Hack@UCF

Collegiate Cyber Defense Club

HackersofUCF.slack.com | www.HackUCF.org

Stay informed!

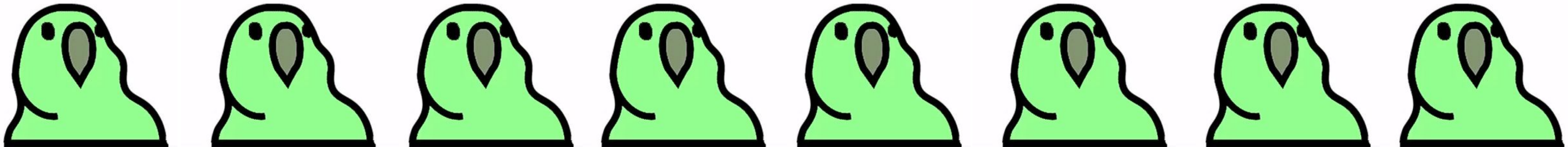
- Join our mailing list
  - https://hackucf.org/mailing-list/
- Join the CECS Slack
  - https://hackersofucf.slack.com/
  - Knights mail required
  - Once registered, chat with us in the #hackucf channel
- Twitter: @HackUCF
- Facebook
  - https://www.facebook.com/HackUCF/

Today’s Topics

- Announcements
- Current Events
- ToolTime w/ Charlton
- Michael Ibeh on Memory Forensics
- Closing

Operations

- Come help run the club!
    - Tuesdays at 8:00pm
    - LMCO Cyberlab
    - Open to anyone



CyberLab Workshops

- Blue Team Workshops
  - Cancelled Until Spring. See you then!

RITSEC CTF

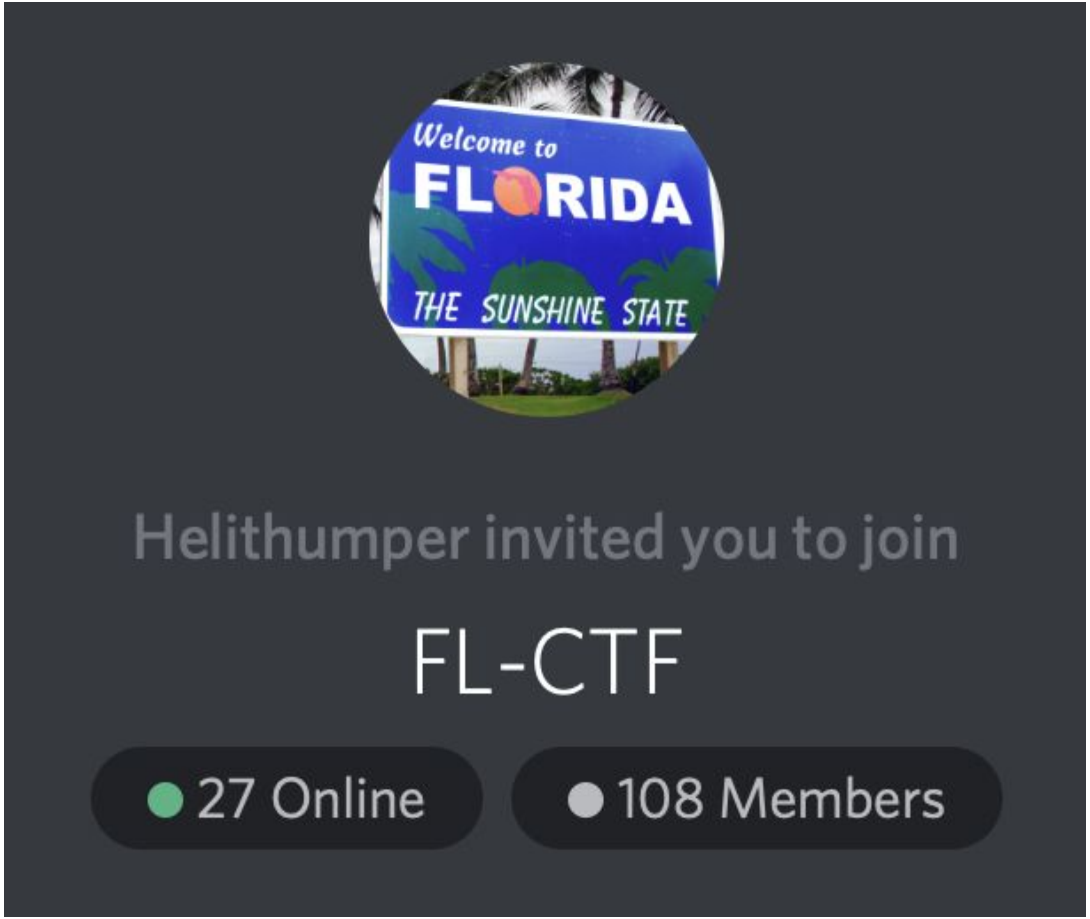
- THIS WEEKEND
- **Tonight in the Cyberlab we will be competing**
- Come learn how to do CTFs

Knightsec Discord!

