Get in through the backdoor:

Post exploitation with Armitage

IT professionals have a dated image of hacking. Many picture the process as running nmap, finding an exploit, and running it to compromise a server.

What you will learn…

- How to attack a network without a memory-corruption exploit
- Tricks to seize internal hosts and keep your network access
- Ways to use the powerful Armitage user interface with Metasploit

What you should know…

- Basic Metasploit use

This romantic scenario was alive around 2003, but it has since gone out of style. Patch management, secure software development, and other good practices have changed the game. Rather than attacking services, the easiest way in to a network is usually through the users.

Using Armitage [1], this article will show you tactics used to break the security of modern organizations. You'll learn how to bypass the perimeter defenses through a social engineering attack. We'll then cover how to use this foothold to pivot through the network and take over more hosts. More over, we will not use a single memory corruption exploit. Does this sound like fun? Keep reading.

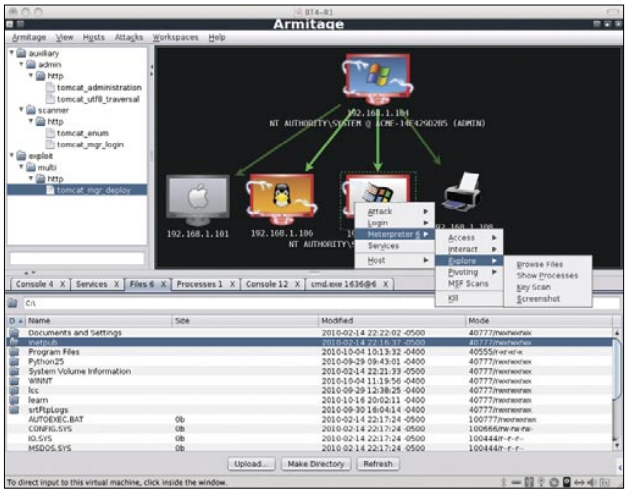

Figure 1. *Armitage User Interface*

Armitage

Armitage is a new interface for Metasploit [2]. Metasploit, as you know, is the popular open source exploitation framework. Metasploit provides tight integration between scanners, evasion techniques, exploits, and payloads.

One of the most powerful Metasploit payloads is Meterpreter. Meterpreter provides post-exploitation capabilities to you. With Meterpreter: you can work with files, route connections through the current host, and dump password hashes. Meterpreter is just a payload

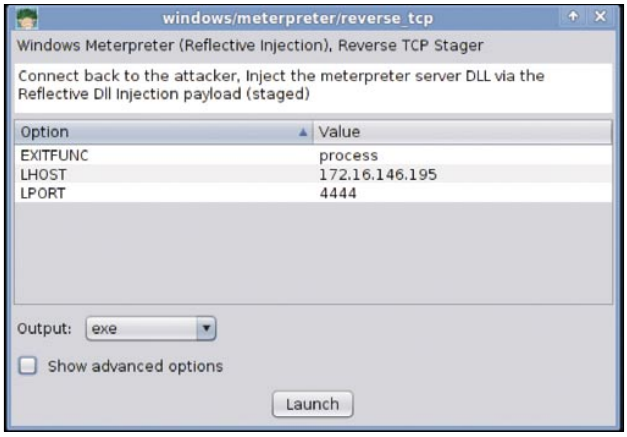

Figure 2. *Payload Generation Dialog*

though. You need to use an exploit (or clever social engineering) to get it on to a host.

Armitage is organized around the attack process. You can import hosts or scan targets through the hosts menu. You can use the *Attacks->Find Attacks* menu to get intelligent exploit recommendations based on scan data. This article won't use exploits, but know that this functionality is there. You need to know what you can do next after you get access. Armitage helps you by providing a user-interface to Meterpreter. We'll cover post-exploitation through Armitage in the rest of this article (see Figure 1).

Figure 1 shows the Armitage user interface. The top left is the module browser. Through the module browser you can access Metasploit's payloads, exploits, and auxiliary modules. The top right is the target area. Armitage displays the current hosts and any sessions you have in the target area. A compromised host appears red with lightning bolts surrounding it. The bottom is the tabs area. Armitage opens each console, browser and dialog in its own tab.

