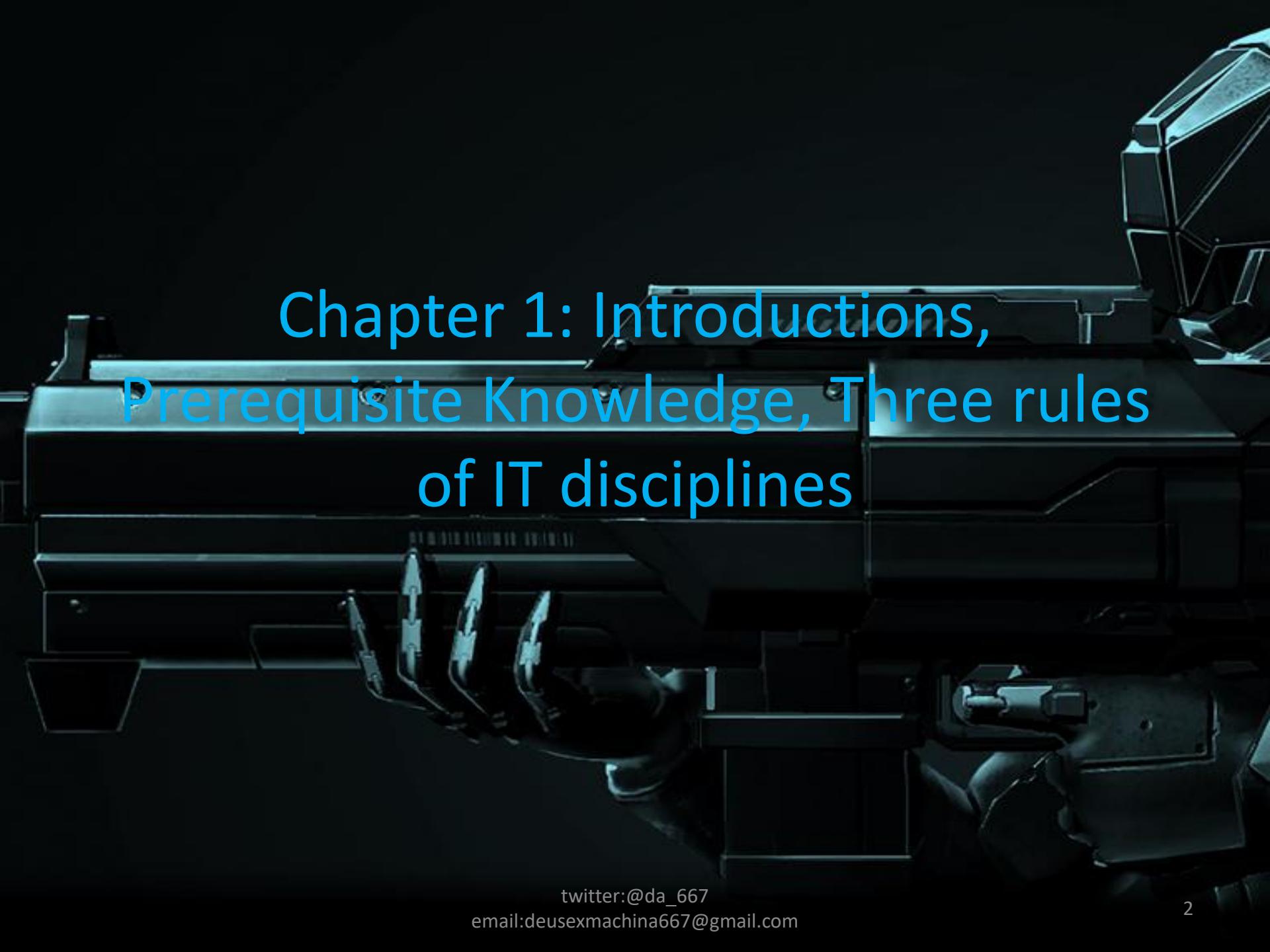


A dark, futuristic robot with glowing purple and blue lights on its chest and arms, holding a glowing purple sphere.

Building Virtual Labs: CCC edition

twitter:@da_667
email:deusexmachina667@gmail.com

A dark, metallic, robotic hand holds a tablet device. The hand has articulated fingers and a thumb. The tablet screen displays the title text.

Chapter 1: Introductions, Prerequisite Knowledge, Three rules of IT disciplines

Hello There

- Tony Robinson/da_667
- Security Analyst,
Hurricane Labs
- I do threat intel,
documentation, and
NSM things



Purpose of this training

- Teach you how to create a VM lab
 - Red team, Blue team, Purple team, etc. You need a place to practice.
- Teach you solid network and system administration practices to make a safe place to practice
- Provide you with a starting point, then let you go wild on your own

Prerequisite Knowledge: TCP/IP Networking

- Are you familiar with OSI or TCP/IP network models?
- Do you know what an IP address is? DNS Servers? DHCP? Default gateway?
- Do you know what RFC1918 addresses are, and why they are used? (192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8)
- Do you know how to configure these things on Linux or Windows (e.g. network adapter properties, ifconfig, ip link, ip route, /etc/resolv.conf, etc.)

Prerequisite Knowledge: TCP/IP Networking (Cont'd)

- Are you familiar with different transport protocols (e.g. TCP, UDP, ICMP) and how TCP/UDP works?
- Can you identify what port common TCP/UDP services operate on (e.g. 53/udp = DNS, 80/TCP = HTTP, 123/udp = NTP, 22/TCP = SSH, etc.)
- Do you understand how stateful firewalls operate, and what criteria they use for blocking/allowing connections? (IP addresses, protocols, port numbers, ICMP types/codes, etc.)

Prerequisite Knowledge: Operating Systems

- Have you ever installed an OS before? Any OS – Windows, Linux/Unix, OSX, etc.
 - Do you know what an installation ISO is, and how to boot from one?
- Are you familiar with the Windows command prompt and/or the Linux/Unix/OSX terminal/CLI?
 - Have you seen or used any of the following commands: ping, netstat, wget, curl, ipconfig, ifconfig, etc.)
 - Have you ever used a command line text editor before? (e.g. Vim, nano, emacs, etc.)
- Are you familiar with SSH and/or SCP protocols?

Prerequisite knowledge: Virtualization

- You've probably used a VM at some point, right?
 - If not, I guess you're here for a reason

I know all of this. Am I going to be bored in this class?

- Maybe a little at first, but making sure all students are on the same page is important
- Maybe you'll learn something new

I don't know any of this. Am I doomed?

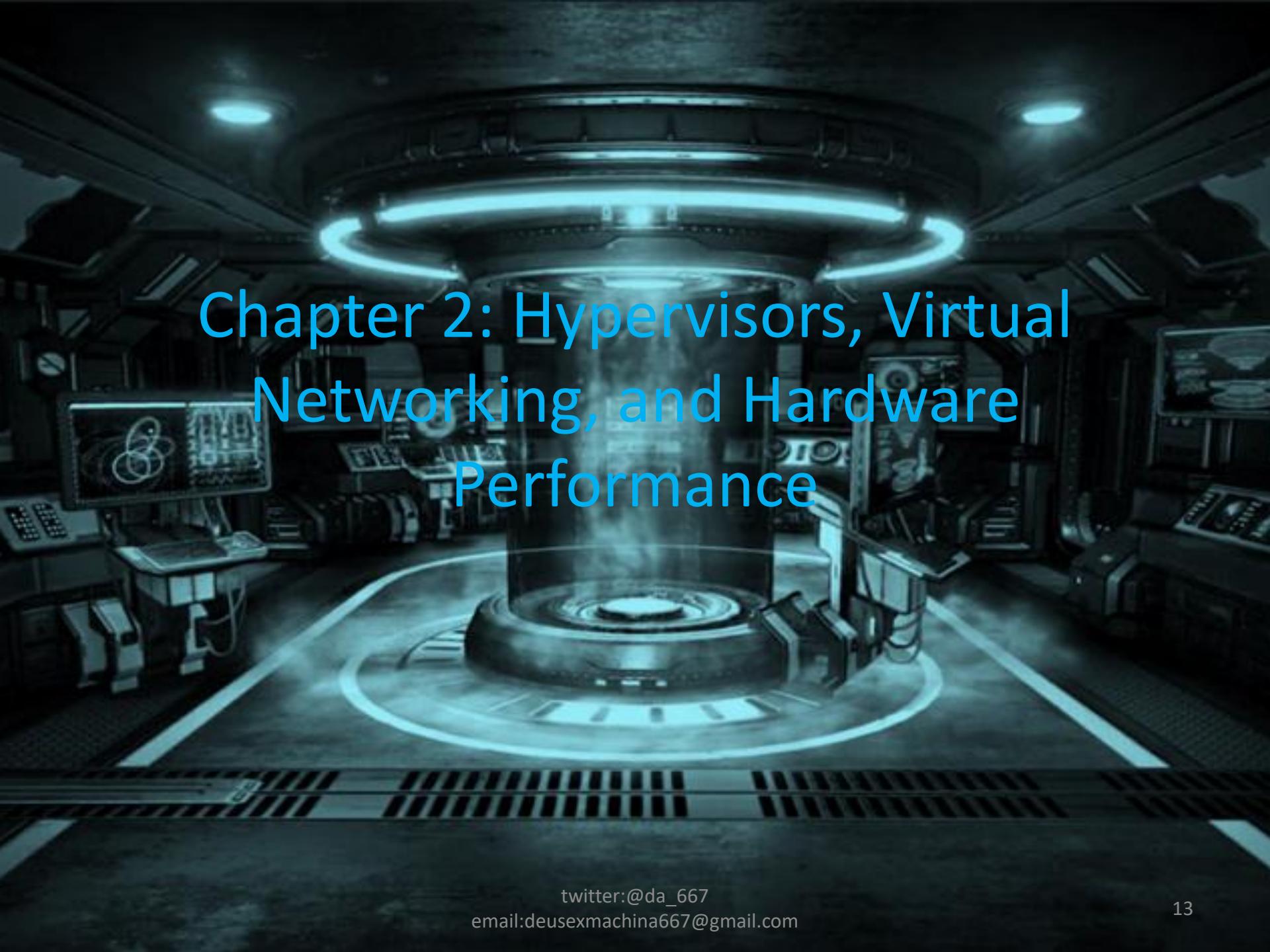
- Follow along as best you can
- If you miss something/mess up, don't fret
 - Leanpub.com/avatar
 - Free PDF copy of the book this training is based off of
 - USB drives going around
 - Free copy of the slides for this training. Use them however you see fit.

Where can I go if I want to learn more?

- Cybrary.it – has a host of different training videos on various subjects
 - Most are centered around IT certifications, but still extremely valuable
- Learn Python The Hard Way – Command-line crash course
 - <https://learnpythonthehardway.org/book/appendixa.html>
- Can't go wrong with No Starch Press books
 - *The Linux Command Line*
 - *TCP/IP Guide*
 - *Network Know-How*
 - *Practical Packet Analysis*

The Three Rules of IT Disciplines

- Don't Panic
 - Being level-headed in the event of unforeseen problems is extremely important.
- Software changes
 - Features and UI elements may be added, removed, or be relocated.
- Consult the documentation
 - Patch notes, product forums, Help menu, PDFs, product support sites, etc.



Chapter 2: Hypervisors, Virtual Networking, and Hardware Performance

Intro to Virtualization

- Virtualization – Taking one physical computer, and splitting its resources into chunks/containers to host smaller, independant computing environments (Virtual Machines, or “VMs”)
 - Think: Computer(s) within a computer
- Hypervisor – Software used to create and manage all aspects of VM creation and operation
 - Baremetal: The hypervisor directly manages physical hardware
 - Hosted: The hypervisor is installed on top of an existing operating system and uses it to manage physical hardware

Oracle VM VirtualBox Manager

Tools

New Settings Discard Start

pfsense Powered Off

General

Name: pfsense
Operating System: FreeBSD (64-bit)
Settings File Location: /Users/trobinson/VirtualBox VMs/pfsense

System

Base Memory: 512 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 16 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Primary Master: pfsense.vdi (Normal, 5.00 GB)

Audio

Disabled

Network

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, en4: Thunderbolt Ethernet)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0')
Adapter 3: Intel PRO/1000 MT Desktop (Internal Network, 'intnet0')

USB

Disabled

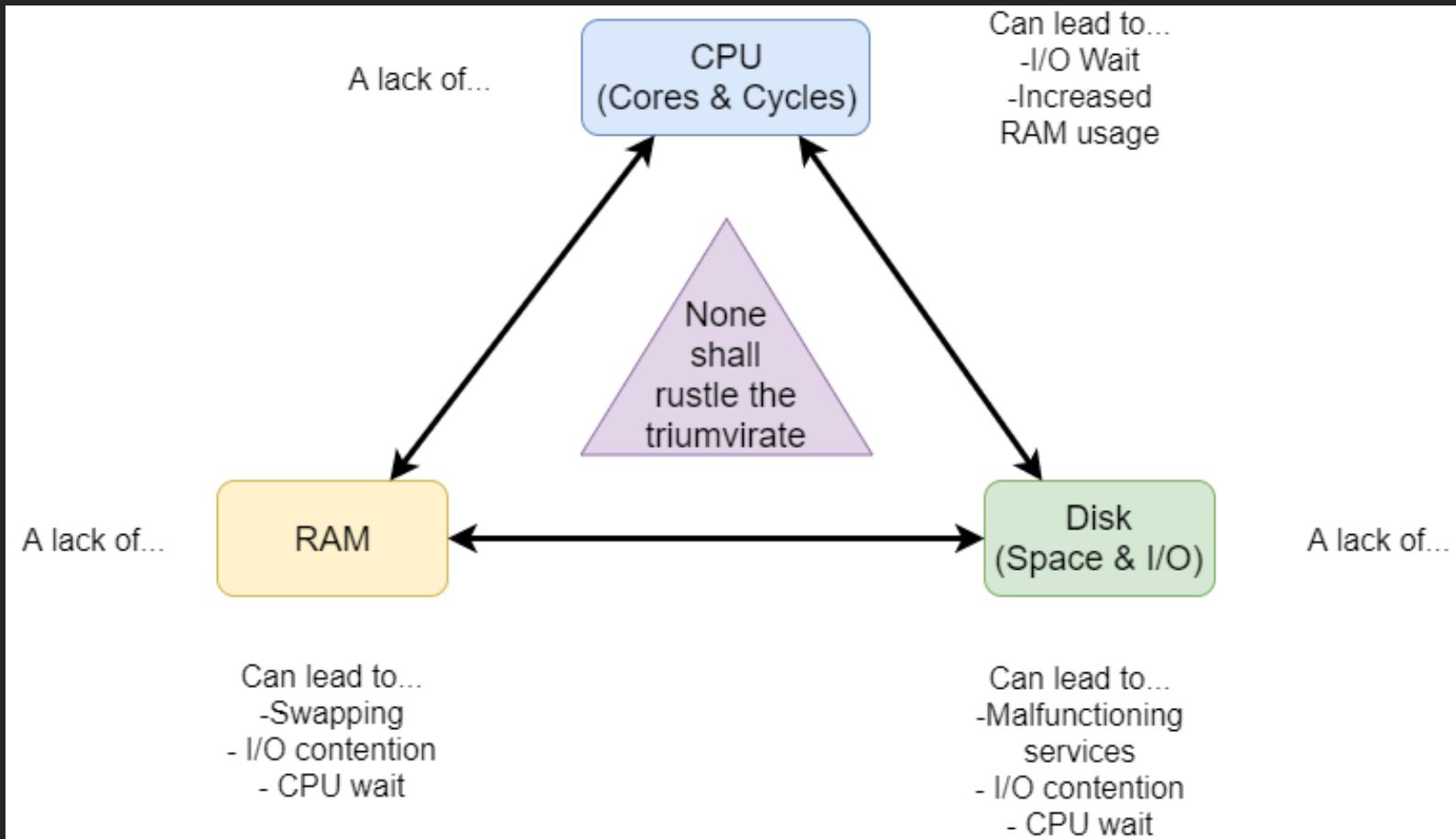
Preview

Intro To Virtual Networking

- Baremetal Hypervisors – Virtual Switches
 - Can be uplinked to a physical NIC for outbound connectivity or unlinked to isolate VMs
- Hosted Hypervisors – Virtual Network Segments
 - Host-only: VMs can only communicate with each other VMs on this segment, or the hypervisor host (through a virtual network adapter)
 - Internal: Variation of host-only network where the host doesn't have a virtual network adapter.
 - NAT: Network Address Translation – Can talk to other VMs on the same network. Uses the hypervisor host's IP address as a NAT provider for outbound network comms
 - Bridged: VMs on this network segment act as though they are physically connected to the same network as the hypervisor host

Hardware Resources

- Virtualization requires RAM, CPU, and Disk Space/IO
 - A lack of any one of these three things leads to poor host and/or VM performance
- Most hypervisors also require specific CPU features
 - AMD-V / VT-x
 - Note: Motherboard must also support VT-x or AMD-V
 - Instructions on how to do this differ by manufacturer
 - 64-bit support



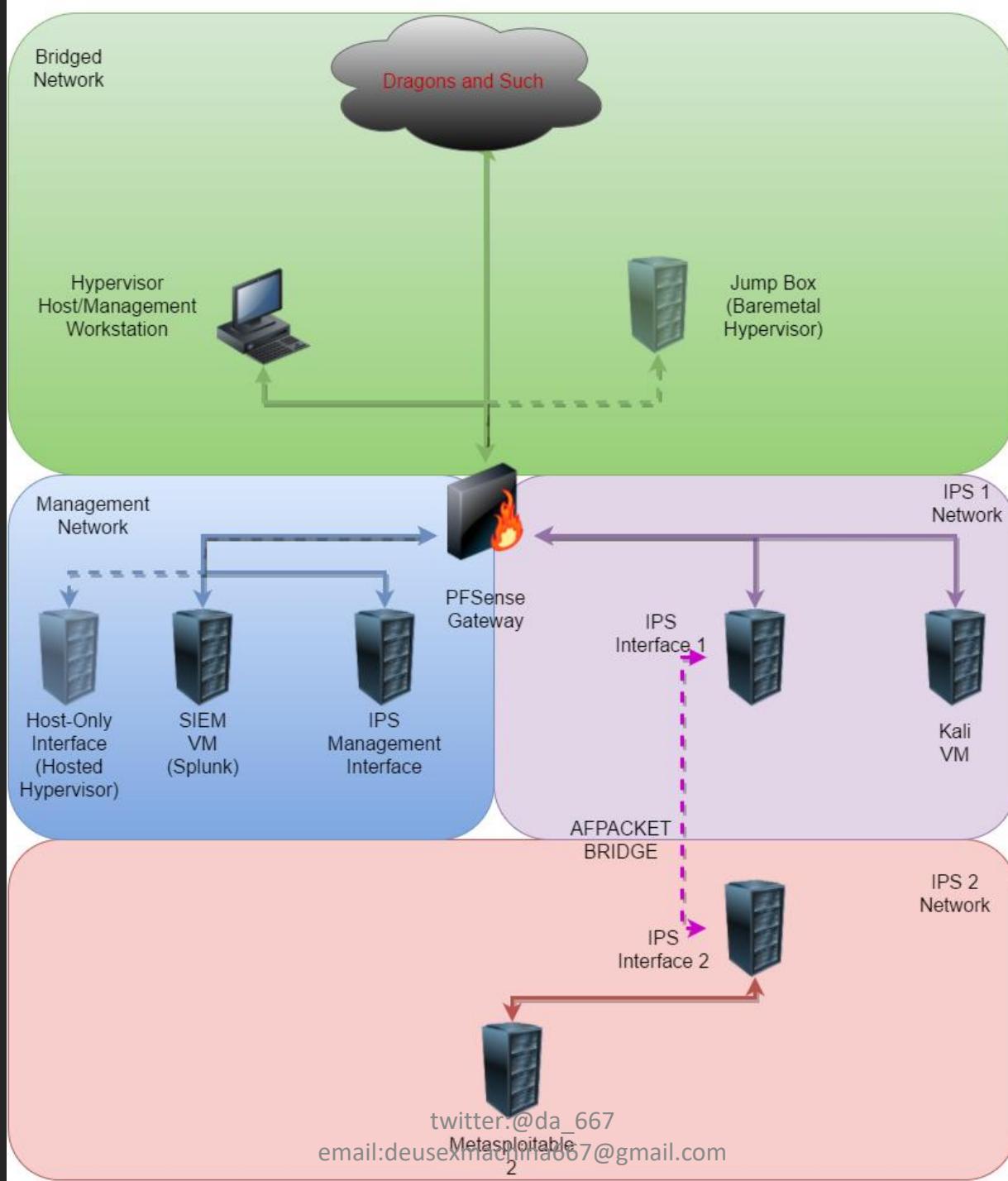
Chapter 3: Network Design and VM resource allocations