- Join our Knightsec CTF Discord
- hackucf.org/discord
  - Anyone is welcome!

https://discordapp.com/invite/

pKr4cN



Helithumper invited you to join

FL-CTF

● 27 Online

● 108 Members

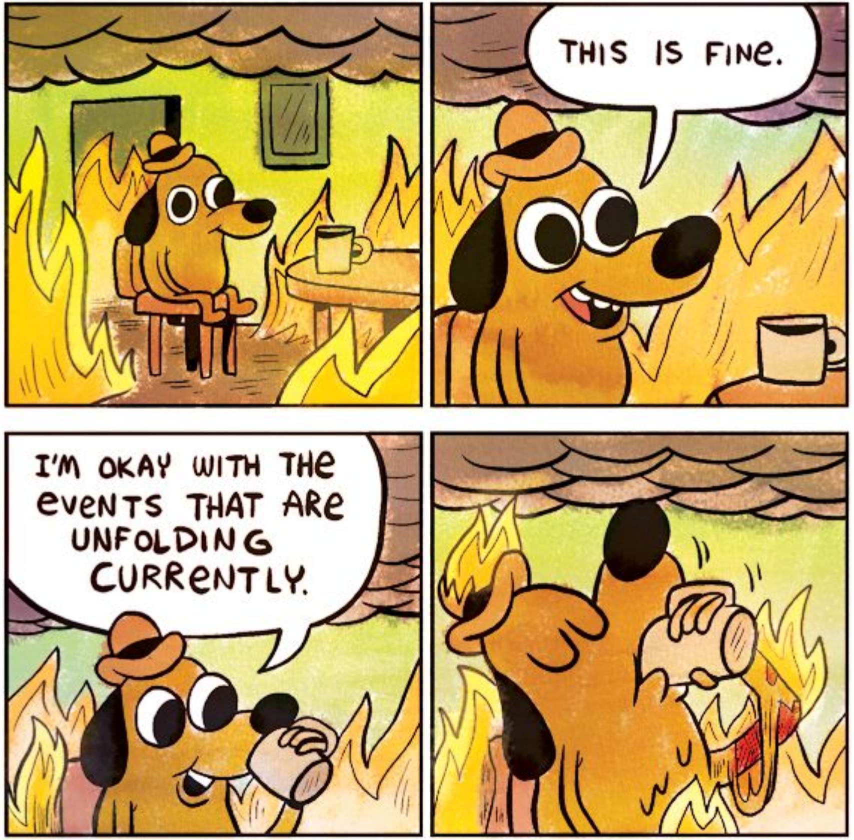
IBM Security Internship Opportunity

- https://ibm.biz/securityservicesintern2020
- Summer 2020
- Submit your own patents!
- Present to IBM Executives
- Work on **Real Security Work**
- Work in IBM's Global Security Command Center
- Message @helithumper for more info

Reliaquest Road Trip

- November 22nd
- Testing their CTF
- Free Lunch
- Sign up in Slack
- ***INFINITE*** Openings

- ***Workshops***
  - ***Redteaming***
  - ***RQ at scale***
  - ***Blueteam***



Current Events (http://gunshowcomic.com/648)

Mirantis Acquires Docker Enterprise

- Docker Enterprise acquired in deal for undisclosed price.
- Container Daddy *Docker ENTERPRISE* estimated value over $1B
- Mirantis is a Kubernetes-as-a-service and certs for Kubernetes

In wild Windows RCE

- Bug in M$ scripting engine allowed users to gain the rights of any user logged in.
- Abused through IE if victim visits malicious web page.
- Patch included in security rollup for the month

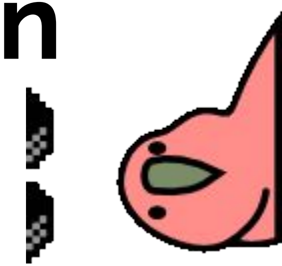
Google Health Hijinx

- Whistleblower announced google holding health data.
- Depart. Health and Human services did not know and are investigating legality
- Reminder Google Acquired *FITBIT* less than a month ago.

fitbit.

McAfee Announces new token

- McAfee Announces goal to release “*Epstein Didn’t Kill Himself*” Token
- *WACKD* is Ethereum-based and is now on McAfee’s Decentralized Crypto exchange.