Create a Payload

Exploits are not always reliable. Why use one when your target will run your post-exploitation program for you. Let's use Armitage to create an executable of Meterpreter.

Navigate to `payloads/windows/meterpreter/reverse_tcp` in the module browser and double click it. Figure 2 shows the dialog that you will see. Double click a value to edit it. The LPORT value is the port your executable will communicate back to. Change it to something common, like 80. Select exe for the output type and click launch. Armitage will ask you where to save the executable. I like backdoor.exe.

You now have a post-exploitation program that will connect to your attack computer on port 80 when run (see Figure 2.).

Figure 3. *IExpress 2.0 from Microsoft (thanks guys!)*

If you run your program now, it will try to connect to your attack computer, fail, and close. It fails because your attack computer is not listening for a connection. Go to *Armitage->Listeners->Reverse Listeners*. Type in the port number (e.g., 80) and click Listen. You attack computer is ready to receive connection attempts from your backdoor program.

To get access to your target you will need to convince a target to run your program.

You can provide your targets with your executable as-is. Sometimes this is enough. However, users may become suspicious when the program you provide seemingly does nothing when run. If you care about being stealthy, you may want to add Meterpreter to another program.

Create a Backdoor

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 silently run in sequence. Figure 3 shows IExpress 2.0 after you first run it. Part of hacking is repurposing legitimate functionality for your nefarious purposes. This is a great example of that.

You can abuse this tool to add Meterpreter to any program you choose. I first read about this technique on Mubix's blog [3] (see Figure 3).

To run IExpress 2.0, go to *Start->Run in Windows*, and type: iexpress. Answer the questions it asks and you will have a combined program, ready to run. The program output by IExpress 2.0 has its own icon. Use the IcoFx [4] icon editor to replace this icon with the icon from the original program. Tape's blog [5] discusses how to do this.

Post Exploitation

Get your victim to run your backdoored executable. If everything works correctly you will see a red computer surrounded, as in Figure 4, by lightning bolts in the target area of Armitage.

Right-click this compromised computer and navigate to the Meterpreter menu. Each Meterpreter session will

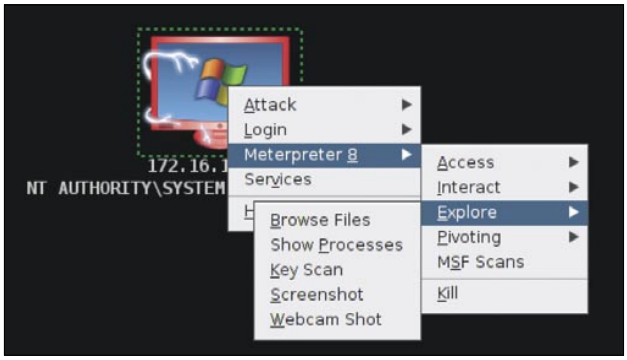

Figure 4. *Ownership Achieved*

have its own menu item. The access menu is where you will dump hashes, escalate privileges, and duplicate your access.

If possible, I recommend using this duplicate option. Armitage will upload and execute another Meterpreter instance so you have two sessions. If something happens to one of your sessions, you will still have access.

Use the interact menu to open a Windows command shell or a Meterpreter shell. Use explore 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. Armitage adds extra features to what Meterpreter already offers. For example, the webcam and screenshot can automatically refresh every 10 seconds, if you choose to activate this option.

Here we've covered some of your system level post exploitation options. Your next two concerns are compromising more hosts and persisting your access.

Pivoting

You need internal network access before you can compromise other internal osts. Metasploit has a powerful feature, called pivoting, that lets you tunnel traffic through an active Meterpreter session. To set up pivoting: right-click a compromised host, go to *Meterpreter 1->Pivoting->Add Pivot*. A dialog similar to Figure 5 will appear. Select a local network from this dialog. Armitage will tell Metasploit to route all traffic destined for that host through the existing meterpreter session. As you discover hosts, Armitage will draw a line from the pivot host to hosts that match this pivot you created.

