Metasploit – Windows Backdoors

- The traditional method of compromising network hosts consists of conducting reconnaissance, identifying one or more vulnerabilities, and then exploiting then using an appropriate tool or utility.

- However, secure coding practices, patch and update management, and other good practices are rapidly reducing the number of vulnerabilities that can be exploited using stack smashing and buffer overflows, which are typically used to inject backdoors into systems.

- Rather than attacking and exploiting services, a much easier way in to a network is usually through its weakest link, the users. Social Engineering exploits are becoming much more prevalent and sophisticated.

- The Metasploit Framework is an application and subproject developed by Metasploit LLC. It was initially created in 2003 in the Perl programming language, but was later completely re-written in the Ruby Programming Language.

- Since the release of Metasploit, exploit development has become a very simple process that anyone with minimal or no coding skills can accomplish.

- It also serves as a development platform for payloads (the code executed after an exploit has successfully been run), payload encoders (to obscure data so that Intrusion Detection Systems [IDS] and Intrusion Protection Systems [IPS] will not detect and block the exploit), and various other tools.

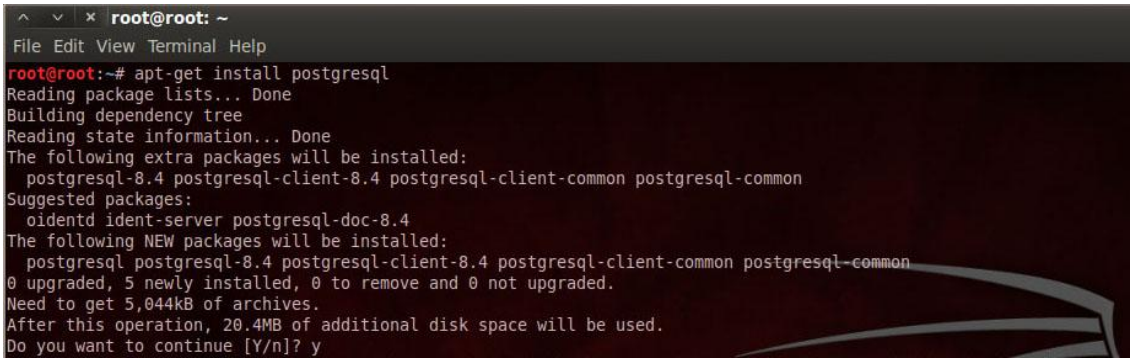
- Armitage is the current user interface for Metasploit, which provides tight integration between scanners, evasion techniques, exploits, and payloads.

- One of the most powerful Metasploit payloads is Meterpreter. Meterpreter provides post-exploitation capabilities. For example, with Meterpreter: one can browse a remote file system, route connections through the current host, and dump password hashes.

- However, Meterpreter is simply a payload and it requires an exploit or social engineering to get it installed on a victim host.

- As a proof of concept we will use the Metasploit package available on the Kali to compromise a Windows host using payload generated through Armitage.

- Note that after Kali has been booted and running, it will be necessary to install “postgresql” in order for Armitage to work properly:



- Then start the both the services as follows:

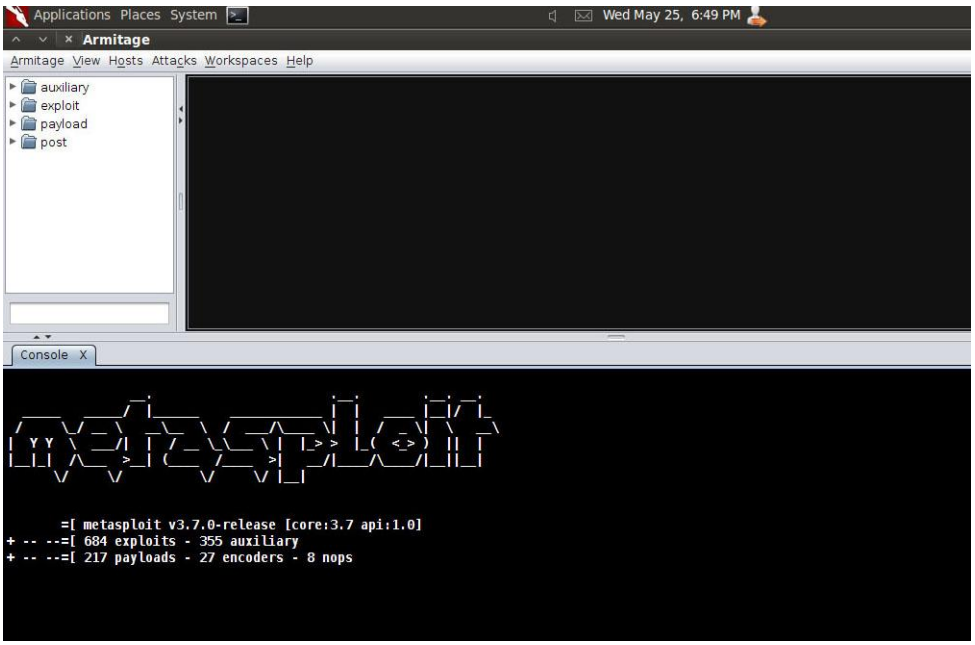
service postgresql start

service metasploit start

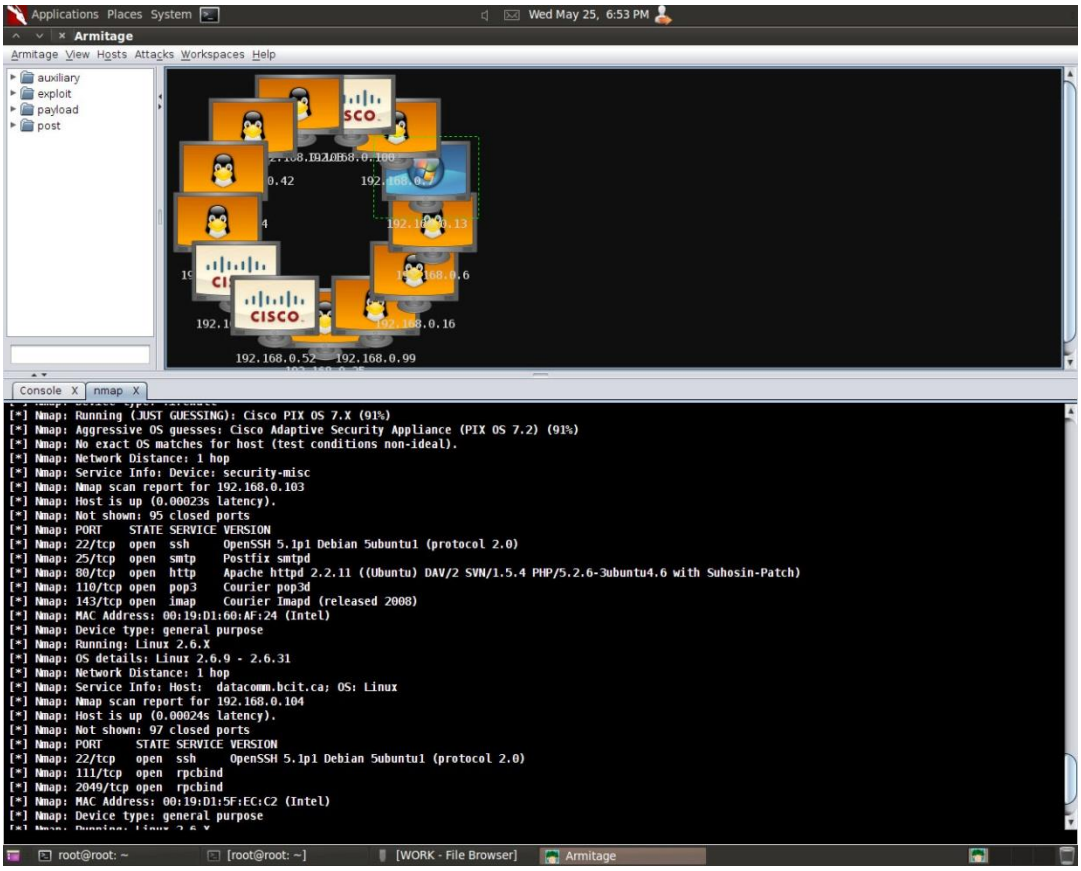
Starting Metasploit and Scanning

- We can run Metasploit first and then select Armitage from the menu, or it can invoked directly from command line by typing “armitage”.

- Select “Start MSF” and then wait for it to connect to the database server. The following screenshots illustrate this process:



- The next step is to scan for target hosts. Armitage provides several network scanning tools, we will nmap (with OS detection) to obtain the following network map:



- The top left is the module browser. Using the module browser we can access Metasploit's payloads, exploits, and auxiliary modules.

- The top right is the target area. Armitage displays the current hosts and any sessions that have been established in the target area.

- A compromised host will appear framed in red with lightning bolts surrounding it. The bottom is the tabs area. Armitage opens each console, browser and dialog in its own tab.