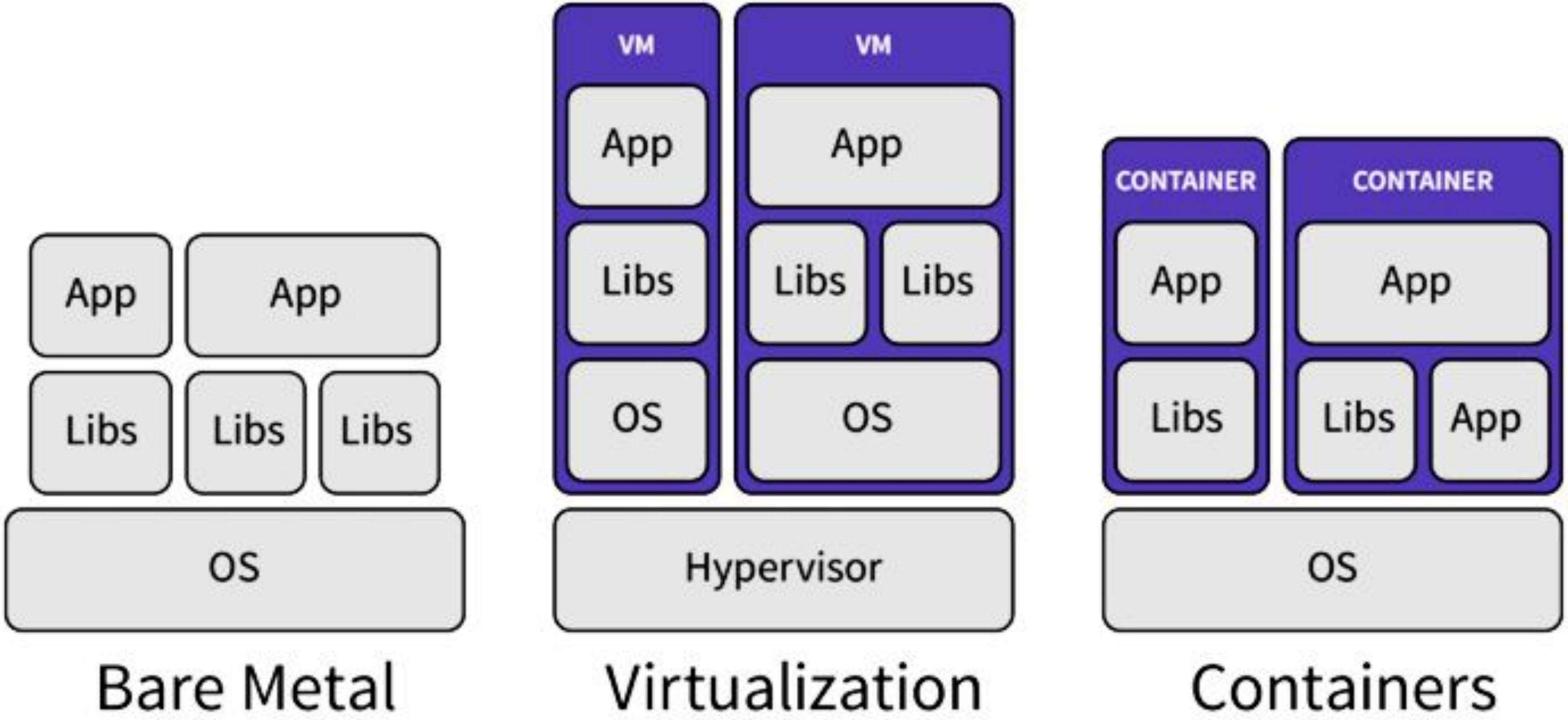


Tool Time is back!

