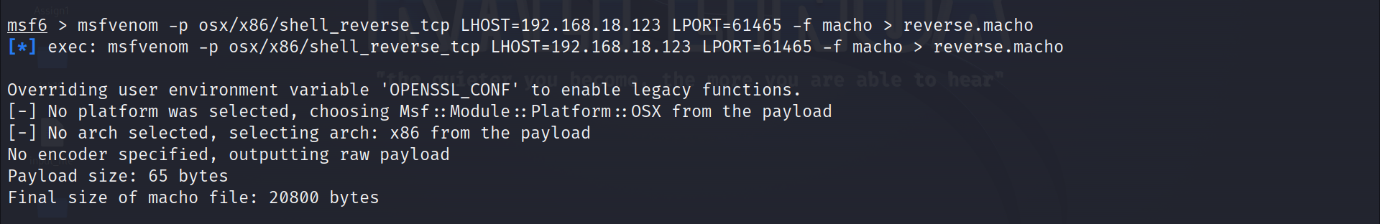
### C:\Users\Hi\Desktop\linux bind shell.png

**SunOS (Solaris):**

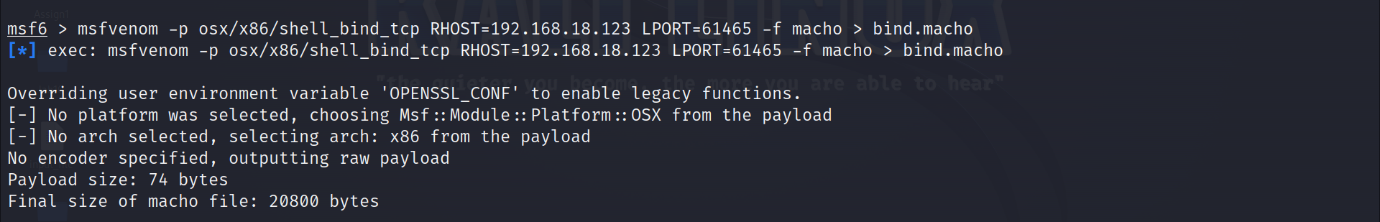
****

## ****MAC Payloads****

### ****Reverse Shell:****



**Bind Shell:**



## ****Web Based Payloads****

### ****PHP****

### ****Reverse Shell:****

### C:\Users\Hi\Desktop\php reverse shell.png

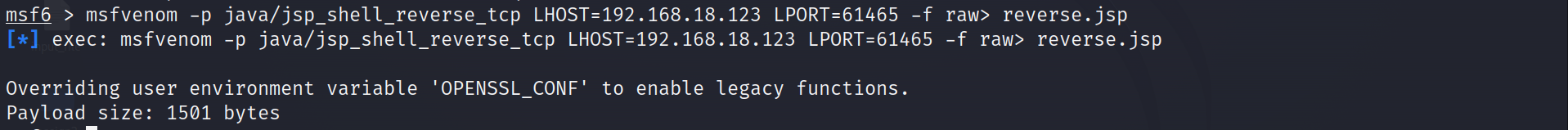
### ASP/x

### ****Reverse Shell:****

### C:\Users\Hi\Desktop\asp reverse shell final.png

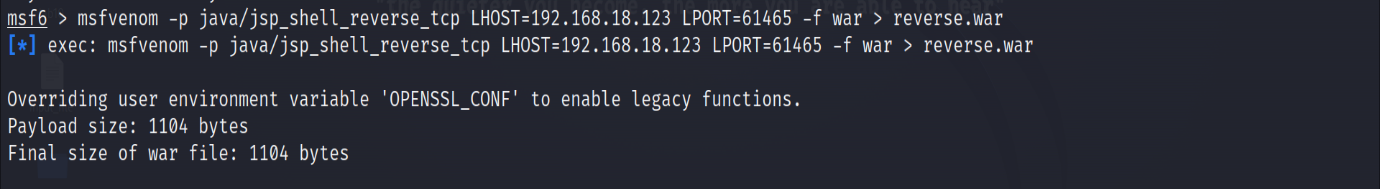
### JSP

### ****Reverse Shell:****

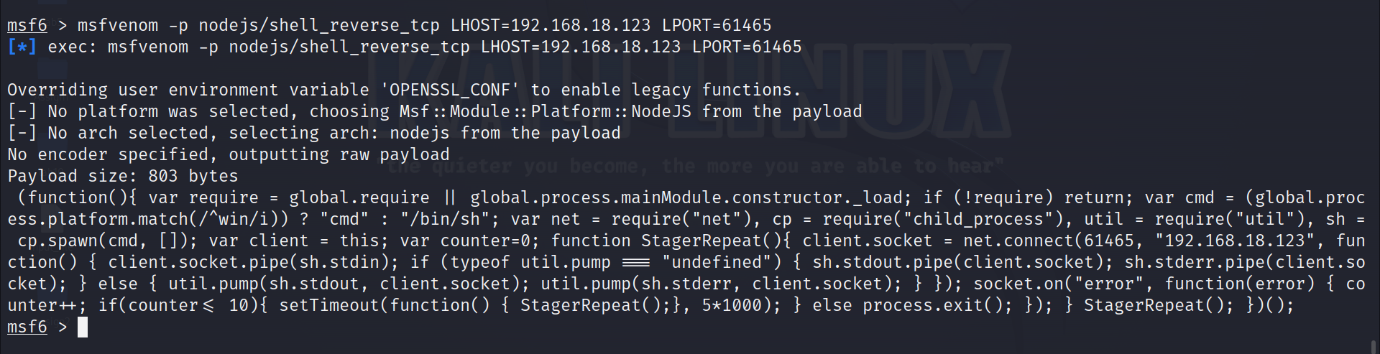


**WAR**

### ****Reverse Shell:****



**NodeJS:**



## ****Script Language payloads****

### ****Perl:****

### C:\Users\Hi\Desktop\perl.png

### Python:

### C:\Users\Hi\Desktop\python.png

### Bash:

### C:\Users\Hi\Desktop\bash.png