Lab VMs and Allocations

- pfSense
 - 512MB of RAM
 - 5GB Disk
 - 1 CPU core
- SIEM VM
 - 2GB of RAM
 - 60GB Disk
 - 1 CPU core
- IPS VM
 - 1-2GB of RAM
 - 40GB Disk
 - 1 CPU core
- Kali Linux
 - 2-4GB of RAM
 - 40GB Disk
 - 1 CPU core
- Metasploitable 2
 - 512MB of RAM
 - 8GB Disk
 - 1 CPU core

Lab VMs and Allocations (cont'd)

- Total Allocations
 - RAM
 - Min: 6GB
 - Optimal: 9GB
 - More is better (allows more VMs to run, allows host OS “breathing room”)
 - Disk
 - VMDKs will require at least 160GB of free disk.
 - Recommend at least 500GB of free space in total
 - ISOs, Support Applications, Snapshots, Additional VMs, etc.
 - Separate disk if possible, SSD if possible
 - Helps to avoid Disk I/O contention (but shouldn't be a big problem)
 - CPU
 - Recommend something with at least 4 cores
 - No, hyperthreading does NOT count
 - As usual, more is better



Chapter 4: Preparation

Tools of the trade

- Useful software packages for your lab
 - Installation ISOs (pfSense, Kali, Ubuntu 18.04)
 - Pre-configured VMs (Metasploitable 2)
 - Supporting applications (text editors, cli tools, remote access suites, etc.)
 - Websites to register to (splunk.com, snort.org)
- USB drive with the entire suite of tools (Windows, Linux, OSX) being distributed
 - This chapter is more for your reference at home and if you want to share this training with others

Tools of the Trade – ISOs and VMs

- Download the following:
 - pfSense – FreeBSD based firewall distribution
 - <https://pfsense.org/download/>
 - Select “AMD64” as architecture, “CD Image (ISO) Installer” as Installer, Closest geographical mirror, then click “Download”
 - Kali Linux – Debian-based penetration testing distribution
 - <https://kali.org/downloads>
 - Locate “Kali Linux 64 bit”, and click on “HTTP”
 - Ubuntu Server – A stable and easy to use Linux server distribution
 - <https://www.ubuntu.com/download/server>
 - Always select the latest LTS (Long-Term Support) release
 - Metasploitable 2 – An intentionally vulnerable Linux VM
 - <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>
 - Select “Download Latest Version” (metasploitable-linux-2.0.0.zip)
 - Note: you will need a compression tool to unzip and use this VM (covered shortly)

Tools of the Trade – Windows Apps

- mRemoteNG – a tabbed front-end for a variety of remote access protocols
 - <https://mremoteng.org/download>
- WinSCP – a windows client application for the SCP protocol
 - <https://winscp.net/eng/download.php>
- 7-zip – an open-source application that can handle a variety of compressed file formats
 - <https://www.7-zip.org/download.html>
- puttygen (64-bit) – a windows application for generating SSH keys
 - <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>
- Notepad++ (64-bit) – a powerful text editor
 - <https://notepad-plus-plus.org/download/>
- KeePassXC (64-bit) – a multiplatform password manager
 - <https://keepassxc.org/download/#windows>

Tools of the Trade – OSX Apps

- Native terminal applications (pre-installed):
 - vi/vim – a very old text editor that is universally available on most UNIX-like operating systems
 - ssh – a client application that allows to connect secure to remote SSH servers
 - scp – secure copy protocol client. Allows you to transfer files to/from a remote system utilizing the SSH protocol
 - ssh-keygen – allows you to generate a public/private key pair. Enables passwordless login, OR two-factor authentication
 - ssh-copy-id – a pain-free method of copying your public key to a remote SSH server to enable key-based authentication
 - zip/unzip, gzip/gunzip – command line utilities that allow you to decompress .zip or .gz files
 - Alias – command line tool that lets you alias entire commands plus their arguments to another name (think: shortcuts)

OSX Apps (cont'd)

- Third-party Tools (download and install):
 - iTerm2 – a better replacement for the OSX terminal application
 - <https://www.iterm2.com/downloads.html>
 - BBEdit – powerful text editor
 - <https://www.barebones.com/products/bbedit/download.html>
 - Note: you do NOT need to pay for the licensed features
 - KeepassXC – multiplatform password manager
 - <https://keepassxc.org/download/#mac>

Tools of the Trade – Linux Apps

- Terminal applications (usually installed as ‘core utilities’):
 - vi/vim – a very old text editor that is universally available on most UNIX-like operating systems
 - ssh – a client application that allows to connect secure to remote SSH servers
 - scp – secure copy protocol client. Allows you to transfer files to/from a remote system utilizing the SSH protocol
 - ssh-keygen – allows you to generate a public/private key pair. Enables passwordless login, OR two-factor authentication
 - ssh-copy-id – a pain-free method of copying your public key to a remote SSH server to enable key-based authentication
 - zip/unzip, gzip/gunzip – command line utilities that allow you to decompress .zip or .gz files
 - alias – command line tool that lets you alias entire commands plus their arguments to another name (think: shortcuts)

Linux Apps (cont'd)

- Graphical text editor (if you don't like vi/vim)
 - Common editors: gedit, kwrite, leafpad, etc.
- A terminal application
 - Common terminal apps: Konsole, Terminal, Gnome-Terminal
 - Special Mention: Gnome Terminator – install this if you can.
 - Very similar to iTerm2
 - <https://gnometerminator.blogspot.com/p/introduction.html>
- A window manager
 - I know you're a leet console cowboy, but I am NOT playing with virtualbox headless.
 - Common WMs: Gnome, Cinnamon, KDE, flux, XFCE, etc.
- KeepassXC – multiplatform password manager
 - <https://keepassxc.org/download/#linux>
 - Recommend using the AppImage installer

Tools of the Trade – Website Registration

- Splunk.com
 - https://www.splunk.com/page/sign_up
 - Download Splunk Enterprise, Universal Forwarder
 - Download the Linux 64-bit “.deb” Splunk Enterprise and Universal Forwarder packages
 - Download Splunk TA for Suricata OR Hurricane Labs Add-On for Unified 2
 - Splunk TA for Suricata: <https://splunkbase.splunk.com/app/2760/>
 - Hurricane Labs Add-On for Unified 2 (Snort):
<https://splunkbase.splunk.com/app/1858/>
 - Request a developer license
 - <https://splunkbase.splunk.com/develop/>
- Snort.org
 - https://snort.org/users/sign_up
 - Register a free account, log in, record your “oinkcode”



Chapter 5: Installing and Configuring Virtualbox

A quick note before we continue..

- I will guide you through the initial installation process on Windows, Linux, and OSX
 - Most demonstrations will be done using vbox on Windows
 - Host OS shouldn't matter terribly much

Acquiring the Hypervisor

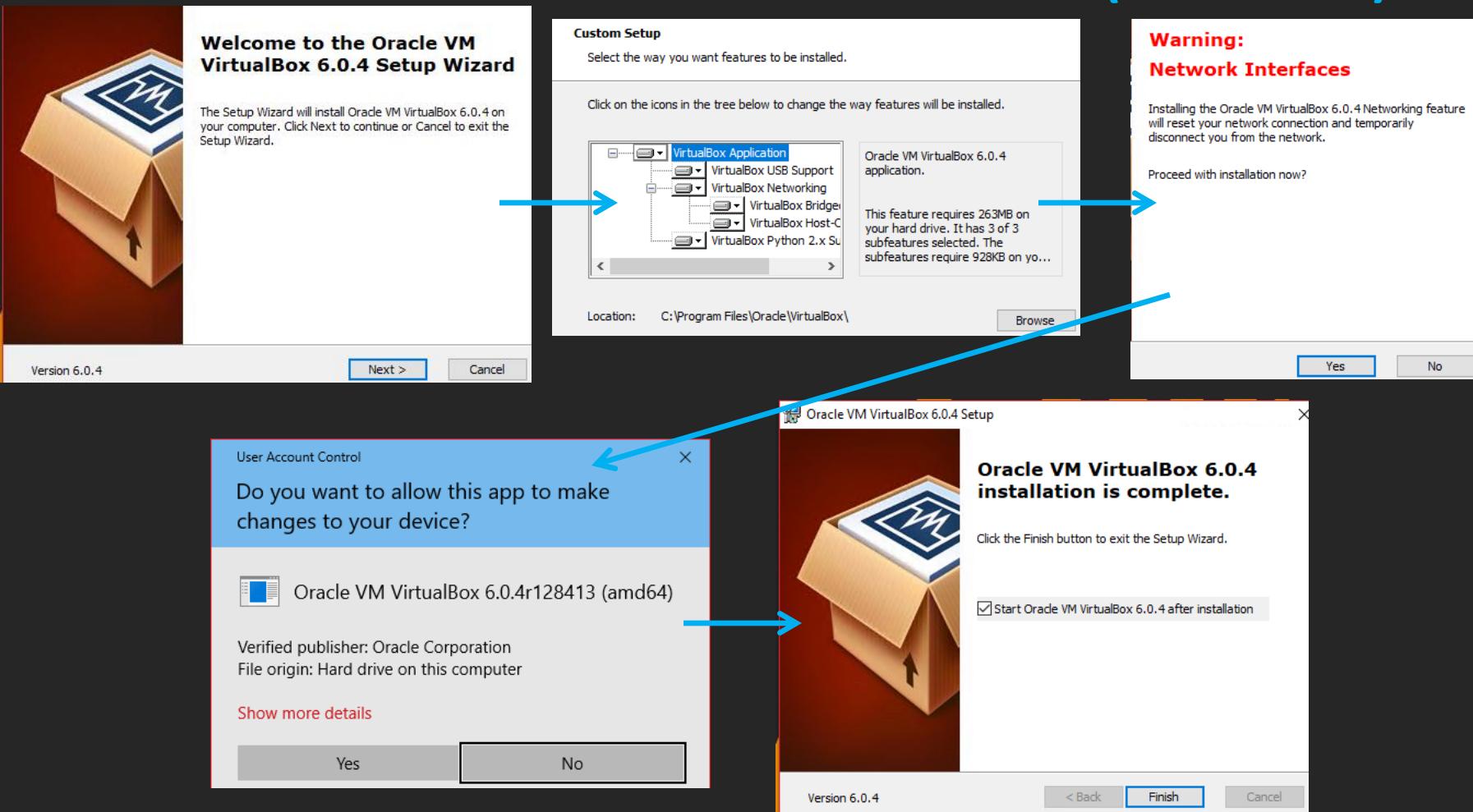
- Acquire the latest Oracle Virtualbox installation package from
<https://www.virtualbox.org/wiki/Downloads>



Installation - Windows

- You will need admin access in order to install vbox
- Download Windows installer
- Double click to begin installer process
- If UAC is enabled, click “yes” to allow vbox to install
- Notes/Warnings:
 - you may be prompted to install drivers (USB and/or network), select “yes” to install the virtualbox drivers
 - Installer warns you that, during installation, network connectivity may be lost temporarily during driver installation
 - As with most Windows things, you may need to reboot to finish the installation

Installation – Windows (cont'd)



Installation - OSX

- Download .dmg
- Double click to mount/open
- Double click .pkg file to start installer
- Select “Continue” to the pop-up prompt, then to the vbox installer window
- Click “Install”
- Enter admin creds
- Installation finishes. Click “Close”

Installation – OSX (cont'd)

1 Double click on this icon:

VirtualBox.pkg

This package will run a program to determine if the software can be installed.

To keep your computer secure, you should only run programs or install software from a trusted source. If you're not sure about this software's source, click Cancel to stop the program and the installation.

Cancel Continue

Welcome to Oracle VM VirtualBox 6.0.4 for macOS! This installer will guide you through the installation process. In a minute from now, you will be able to execute virtual machines running different operating systems on your desktop. You will find that VirtualBox delivers a great feature set and excellent performance.

Go Back Continue

Standard Install on "Macintosh HD"

This will take 296.8 MB of space on your computer.

Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.

Change Install Location...

Customize Go Back Install

Installer is trying to install new software.

Enter your password to allow this.

User Name: Tony Robinson

Password:

Cancel Install Software

The installation was successful.

The software was installed.

Go Back Close

Installation - Linux

- Download .run package
- Download and install linux kernel development headers
 - Apt distros: apt-get install linux-headers-amd64
 - Yum distros: yum install kernel-devel
 - Other distros: read the docs (Sorry, I'm not enough of a nerd for slackware, arch, or gentoo)
- Run “chmod u+x Virtualbox-x.x.x-xxxxxx-Linux_amd64.run”
- Run (as root, or pre-fixed with “sudo”) ./Virtualbox-x.x.x-xxxxxx-Linux_amd64.run
- Installation finishes (installs to /opt/virtualbox)
 - Virtualbox can be started by running “virtualbox” in a terminal window (or /usr/bin/virtualbox, if your PATH variable isn't set up with /usr/bin)

Installation – Linux (cont'd)

```
:~/Downloads# apt-get -y install linux-headers-amd64
```

```
root@kali:~/Downloads# whoami  
root  
root@kali:~/Downloads# chmod u+x VirtualBox-6.0.4-128413-Linux_amd64.run  
root@kali:~/Downloads# ./VirtualBox-6.0.4-128413-Linux_amd64.run
```

```
Verifying archive integrity... All good.  
Uncompressing VirtualBox for Linux installation.....  
VirtualBox Version 6.0.4 r128413 (2019-01-25T20:35:08Z) installer  
Installing VirtualBox to /opt/VirtualBox  
Python found: python, installing bindings...  
  
VirtualBox has been installed successfully.  
  
You will find useful information about using VirtualBox in the user manual  
    /opt/VirtualBox/UserManual.pdf  
and in the user FAQ  
    http://www.virtualbox.org/wiki/User\_FAQ  
  
We hope that you enjoy using VirtualBox.
```

Configuring Virtualbox

- Configuration tasks:
 - Set host-only adapter to “Configure Adapter Manually”
 - Disable host-only network DHCP server
 - Configure host-only network adapter to utilize IP address 172.16.1.2 with netmask 255.255.255.0
 - Review Default Machine Folder settings, and reconfigure as necessary

Host-Only Network Interface

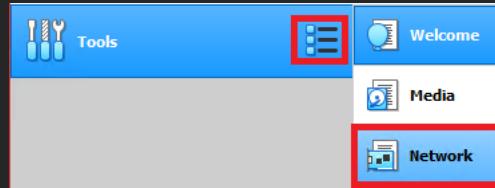
- By default, virtualbox installs a host-only network interface
 - Windows: Virtualbox Host-Only Network Adapter
 - Control Panel > Network and Internet > Network connections (ncpa.cpl)
 - Network configuration settings will persist beyond reboot
 - OSX/Linux: vboxnet0
 - ifconfig (Linux or OSX) or ip (Linux)
 - Network settings (and the interface itself) will NOT persist between reboots

Accessing the Host Network Manager

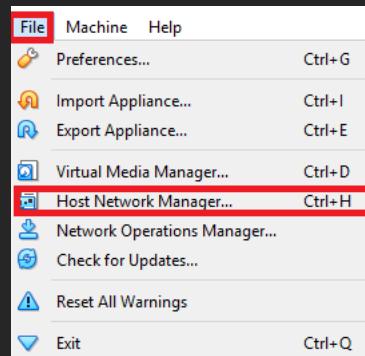
- Tool that allows you to:
 - Configure the default host-only adapter
 - IP Address/Netmask (not reliable)
 - Enable/Disable/Reconfigure DHCP service for host-only network
- Can be accessed from the GUI:
 - File > Host Network Manager
 - Tools > Network

Accessing the Host Network Manager (cont'd)

- Method 1:



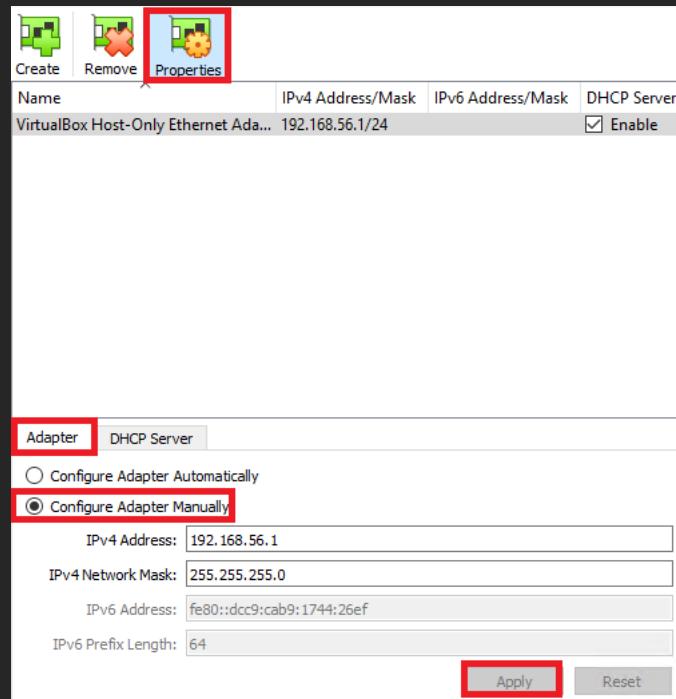
- Method 2:



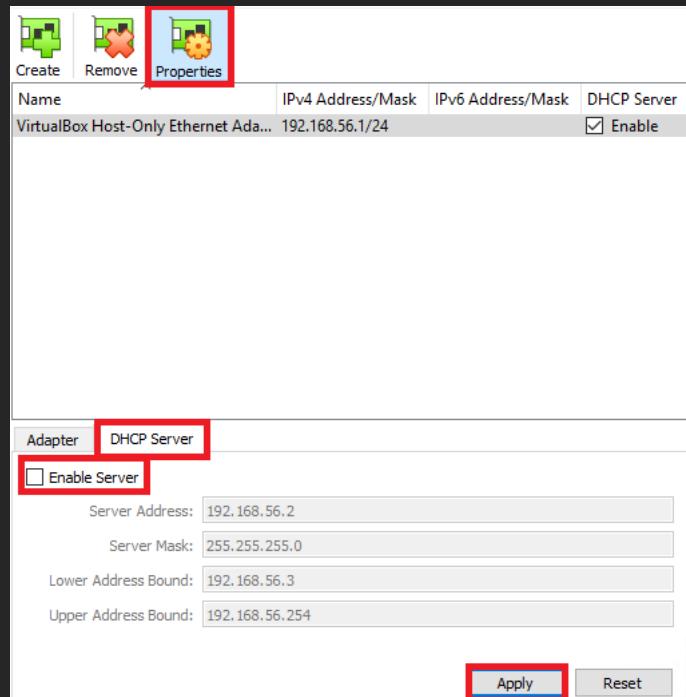
Tasks to complete

- Click Properties, select “Adapter” tab, confirm radio button “Configure Adapter Manually” is selected
- Click the “DHCP Server” tab , ensure that “Enable Server” checkbox is unchecked
- Click “Apply” if highlighted

Task 1



Task 2



Setting IP address and netmask for host-only adapter

- Can be done through the Host Network Manager, but its unreliable garbage
 - The IP address settings don't stick on Linux and OSX hosts.
- Recommended method: utilize native tools to configure the host-only network adapter
 - Windows: ncpa.cpl
 - Linux/OSX: ifconfig

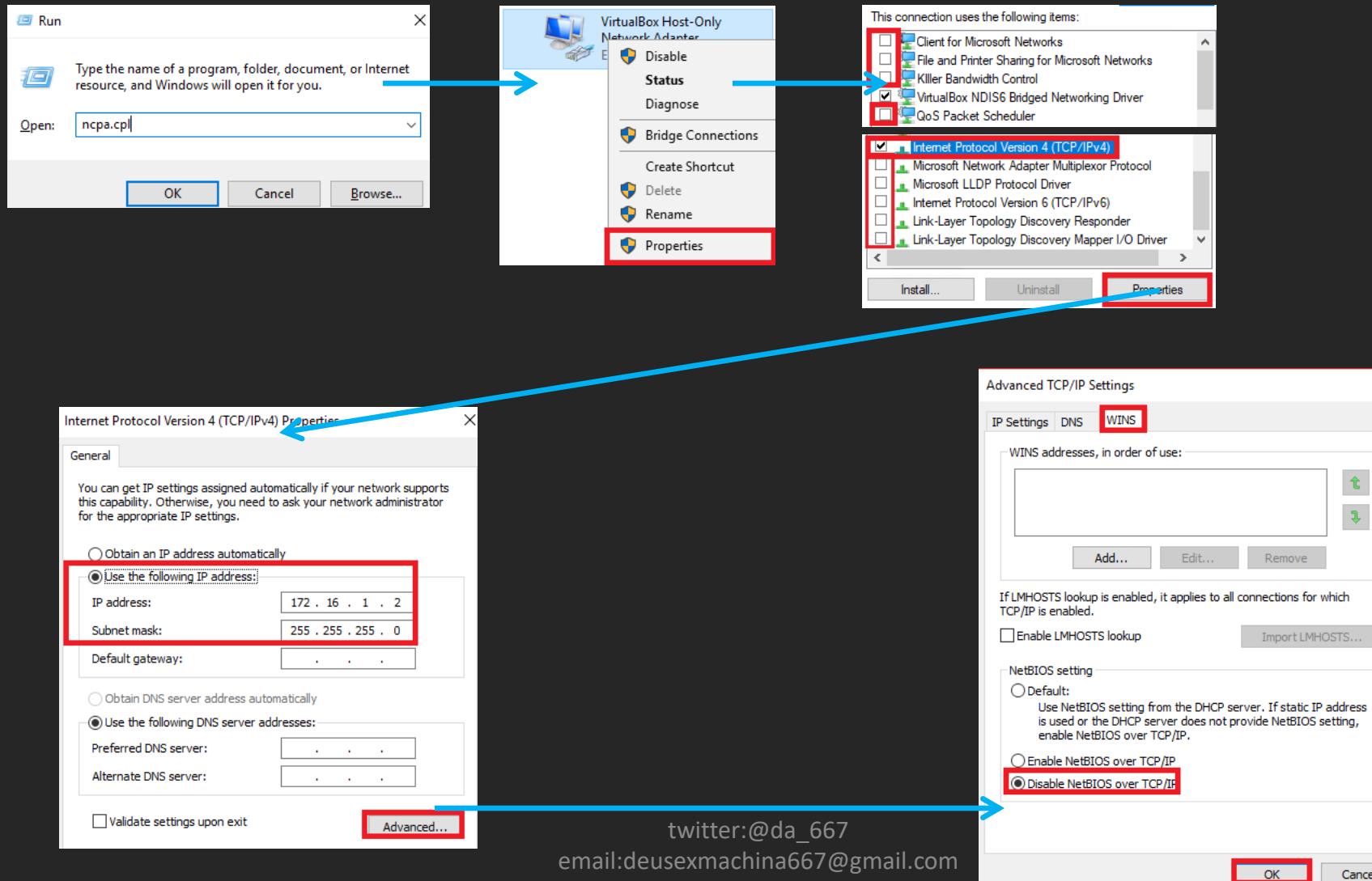
Configure IP address: Windows

- Windows Key + R (run prompt) > ncpa.cpl
- Virtualbox Host-Only Network Adapter > right click > properties
- Disable:
 - Client for Microsoft Networks
 - File and Printer Sharing for Microsoft Networks
 - QoS Packet Scheduler
 - Microsoft LLDP Protocol Driver
 - Internet Protocol Version 6 (optional)
 - Link-Layer Toplogy Discovery Responder
 - Link-Layer Topology Discovery Mapper I/O Driver

Configure IP address: Windows (cont'd)

- Highlight “Internet Protocol Version 4 (TCP/IPv4)” then click “Properties”
- Select the “Use the following IP address:” radio button
 - Enter 172.16.1.2 in the input box labeled “IP Address:”
 - Enter 255.255.255.0 in the input box labeled “Subnet mask:”
 - Leave the “Default gateway:”, “Preferred DNS server:”, and “Alternate DNS server:” blank
- Click “Advanced”
- Click on the “WINS” tab
 - Click the “Disable NetBIOS over TCP/IP” radio button, then click OK
- Click OK on the “Internet Protocol Version 4 (TCP/IPv4) Properties” window
- Click OK on the “Virtualbox Host-Only Network Adapter Properties” window

Configure IP address: Windows (cont'd)



Configure IP address: OSX

- Open Terminal (or iTerm2, if you installed it)
 - Default Terminal location: Applications > Utilities > Terminal
- Open virtualbox/ensure virtual box is running
- `sudo ifconfig vboxnet0 172.16.1.2 netmask 255.255.255.0`
 - Note: requires Administrator privileges
- `ifconfig vboxnet0` to confirm your configuration changes

Configure IP address: OSX (cont'd)



Configure IP address: Linux

- Open your Terminal app of choice
- Ensure virtualbox is running
- `ifconfig vboxnet0 172.16.1.2 netmask 255.255.255.0`
 - Add “sudo” for non-root users
 - `sudo ifconfig vboxnet0 172.16.1.2 netmask 255.255.255.0`
- `ifconfig vboxnet0` to verify results
- Note: some distros don’t ship with `ifconfig`
 - `ip` command is considered the new hotness.
 - Recommendations:
 - **Install package(s) required to use `ifconfig` (other portions of the lab utilize it)**
 - `[sudo] ip addr add 172.16.1.2/24 dev vboxnet0`
 - `[sudo] ip link set up dev vboxnet0`
 - `ip addr show vboxnet0` to verify results

Configure IP address: Linux



The screenshot shows a terminal window within the Oracle VM VirtualBox Manager interface. The terminal window has a blue header bar with the text "root@kali: ~". Below the header is a standard window menu bar with options like File, Edit, View, Search, Terminal, and Help. The main area of the terminal window displays a command-line session:

```
root@kali:~# whoami
root
root@kali:~# ifconfig vboxnet0 172.16.1.2 netmask 255.255.255.0
root@kali:~# ifconfig vboxnet0
vboxnet0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.16.1.2 netmask 255.255.255.0 broadcast 0.0.0.0
        ether 0a:00:27:00:00:00 txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Setting the Default Machine Folder (and other vbox settings)

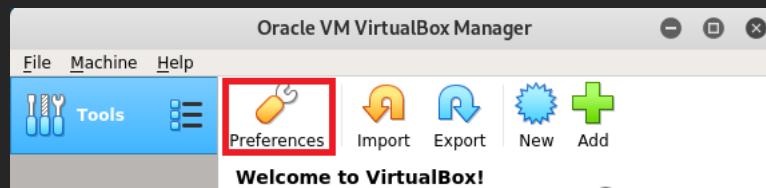
- The Preferences menu can be used to modify a host of virtualbox behaviors, and are divided into subcategories:
 - General
 - Input
 - Update
 - Language
 - Display
 - Network
 - Extensions
 - Proxy

Setting the Default Machine Folder (and other vbox settings) (cont'd)

- We're interested in the “General” sub-menu.
- To access vbox preferences you can:
 - Click the preferences icon from the virtualbox manager window
 - Click File > Preferences...
 - OSX: Virtualbox > Preferences...

Setting the Default Machine Folder (and other vbox settings) (cont'd)

- Option 1:



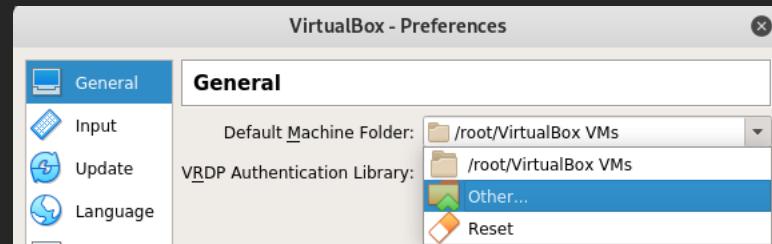
- Option 2:



Setting the Default Machine Folder

- Select “General” (should be selected by default)
- Default Machine Folder input box
 - Defines what folder/drive VM files are stored in by default
 - Click drop-down, select “Other...” and navigate to where you want your VMs stored

Setting the Default Machine Folder (cont'd)

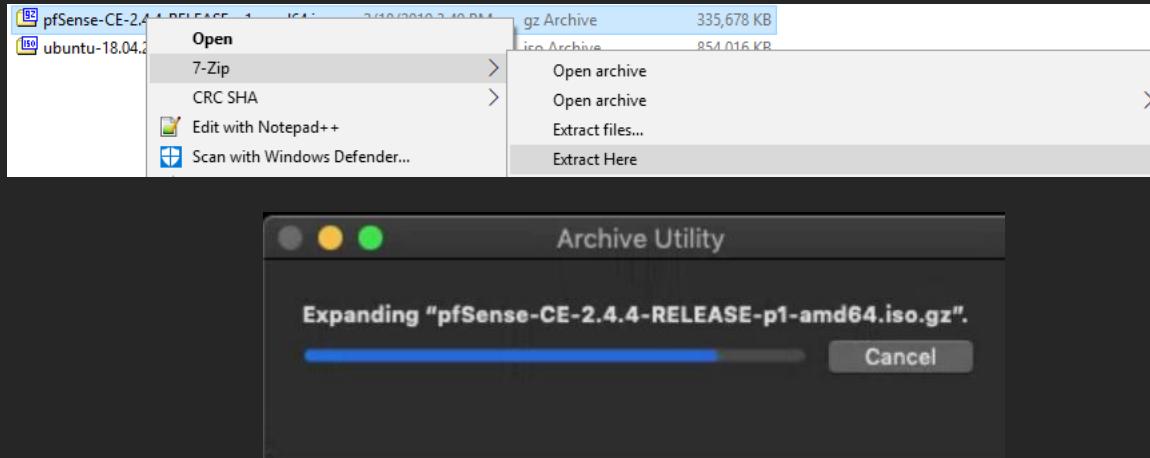


Chapter 6: Creating and Configuring our first VM, pfSense

Decompress the ISO

- Need to decompress the pfSense ISO
 - ISO is gzipped
- Windows: Use 7-zip
 - Right Click pfSense-CE-x.x.x-RELEASE-px-amd64.iso.gz -> “Extract Here”
- Linux/OSX:
 - Option 1: Utilize your window manager’s filemanager and unzip the file with it
 - Linux: YMMV
 - OSX: Double click pfSense-CE-x.x.x-RELEASE-px-amd64.iso.gz
 - Automatically decompresses gz file.
 - Option 2: `gunzip/gzip -d`
 - Open terminal
 - `cd /path/to/ISO`
 - `gunzip pfSense-CE-x.x.x-RELEASE-px-amd64.iso.gz`
 - `gzip -d pfSense-CE-x.x.x-RELEASE-px-amd64.iso.gz`
 - Note: `gzip -d/gunzip` will delete the original gz file after decompressing it

Decompress the ISO cont'd

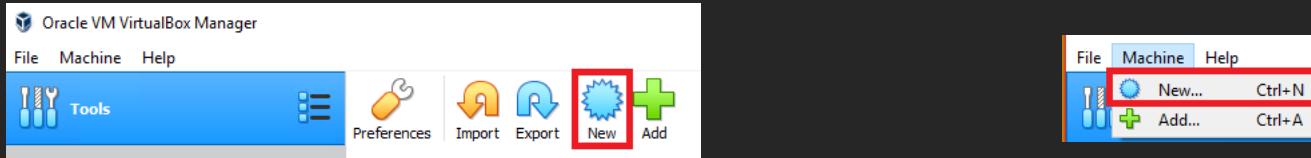


```
root@kali:~# pwd  
/root  
root@kali:~# gunzip pfSense-CE-2.4.4-RELEASE-p1-amd64.iso.gz  
root@kali:~# ls *.iso  
pfSense-CE-2.4.4-RELEASE-p1-amd64.iso  
root@kali:~#
```