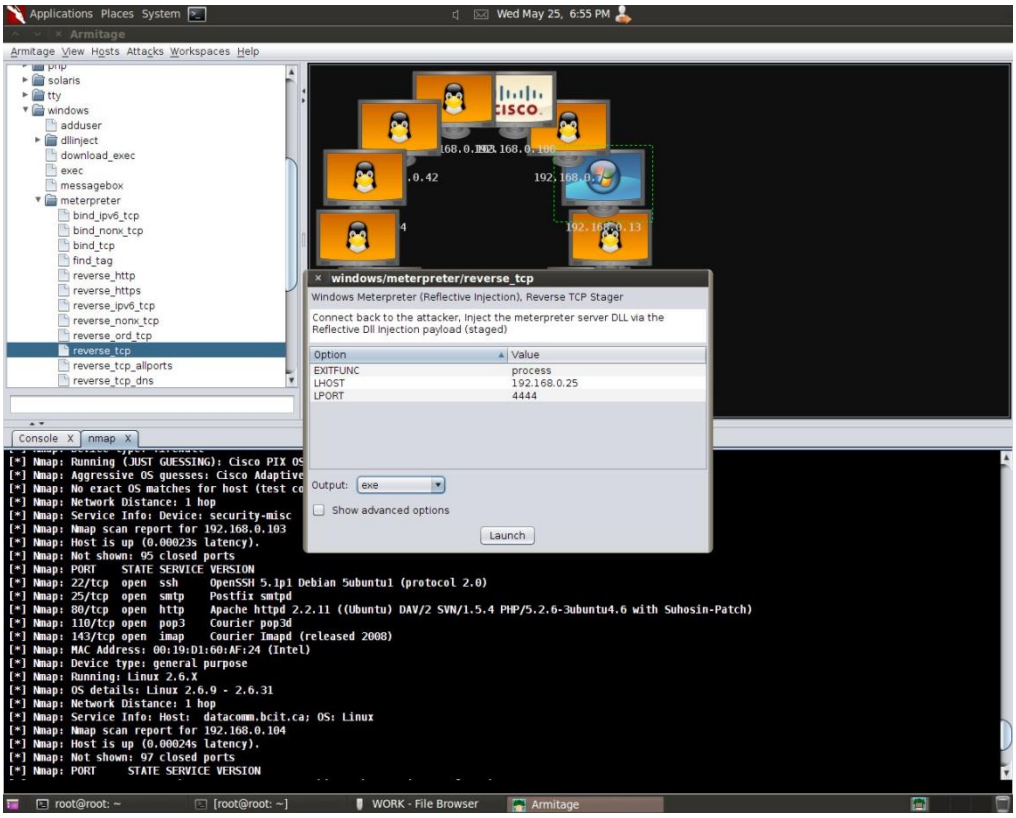
- We will target the Windows host, which means that it will run the payload generated by Meterpreter and connect back to the Metasploit (attacker's host) host.

Generating the Payload

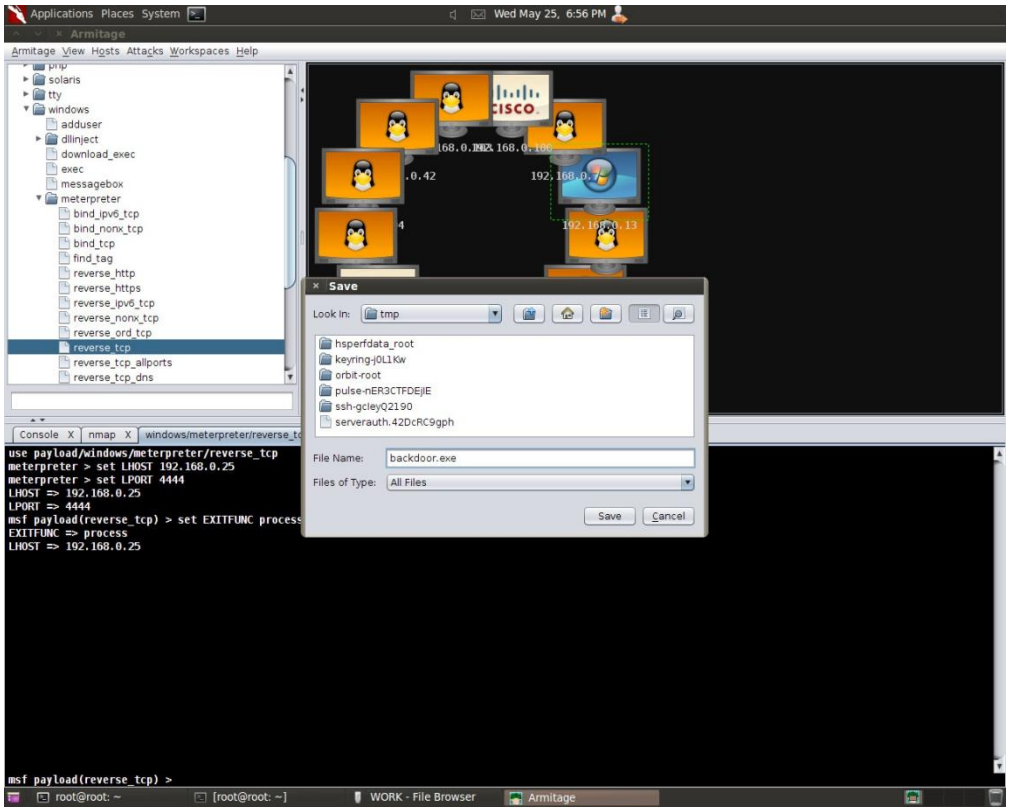
- We will use Armitage to create an executable version of Meterpreter. Navigate to ***payloads/windows/meterpreter/reverse_tcp*** in the module browser and double click it.