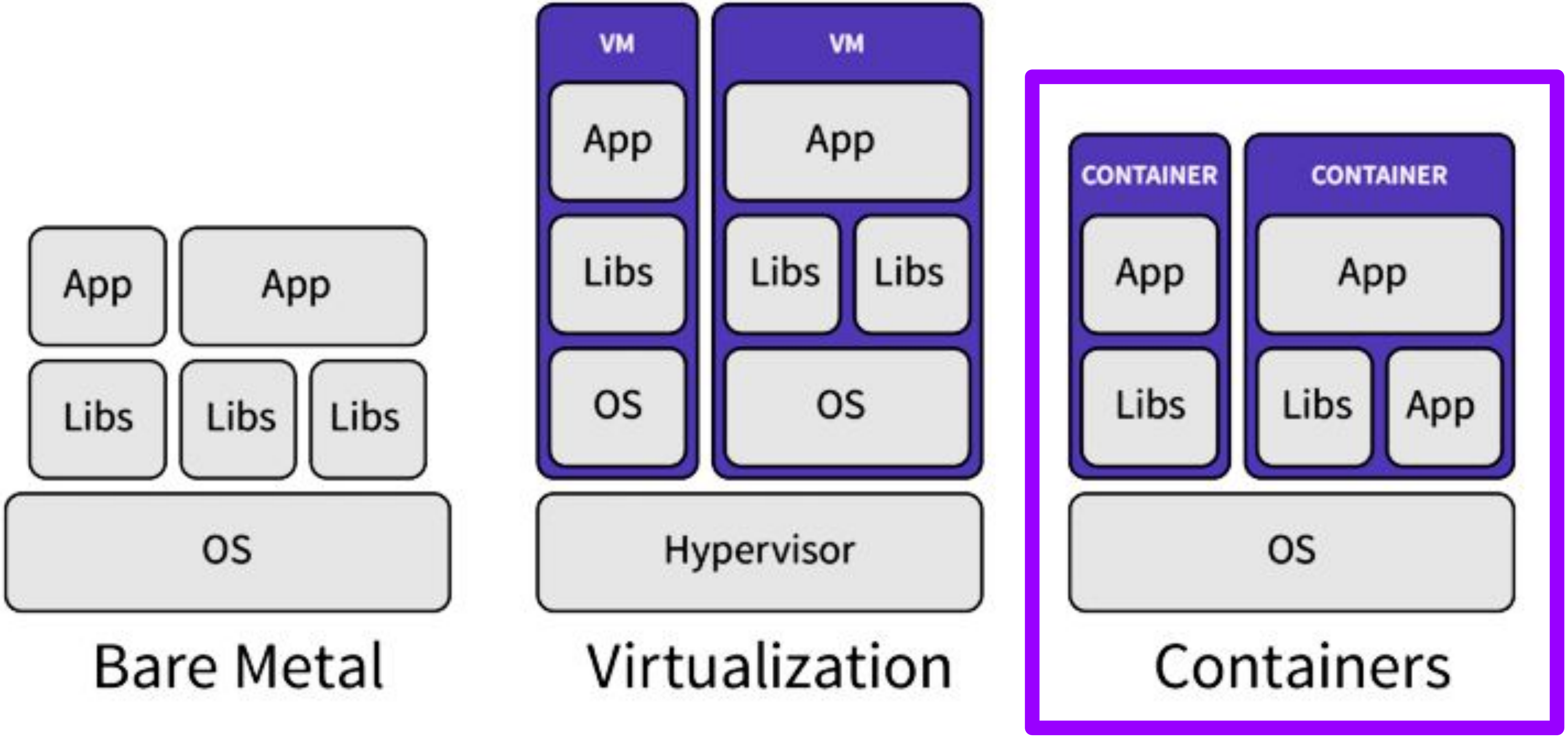
This week we will be going over…

LXD

VIRTUALIZATION

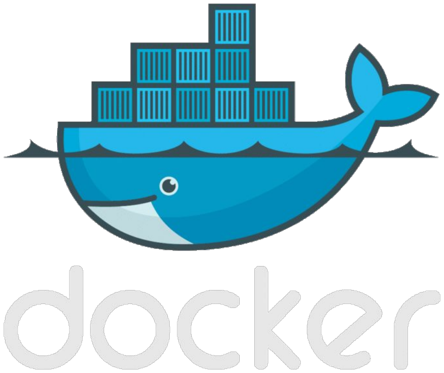


VIRTUALIZATION



What’s Docker?

- Lightweight *application* containers
- Dockerfiles, docker-compose
- Docker registry
- Online repository of application container images (Docker hub)



What’s LXD?

- Lightweight *Linux* containers providing a full OS environment
- VM-style management (snapshots, clones, live migration, images, etc)
- Architecture agnostic
- In-kernel since 2008

Tupperware
Magnificent
Freezing

Magnificent

Freezer Mates-Set (7)
Freezer Cube + 2 x 450 ml +
2 x 1 l + 1.1 l + 2.25 l

Tupperware

Magnificent

Freezing

Magnificent

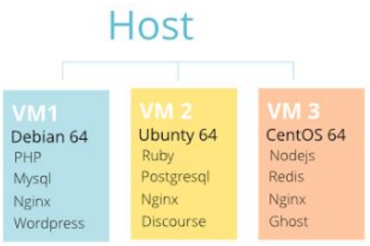
Freezer Mates-Set (7)
Freezer Cube + 2 x 450 ml +
2 x 1 l + 1.1 l + 2.25 l

Tupperware Magnificent Freezing

Magnificent
Freezer Mates-Set (7)
Freezer Cube + 2 x 450 ml +
2 x 1 l + 1.1 l + 2.25 l

Key differences between LXC and Docker

LXC



Host

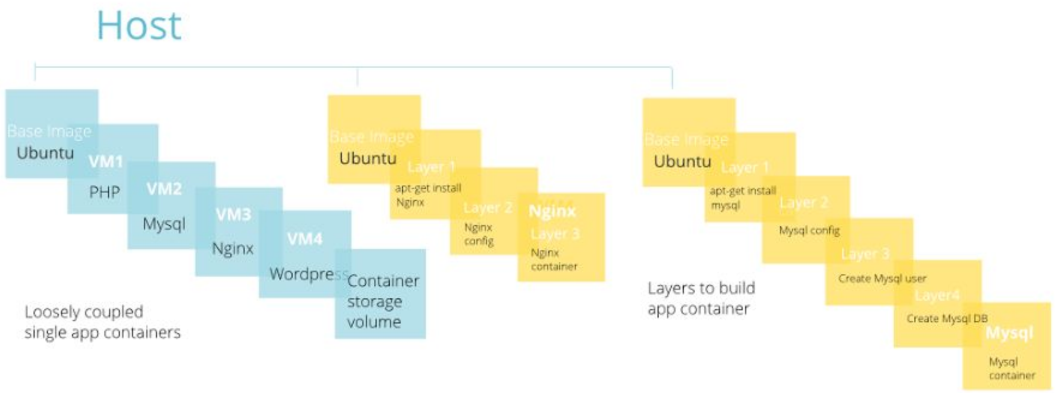
VM1
Debian 64
PHP
Mysql
Nginx
Wordpress

VM 2
Ubunty 64
Ruby
Postgresql
Nginx
Discourse

VM 3
CentOS 64
Nodejs
Redis
Nginx
Ghost

- Filesystem neutral
- Containers are like VMs with a fully functional OS
- Data can be saved in a container or outside
- Build loosely coupled or composite stacks