```
root@kali:~# pwd  
/root  
root@kali:~# gzip -d pfSense-CE-2.4.4-RELEASE-p1-amd64.iso.gz  
root@kali:~# ls *.iso  
pfSense-CE-2.4.4-RELEASE-p1-amd64.iso  
root@kali:~#
```

Creating a new VM

- Two options:
 - Click the New icon on the vbox GUI
 - Click Machine > New...



Create Virtual Machine Wizard:

- Screen 1:
 - Name: pfSense
 - Machine Folder: Default
 - Type: BSD
 - Version FreeBSD (64-bit)
- Screen 2:
 - Memory size: 512MB
- Screen 3:
 - Create virtual hard disk now
- Screen 4:
 - VDI (VirtualBox Disk Image)
- Screen 5:
 - Fixed size
- Screen 6:
 - Name: PfSense
 - Size: 5.00GB

Create Virtual Machine Wizard (cont'd):

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: pfSense
Machine Folder: E:\VMs
Type: BSD
Version: FreeBSD (64-bit)

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 1024 MB.
 MB

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is 16.00 GB.

Do not add a virtual hard disk
 Create a virtual hard disk now

File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
pfSense

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
 MB

Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

Dynamically allocated
 Fixed size

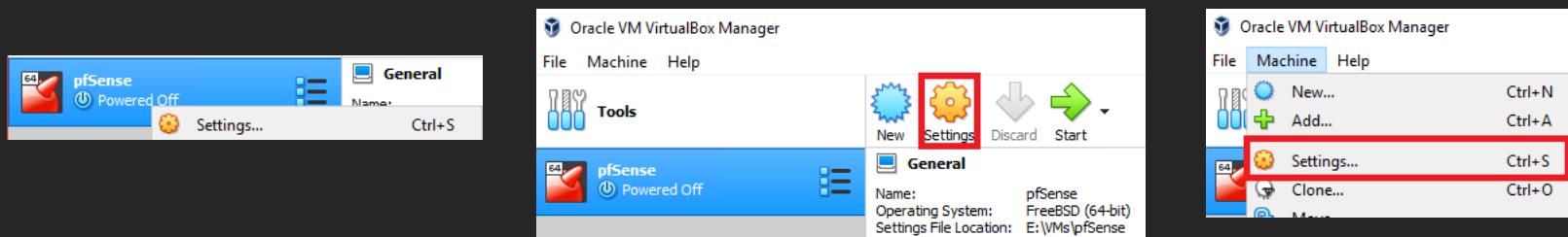
pfSense General System Display Storage Audio Network USB

pfSense
Powered Off
Name: pfSense
Operating System: FreeBSD (64-bit)
Settings File Location: E:\VMs\pfSense
System
Base Memory: 512 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging
Display
Video Memory: 16 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Primary Master: pfSense.vdi (Normal, 5.00 GB)
IDE Secondary Master: [Optical Drive] Empty
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB

pfSense Preview

Customizing VM settings

- Access the VM settings menu
 - Right click VM > Settings...
 - Highlight VM > Machine > Settings...
 - Highlight VM > click Settings gear icon
 - Are you starting to notice a pattern?



Change the following settings

- Audio:
 - Uncheck “Enable Audio”
- USB:
 - Uncheck “Enable USB”
- Shared Folders
 - Verify there are NO shared folders specified
- Serial Ports:
 - Verify “Enable Serial Port” is unchecked for Port 1, Port2, Port 3, and Port 4

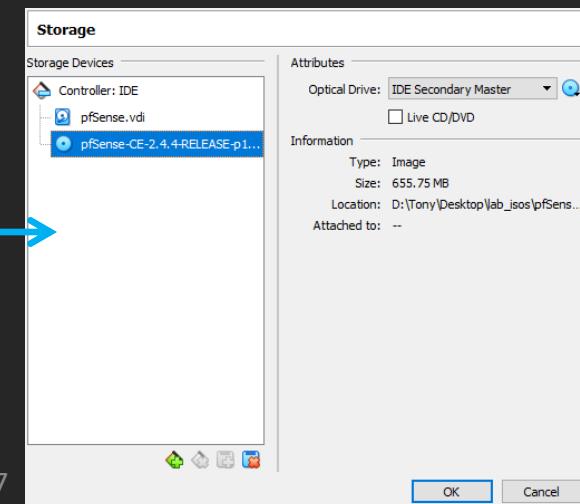
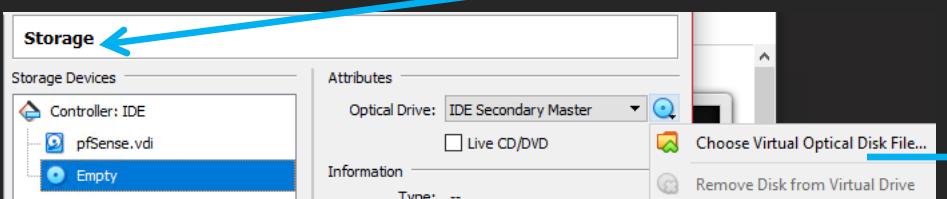
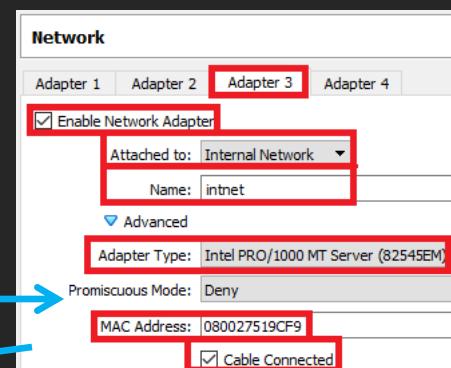
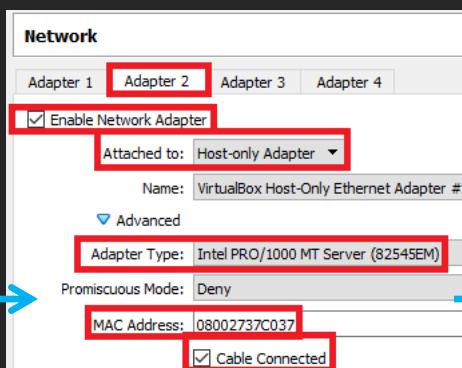
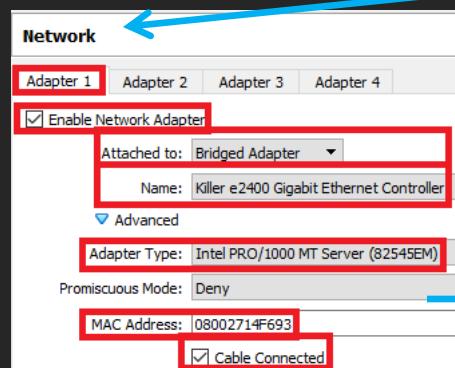
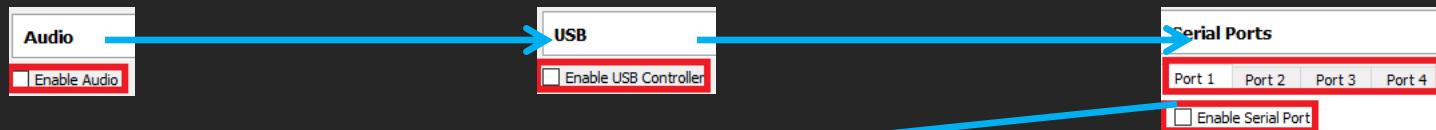
Change the following settings (cont'd)

- Network:
 - Adapter 1 Tab:
 - Verify “Enable Network Adapter” is checked
 - Attached to: Bridged Adapter
 - Name: Select network card on host OS you use for connecting to the LAN/Internet
 - Click “Advanced” Drop-down
 - Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - MAC Address: copy the contents of this field to a text file, notebook, along with the network it is attached to and VM it belongs to (important for later)
 - Adapter 2 Tab:
 - Verify “Enable Network Adapter” is checked
 - Attached to: Host-Only Adapter
 - Advanced:
 - Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - MAC Address: Same as Adapter 1, Copy the contents, network and VM this corresponds to
 - Adapter 3 Tab:
 - Verify “Enable Network Adapter” is checked
 - Attached to: Internal Network
 - Name: intnet
 - Advanced:
 - Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - MAC Address: Same as Adapter 1, Copy the contents, network and VM this corresponds to

Change the following settings (cont'd)

- Storage:
 - Click on “Empty” under “Storage Devices”
 - Click on CD/DVD icon next to the “Optical Drive:” drop-down under “Attributes”
 - Select “Choose Virtual Optical Disk File, browser to decompressed pfSense ISO, then click “OK”
 - Note: this will apply the settings from the other “Change the following settings” slides

Change the following settings (cont'd)



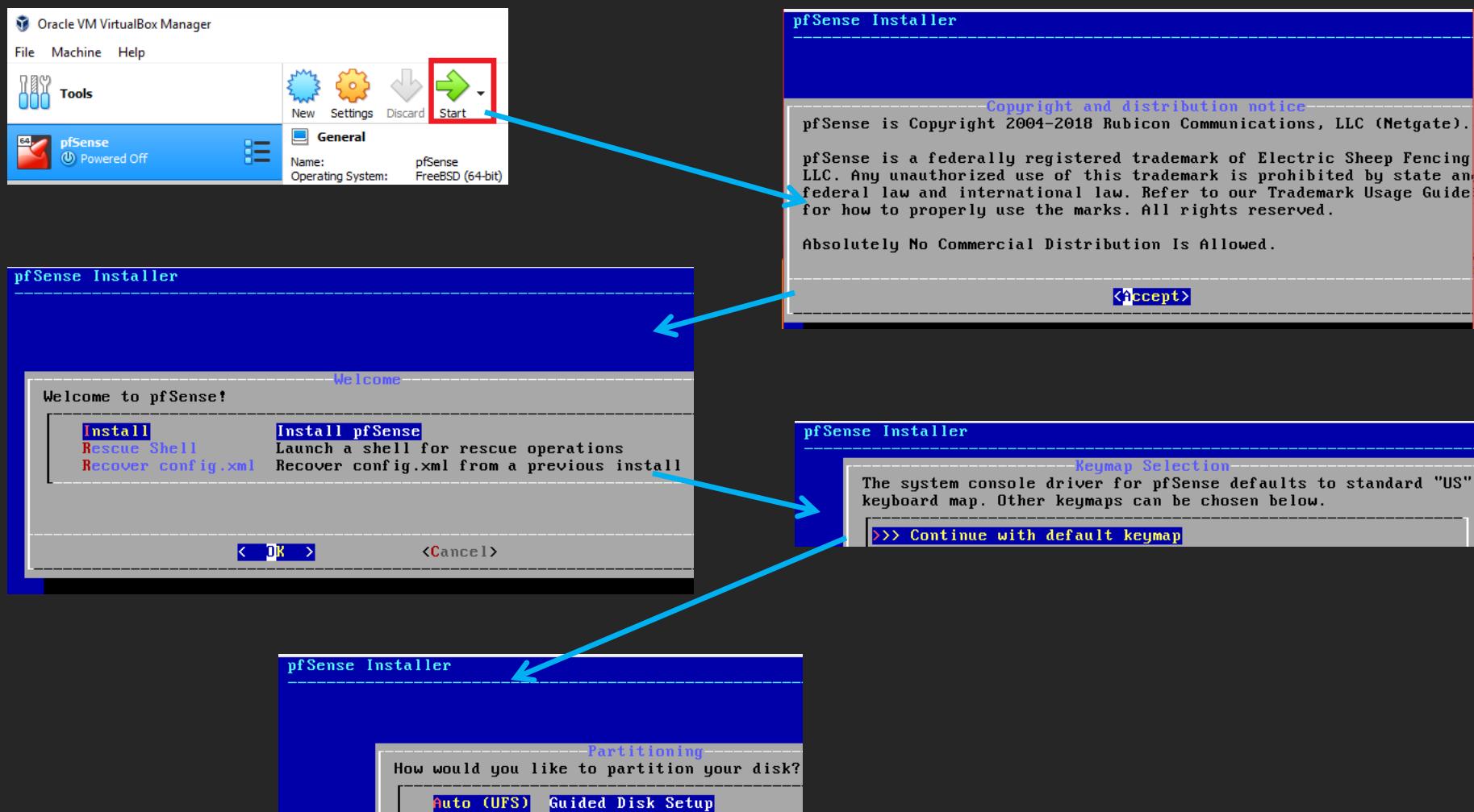
Installing the OS

- Click that big green start button
 - Be sure to select “Normal Start”
 - Console window will appear
 - Note: Clicking this window “attaches” your keyboard/mouse to the VM. “Host Key Combination” gives the keyboard/mouse back to the host OS:
 - Windows/Linux: Right ctrl
 - OSX: Left meta (that weird clover thing)
 - Key can be changed in Preferences > Input > Virtual Machine >Host Key Combination

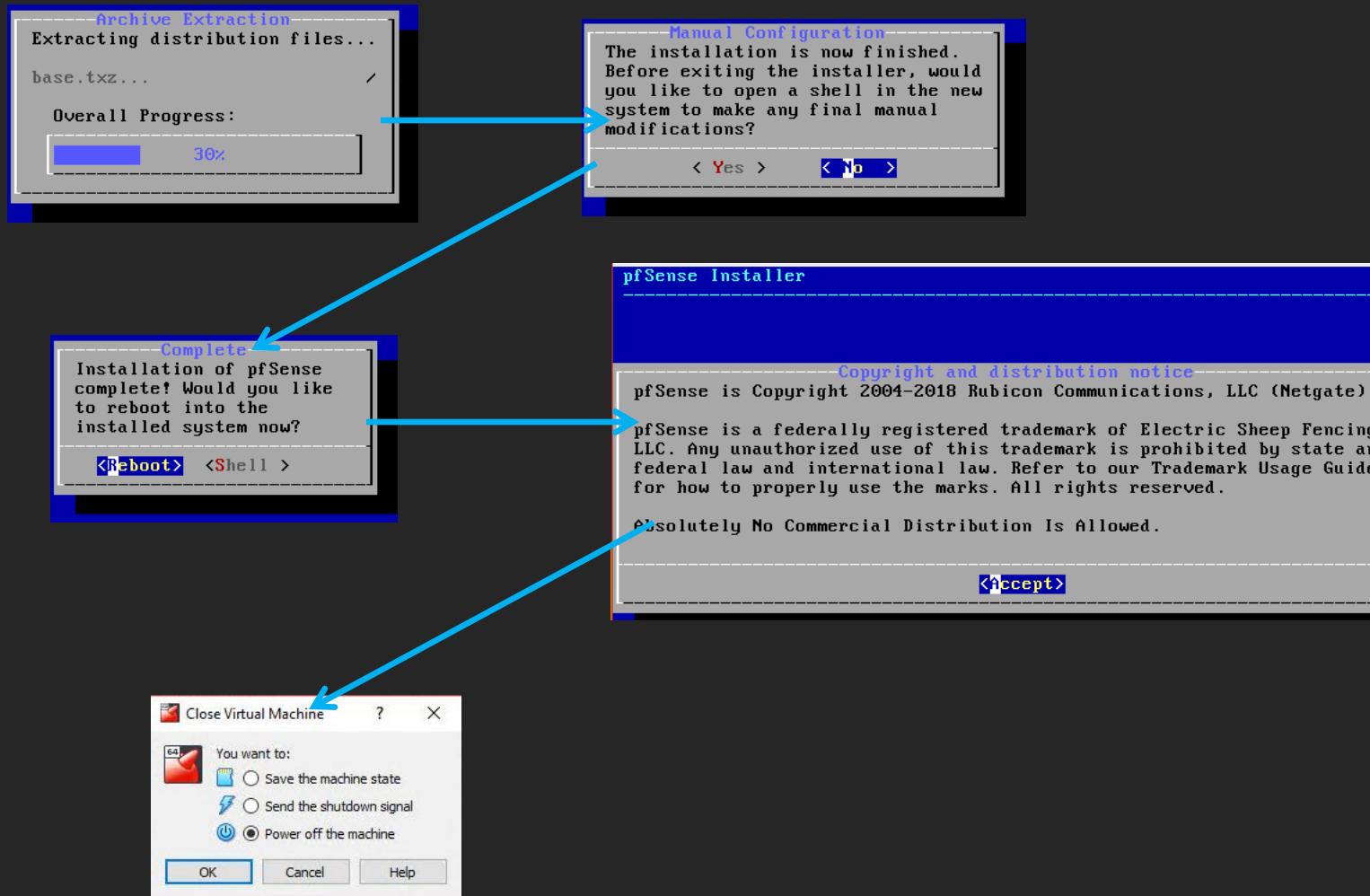
Installing the OS (cont'd)

- Should boot to the pfSense Installer
 - Select Install
 - Select your keymap (Default: US)
 - Select your partitioning setup (Auto (UFS) Guided Disk Setup)
 - Select No on “Manual Configuration” screen (hit tab key)
 - Select “Reboot” on “Complete screen (hit enter)
 - After system reboots, (probably into the pfSense installer), close the VM console. When prompted, select “Power off the machine”.

Installing the OS (cont'd)



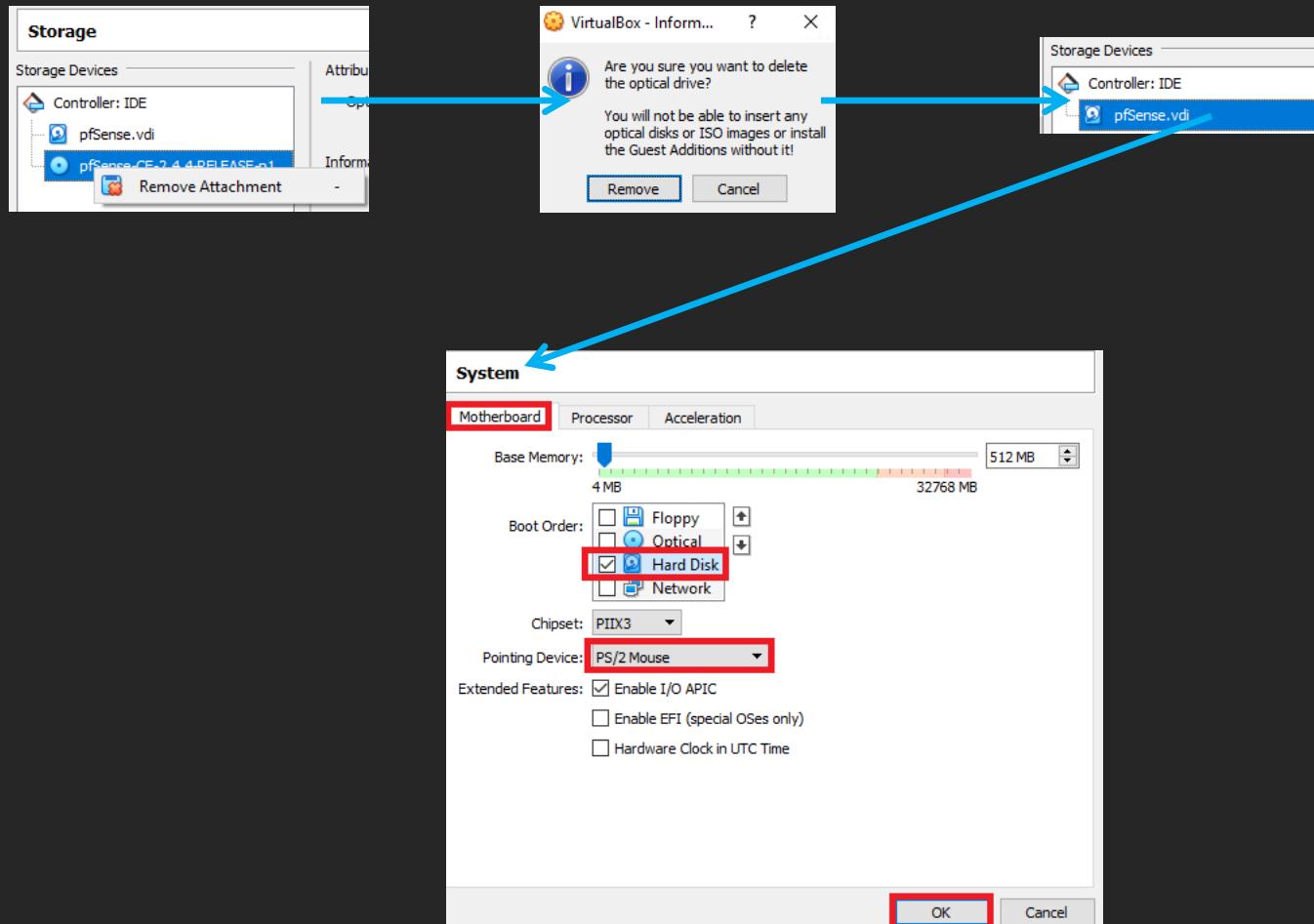
Installing the OS (cont'd)



Few more settings to mess with...

- Navigate back to the pfSense VM settings and perform the following actions:
 - Navigate to “Storage”
 - Remove the pfSense ISO and Virtual CD drive located under Storage Devices (should be second entry, under “Controller: IDE”, right below “pfSense.vdi”)
 - Navigate to “System”
 - Under the “Motherboard” tab, uncheck all boot options EXCEPT for “Hard Disk”
 - Verify that “Pointing Device:” is set to “PS/2 Mouse”
 - Click “OK” to apply settings for both Storage, and System, and exit the pfSense VM Settings menu

Few more settings to mess with... (cont'd)



Why Bother?

- Information security discipline “attack surface reduction”
 - TL;DR: If you aren’t going to use it, disable or remove it
 - Make yourself a harder target

pfSense: Initial setup (CLI)

- Perform initial pfSense configuration tasks:
 - Map virtual network interfaces, network segments they are assigned to (bridged, host-only, intnet), to pfSense network interfaces (e.g. em0, em1, em2) to pfSense network interfaces (WAN, LAN, OPT1)
 - Assign IP addresses to WAN, LAN and OPT1 interfaces
 - Configure DHCP service and scopes for LAN and OPT1 interfaces
 - Perform some basic connectivity checks (ping, nslookup, curl) to verify basic net connectivity

pfSense Initial setup: Assign Interfaces

- Select option 1 on the command line menu, “Assign Interfaces”
- Select “n” to should VLANs be set up now?
- Assign the WAN, LAN, and OPT1 interfaces to em0, em1, and em2
 - WAN = Bridged virtual nic
 - LAN = Host-only virtual nic
 - OPT1 = intnet virtual nic
 - Tip: Use the MAC address to figure out which network maps to what network segment.

This right here is why you record the MAC addresses of your VMs

```
lab_mac_addresses.txt x
1 pfSense
2 nic 1: bridged
3 MAC address: 08:00:27:14:F6:93
4 nic 2: host-only
5 MAC address: 08:00:27:37:C0:37
6 nic 3: intnet
7 MAC address: 08:00:27:51:9C:F9

Valid interfaces are:
em0      08:00:27:37:c0:37  (up)
em1      08:00:27:51:9c:f9  (up)
em2      08:00:27:14:f6:93 (down)

Do VLANs need to be set up first?
If VLANs will not be used, or only say no here and use the webConfig

The interfaces will be assigned as follows:
WAN  -> em2
LAN  -> em0
OPT1 -> em1

Do you want to proceed [y\?n]? y
```

pfSense Initial setup: Set Interface(s) IP address

- Select option 2 on the command line menu, “Set Interface(s) IP address”
 - We will be doing this twice, once for the “LAN” interface, and once for the “OPT1” interface
 - Lan Interface:
 - IPv4 Address: 172.16.1.1
 - Netmask: 24 (255.255.255.0)
 - Do NOT set an IPv4 upstream gateway address (just hit enter)
 - Do NOT set up IPv6 (just hit enter)
 - Do you want to set up DHCP server on LAN? (yes)
 - Start address: 172.16.1.10
 - End address: 172.16.1.254
 - Do NOT reset the webconfigurator to HTTP (ever)
 - OPT1 Interface:
 - IPv4 Address: 172.16.2.1
 - Netmask: 24
 - Do NOT set an IPv4 upstream gateway address (just hit enter)
 - Do NOT set up IPv6 (just hit enter)
 - Do you want to set up DHCP server on OPT1? (yes)
 - Start address: 172.16.2.10
 - End address: 172.16.2.254
 - Do NOT reset the webconfigurator to HTTP (ever)

pfSense Initial setup: Set Interface(s) IP address (cont'd)

```
Available interfaces:  
1 - WAN (em2 - dhcp, dhcp6)  
2 - LAN (em0 - static)  
3 - OPT1 (em1)  
  
Enter the number of the interface you wish to configure: 2  
  
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 172.16.1.1  
  
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
      255.255.0.0   = 16  
      255.0.0.0     = 8  
  
Enter the new LAN IPv4 subnet bit count (1 to 31):  
> 24  
  
For a WAN, enter the new LAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
  
Enter the new LAN IPv6 address. Press <ENTER> for none:  
> ■  
  
Do you want to enable the DHCP server on LAN? (y/n) y  
Enter the start address of the IPv4 client address range: 172.16.1.10  
Enter the end address of the IPv4 client address range: 172.16.1.254  
Disabling IPv6 DHCPD...  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

```
Available interfaces:  
1 - WAN (em2 - dhcp, dhcp6)  
2 - LAN (em0 - static)  
3 - OPT1 (em1)  
  
Enter the number of the interface you wish to configure: 3  
  
Enter the new OPT1 IPv4 address. Press <ENTER> for none:  
> 172.16.2.1  
  
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
      255.255.0.0   = 16  
      255.0.0.0     = 8  
  
Enter the new OPT1 IPv4 subnet bit count (1 to 31):  
> 24  
  
For a WAN, enter the new OPT1 IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
  
Enter the new OPT1 IPv6 address. Press <ENTER> for none:  
> ■  
  
Do you want to enable the DHCP server on OPT1? (y/n) y  
Enter the start address of the IPv4 client address range: 172.16.2.10  
Enter the end address of the IPv4 client address range: 172.16.2.254  
  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

The IPv4 LAN address has been set to 172.16.1.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
<https://172.16.1.1/>

Remember This.

