Meeting 100

// Docker and Vulnerability Scanning //

If You’re New!

- Join our Slack: cyberatuc.slack.com
- **SIGN IN!** *(Slackbot will post the link in slack)*
- Feel free to get involved with one of our committees:

  Content Finance Public Affairs Outreach Recruitment Lab

Cyber@UC

Announcements / Upcoming Events

- 10.11 GE Aviation SOC visit
- 10.16 NSA Visit

BATTELLE + Cyber@UC

September 25th, at 6:30pm in Rhodes 850D

Information Session + Interactive Demo

Topics Covered:

- What does it mean to be a cyber professional?
- How does a non-profit exist in this field?
- The RE/VR Lifecycle: How are vulnerabilities found?
- Interactive Demo of AFL-Unicorn, one of Battelle's many open source tools.

Bring Laptops, Resumes, and Questions!
Stay after and hang out!

https://github.com/Battelle/afl-unicorn

Weekly News

Where's The Band-Aids?

- 15,000 private webcams open to exploitation
- Webcams have open ports with no authentication
- Implications:
  - stealing intellectual property
  - live feed of children home alone
  - criminals can delete/manipulate footage

https://cyware.com/news/researcher-discovers-15000-private-webcams-that-can-be-possibly-exploited-6bee4201

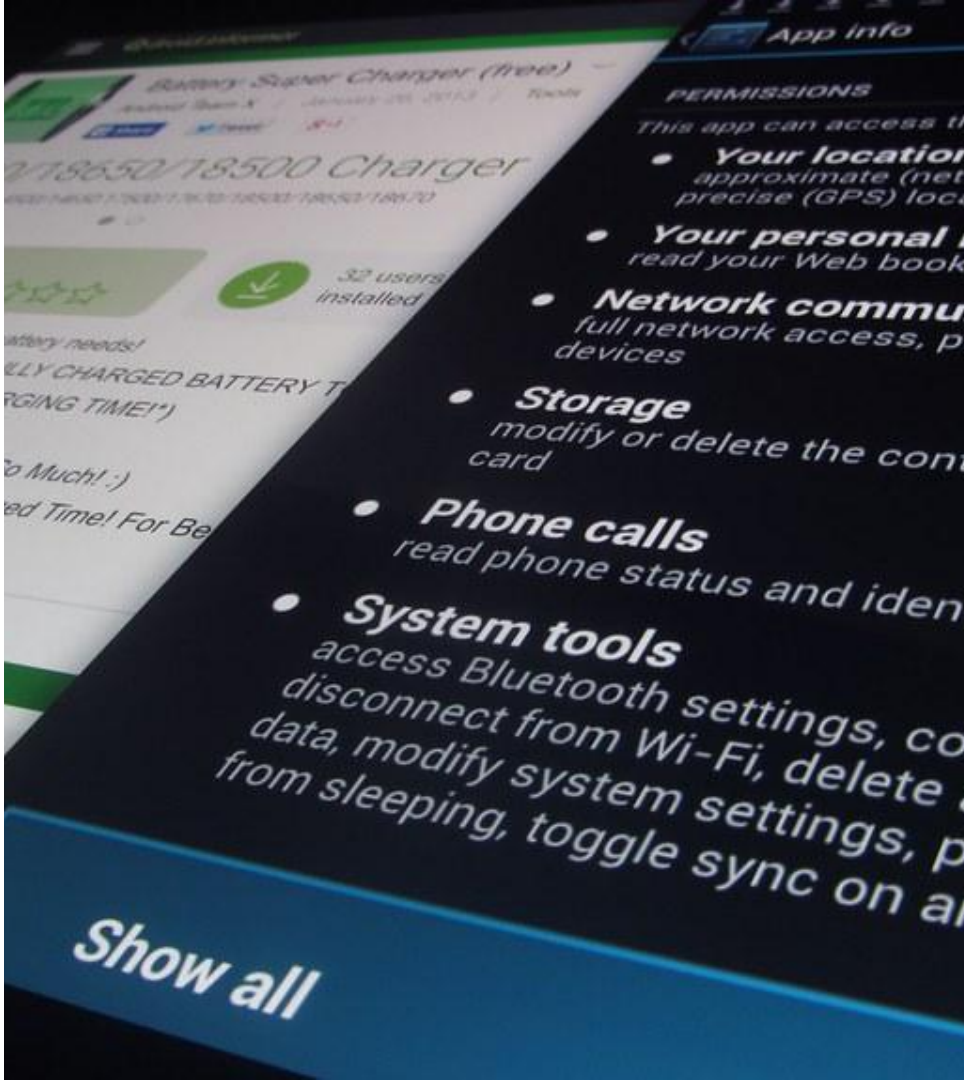
Panda Cryptomining

- Started with MassMiner in 2018
- Use web vulnerabilities to install cyptomining malware
- Updated infrastructure, payloads, and targeting
  - Pulling down “BBBBB” and execute via PowerShell
  - Uses Certutil utility to download second miner
  -
- Attack the same targets over and over

CamScanner App

- Downloaded by more than 100 million users
- Researchers at Kaspersky found malware in the app to serve users ads and snoop credentials
- App is legitimate but somehow included third party software
- Part of a sharp increase of malware infecting Google Play store apps

https://www.bbc.com/news/technology-49495767?intlink_from_url=https://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-story



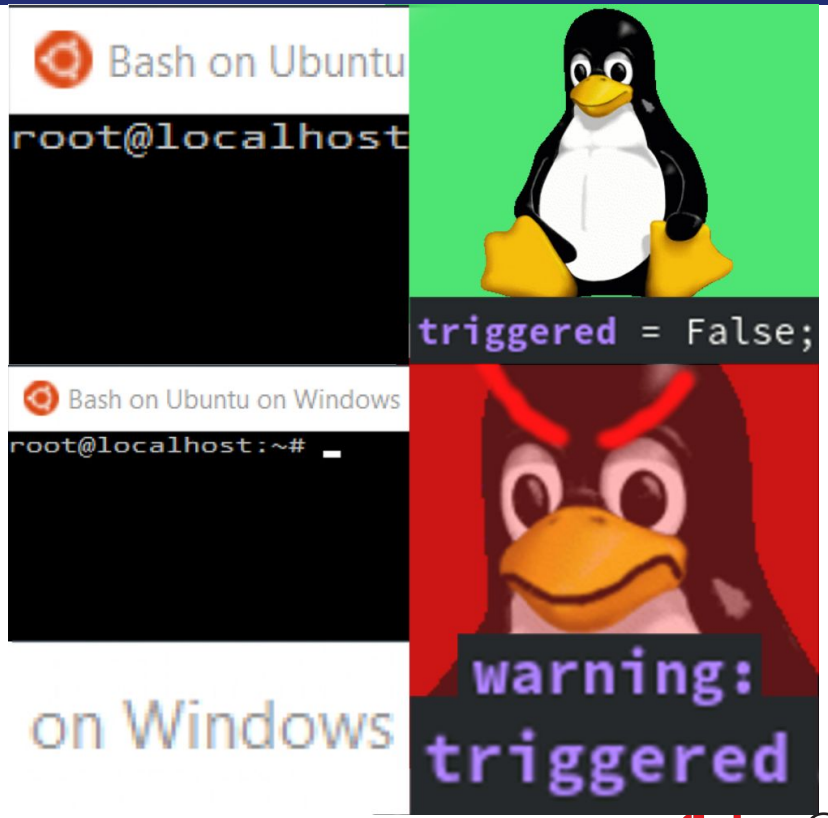
Docker and OpenVAS

Agenda

- I wasn’t here last week!
- Forewarning
- Installing docker
- What/Why/Where is this
- Playing with docker
- Docker is actually cool
- OpenVAS / Metasploit via docker

I wasn’t here last week!

