Meeting 98

// Virtual Machines //

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

Announcements / Upcoming Events

- NSA coming Oct. 16th
- Battelle Visiting us later this semester
- GE Aviation SOC visit in the works
- Mason High School Hack club needs help with Cyber Month

Weekly News

Huawei Accusations

- US had launched cyber-attacks to infiltrate its networks
- FBI agents were being sent to the homes of its employees to pressure them to collect information on the company
- US thinks Huawei products could be used for surveillance

https://www.techradar.com/news/huawei-claims-us-enticed-and-coerced-its-staff-to-provide-company-info

North Korean Malware

- Used cyber-attacks to steal over $2 billion from financial institutions
- Used that money to fund nuclear weapons research

https://www.oodaloop.com/briefs/2019/08/06/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report/

Social Engineering Toolkit

- Name: Domen
- Generates fake software updates to install a remote access trojan
- Extremely customizable
- Different schemes based on geolocation or browser/OS type

https://www.computerweekly.com/news/252470034/Cyber-criminals-tap-into-Web-social-engineering-toolkit

Other Stories

- https://www.computerweekly.com/news/252470034/Cyber-criminals-tap-into-Web-social-engineering-toolkit
- https://techcrunch.com/2019/08/15/cyber-command-north-korea-malware/
- https://www.forbes.com/sites/daveywinder/2019/08/19/texas-cyber-attack-has-taken-23-government-agencies-offline/#7a13e4172d65
- https://www.wired.com/story/supermicro-bug-virtual-usb/?itm_campaign=TechinTwo

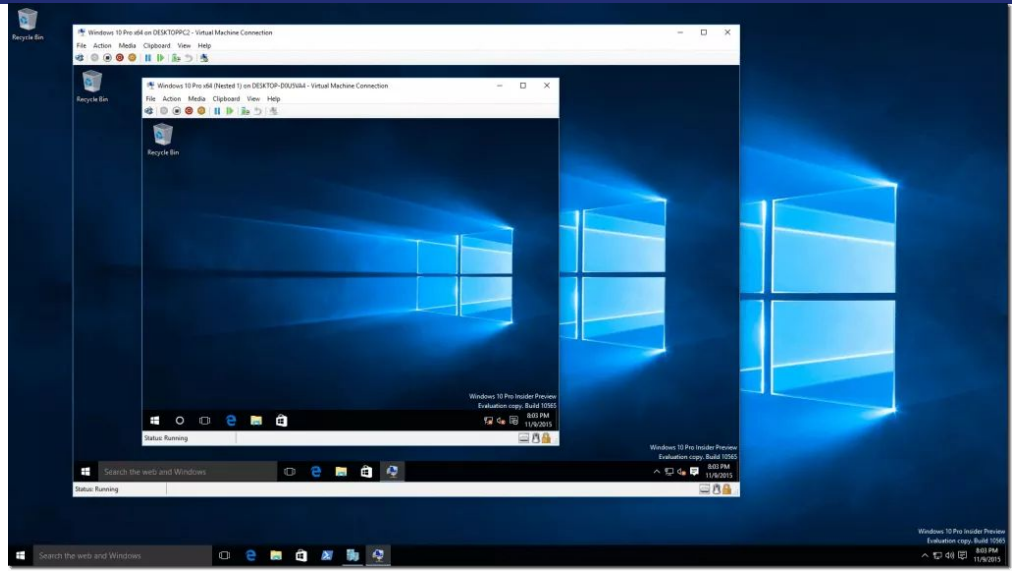
Virtual Machines

Agenda

- What are Virtual Machines
- Getting Setup
- Hypervisors/Cloud Environments
- Meta-Tools
- Containers

Virtual Machines

- Software only machines
- Can share resources with the host machines
- Hard drive is stored as a file on the host machine or a real hard drive that the host passes through
- Lets a single machine run multiple OS’s simultaneously



Getting Setup

Install VirtualBox and get a Debian 9.9 ISO

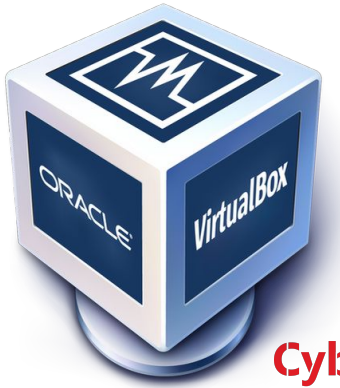
Windows / Mac:

- **virtualbox.org**

Debian / Ubuntu

- **apt install virtualbox**

Errors on booting? Enable Virtualization in your BIOS



Getting Setup (cont.)

In VirtualBox:

1. Create a new machine
2. Name the new machine “debian”, VirtualBox will auto configure some settings
3. Set how much memory you want the machine to be able to use, 2048 is usually plenty for a Linux VM
4. Create a Virtual Hard Disk
5. Attach the ISO you’ve already downloaded under Machine>Settings>Storage
6. Boot the machine to install the OS from the ISO

Hypervisors

- Hypervisors are the software components that run virtual machines
- Common Self-Hosted Hypervisors
  - VirtualBox - Cross platform, free
  - VMWare - Product line, more business oriented
  - Hyper-V - Microsoft's version of VMWare
  - QEMU+KVM - Open Source. Fast and capable of cross-architecture emulation
  - Proxmox VE - OS for hosting VMs on a server
- Cloud Hypervisors
  - AWS EC2
  - Azure
  - Google Cloud

Meta Tools for VMs

- Vagrant - Tool and Language for setting up VM's
- Libvirt - Open Source Multi-hypervisor API
  - Used in our range-master project
- Meta-VM's for specific tasks
  - FLARE VM - Windows RE
  - Commando VM - Windows Offensive testing VM
  - Metasploitable - VM for testing Kali tools
- Cuckoo
  - Tool for automated malware RE that relies on a network of VM's to operate

Where are VMs in the wild?

- Home users
  - Almost never unless technical person(s)
  - Use other OS's on one box
- Business users
  - Virtualized Servers in Production (On-Prem or cloud)
  - Development testing