```
*** Welcome to pfSense 2.4.4-RELEASE-p1 (amd64) on pfSense ***  
  
WAN (wan)      -> em2          -> v4/DHCP4: 10.0.0.180/24  
                           v6/DHCP6: 2601:408:502:a00:27ff:fe14:f693/  
64  
LAN (lan)      -> em0          -> v4: 172.16.1.1/24  
OPT1 (opt1)    -> em1          -> v4: 172.16.2.1/24
```

pfSense Initial setup: Connectivity checks

- Select option 8 “Shell”
 - Opens a bourne shell on the firewall
 - Usefull for troubleshooting the underlying OS
- Run the following commands:
 - `ping -c4 www.google.com`
 - Why: ICMP connectivity check. Can we resolve a host on the internet, and get ICMP ECHO request/replies?
 - `nslookup www.google.com`
 - Why: DNS check. Verify that we are able to resolve hostnames
 - `curl -i www.google.com`
 - Why: HTTP/HTTPS connectivity check. Can we interact with a remote system on the internet over port 80 (http) or port 443 (https)?

pfSense Initial setup: Connectivity checks (cont'd)

```
Enter an option: 8

[2.4.4-RELEASE][root@pfSense.loca.../root: ping -c 4 www.google.com
PING www.google.com (172.217.4.36): 56 data bytes
64 bytes from 172.217.4.36: icmp_seq=0 ttl=54 time=26.914 ms
64 bytes from 172.217.4.36: icmp_seq=1 ttl=54 time=32.131 ms
64 bytes from 172.217.4.36: icmp_seq=2 ttl=54 time=20.117 ms
64 bytes from 172.217.4.36: icmp_seq=3 ttl=54 time=22.216 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 20.117/25.345/32.131/4.627 ms

[2.4.4-RELEASE][root@pfSense.loca.../root: nslookup www.google.com
Server:      127.0.0.1
Address:     127.0.0.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.216.68
Name:   www.google.com
Address: 2607:f8b0:4009:804::2004

[2.4.4-RELEASE][root@pfSense.loca.../root: curl -I www.google.com
HTTP/1.1 200 OK
Date: Thu, 28 Mar 2019 16:03:54 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-03-28-16; expires=Sat, 27-Apr-2019 16:03:54 GMT; path=/;
domain=.google.com
Set-Cookie: MID=180=y5F1bwR0UuF7ij2-ieeEQreqjLvtfH0gXDC9L3v7FOw3uBLrgIPk7icYeETJ
Engpu1R0JJ4QpuS5vnGd6tb-8I_SPsFhqCUBtkHP5fvkKqQ6vbQf74DmG76DMGdtttHjr02xpSIwlJK_
baFileSMbXezOXGcH19IQAq5Cbzifsrc; expires=Fri, 27-Sep-2019 16:03:54 GMT; path=/;
domain=.google.com; HttpOnly
Transfer-Encoding: chunked
Accept-Ranges: none
Vary: Accept-Encoding
```

Help! My network checks aren't working

- If you're here at CCC with me...
 - Remember that this is a conference network
 - There are hackers on this network spamming deauths and doing who the hell knows what else
 - We have to share this pipe with hundreds of other nerds downloading who knows what (300+ MB Metasploit framework updates, etc.)

Help! My network checks aren't working (cont'd)

- Now that your expectations are lowered (or for those of you at home)...
 - Are you familiar with the OSI or TCP/IP network models? (Don't worry if you have no idea what this is)
 - Start low (physical connectivity) and work your way up (MAC Addressing, IP address configs, etc.)
 - Is your network cable plugged in? Are you connected to the wi-fi network?
 - Is the WAN interface acquiring an IP address automatically?
 - » It should be getting one via DHCP from your local network
 - » It should also be getting its default gateway and DNS server(s) from this DHCP server
 - Did you assign the WAN interface to the correct virtualbox network interface?
 - » You need to match the MAC address of the virtualbox bridged network adapter to the correct pfsense network interface (e.g. emX), and assign that interface as the WAN interface

Help! My network checks aren't working (cont'd)

- Your local network may be restricting your connectivity
 - Some networks do MAC address filtering and/or port security
 - Talk to your system or network admins about getting approval for your lab environment
 - Try switching the bridged network adapter in virtualbox to “NAT”
 - Remember that NAT mode uses the hypervisor host’s IP address and network settings to communicate with external networks.
 - Check your SOHO router/firewall to ensure there aren’t firewall rules blocking your connectivity checks
 - Need to allow ICMP echo request outbound, and echo reply inbound for ping to work
 - Need to allow port 53/udp outbound for nslookup to work
 - Need to allow port 80/tcp and port 443/tcp outbound for HTTP/HTTPS connectivity (curl checks, software updates, etc.)
 - This shouldn’t be a problem on your network at home. Most SOHO/ISP routers allow practically anything outbound

Remember these connectivity check commands

- We'll be using the same connectivity checks (ping -c 4, nslookup, curl -I) to ensure the SIEM, IPS, and Kali VMs can all achieve outbound connectivity
- Note: We will be hardening network access in a later chapter
 - This will affect your ability to use ping (ICMP)
 - Unless you create a firewall rule to explicitly allow it

Accessing the pfSense WebConfigurator

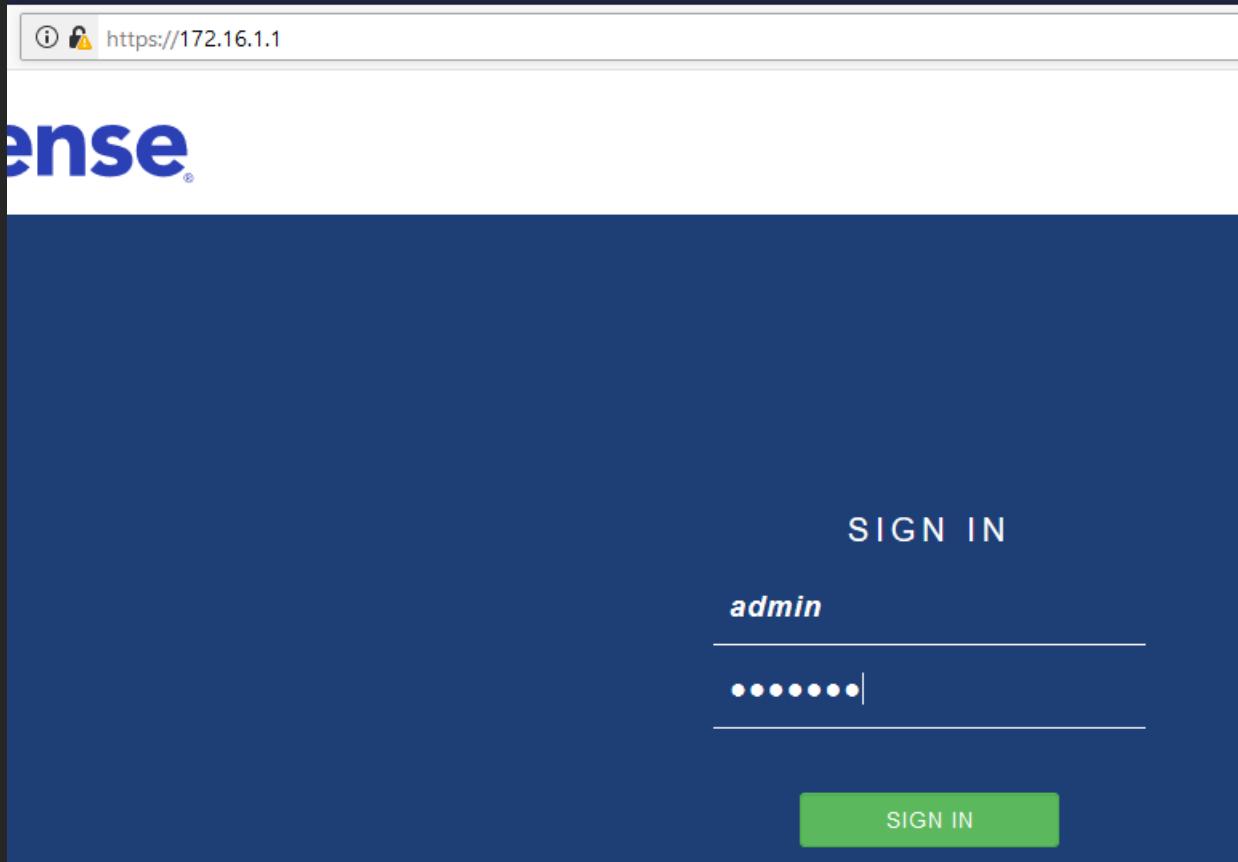
- Remember this earlier?

The IPv4 LAN address has been set to 172.16.1.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
<https://172.16.1.1/>

Remember This.

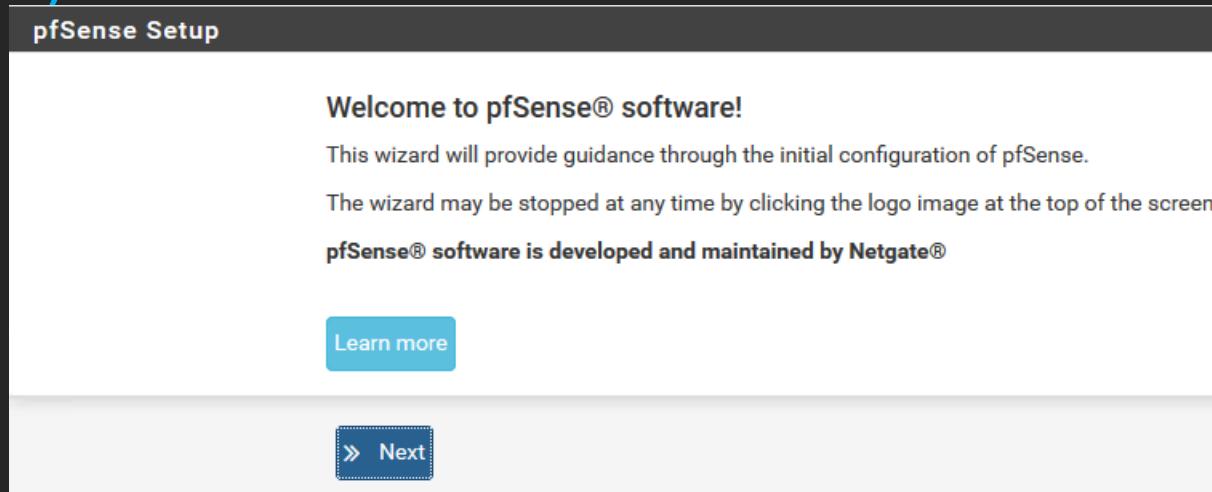
- Remember when we set the host-only network interface on (Linux/OSX/Windows) manually to 172.16.1.2/24?
 - Open your favorite web browser and point it to <https://172.16.1.1>
 - The default username and password for the webConfigurator is:
username: admin
password: pfsense
 - Don't worry, you'll be changing this in a minute
 - Note: the web interface uses a self-signed SSL cert. Modern browsers are paranoid and will tell you this is pure evil. You may need to create exceptions for 172.16.1.1 and/or choose "accept and continue" in order to log in.

Accessing the pfSense WebConfigurator (cont'd)



WebConfigurator first-time setup wizard

- Upon login, you'll be required to go through a first-time setup assistant.
 - As always, hit next to ignore the wall of text.
 - You can click next on the next page as well (step 1 of 9)



WebConfigurator first-time setup wizard (cont'd)

- Step 2 of 9 – General Information
 - Set the hostname and domain suffix
 - The defaults of “pfSense” and “localdomain” are fine
 - Primary/Secondary DNS Server
 - If you want pfSense to recurse to particular DNS servers (e.g. Cloudflare (1.1.1.1), Quad 9 (9.9.9.9), Google (8.8.8.8, 8.8.4.4) or your ISP’s DNS servers, enter them here.
 - Override DNS
 - If checked (recommended): Whatever DNS server DHCP tells the WAN interface to use will be what your lab uses for DNS resolution
 - If unchecked: Whatever DNS server(s) you enter here (or on the general page) will be the DNS servers used for DNS resolution in your lab
 - Network troubleshooting tip: Some ISPS (and corporate networks) require you to use only their DNS servers for hostname resolution. Keep this in mind, if DNS isn’t working in your lab environment

WebConfigurator first-time setup wizard (cont'd)

General Information

On this screen the general pfSense parameters will be set.

Hostname	<input type="text" value="pfSense"/>
EXAMPLE: myserver	
Domain	<input type="text" value="localdomain"/>
EXAMPLE: mydomain.com	
<p>The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.</p>	
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Override DNS	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN
» Next	

WebConfigurator first-time setup wizard (cont'd)

- Step 3 of 9 – Time Server Information
 - Leave both settings (Time Server Hostname and Timezone) default (click Next)

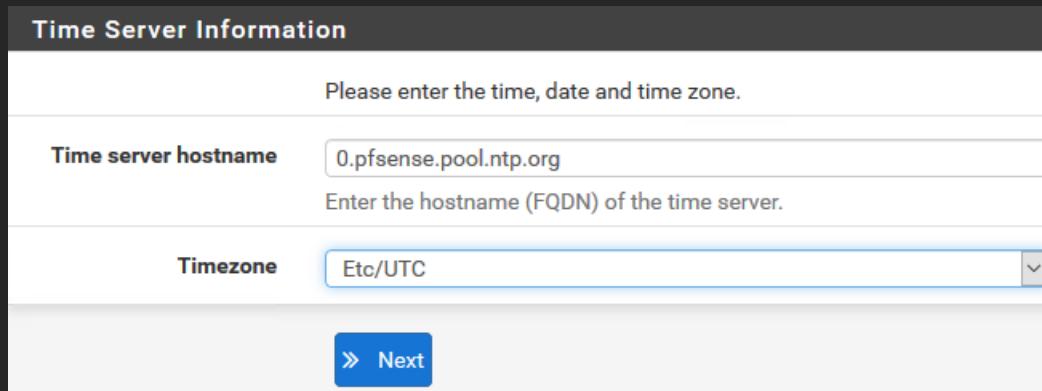
Time Server Information

Please enter the time, date and time zone.

Time server hostname Enter the hostname (FQDN) of the time server.

Timezone

[» Next](#)



WebConfigurator first-time setup wizard (cont'd)

- Step 4 of 9 – Configure WAN Interface
 - This page contains a bunch of other configuration options (E.g. MTU, MSS, DHCP hostname, PPTP and/or PPPoE credentials, etc.)
 - You would know better than I would if you need to change these things for your home/office network
 - Ensure SelectedType drop-down is set to DHCP. Leave all other settings default. Click Next



WebConfigurator first-time setup wizard (cont'd)

- Step 5 of 9 – Configure LAN Interface
 - Verify LAN IP Address is 172.16.1.1, and Subnet Mask is 24. Click Next

Configure LAN Interface

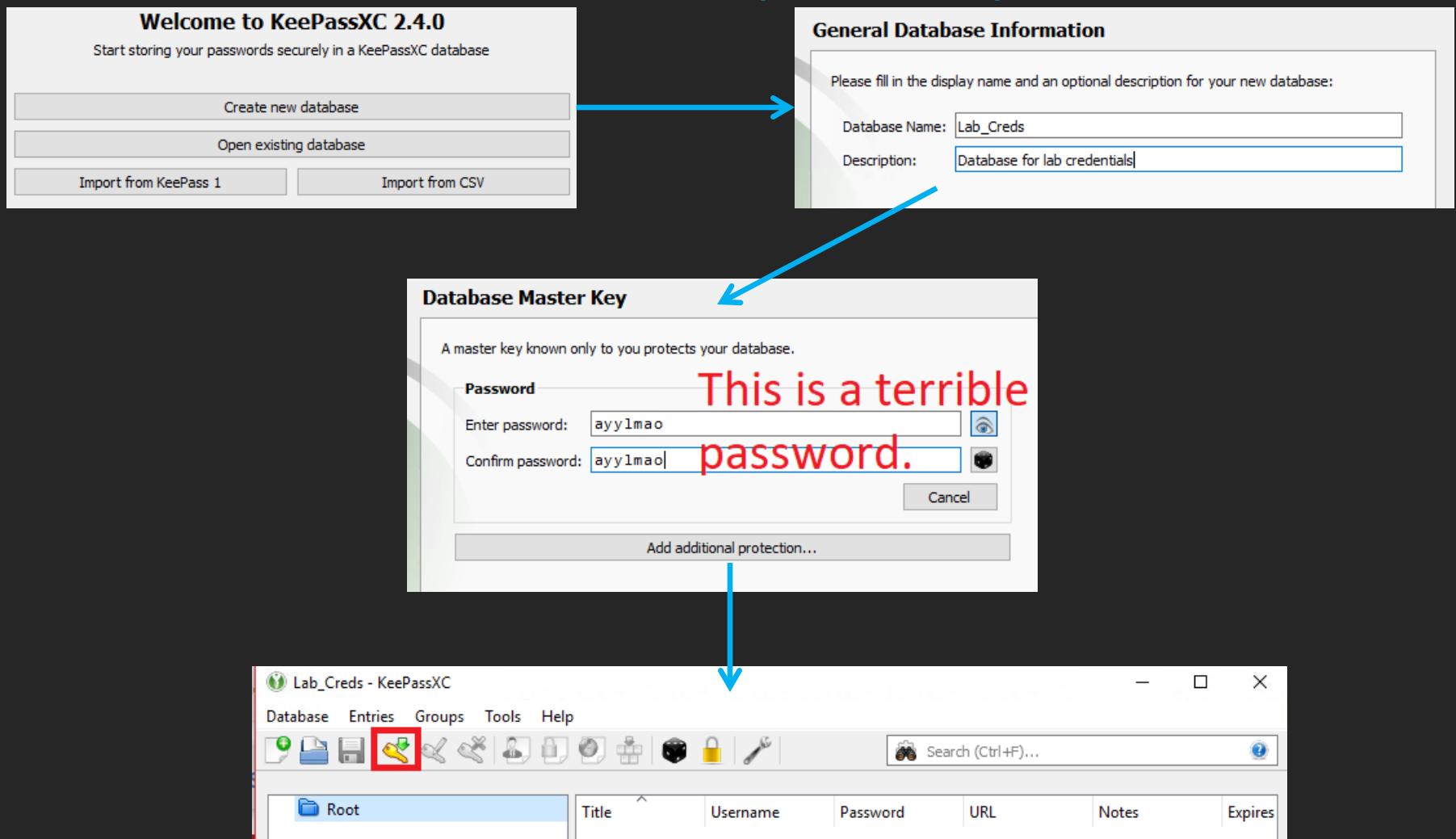
On this screen the Local Area Network information will be configured.

LAN IP Address	<input type="text" value="172.16.1.1"/>
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	<input type="text" value="24"/> <input type="button" value="▼"/>
<input type="button" value="» Next"/>	

WebConfigurator first-time setup wizard (cont'd)

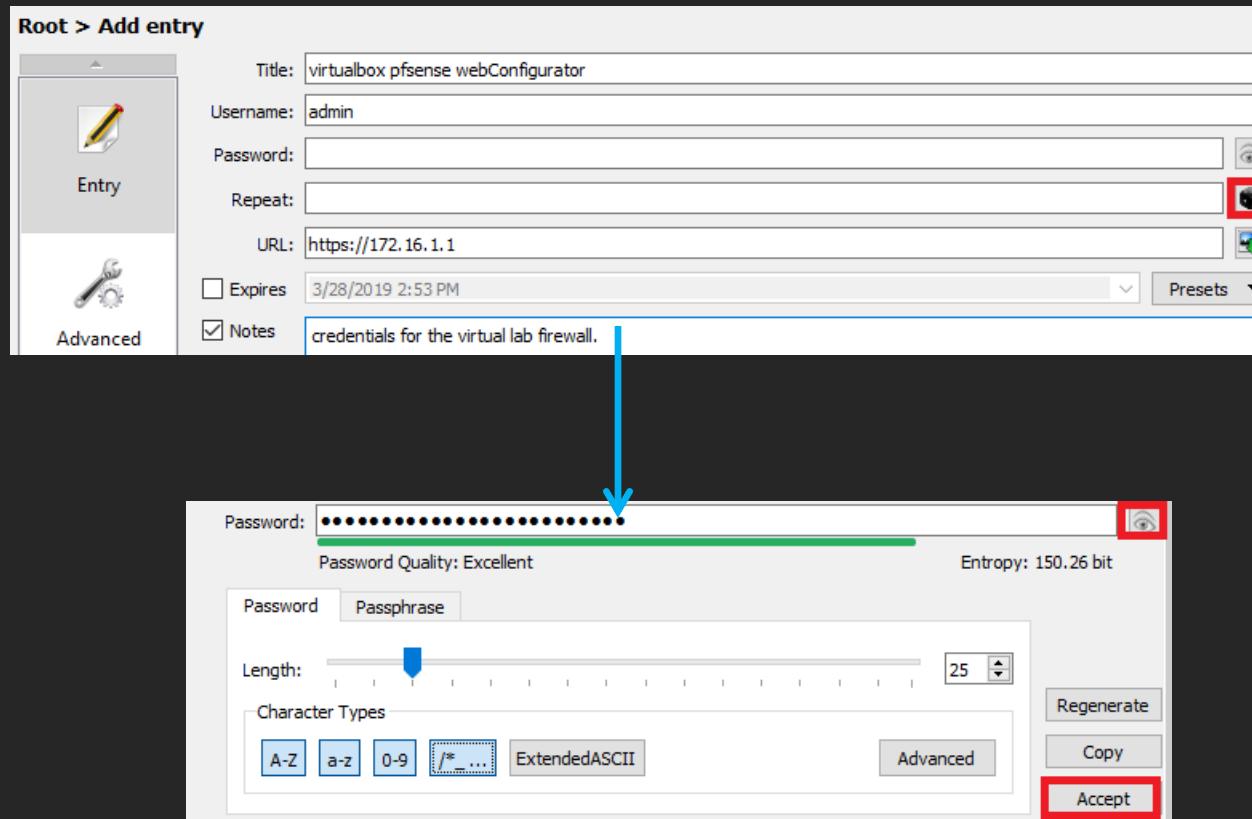
- Step 6 of 9 – Set Admin WebGUI Password
 - You'll need to change the default password.
 - If you haven't done so already, open up Keepass2 or KeepassXC, create a password database, create an entry for the webConfigurator, then click Next

WebConfigurator first-time setup wizard (cont'd)

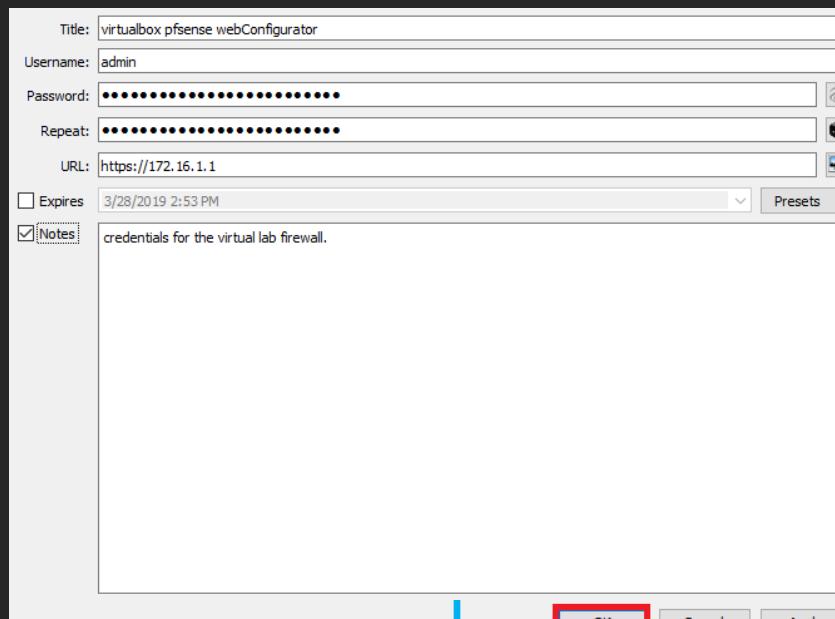


twitter:@da_667
email:deusexmachina667@gmail.com

WebConfigurator first-time setup wizard (cont'd)



WebConfigurator first-time setup wizard (cont'd)



Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: [REDACTED]

Admin Password AGAIN: [REDACTED]

>> Next

WebConfigurator first-time setup wizard (cont'd)

- Steps 7,8 of 9 – Reload configuration
 - Click the Reload button to apply your changes (including the new admin password)
- Step 9 of 9 – Wizard completed
 - Click the “Check for updates” button (recommended) or click “Finish” to be redirected to the Dashboard

WebConfigurator first-time setup wizard (cont'd)

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Checking for updates

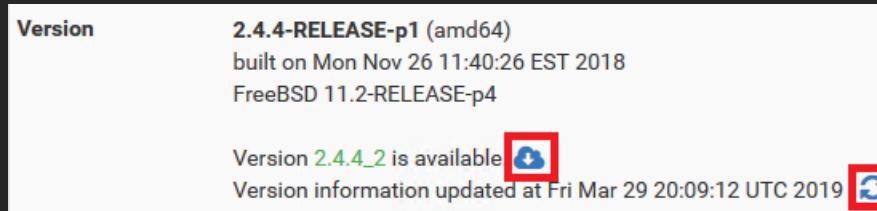
- Click “Check for updates” from the Webconfigurator first-time setup wizard

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

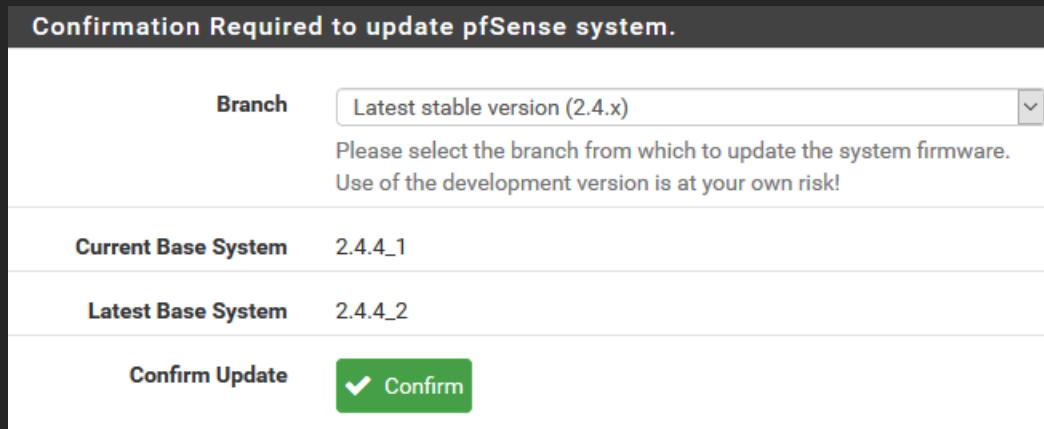
- OR on the Dashboard, under System Information, check the Version field.



- OR Select System > Update in the drop-down menu

Checking for updates (cont'd)

- On the System Update page:
 - Ensure “Latest stable version” is selected
 - Click Confirm
 - Note: will cause the VM to reboot. Log back in, and the update(s) should be applied.



Checking for updates (cont'd)

System / Update / System Update

Please wait while the system update completes.
This may take several minutes. Do not leave or refresh the page!

System Update Update Settings

Updating System