Docker



Host

Base Image
Ubuntu

VM1
PHP

VM2
Mysql

VM3
Nginx

VM4
Wordpress

Container
storage
volume

Loosely coupled
single app containers

Base Image
Ubuntu

Layer 1
apt-get install
Nginx

Layer 2
Nginx
config

Nginx
Layer 3
Nginx
container

Base Image
Ubuntu

Layer 1
apt-get install
mysql

Layer 2
Mysql config

Layer 3
Create Mysql user

Layer4
Create Mysql DB

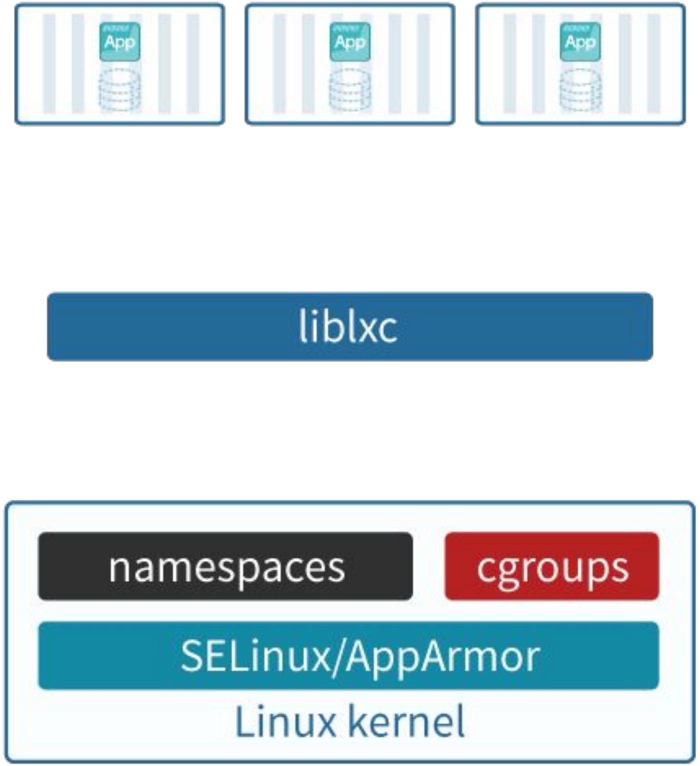
Mysql
Mysql
container

Layers to build
app container

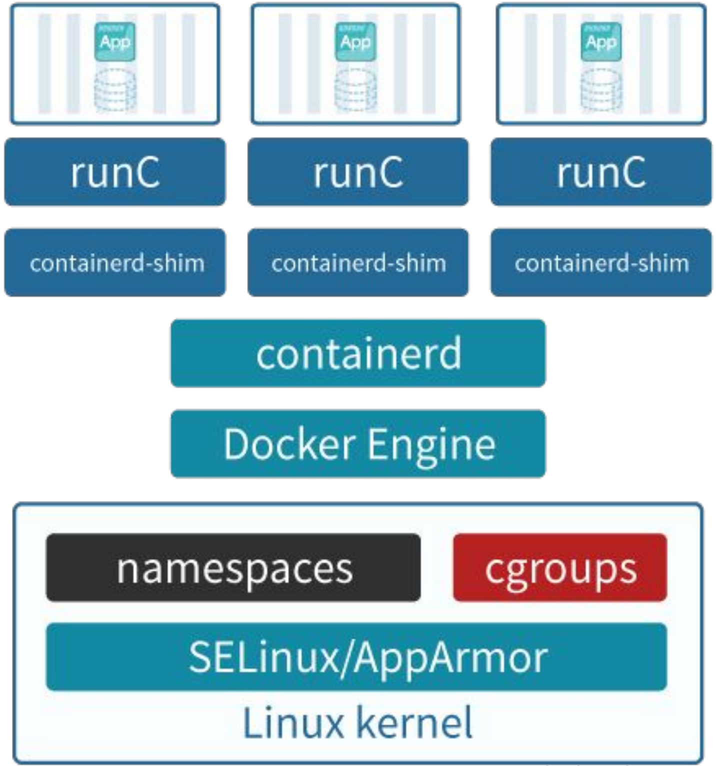
- Containers are made up of read only layers via AUFS/Devicemapper
- Containers are designed to support a single applicaton.
- Instances are ephemeral, persistent data is stored in bind mounts to host or data volume containers

