CYBER STORM

CHAMAELEON CHEAT SHEET

**Starting Up –**

1. Plug in server
2. Hold down UPS Power until it beeps
3. Turn on server
4. Ctrl-Alt-T to bring up terminal
5. ifconfig to get Ethernet device
   1. There should be two: enp0sf0 and enp0sf1. The f0 one is routed to the VM
6. sudo ifconfig $eth down
7. sudo ifconfig $eth 10.5.5.12 up
8. We should now be able to plug in our laptops to the Ethernet port to connect
   1. MAKE SURE YOU DO NOT HAVE YOUR WIFI CHIP ON WHEN YOU SSH!
9. Make sure you are routing your Ethernet device through if you are using a VM
10. Drop your own Ethernet devices and bring them back up to the 10.5.5.x family
11. One person needs to ssh –XC [chamaeleon@10.5.5.12](mailto:chamaeleon@10.5.5.12)
    1. xpra start :11
    2. xpra attach :11
    3. ctrl-alt-t
    4. DISPLAY=:11 screen
    5. virtualbox
    6. start chamVM
    7. ifconfig chamVM to 10.5.5.10
12. Everybody else ssh [chamvm@10.5.5.10](mailto:chamvm@10.5.5.10)
13. Keep off the host unless necessary

**Playing With Files**

1. Pulling from an FTP server
   1. ftp 10.5.5.10
   2. get filename.ext
   3. This puts the file on your local machine (where you were when you first made the ftp command
2. Copying with ssh
   1. Note when you ssh to a server, scp views the server as the local machine
   2. scp [from] [to]
   3. scp [pi@192.168.2.2:~/remote.txt local.txt](mailto:pi@192.168.2.2:~/remote.txt%20local.txt) - Pulling
   4. scp local.txt [pi@192.168.2.2:~/remote.txt](mailto:pi@192.168.2.2:~/remote.txt) - Pushing
3. From VM to Host (and vice versa)
   1. Go to Devices at the top of your running virtual machine
   2. Select Shared Folders
   3. Click the folder with a green plus on it
   4. Browse for the folder on your host OS you want to be visible from the VM
   5. Name the folder something appropriate
   6. Check auto-mount and make permanent
   7. You should now have a folder in /media/ that is shared between host and guest
   8. Whatever files you place in it will be visible from both

**Useful Commands**

**Python**

1. ''.join('{0:08b}'.format(x, 'b') for x in bytearray(byte)
   1. Make a binary string of length 8 from a character byte
2. int('100101',2)
   1. Convert a binary string to an integer
3. ord('A')
   1. Converts a byte to it's ASCII map

**Bash**

1. cp –r ./folder1 ./folder2
   1. Recursively copy folder1 to folder2
2. touch file.txt
   1. Create a file named file.txt
3. mkdir folder
   1. Creates a new directory named folder
4. rm –r folder
   1. removes a folder recursively
5. nmap 192.168.2.0/24
   1. Find out what IPs have what services running on the 192.168.2.0/24 family
6. sudo netstat –alpn | grep ‘ LISTEN ‘
   1. Get what services we are running

**VIM**

1. i
   1. insert mode
2. esc
   1. command mode
3. :wq
   1. Write and quit
4. /stringtofind
   1. Find all occurences of stringtofind in file
5. dd
   1. delete a line

**FTP**

1. Config file is located at /etc/vsftpd.conf
2. Change the listen port (default port 21)
   1. Add the line listen\_port=2121
3. Allow anonymous logins
   1. anonymous\_enable=YES
   2. anon\_root=/home/ftp
   3. Make sure you sudo chmod a+r,a+x /home/ftp
4. Restart
   1. sudo service vsftpd restart

**HTTP**

1. Server files are located at sudo vim /var/www/index.html
2. Changing ports:
   1. sudo vim /etc/apache2/ports.conf
      1. Change the line Listen 80
   2. sudo vim /etc/apache2/sites-enabled/000-default.conf
      1. change the following line to match the new port: <VirtualHost \*:80>
   3. sudo service apache2 restart

**MySQL**

1. Changing Ports
   1. sudo vim /etc/mysql/my.cnf
   2. find the [client] section and change the port
      1. port = 3306
   3. find the [mysqld] section and change the port
      1. port = 3306
   4. sudo service mysql restart
2. Root login: mysql -uroot –p
3. Make a new user:
   1. CREATE user 'dude'@'%' IDENTIFIED BY 'password';
4. Make a new database:
   1. CREATE DATABASE test;
5. KEEP TRACK OF DATABASE TAG! MY SCRIPT DOES NOT CHECK IT!

**Misc Scripts**

1. Hack.sh
   1. This is intended to be used as a bait. Ignore all the comments inside. Our goal is to get another team to run the script with super user privileges. The script changes the root password and creates a user cyber2 that we can ssh into their server with. The password for both the user and the new root is “new\_password”. If I get a minute tomorrow, I will make a script that runs through our opponent’s servers and tries to ssh into them. Even if we do not get to ssh into their servers, changing the root password is really annoying, and they will probably need to reboot to change it.
   2. To use it, rename it to something innocuous (like newchallenge.sh) and place it in a vulnerable location with a readme specifying its usage.
2. file\_dif.sh
   1. Looks for our configuration files and replaces them with ones from a backup folder if it finds a difference. This is useful if we get hacked.