```
Installed packages to be UPGRADED:  
pfSense-rc: 2.4.4_1 -> 2.4.4_2 [pfSense-core]  
pfSense-kernel-pfSense: 2.4.4_1 -> 2.4.4_2 [pfSense-core]  
pfSense-default-config: 2.4.4_1 -> 2.4.4_2 [pfSense-core]  
pfSense-base: 2.4.4_1 -> 2.4.4_2 [pfSense-core]  
pfSense-Status_Monitoring: 1.7.6 -> 1.7.7 [pfSense]  
pfSense: 2.4.4_1 -> 2.4.4_2 [pfSense]  
nginx: 1.14.0_6,2 -> 1.14.1,2 [pfSense]  
libzmq4: 4.2.3 -> 4.3.1 [pfSense]  
curl: 7.62.0 -> 7.64.0 [pfSense]  
  
Number of packages to be upgraded: 9  
  
53 MiB to be downloaded.  
[1/9] Fetching pfSense-rc-2.4.4_2.txz: .. done  
[2/9] Fetching pfSense-kernel-pfSense-2.4.4_2.txz: ....
```

A few more things to do

- System > General Setup
 - Change to the dark theme (your eyes will thank you)
 - Set up additional DNS resolvers (optional)
- System > Package Manager
 - Install and enable the Squid proxy service
- Firewall > Rules
 - (Temporary) allow any/any rules to set up our VMs
- Snapshots
 - Revert your VM, in case you make mistakes

System > General Setup

- DNS Server Settings
 - You can specify additional DNS servers here and/or DNS Server Override settings
- webConfigurator
 - Select “pfSense dark” from the Theme drop-down
 - Note: Theme will not change until after you click Save AND navigate away from this page
- Be sure to click Save on the bottom of the page for your settings to apply

System > General Setup (cont'd)

DNS Server Settings

DNS Servers	<input type="text" value="DNS Server"/> <input type="button" value="none"/>
Add DNS Server	<input type="button" value="Add DNS Server"/>
DNS Server Override	<input checked="" type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.
Disable DNS Forwarder	<input type="checkbox"/> Do not use the DNS Forwarder/DNS Resolver as a DNS server for the firewall By default localhost (127.0.0.1) will be used as the first DNS server where the DNS Forwarder or DNS Resolver is enabled and set to listen on localhost, so system can use the local DNS service to perform lookups. Checking this box omits localhost from the list of DNS servers in resolv.conf.

webConfigurator

Theme	<input type="text" value="pfSense-dark"/>
Choose an alternative css file (if installed) to change the appearance of the webConfigurator. css files are located in /usr/local/www/css/	

Status / Dashboard

System Information	
Name	pfSense.localdomain
User	admin@172.16.1.2 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 28a07c87d75f0a5bca56
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.4.4-RELEASE-p2 (amd64) built on Wed Dec 12 07:40:18 EST 2018 FreeBSD 11.2-RELEASE-p6
The system is on the latest version. Version information updated at Sat Mar 30 17:04:43 UTC 2019	

System > Package Manager

- Click on Available Packages, search for squid and install the package named “squid”
 - Not squidGuard, not Lightsquid, just squid.
- Just like the system update, click confirm, and let pfSense do its thing.

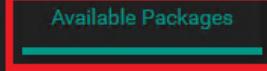
System > Package Manager

System / Package Manager / Available Packages



Installed Packages

Available Packages



Search



Search term

squid

Both



Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name Version Description

Lightsquid 3.0.6_5 LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.



Package Dependencies:

lighttpd-1.4.49 lightsquid-1.8_5

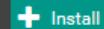
squid 0.4.44_7 High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.



Package Dependencies:

squidclamav-6.16 squid_radius_auth-1.10 squid-3.5.27_3 c-icap-modules-0.5.2

squidGuard 1.16.18_1 High performance web proxy URL filter.



Package Dependencies:

squidguard-1.4_15

Confirmation Required to install package pfSense-pkg-squid.

Confirm

Services > Squid Proxy Server

- Menu option appears after squid is installed
- Need to change things on the “General” and “Local Cache” tabs
- Local Cache:
 - Scroll to the bottom of the tab and click Save
 - Why: Squid service demands you to set the Local Cache policy in order to run
- General tab:
 - Under Squid General Settings:
 - Check Enable Squid Proxy
 - Change Proxy Interface(s) to LAN and OPT1
 - Under Headers Handling, Language and other Customizations:
 - Set X-Forwarded Header Mode drop-down to off
 - Check “Disable VIA Header”
 - Check “Suppress Squid Version”
 - Why: Deception
- Click Save when you have made these changes

Services > Squid Proxy Server (cont'd)

Squid General Settings

Enable Squid Proxy Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Proxy Interface(s) LAN
OPT1
WAN
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Headers Handling, Language and Other Customizations

Visible Hostname localhost
This is the hostname to be displayed in proxy server error messages.

Administrator's Email admin@localhost
This is the email address displayed in error messages to the users.

Error Language en
Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode off
Choose how to handle X-Forwarded-For headers. Default: on [i](#)

Disable VIA Header If not set, Squid will include a Via header in requests and replies as required by RFC2616.

URI Whitespace Characters Handling strip
Choose how to handle whitespace characters in URL. Default: strip [i](#)

Suppress Squid Version Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Firewall > Rules

- Navigate to the LAN tab:
 - Delete “Default allow LAN IPv6 to any rule (click the trashcan Action icon)
 - Add Allow rule for IPv4 TCP src: 172.16.1.2 dst: 172.16.1.1 port: 443 (HTTPS) description: better anti-lockout rule
 - If necessary, re-arrange rule to where it sits just below the rule labeled “Anti-Lockout Rule”
- Navigate to OPT1 tab:
 - Create IPv4 deny src 172.16.2.2 dst:any protocol: any
 - Metasploitable2 should never be allowed to talk to ANYTHING outside of our lab
 - Create IPv4 allow any src/dst, any protocol
 - Place this BELOW the deny rule
- Apply your firewall rule changes
 - Note: If you had to rearrange any rules, click Save to save the rule order, before applying your changes.
- Delete “Anti-Lockout Rule” (back on LAN tab)
 - Click the gear, click the checkbox next to “Anti-lockout” on System > Advanced > Admin Access, click Save
 - Navigate to Firewall > Rules > LAN, **MAKE ABSOLUTELY SURE** “better anti-lockout rule” is the first rule on the top

Firewall > Rules (cont'd)

Source

Source	<input type="checkbox"/> Invert match.	Single host or alias	172.16.1.2
---------------	--	----------------------	------------

Destination

Destination	<input type="checkbox"/> Invert match.	Single host or alias	172.16.1.1	
Destination Port Range	From	Custom	To	Custom
	HTTPS (443)		HTTPS (443)	

Description

Better Anti-Lockout Rule

A description may be entered here for administrative reference. A maximum log.

Firewall > Rules (cont'd)

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1 / 5.09 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
■	✓	0 / 3 KiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	
■	✓	0 / 0 B	IPv4 TCP	172.16.1.2	*	172.16.1.1	443 (HTTPS)	*	none	Better Anti-Lockout Rule	

Add Add Delete Save



Floating	WAN	LAN	OPT1								
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 / 6.53 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
■	✓	0 / 0 B	IPv4 TCP	172.16.1.2	*	172.16.1.1	443 (HTTPS)	*	none	Better Anti-Lockout Rule	
■	✓	0 / 3 KiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	

Add Add Delete Save

Firewall > Rules (cont'd)