- The following screenshot illustrates the ensuing dialog. Double click a value to edit it. We can either accept the defaults or change each option by checking the "Show Advanced Options" box and modifying the settings.

- The LPORT value is the port that the executable will communicate back to. It would be a good idea to change it to a more common port, which will be accessible through the firewall, port 80 for example.



- Select **exe** for the output type and the click **launch**. Armitage will prompt for the location to save the executable to.



- We now have a post-exploitation program that will connect back to our attacking machine on port 4444 when it is execute on the victim machine.

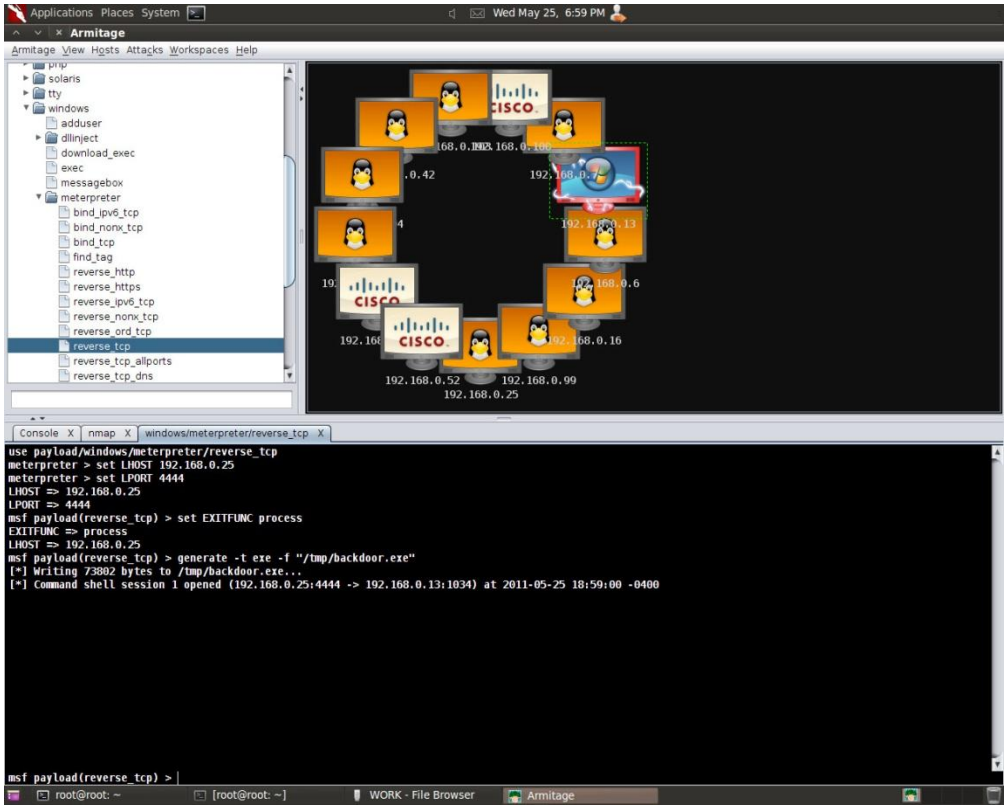
- Before the victim machine executes our post-exploitation code, we must ensure that the attacking machine is set up as a listener on the port that was specified in the payload.

- We can accomplish this step by setting the listener mode: *Armitage->Listeners->Reverse*. Set the port number (4444 in this example) to the same as that used in the payload.

- Also set the "**Type**" to "**Meterpreter**". Click "**Start Listener**", and the system is ready to receive connection attempts from our backdoor program.

Post Exploitation

- Once the victim machine executes our executable that contains the backdoor, a connection back to the attacker host will be established and we will see the compromised system in the target area framed in red, with lightning bolts as illustrated below.



- At this point we can right-click this compromised machine and navigate to the Meterpreter menu. Each Meterpreter session will have its own menu item.

- The Access menu is used to dump hashes, escalate privileges, and duplicate access.

- Using the Duplicate option, Armitage will upload and execute another Meterpreter instance so we have two sessions. This way if something happens to one of the sessions, we will still maintain access.

