Getting Started

Linux, Labs and Fun

Who Am I?

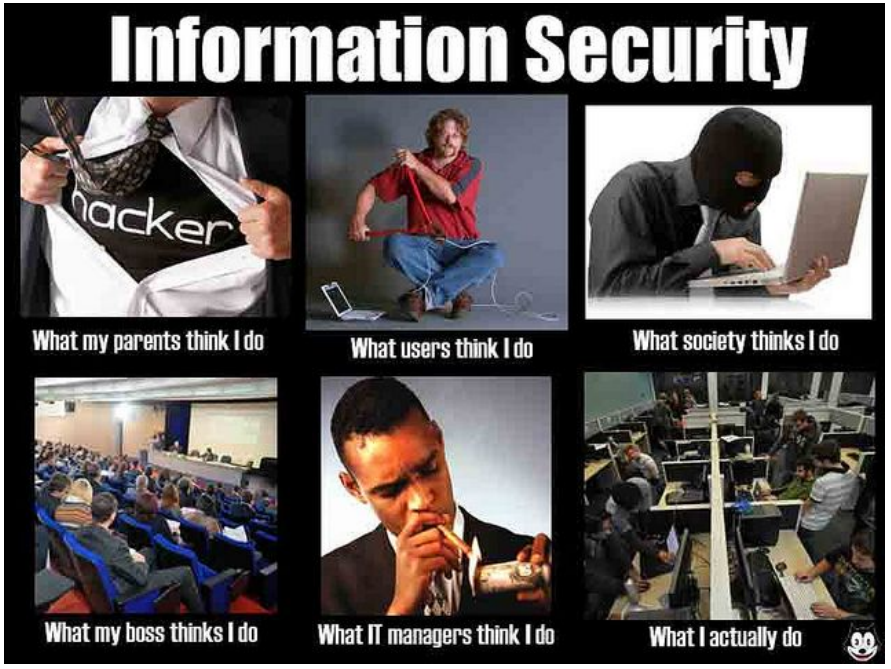
- Trevon (blackmanta)
- Graduate Student
- Linux Junky
- **MY KNOWLEDGE IS LIMITED**

Structure of Education Nights

- Small taste of a variety of topics
- Place to find interest
- Voice your opinion in #education_n_training
- Plethora of resources
- CTF challenges… **fingers crossed**

Information Security Fields

- Computer Forensics
- Malware/Reverse Engineer
- Exploitation Developer
- Incident Responder
- Secure Programmer
- Application Tester



What is Linux?

- An Open Source Operating System (Kernel)
- Powers 96.5 percent of the top one million domains in the world

What does this mean?

- Learning Linux could be useful
- It’s honestly not everything
- The is more to security than Linux

Lab Setup

We won't be using Kali :)

- Download Vmware *(Free with UNCC Account)*
  - *https://e5.onthehub.com/WebStore/Welcome.aspx?ws=8da10652-aea5-e111-9b64-f04da23e67f6*
- Download VirtualBox
  - https://www.virtualbox.org/wiki/Downloads
- Download the latest ISO of Debian
  - https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-10.1.0-amd64-netinst.iso
- Create Virtual Machine for Debian
  - https://www.howtogeek.com/196060/beginner-geek-how-to-create-and-use-virtual-machines/
- Install Debian

http://leanpub.com/avatar (Free Book about setting up Security Labs)

Guest Additions

- Why is my VM so small?
  - Virtualbox guest additions installation
    - https://kifarunix.com/install-virtualbox-guest-additions-on-debian-10-buster/
  - Vmware Workstation/Player
    - sudo apt install open-vm-tools linux-headers-$(uname -r)

Install Kali Repo’s

Repo list - https://docs.kali.org/general-use/kali-linux-sources-list-repositories

- sudo vim or nano /etc/apt/source.list
- Add the line
  - deb http://http.kali.org/kali kali-rolling main non-free contrib
- sudo apt update
- Add the key which is giving the error
  - gpg --keyserver pgpkeys.mit.edu --recv-key {KEY}
  - gpg -a --export {KEY} | sudo apt-key add -

We are only going to install the tools we need

Why?

- Light weight
- Learn to use the tools you need
- Custom VM

Windows Alternative

- Offensive Windows Image
- CommandoVM
  - https://github.com/fireeye/commando-vm
  - https://hacknews.co/tech/20190402/commando-vm-is-a-windows-based-kali-alternative-for-ethical-hacking.html

Learn Linux via Games

- OverTheWire – Bandit
  - http://overthewire.org/wargames/bandit/
- CTF 365 *(Hardcore Mode)*
  - https://ctf365.com
- Terminus
  - http://web.mit.edu/mprat/Public/web/Terminus/Web/main.html