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICM whereas with block the packet is dropped silently. In either case, the original packet is dis	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	OPT1
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any
Choose which IP protocol this rule should match.	
Source	
Source	<input type="checkbox"/> Invert match. any
Destination	
Destination	<input type="checkbox"/> Invert match. any
Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing the Status: System Logs: Settings page).
Description	OPT1 Allow ANY/ANY rule
A description may be entered here for administrative reference. A maximum of 52 character log.	

Firewall > Rules (cont'd)

Floating WAN LAN **OPT1**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✓ 0 /0 B	IPv4 *	*	*	*	*	*	none		OPT1 Allow ANY/ANY rule	

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.



 Apply Changes

Firewall > Rules (cont'd)

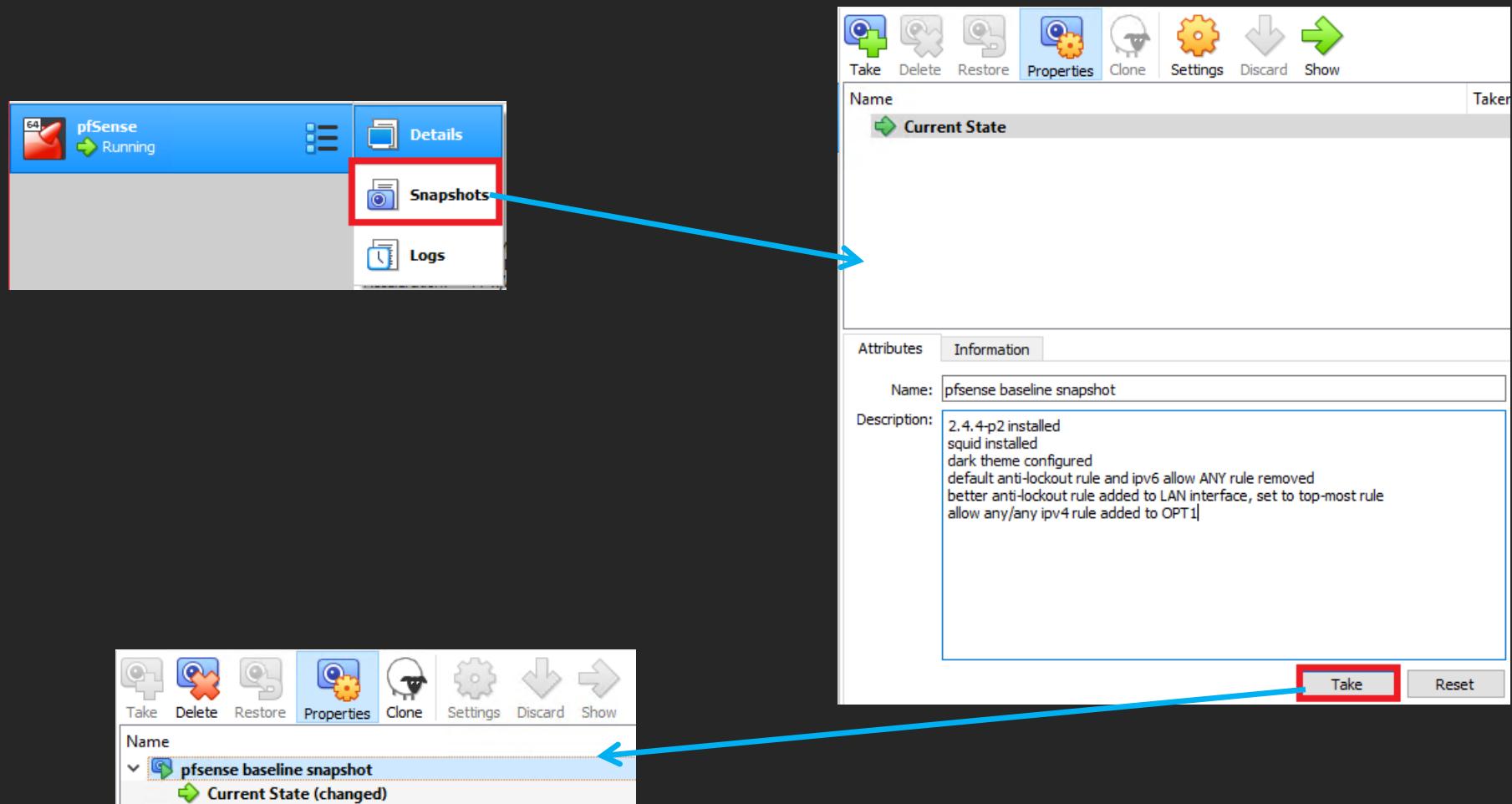
Floating	WAN	LAN	OPT1								
Rules (Drag to Change Order)											
#	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✓ 0 / 6.53 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
■	✓ 0 / 0 B	IPv4 TCP	172.16.1.2	*	172.16.1.1	443 (HTTPS)	*	none		Better Anti-Lockout Rule	
■	✓ 0 / 3 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

Rules (Drag to Change Order)											
#	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✓ 1 / 14 KiB	IPv4 TCP	172.16.1.2	*	172.16.1.1	443 (HTTPS)	*	none		Better Anti-Lockout Rule	
■	✓ 0 / 3 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

Snapshots

- TL;DR: capture the status of a VM in a particular point in time
 - Why: Can be used to revert (undo) recent changes
 - Bad configuration change/change management
 - Malware analysis
- Virtualbox manager > Bullet List Icon > Snapshots
 - Enter a snap shot name, brief description, and click Take

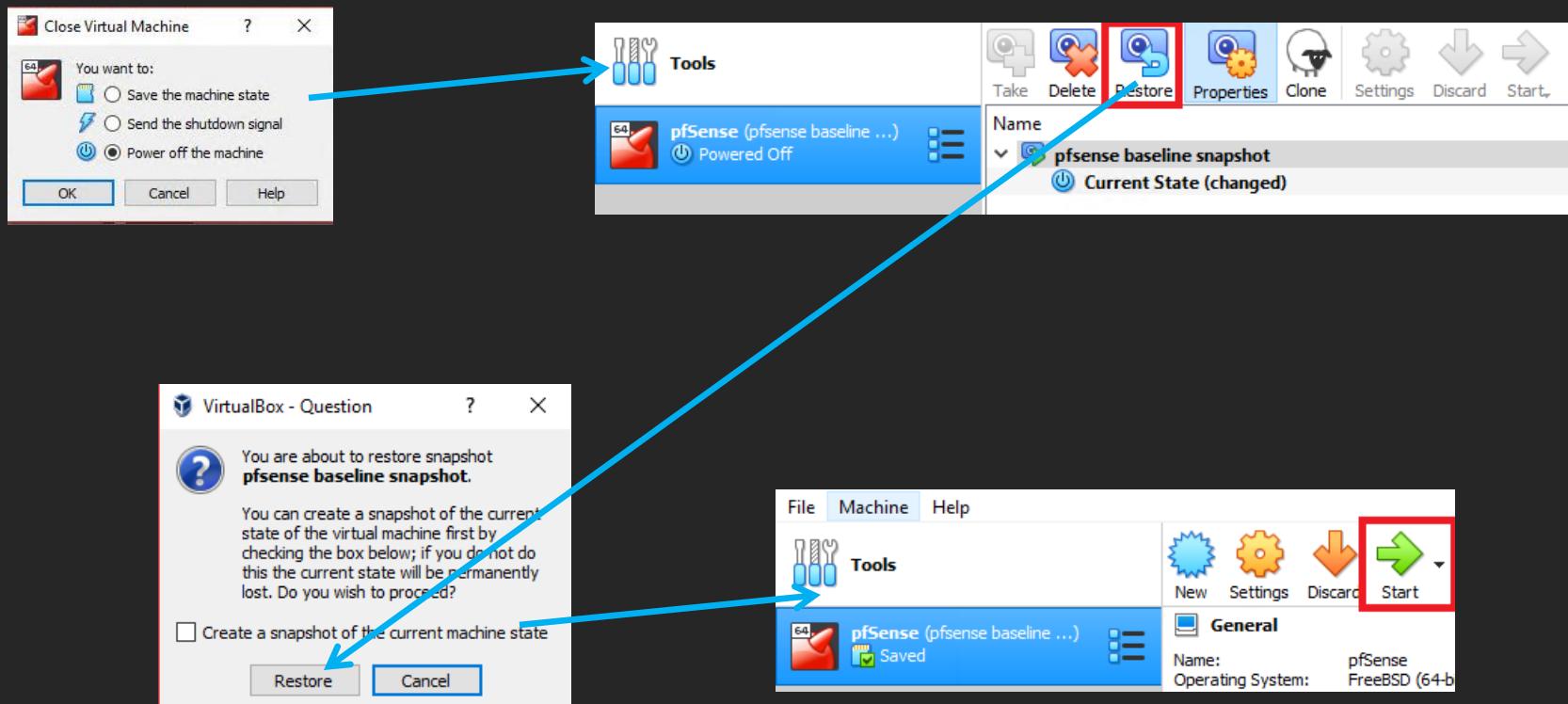
Snapshots (cont'd)



Snapshots (cont'd)

- Snapshots are NOT backups
- Snapshots are NOT a substitute for backups
 - EVER.
- To restore a snapshot:
 - Power off your VM
 - Navigate to snapshots
 - Select your snapshot
 - Click “restore”
- Don't need a snapshot? Delete it.
 - Keep at least one known good snapshot per VM
 - Use descriptive names, and make use of the notes field so you know what the hell it is you are restoring to
 - Keep your snapshots up to date
 - Nothing sucks more than restore a snapshot and finding out you have gigabytes of updates to apply, and a reboot to do before you can get anything done.

Snapshots (cont'd)



A large, white, metallic mecha stands in a dark, smoky environment, holding a large gun.

Chapter 7: The SIEM VM

twitter:@da_667

email:deusexmachina667@gmail.com

SIEM

- Security Information and Event Management
 - This is going to be our system that hosts IDS/IPS logs
 - OS: Ubuntu Server 18.04
 - SIEM software: Splunk Enterprise

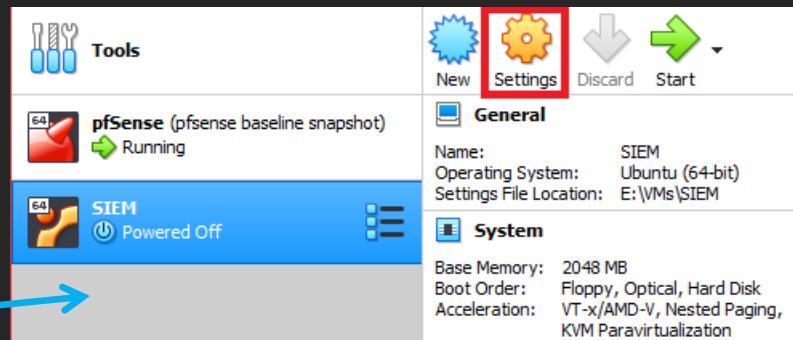
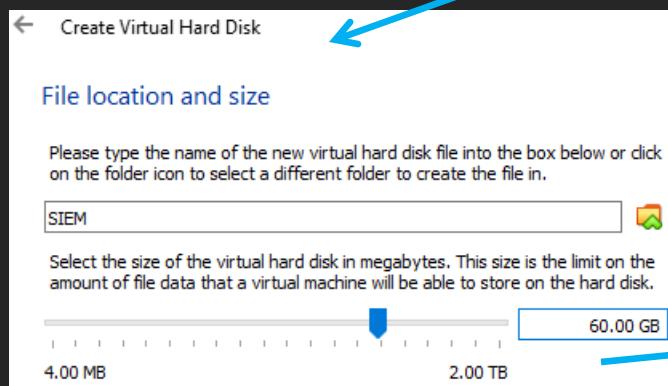
Tasks to Perform

- Create SIEM VM
 - Create static DHCP mapping on pfSense LAN network
- Strip away excess virtual hardware
- Install Ubuntu 18.04
- Strip remaining excess virtual hardware
- Perform connectivity checks
- Update VM
- Take baseline snapshot

Create Virtual Machine Wizard:

- Screen 1:
 - Name: SIEM
 - Machine Folder: Default
 - Type: Linux
 - Version: Ubuntu (64-bit)
- Screen 2:
 - Memory size: 2GB
- Screen 3:
 - Create virtual hard disk now
- Screen 4:
 - VDI (VirtualBox Disk Image)
- Screen 5:
 - Fixed size
- Screen 6:
 - Name: SIEM
 - Size: 60.00GB

Create Virtual Machine Wizard (cont'd)



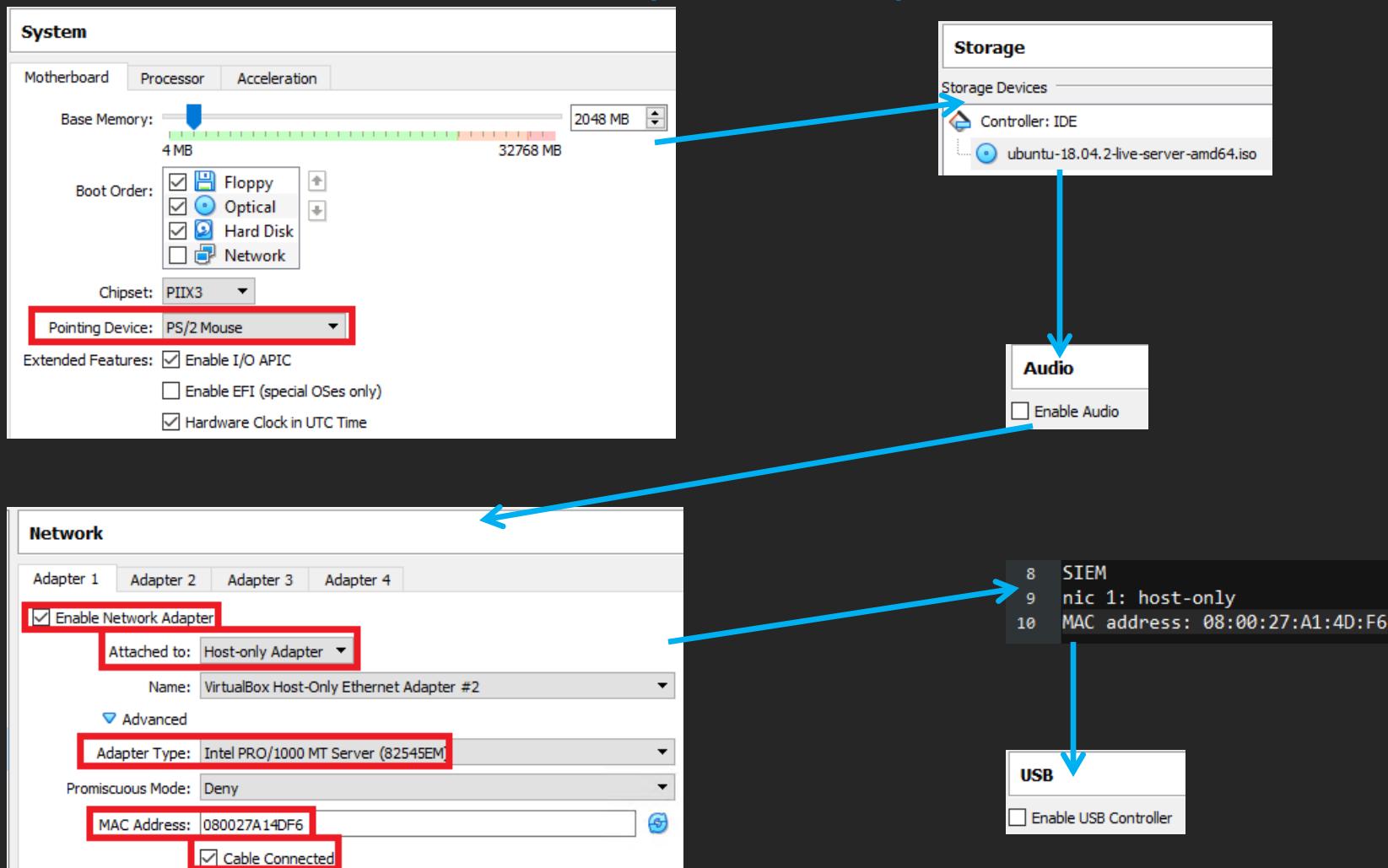
Strip away excess virtual hardware

- System:
 - Set Pointing Device drop-down to PS/2 Mouse
- Storage: Choose Virtual Optical Disk file
 - Ubuntu-18.04.X-live-server-amd64.iso
- Audio: Uncheck Enable Audio
 - Its PulseAudio and doesn't work half the time, anyhow.
- Network: Verify Enable Network Adapter checkbox is checked for Adapter 1 ONLY
 - Attached to: Host-only Adapter
 - Advanced Settings
 - Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - Copy the MAC Address to your MAC address text file/document
 - Ensure Cable Connected is checked

Strip away excess virtual hardware (cont'd)

- Serial Ports
 - Ensure no serial ports are enabled (should be default)
- USB: Uncheck Enable USB Controller
- Shared Folders
 - Ensure no shared folders are configured (should be default)

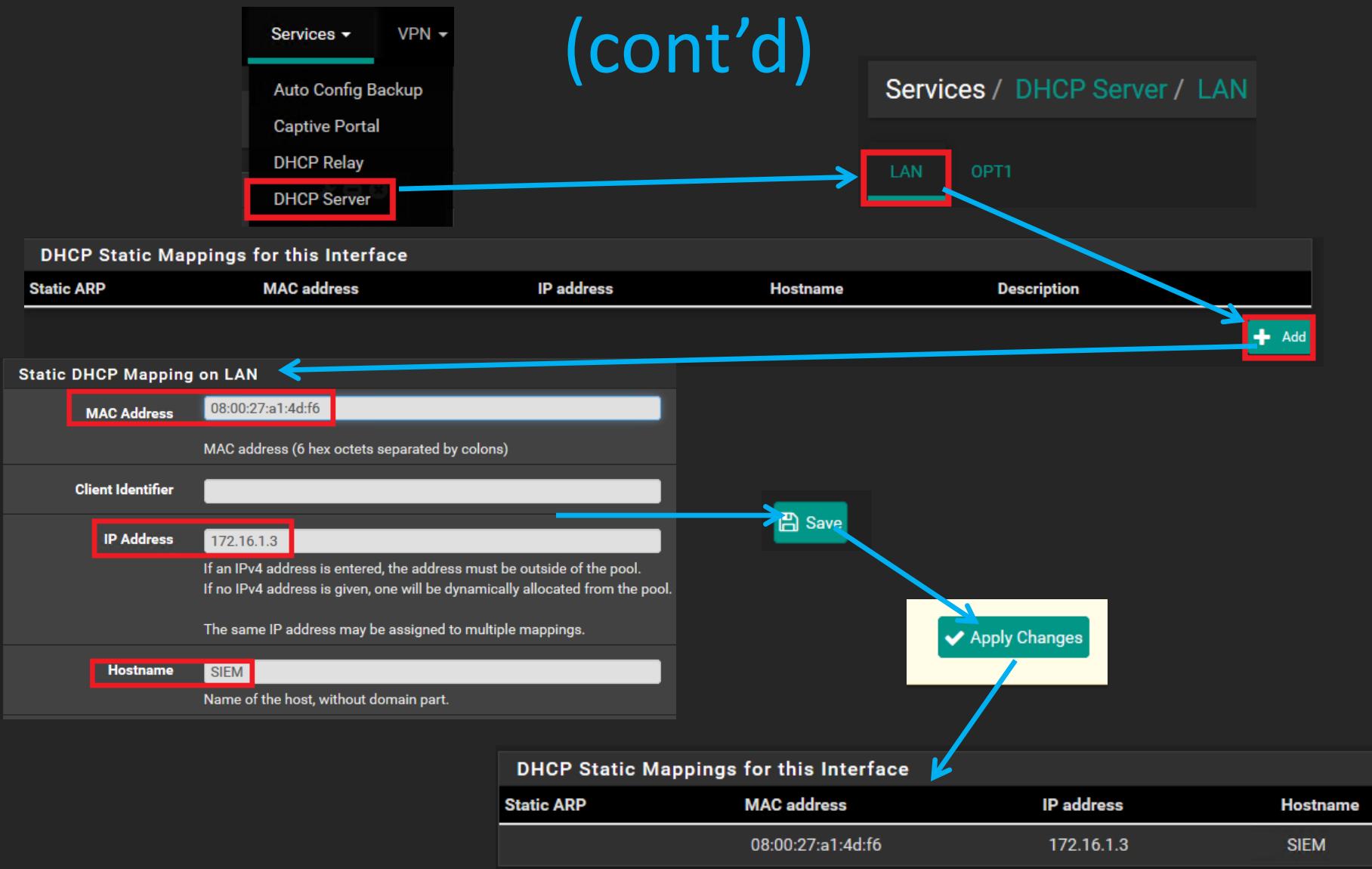
Strip away excess virtual hardware (cont'd)



Creating a Static DHCP Mapping

- Log in to pfSense webConfigurator (<https://172.16.1.1>)
- Navigate to Services > DHCP Server
 - Select LAN tab
 - Scroll all the way to the bottom of the page
 - DHCP Static Mappings for this Interface
 - Click Add
- Input the MAC address for the SIEM VM
 - With the colon symbol (:) every two characters
- Input 172.16.1.3 for the IP Address
- Optional: Enter “SIEM” as the hostname and/or enter a description
 - Scroll to the bottom of the page, and click Save
 - Back on the previous page, click Apply Changes
- Confirm the new DHCP Static Mapping, by scrolling to the bottom of the page

Creating a Static DHCP Mapping (cont'd)



Creating a Static DHCP Mapping

- Remember how to do this
 - We'll be doing it again at least 3 more times
 - LAN: SIEM (you are here), IPS
 - OPT1: Kali, Metasploitable2
- Why: pfSense Static DHCP Mappings ensure VMs get the same IP address
 - Consistent network access
 - Without having to statically configure IP addresses
 - Or use vbox's (terrible) DHCP server.

Installing Ubuntu 18.04

- Install process (Note: arrow keys to move, space bar to select things, Enter to confirm your selections):
 - Start the VM
 - Choose English as the preferred language
 - Select English (US) as the Layout and Variant for your keyboard (selected by default)
 - Select Install Ubuntu
 - Confirm network connection settings (Verify MAC address of SIEM VM, confirm IP address of 172.16.1.3/24)

Installing Ubuntu 18.04 (cont'd)

- Set `http://172.16.1.1:3128` on the configure proxy page
 - Note: If you fail to do this, its okay! Check out:
<https://askubuntu.com/questions/257290/configure-proxy-for-apt>
 - TL;DR: as root, create `/etc/apt/apt.conf` and enter:
 - » `Acquire::http::Proxy "http://172.16.1.1:3128";`
- Hit enter on the next screen to use the default Ubuntu archive mirror

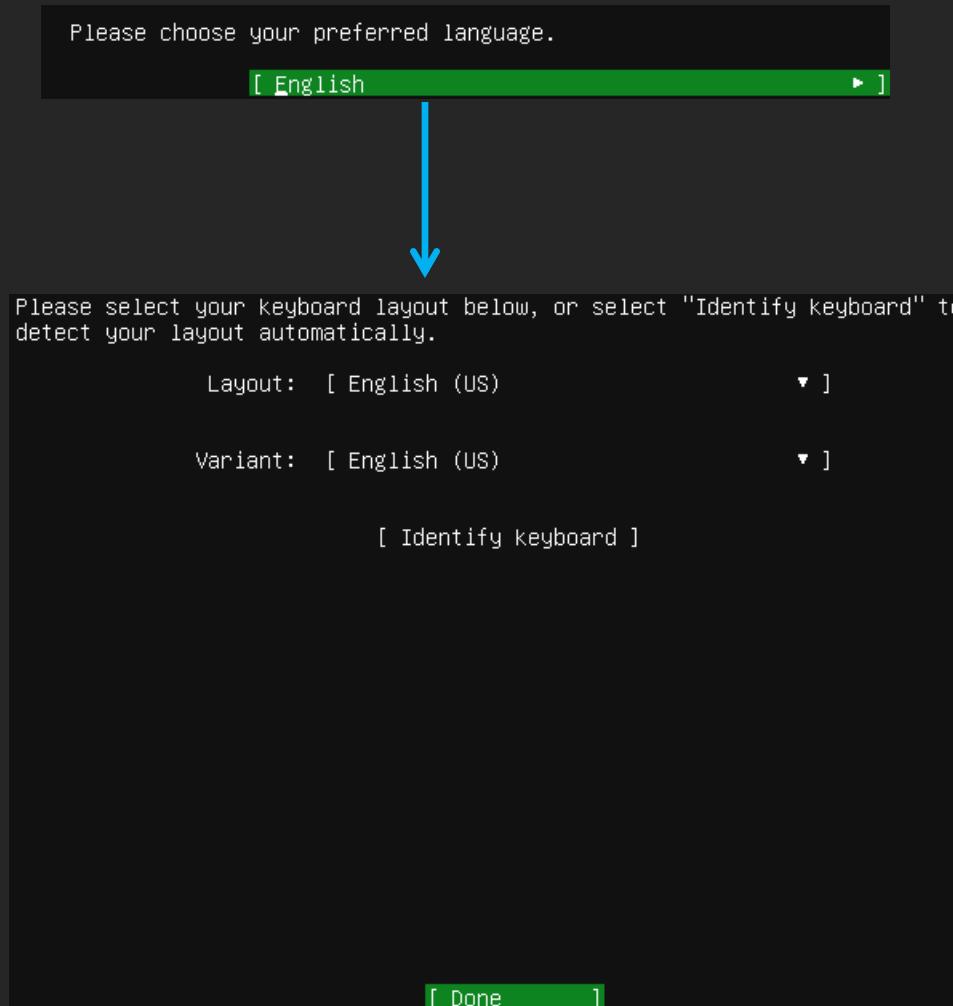
Installing Ubuntu 18.04 (cont'd)

- On Filesystem setup, select Use an Entire Disk
- Hit Enter to Choose the disk to install to (the only disk available)
- Select Done to begin formatting the disk
- Fill out the Profile setup screen
 - Your Name
 - Server name (optional)
 - Username
 - Password
 - Note: Be sure to enter the username and password into your password manager

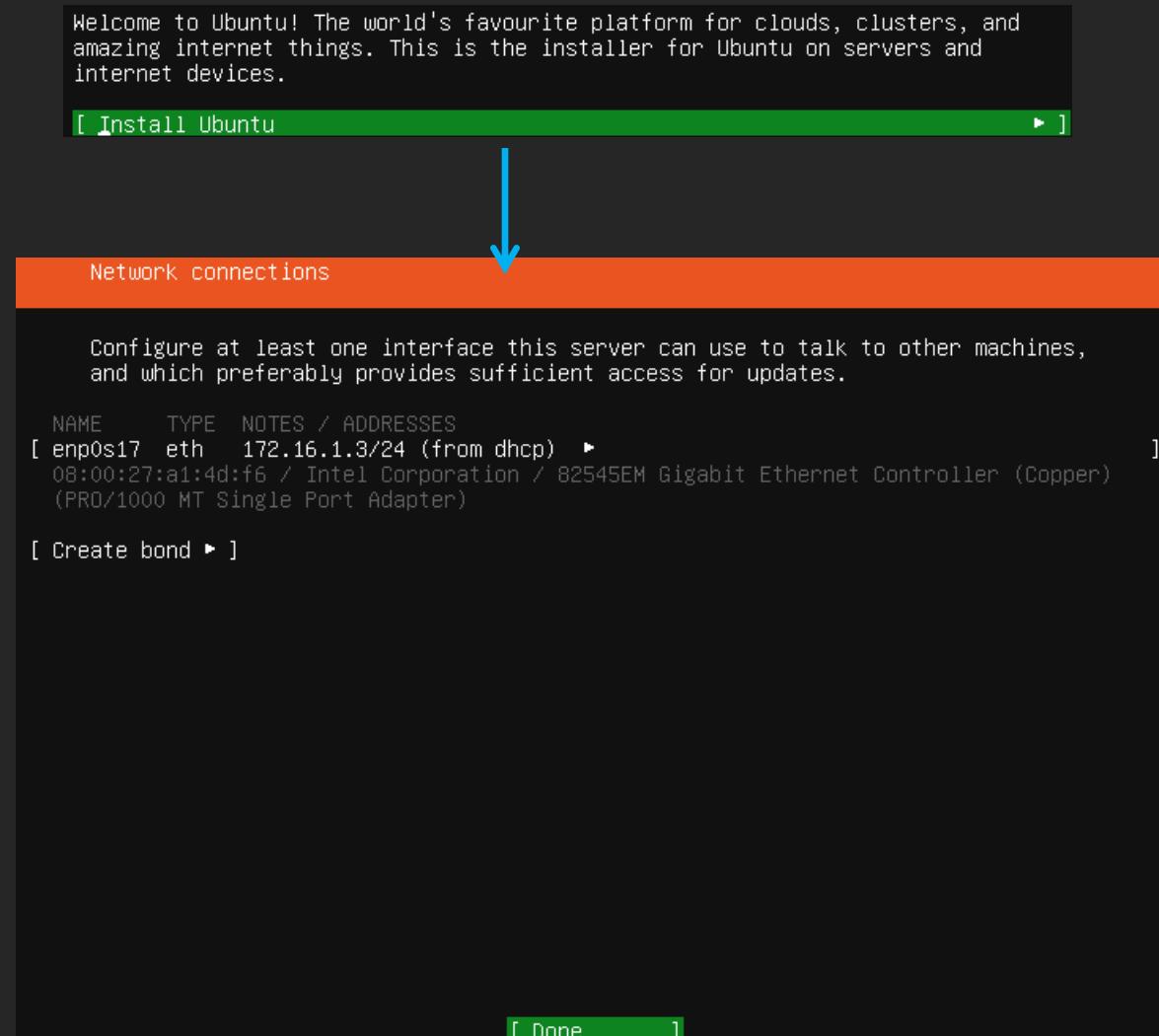
Installing Ubuntu 18.04 (cont'd)

- Install OpenSSH server (hit spacebar) then use the arrow keys to select Done, then hit Enter
- On Featured Server Snaps, hit tab to highlight Done and hit enter
 - We don't need to install anything here
- After the installation process completes and Reboot Now is highlighted, close the virtual machine console to shut down the VM

Installing Ubuntu 18.04 (cont'd)

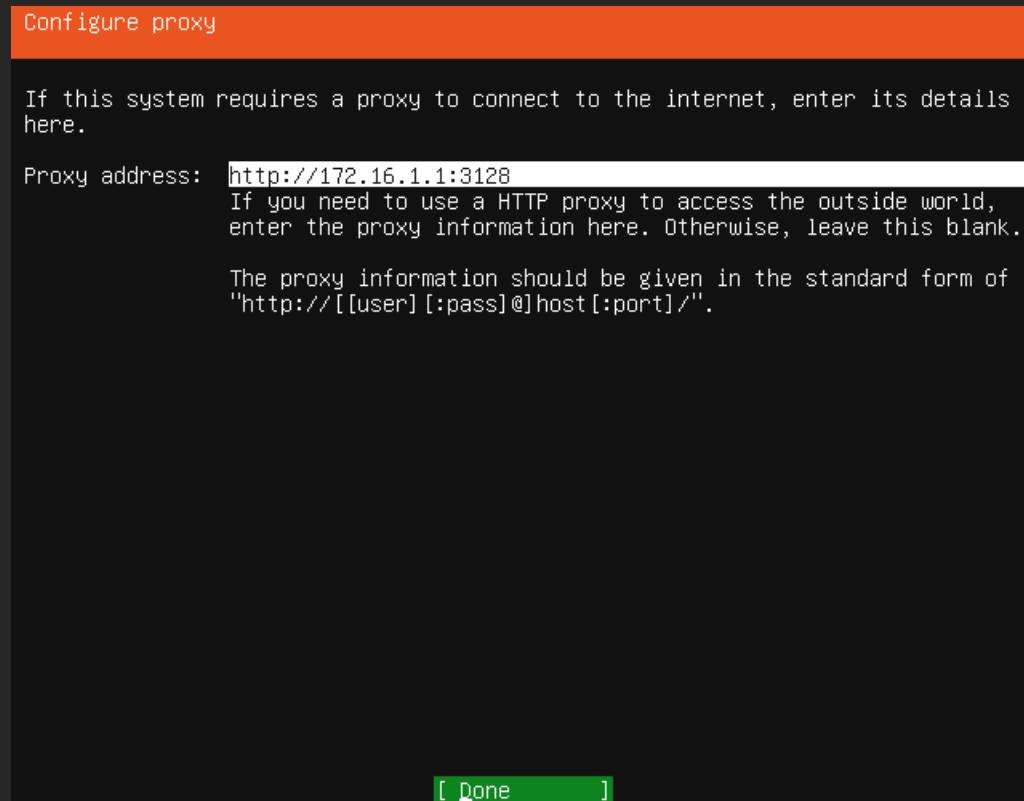


Installing Ubuntu 18.04 (cont'd)

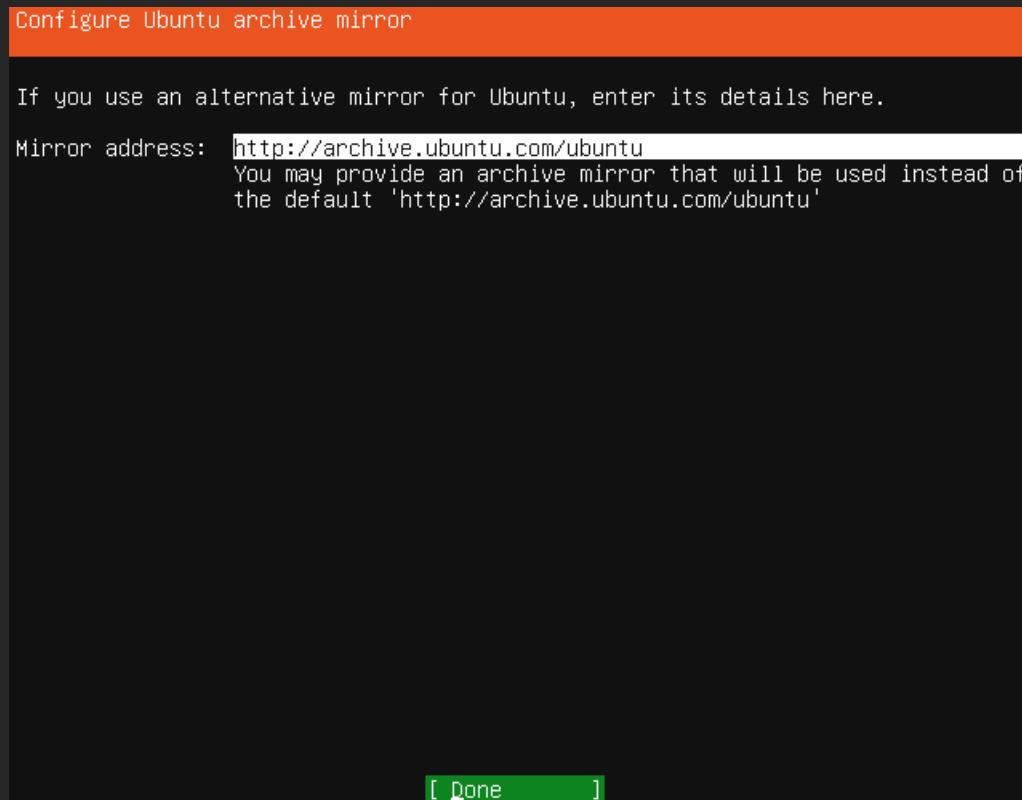


twitter:@da_667
email:deusexmachina667@gmail.com

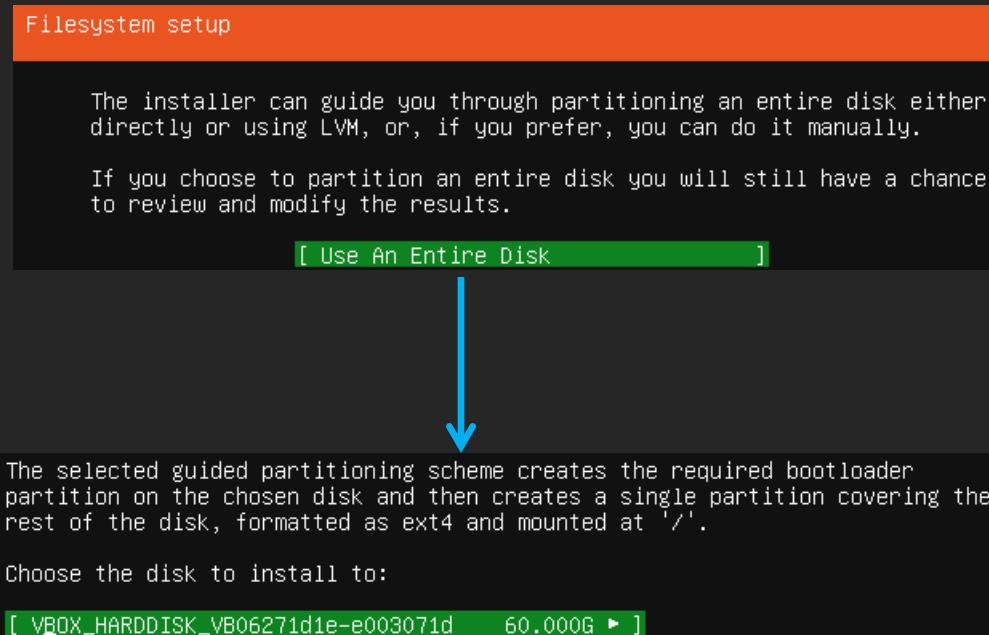
Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)