Metasploit also includes a SOCKS proxy server. Any tools that you configure to use this proxy server will have their traffic routed based on the pivots you've set up. The Metasploit proxy server module allows you to use your web browser to browse other hosts on the network you've compromised. Go to *Armitage->SOCKS Proxy* and click Launch to activate the proxy server.

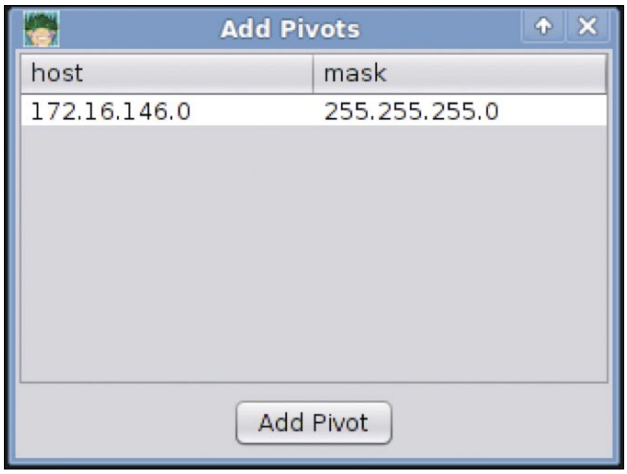

Figure 5. *Set up pivoting*

Discovery Scans

Now you have access the internal network of your victim. You should scan and see what is there. Metasploit has many auxiliary modules to identify services and fingerprint hosts. Go to *Hosts->MSF Scans* and enter the address of the network you want to scan. Armitage will launch 19 discovery modules and record its findings in the Metasploit database. New hosts will show up in the target area as they're discovered. These scans will take advantage of the pivoting you have set up (see Figure 6).

Attack: Pass the Hash

Now that you have discovered hosts on the internal network, it's time to attack them. When you login to a Windows host, your password is hashed and compared to a stored hash of your password. When they match, you're able to login. When you attempt to access a resource on the same Windows domain, this stored hash is sent to the other host and used to authenticate you. You can use captured hashes to authenticate to other hosts on the same Windows domain. This is a pass-the-hash attack.

You need administrative privileges to dump hashes on a Windows host. To escalate privileges in Armitage, right-click the compromised host, and go to *Meterpreter N->Access->Escalate Privileges*. Metasploit will try several Windows privilege escalation techniques. A dialog will tell you the process succeeded or failed.

Right-click the compromised host, go to *Meterpreter N->Access->Dump Hashes*. Meterpreter will dump the password hashes and store them in Metasploit's credentials database. Go to *View->Credentials* to see the contents of this database.

Click *Attacks->Find Attacks->by port* and wait. A dialog will tell you the attack analysis is complete. The discovery

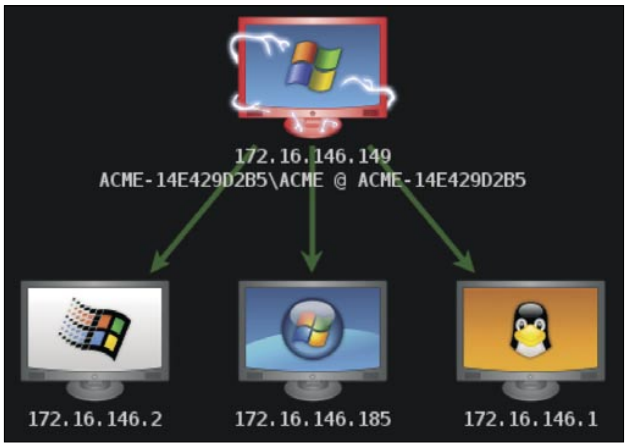

Figure 6. *Host discovery with pivoting*

scans you executed gave Metasploit and Armitage information used to recommend these attacks.

Right-click a Windows host and go to *Attack->smb->pass the hash*. Select a username and password (or hash) to login to that host with (see Figure 7). Highlight several hosts to try this attack on all of them. You will see the iconic red computer with lightning bolts if your attack is successful.

Attack: Launching an Exploit

If you do not get administrative privileges on your first host, all is not lost. Look for a Windows XP host or Windows Server 2003 among your targets. There are usually a few of these hosts on a large network.

