Pivoting and Tor lab

1 Lab Overview

This lab will show why having the source IP of a network attack doesn’t mean all that much, as attackers can leverage other compromised machines, or services such as Tor, to complicate tracking efforts.

1.1 Summaries: Pivot and Tor

Attack Summary  Attacker will scan the network, and attack the only vulnerable machine they can see. After successful exploitation, Attacker will pivot through the compromised machine, and attempt to compromise any other machines now accessible.

Tor Summary  Students will install Tor and browse specified websites anonymously, noting that from the perspective of the server’s browser, the traffic originates from a Tor exit node, as opposed to the student’s machine. We will not use Tor to attack any machines, due to legal and security issues, but the point is that attack traffic can in fact be routed through the Tor network.

2 Setup

Lab Setup is to include the virtual machines from Project 1 and Project 2, namely one SEEDUbuntu machine, one unpatched Windows XP Pro SP3 machine, and one Metasploitable2 machine.

Luckily for us, this doesn’t require too much additional setup from the previous labs. Login to the Metasploitable machine, and run the following, replacing <attacker_IP_here> with the ip address of your SEEDUbuntu machine.

```
iptables -I INPUT --src <attacker_IP_here> -j DROP
```

This command will add a rule to the firewall that will drop any packets from the attacker’s machine. Mine looked like this:

```
iptables -I INPUT --src 192.168.170.140 -j DROP
```

Now, open up the BASE interface running on the Metasploitable machine, go to “Cache and Status”, and press the “Clear Data Tables” button. This will drop all the alerts from the database. Now restart the snort service on Metasploitable, and you should be all set.

Confirm that you can ping the Metasploitable machine from the Windows XP machine, but not the SEEDUbuntu machine. SEEDUbuntu should be able to talk to the XP machine, but not the Metasploitable machine.
3  Task 1 - The Attack

3.1  Armitage

For this, we’ll be using Armitage, a very nice GUI to the Metasploit framework. Please read through http://fastandeasyhacking.com/manual and http://fastandeasyhacking.com/start and fire up armitage by typing (as root): armitage

Keep in mind that the second link, above, covers getting armitage running correctly.

3.2  Ops

Once you have Armitage running, go to the top-left menu and select Hosts → Nmap scan → Quick scan (OS Detect). A dialog will pop up, asking for the network to scan. Enter the /24 network that has all of the virtual machines. Armitage will launch an nmap scan, and the results will display as graphics for each host. You should see your own attacker’s machine and the XP machine, but not the Metasploitable machine.

Open up BASE: you can see the scan from the attacker’s machine, right?

Go back to Armitage: We’re going to attack the XP machine with the MS08-067 NetAPI exploit. Go to the top-left menu, “select attacks”, and choose “find attacks”. Wait for the “Analysis Complete” message. Now, right click the Windows XP machine, go to attack, smb, ms08_067_netapi. A dialog box will pop up detailing different options for the netapi module. Everything should be filled out for a successful attack, so just click Launch. If it works, the Windows graphic should have lightning bolts around it.

Pivoting  Once you’ve successfully exploited the XP box, right click it, select meterpreter l - pivoting - setup

Confirm that the subnet is the correct one (i.e. the same one that has all the virtual machines, including the Metasploitable box), and continue. Now run another scan (Try the top-menu’s Hosts - MSF scans option) and scan the same range as before. Now, you should see the Metasploitable machine.

Check BASE again. Where’s the latest scan from?

Now “find attacks” again, and use the ”distc_exec” exploit to attack Metasploitable, continuing to use the XP VM as a pivot. Once you have a shell, see what privileges you have - not root, sadly. Get root with the ”unreal_ircd_3281_backdoor”, and then check the BASE interface and see where all the attacks are coming from.

You’ve successfully exploited two hosts, using the first to attack the second, concealing your actual source from your final target.

4  Task 2 - Tor

This is a very short section, consisting entirely of installing Tor, and then using it to browse websites that display the IP address they think the connection originates from, such as whatsmyip.org

Follow installation directions from

https://www.torproject.org/docs/installguide.html.en
for any help.

Using a modern Ubuntu installation, in a Virtual Machine or otherwise, install Tor ( `apt-get install tor` ), and then direct your browser to use 127.0.0.1:9050 as a socks v5 proxy. Any traffic directed towards that proxy should go through the Tor network, so visit whatismyip.org or a similar website, and confirm that the IP shown is not your publicly routable IP address ( if you’re at UMass Lowell, that means it shouldn’t be in the 129.63.0.0/16 net). If it worked, you’re done.

**Document the ip address shown by whatismyip.org and explains why.**