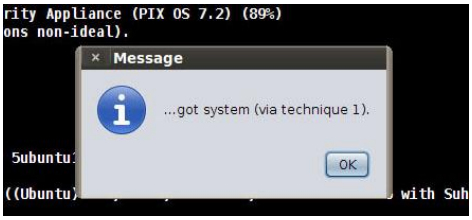
- We can use the Interact menu to open a Windows command shell or a Meterpreter shell. The Explore option can be used to access the local system. Here you can browse the file system, view a process list, start a key logger, take a screenshot, or even take a picture with any built-in camera.

Dumping the Hashes

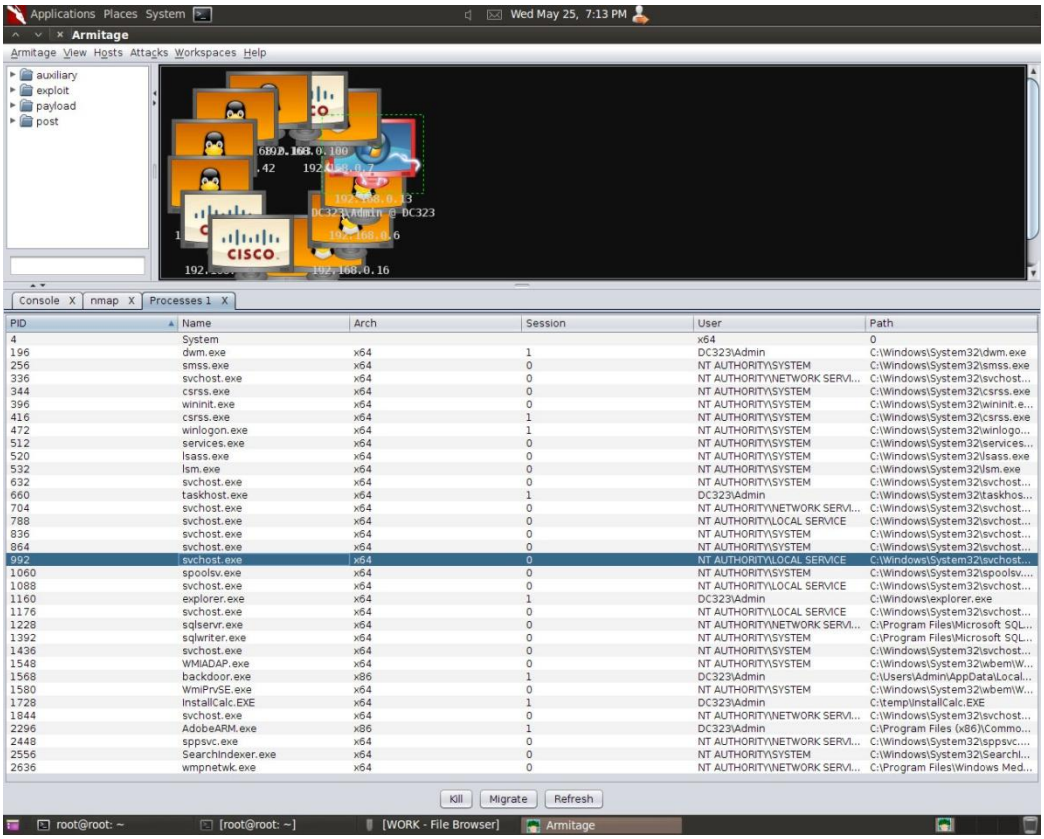
- This attack will provide access to all of the password hashes on the victim machine. These can be used to obtain the passwords using a password cracker, or we can use captured hashes to authenticate to other hosts on the same Windows domain.

- Since we need administrative privileges to dump hashes on a Windows host, we will need to escalate our access privileges. To escalate privileges in Armitage, right-click the compromised host, and go to *Meterpreter1->Access->Escalate Privileges*.

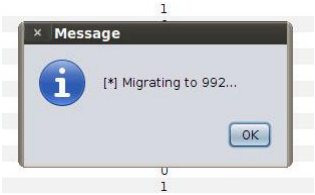
- Metasploit will try several Windows privilege escalation techniques. A dialog will indicate whether or not the process succeeded:



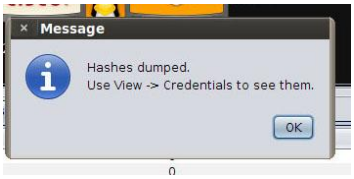
- The next step is to migrate the backdoor process on the victim machine to another system-owned process:



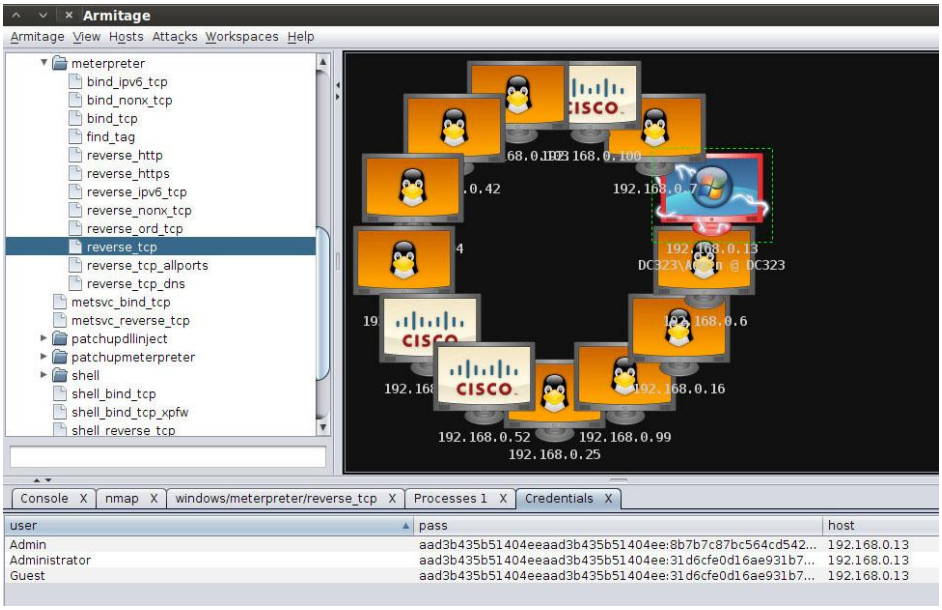
- Once we click “Migrate”, a dialog will indicate whether or not the process succeeded:



- We can now right-click the compromised host, go to *Meterpreter1->Access->Dump Hashes*. Meterpreter will dump the password hashes and store them in Metasploit’s credentials database.

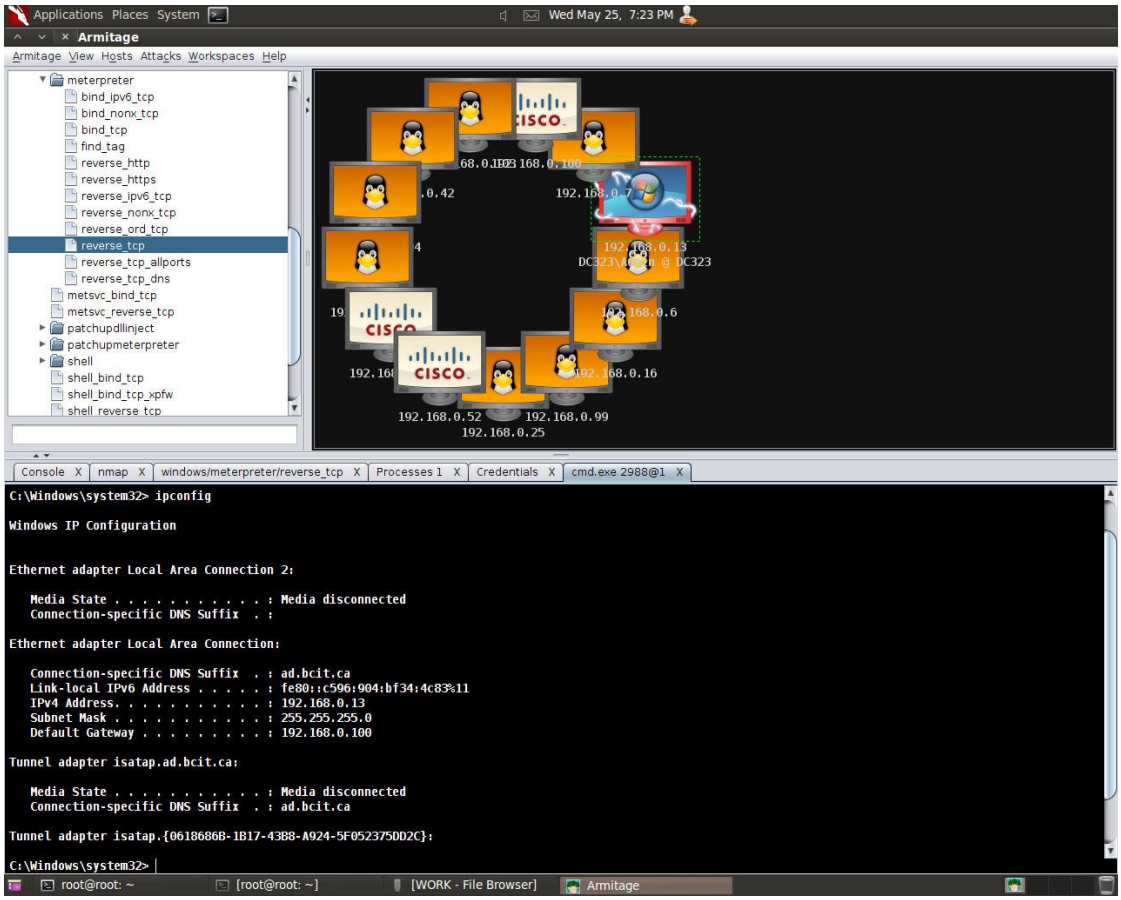


- Go to *View->Credentials* to view the contents of this database:



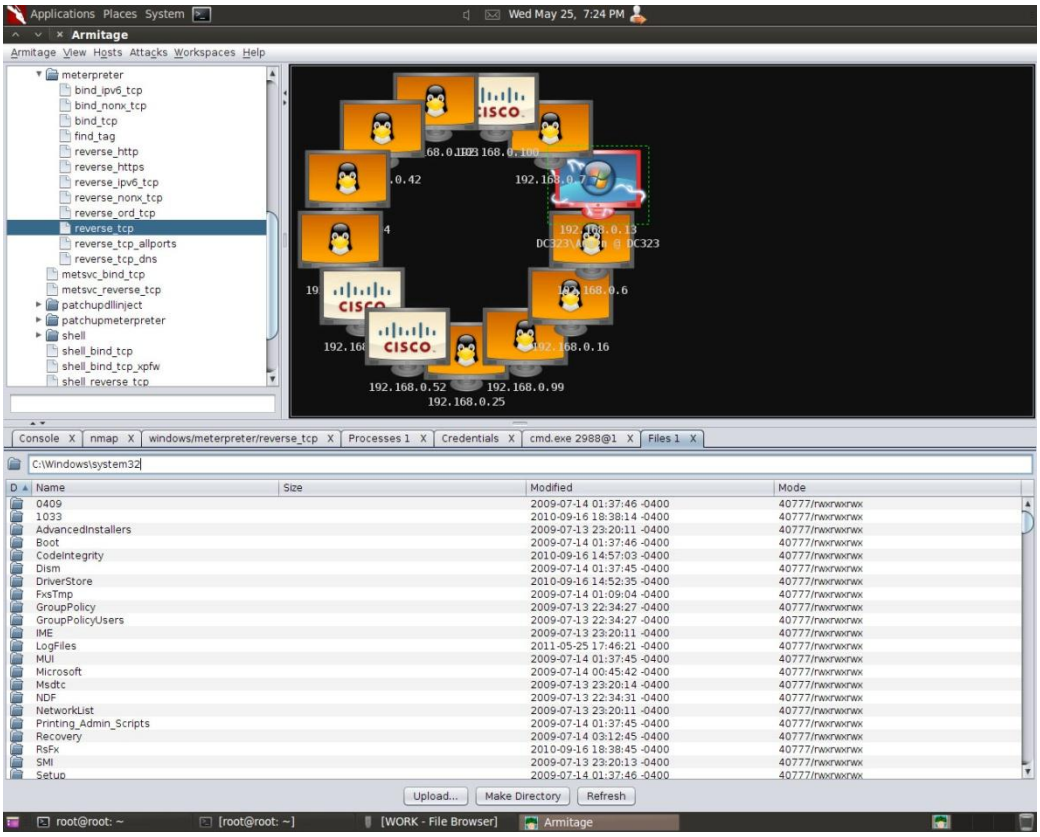
Getting a Command Shell

- We can get a command shell on the victim machine by going to: *Meterpreter1->Interact->Command Shell*.