Highlight these Windows hosts in the target area. Search for `ms08_067` in the module browser. Double click the module name and click launch. If this exploit is successful, you'll have administrative access to the host. This will allow you to follow the pass-the-hash steps to access the patched hosts. I said we wouldn't use exploits in this article. My apologies, I couldn't help myself.

Persistence

Now that you've compromised the network and gained access to more hosts, it's time to persist your access. Persistence assures your access to the network in the future. If you're evil, you will persist on a host other than your initial access host. This will make it harder to discover how you're getting back into the network.

Let's persist your access using a backdoor. Right-click a compromised host and select *Meterpreter N->Explore->Browse Files*. You will now see a tab, similar to Figure 8, that lets you navigate the local file system, upload files, and download files.

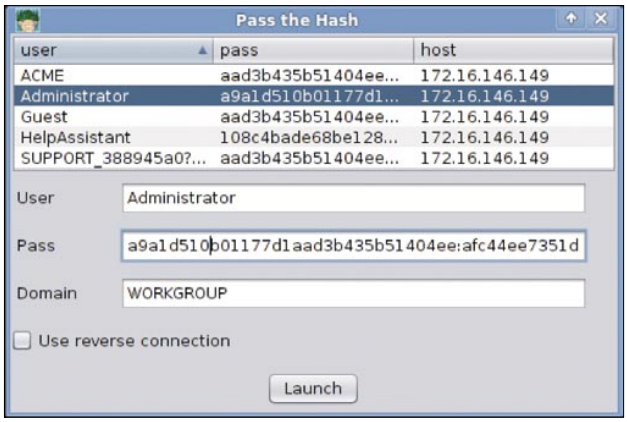

Figure 7. *Pass the Hash*

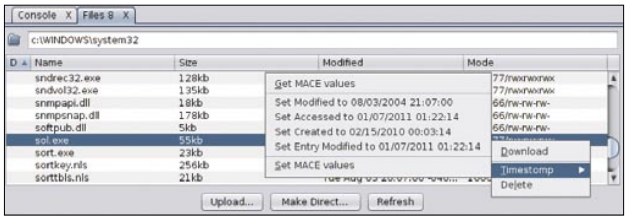

Figure 8. *The File Browser*

On The 'Net

- Armitage Project, *http://www.fastandeasyhacking.com/*
- Metasploit Project, *http://www.metasploit.com/*
- Metasploit Heart's Microsoft. *http://www.room362.com/blog/2009/3/2/metasploit-hearts-microsoft.html.*
- IcoFX, *http://icofx.ro*
- Creating an executable with Metasploit and gaining access to target PC. *http://adaywithtape.blogspot.com/2010/05/creating-backdoored-exe-with-metasploit.html*

Navigate to an executable that the user is likely to use. Right-click the executable and select Download to save it locally. Use IExpress 2.0 to add your Meterpreter executable to the downloaded program.

In the file browser, right-click the program you want to replace and select *Timestomp->Get MACE* values. This will save the file's current access, modified, and creation times to Armitage. Right-click the program and choose Delete to delete the file. Now use the Upload button to upload your backdoored version of the program. Right-click the uploaded file and select *Timestomp->Set MACE* values. This will set the access, modified, and creation time values of the file to what you saved a moment ago.

You have now replaced the original program with a backdoored version and updated the time/date information to match the original file. To the user, the program will function as normal. When they close it, they will give you a connection to their machine through your backdoor.

Conclusion

This article explored the hacking process without exploits. You saw how to get a foothold in a network with a social engineering attack. From there, you set up a pivot and executed the attack process anew. You discovered hosts, executed a pass-the hash attack, and established persistent access to the network. Armitage provided you an interface organized around these tasks.

I recommend staging target virtual machines and trying these techniques on your own. Reproduce the steps from this article to gain a greater awareness of how attackers think. It is my hope that you will reflect on your defensive posture and develop ideas to improve it. Good luck and happy hacking.

RAPHAEL MUDGE

Raphael is a Washington, DC based security engineer. He is also the developer of Armitage. You may contact him at http://www.hick.org/~raffi/