Welcome to IASA - Area 51 Raid Day

Don’t forget to sign in! 👾👽👾

Agenda for tonight 

1. Quick intro to Google Cloud
2. Get y’all logged into GCloud
3. Quick information on how we provisioned the boxes
4. Linux 101 and hardening fun

Google Cloud

- **Description**
  - Google Cloud Platform, offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube
- Sounds intimidating, but it really isn't
  - cloud.google.com
- Log in with your @emich.edu emails for ***free money***, hype.

Terraform 👽

- We created these boxes with Terraform
- Easy to pick up, hard to master
- Check out our code on GitHub!
  - Make suggestions 🙂

Linux Fun  - Getting Started

- **Remember your box number!** We are going to use them again
- SANS
  - https://www.sans.org/media/score/checklists/LinuxCheatsheet_2.pdf
- Set a Root password:
  - `sudo passwd root`

Linux Fun  - Getting Started

- Fix Google SSH timeout issue:
  - **sudo vim /etc/ssh/ssh_config**
  - Go all the way to the bottom
  - **sudo systemctl restart ssh**
  - **sudo systemctl restart sshd**

```
# Google Compute Engine times out connections after 10 minutes of inactivity.
# Keep alive ssh connections by sending a packet every 2 minutes.
ServerAliveInterval 120
```

⟵ This is the seconds before timeout

Linux Fun  - Quick updates

- Update your VM part 1
  - `sudo apt-get update`
  - This checks all of the installed packages on your VM against the current most updated repository version
  - This **DOES NOT** download updates
- Update your VM part 2
  - `sudo apt-get upgrade`
  - This will **actually download** and **apply** the updates to your VM
- Update your VM part 3
  - `sudo apt autoremove`
  - `Removes unneeded packages`

Linux Fun  - Basic commands

- `cd`
  - Change directory
- `ls`
  - List
- `touch`
  - Creates a file
- `mv, cp, rm`
  - Move, copy, remove
- `vim / vi`
  - Text editor we use often

Linux Fun  - Hotkeys to save your life

- Tab
  - Complete all the things
- Control + C
  - Kill running task
- Control + Z
  - Suspend a task in the background. Resume it by typing `%X`
  - Where X is the number it displayed when you hit CTRL + Z
- Control + A
  - Move cursor to the start of the line
- Control + E
  - Move cursor to the end of the line

Linux Fun  - Diagnostics

- `Netstat`
  - Our best friend
    - Even though its slowly going away 💔
- Extremely versatile tool for showing you what is connected
  - There are other tools, such as iftop, but netstat is installed on ***most*** Linux distros by default
- `top / htop`
  - CPU and Memory monitoring tool
  - Top is usually installed by default, `htop` is a more visual and verbose version of `top`
- `who / w`
  - Who is logged into your device 🤔

Linux Fun  - Quick Filesystem Setup

- First things first - Let's disable IPv6
- `sudo vim /etc/sysctl.conf`
  - `net.ipv6.conf.all.disable_ipv6 = 1`
  - `net.ipv6.conf.default.disable_ipv6 = 1`
  - `net.ipv6.conf.lo.disable_ipv6 = 1`
- `sudo sysctl -p`
  - This will reload the running config so your changes take effect
- Verify!
  - `cat /proc/sys/net/ipv6/conf/all/disable_ipv6`
  - If it returns 1, you're good

Linux Fun  - Quick Filesystem Setup

- `sudo apt install vsftpd`
- Config time!
  - `sudo vim /etc/vsftpd.conf`
  - `listen=YES`
  - `listen_ipv6=NO`
  - `listen_address=0.0.0.0`
  - `listen_port=21`
  - `anonymous_enable=YES`
- During installation a ftp user is created with a home directory of /srv/ftp. This is the default FTP directory.

Linux Fun  - Quick Filesystem Setup

- Start service and Verify!
  - `sudo systemctl restart vsftpd`
  - `sudo systemctl status vsftpd`

Linux Fun  - Quick Filesystem Setup

- You should see something like this:

```
root@chris-box-o-fun:~# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; vendor preset: enabled)
   Active: active (running) since Fri 2019-09-20 18:34:26 UTC; 4s ago
  Process: 2789 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
 Main PID: 2790 (vsftpd)
    Tasks: 1 (limit: 1999)
   CGroup: /system.slice/vsftpd.service
           └─2790 /usr/sbin/vsftpd /etc/vsftpd.conf

Sep 20 18:34:26 chris-box-o-fun systemd[1]: Starting vsftpd FTP server...
Sep 20 18:34:26 chris-box-o-fun systemd[1]: Started vsftpd FTP server.
```

Linux Fun  - Quick Filesystem Setup

- What we have now
  - Insecure File server running on our Google Cloud VM! Hype
- What port is it on?
  - (Let’s pretend nobody knows what port FTP uses)

Linux Fun  - Quick Filesystem Setup

netstat -plantu | grep vsftpd

```
root@chris-box-o-fun:~# netstat -plantu | grep vsftpd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      3163/vsftpd
```

Protocol | Local Address | Foreign Address | State | PID and Process

- Please run `sudo systemctl stop vsftpd`
  - Will explain in a sec, just stopping the service temporarily

Important:

- This FTP server is **very insecure**
- Why?
  - Anonymous logins are **E N A B L E D**
    - This is bad
  - It is bound to **ALL IP addresses**
    - This means every IP address on the box will listen for the FTP server
  - It is on a standard port
    - This means the automated scripts and scrapers will find this service **Very quickly**

How to fix these issues

1. Anonymous logins are **E N A B L E D**
   a. Change `anonymous_enable=YES` to `anonymous_enable=NO`
   b. Easy
2. It is bound to ALL IP addresses
   a. Change `listen_address=0.0.0.0` to `listen_address=TheIPyouWantToUse`
3. It is on a standard port
   a. Change `listen_port=21` to `listen_port=SomeHighPort`