Browsing the Remote Filesystem

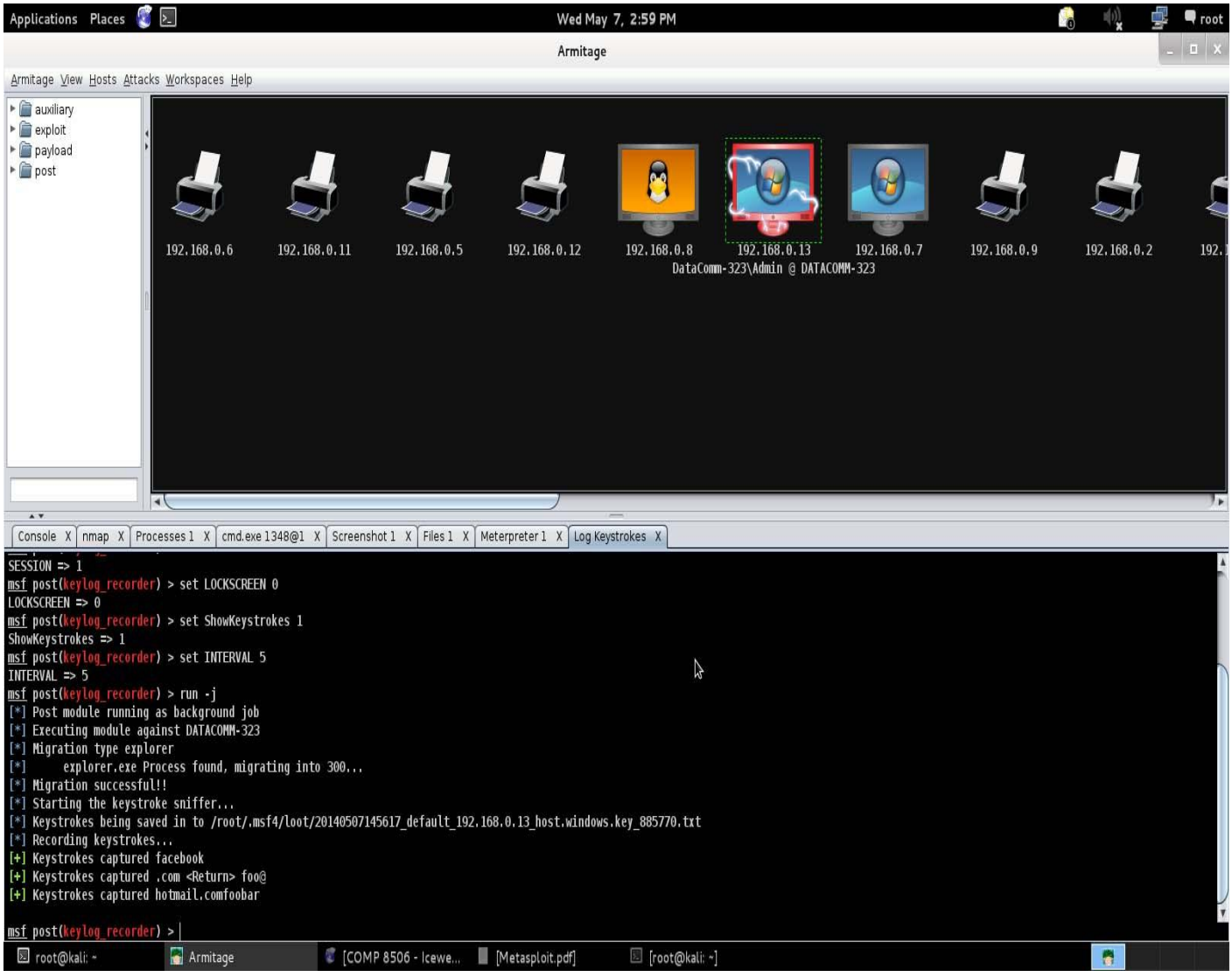
- We browse the filesystem on the victim machine by going to:
  Meterpreter1->Interact->Browse Files



Activating a Keylogger on the compromised machine

- We start a keylogger process on the remote machine which will capture any keystrokes entered by a user and send them over to our system.

- The keylogger is activated by going to:
  Meterpreter1->Explore->Keylogger



Social Engineering the Backdoor

- This attack hinges on getting the target machine to execute our backdoor payload. A clever (and stealthy) way to accomplish this is to combine Meterpreter with another useful, legitimate program so that it gets executed when a user runs the combined application.

- One technique to combine two programs is to use IExpress 2.0 from Microsoft. IExpress 2.0 combines multiple programs into a self-extracting and self-running executable.

- The combined programs stealthily run in sequence. We simply run "ixpress" from the run menu and follow the instructions. For the purposes of this example we will combine the backdoor with "calc.exe".

- We will go through some of the key settings. We want to make sure that it extracts and runs automatically:

- Next we give it a useful and legitimate name:

- Best to run it with no prompt (after all they chose to execute it):

- Next we add the two executables to the package:

- The next step is important. What we want to have happen is to have “calc.exe” run first and then when it exits, “backdoor.exe” will run in the background. This is accomplished as follows:

- Next we want to make sure that all of our activities run in “hidden mode”:

- No need to restart:

- Don’t save anything:

- Finally create the package:

- Now when the use executes “SuperCalc.exe” they will see the calculator application and when they exit from that application, our “backdoor.exe” will execute in the background and connect back to the attacking machine.

Caveat Emptor

- Note that the program output by IExpress 2.0 has its own icon. This is obviously very suspicious to any observant user so it must be changed. A useful application to do just that is the IcoFx icon editor, which can be used to replace the icon.

- The “backdoor.exe” will be visible in the process list. Obviously names such as “backdoor.exe” are to be avoided. A good process name would be something like “svchost.exe” or some other such Windows process name.