https://archives.flockport.com/lxc-vs-docker/

Linux Containers

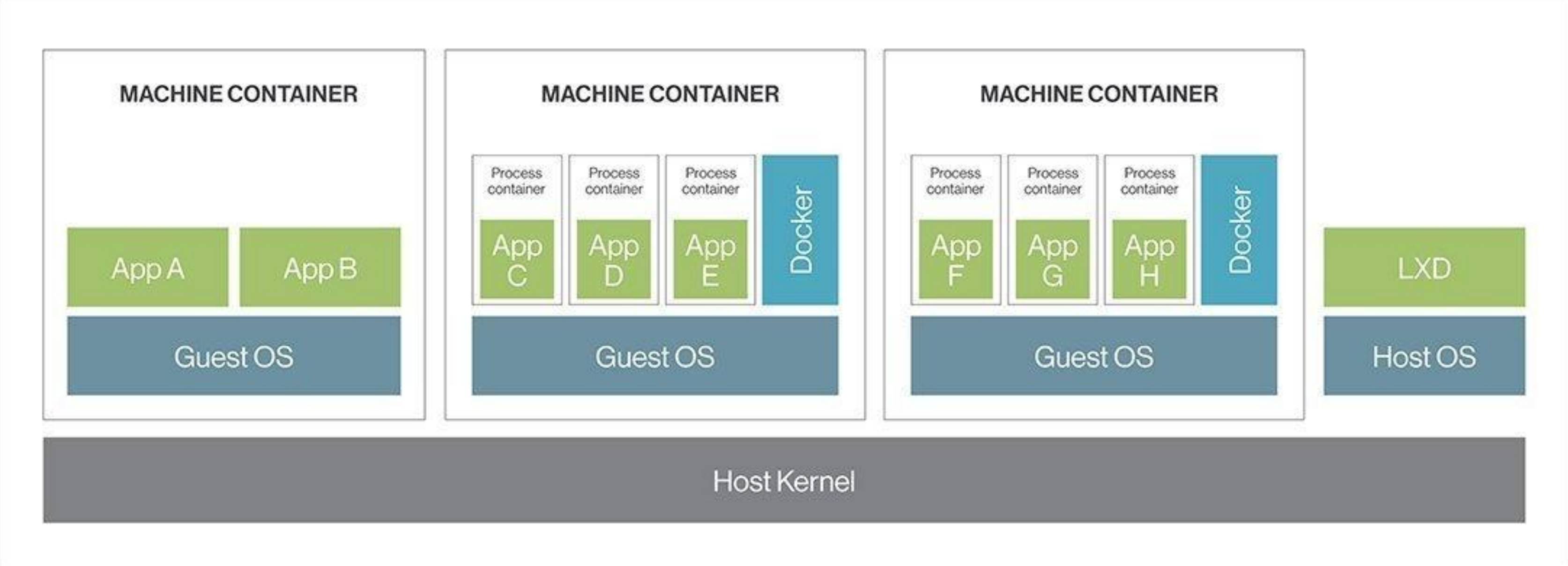


Docker 1.10 and later



https://www.techdivision.com/_Resources/Persistent/a9b527ac5f88df7435af6b68727cc1292cdb651b/Blogbeitrag1.png

LXD (Linux container hypervisor)



SOURCE: CANONICAL

https://cdn.ttgtmedia.com/rms/onlineImages/LXD_machine_container.jpg

Thank you!

HACK@UCF

HackersofUCF.slack.com | HackUCF.org/discord

https://hackucf.org ● https://www.facebook.com/HackUCF

Intro to Memory Forensics

By Michael Ibeh

This Talk

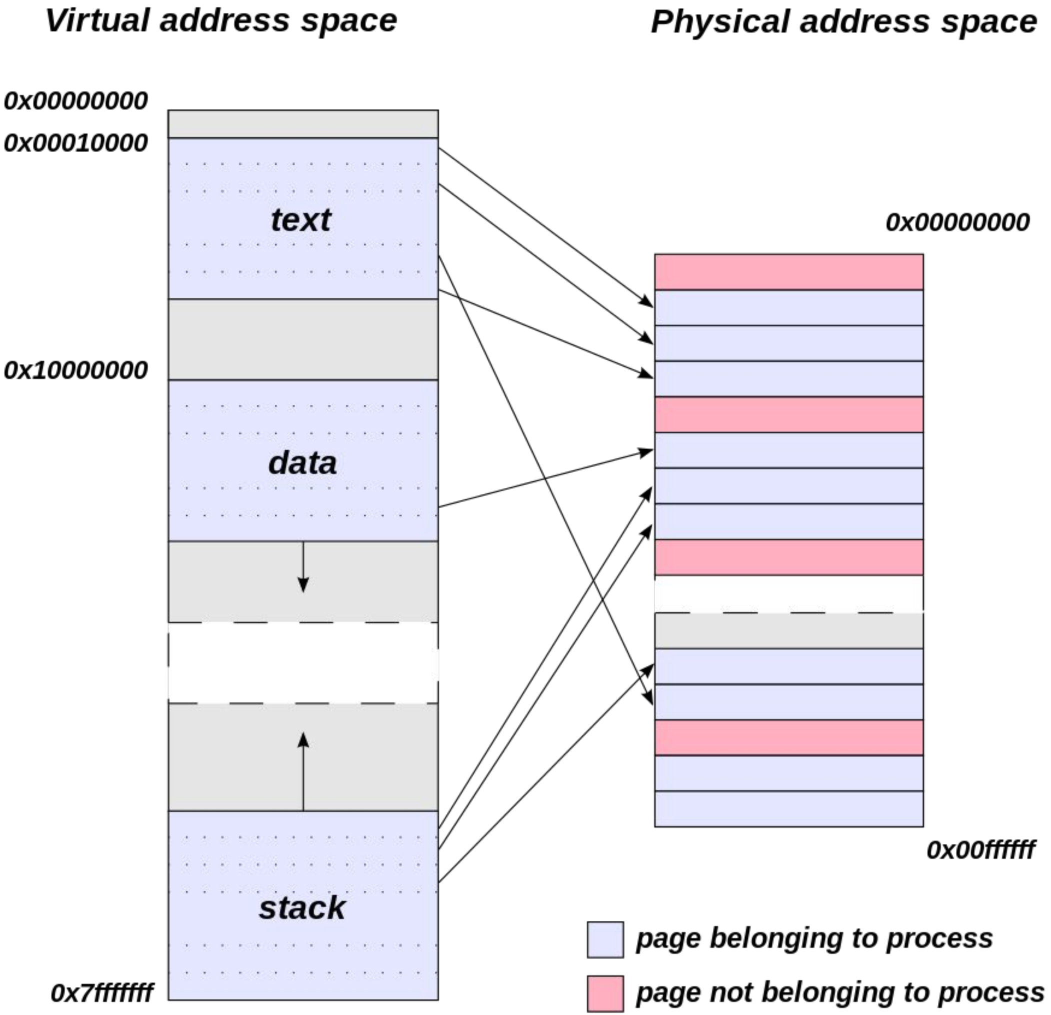
- What is this?
- BUT WHAT DOES IT MEAN?!?!?
- F*ck malware, get images
- Analysis tools
- Stuff & Things