- Shame on you
- Previously, we went over the core linux commands (although there’s thousands more)
- Today requires our previous Debian VM or an Ubuntu VM to work smoothly
- You can do this on Windows but it takes a way longer (on windows you have to disable WSL to use docker)



Forewarning

- Docker uses a lot of disk space if you start downloading a bunch of images
- OpenVAS and Metasploit can be used to do malicious things so don't be fucking stupid
- We do not condone using either of these tools on devices you do not own or have permission to modify
- We're going to run everything as root today so we don't have to stop and configure docker socket permissions so don't delete your whole disk on accident

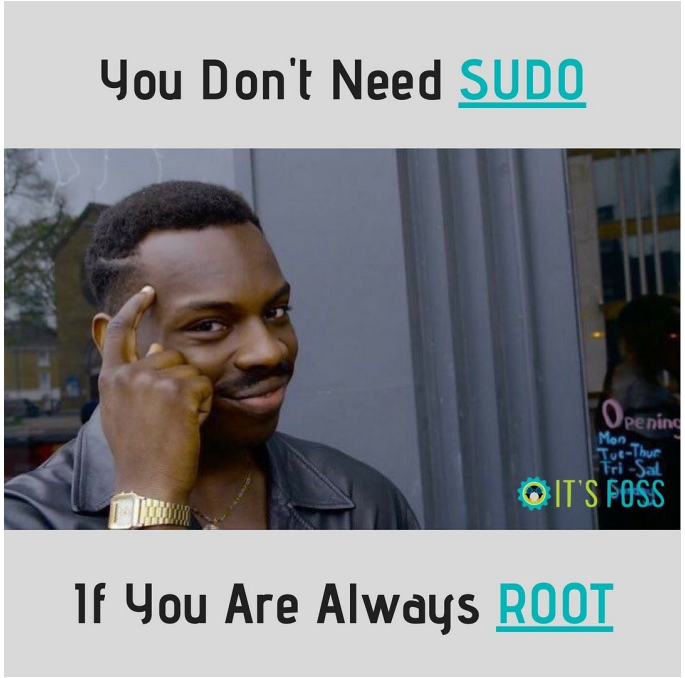
Installing Docker

Debian / Ubuntu

- **wget get.docker.com**
- **mv index.html install_docker.sh**
- **su**
- **sh install_docker.sh**

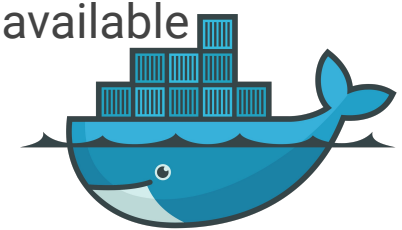
Anything else

- Details on **docker.com** but we're not going over that today because it takes a long time



What is Docker?

- Open source and commercial container engine
- Basically manages mini virtual machines called containers
  - OS-level virtualization instead of machine-level
  - That means it shares hardware with your host machine
- Docker hub is a website with a bunch of premade containers
- Containers can be declared as scripts that build themselves from other containers
  - Service deployment as source code
- Most major OS's have some containerized version available



docker

Cyber@UC

Where is Docker?

- Currently used widely in development and production environments

- Development environments (like gitlab CI) spin up a fresh image every so often and work through a series of code tests

- Google runs “billions” of containers every week to the point that they made the kubernetes system to efficiently manage a huge number

Playing with docker

- **docker run hello-world** - basic install check
- **docker search** - search for containers on docker hub
- **docker run** - start a new container
- **docker start** - start an existing container
- **docker exec** - run a command on a running container
- **`docker stop`** - stops a running container
  - Containers made with the '`--rm`' flag will be deleted when stopped
- **`docker ps -a`** — Show all containers, running or stopped

Docker is actually cool

- You now have access to 90% of interesting linux applications
- All of those can be distributed to any machines in a matter of seconds
- Anything that doesn't exist can just be dumped into a container and made into a new base image

Using the OpenVAS Container

```
docker run -d -p 443:443 --name openvas mikesplain/openvas
```

- Takes up to 5 minutes to start up the first time
  - Beats setup time for a host installation of OpenVAS (~15 minutes)
- Go to https://localhost when it's ready
- Default credentials are admin/admin
- Play around with a scan on your local device
- OpenVAS looks for known software vulnerabilities on its scan targets that could be potentially exploited

More Container info

- Kubernetes - project for efficiently controlling ridiculous amounts of containers, made by Google
- Containers can run on virtual machines
- Docker-compose is a tool/language for setting up docker containers for programmatic deployment
    - Also supports multiple containers
- Containers can X11 forwarding which means you can use them on Linux to use native graphical applications