Memory Overview

- CPU’s main memory, RAM
    - Stores the code, data, and OS that the processor needs to access
- Basically everything that’s happening on a computer at a given time
- Processor architecture -> memory structure
- Volatile - must maintain electrical current to maintain data

Memory Overview

- CPUs NEED unique addresses
- Virtual (Linear) address != Physical address
- Segmentation & Paging


Virtual address space
Physical address space
0x00000000
0x00010000
text
0x10000000
data
stack
0x7fffffff
0x00000000
0x00ffffff
page belonging to process
page not belonging to process

Paging

- Virtualizes the linear address space
  - Broken up into fixed length sections called pages
- Arbitrarily mapped to physical memory
- Difference between 32 & 64 bit
  - 32 - 4GB (32bits), with exception
  - 64 - up to 64 bits, usually 48. Rest will be all 0s or 1s
- Page Directory -> Page Table -> Page
- Pages are some combo of R, W, X by VAD nodes
  - PTE protection bits

Memory Formats

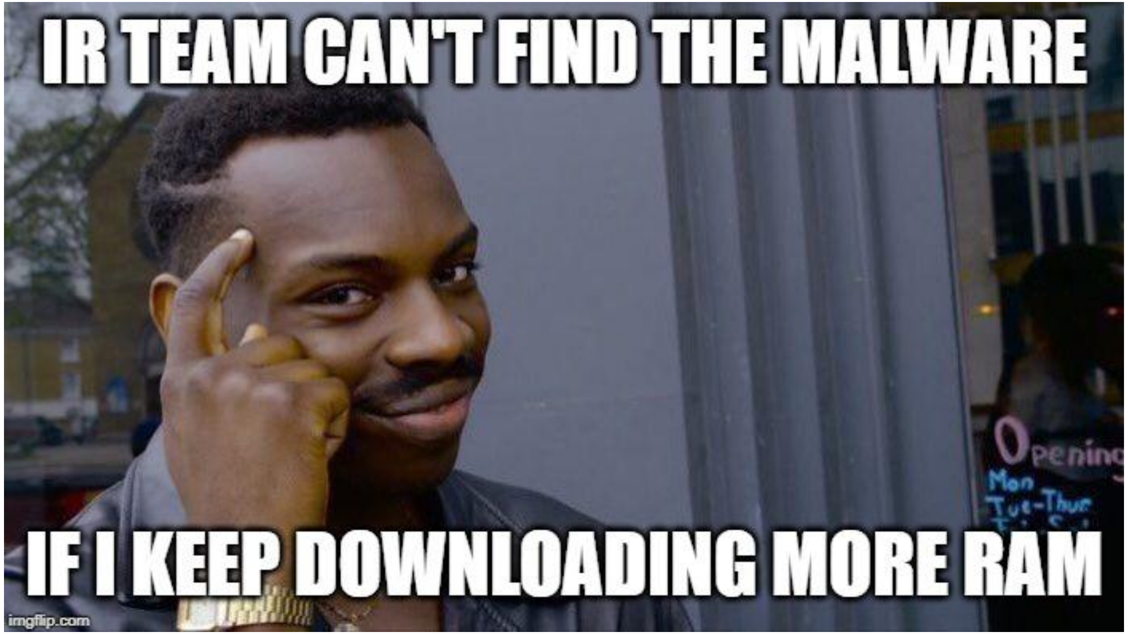
- Raw
- Crash Dumps
- VM memory files
- hiberfil.sys - RAM stored during machine hibernation
  - %SystemRoot%\hiberfil.sys
- pagefile.sys - Virtual memory used by Windows
  - %SystemDrive%\pagefile.sys
- swapfile.sys - Virtual memory used by Windows Store Apps
  - %SystemDrive%\swapfile.sys

Why Look at Memory?

- Develop IOCs
- Security validation
- Gather evidence

Where to Start Looking?

- Processes
- Network connections
- Loaded DLLs
- CMD history
- Clipboard
- Execution artifacts

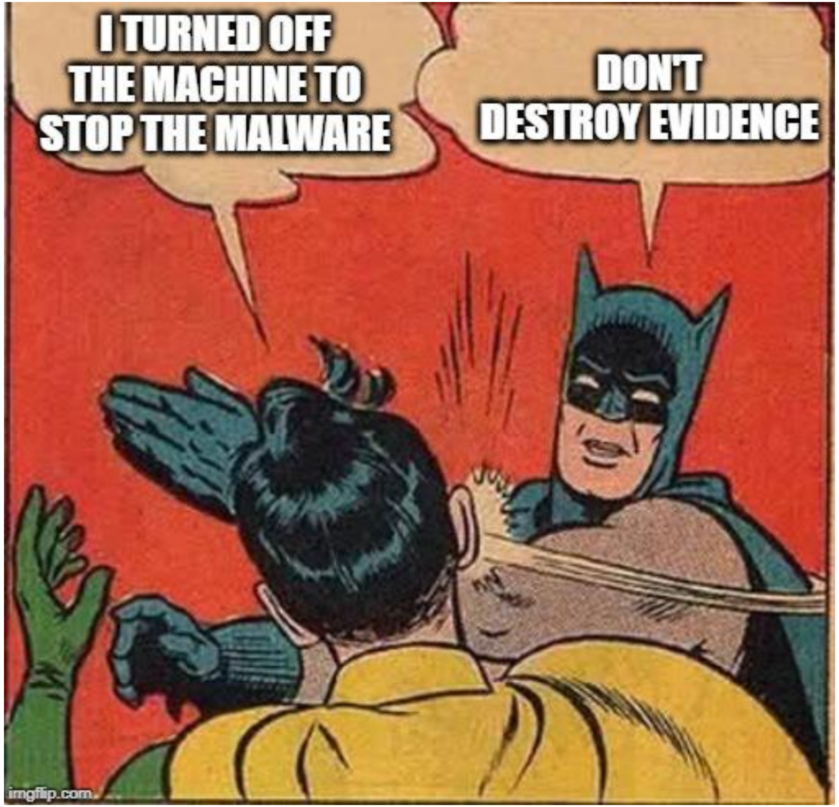

IR TEAM CAN'T FIND THE MALWARE
IF I KEEP DOWNLOADING MORE RAM
Opening
Mon
Tue-Thur
imgflip.com

Memory Acquisition

- Capture volatile data -> store in non-volatile format
- A sample of memory at a given time
- Tools:
    - memdump
    - FTK imager
    - Winpmem
    - Many paid tools...

Acquisition Considerations

- Remote vs Local
- Budget/Time
- Format
- What tool?
- Is it worth it?



VOLATILITY

- A memory forensics framework
- Cross platform, custom plugins available
- Can analyze most versions of Windows, Linux, and OSX 10 (32 & 64 bit)

Volatility Usage

```
$ volatility -f <mem_dump> --profile=<profile> <plugin>
```

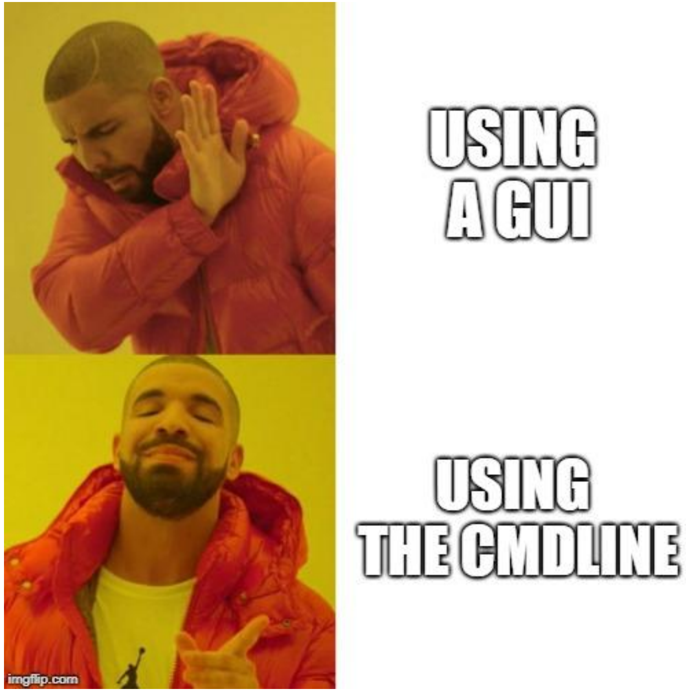
```
$ volatility3 -f <mem_dump> <os>.<plugin>
```

Helpful Plugins

imageinfo (Run first!!) - only old volatility
pslist
netscan
svcscan

<u>Windows:</u>
hashdump
lsadump
iehistory
consoles
hivelist
dlllist

<u>Other:</u>
strings
procdump
yarascan



Other Tools

- Rekall
- Redline
- YARA
- Encase/Blacklight/X-Ways Forensics
- … much more

Demo

Resources

Volatility Wiki:

https://github.com/volatilityfoundation/volatility/wiki

Volatility3 Docs:

https://volatility3.readthedocs.io/en/latest/

OLD Volatility Cheat Sheet:

https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf

The Art of Memory Forensics:

https://www.memoryanalysis.net/amf