```
FILE SYSTEM SUMMARY

  MOUNT POINT      SIZE   TYPE   DEVICE TYPE
  [ /           59.997G ext4   partition of local disk ▶ ]


AVAILABLE DEVICES

  No available devices

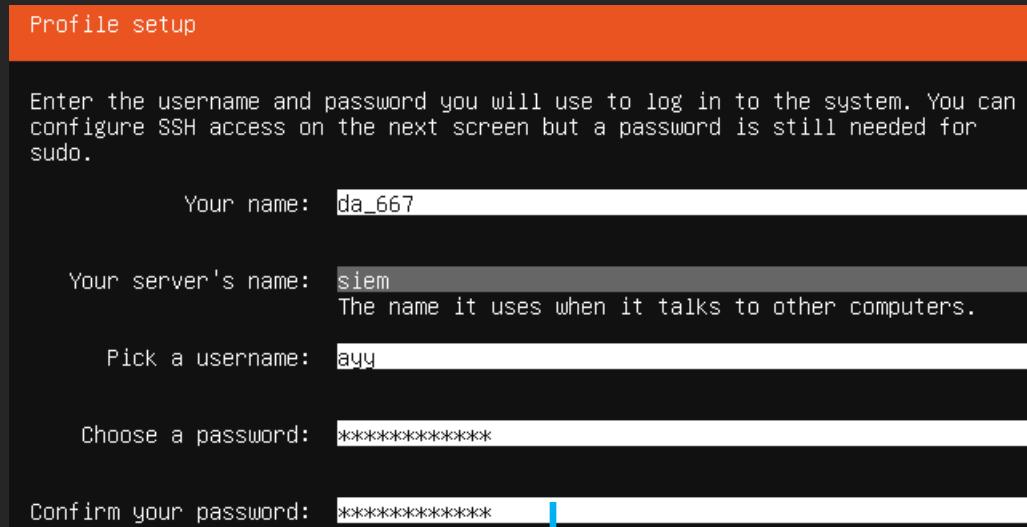
  [ Create software RAID (md) ▶ ]
  [ Create volume group (LVM) ▶ ]


USED DEVICES

  DEVICE
  [ VBOX_HARDDISK_VB06271d1e-e003071d    60.000G local disk ▶ ]
  [   partition 1                      1.000M (0%)     ▶ ]
  [     bios_grub
  [   partition 2                      59.997G (99%)     ▶ ]
    formatted as ext4, mounted at /


  [ Done ]
```

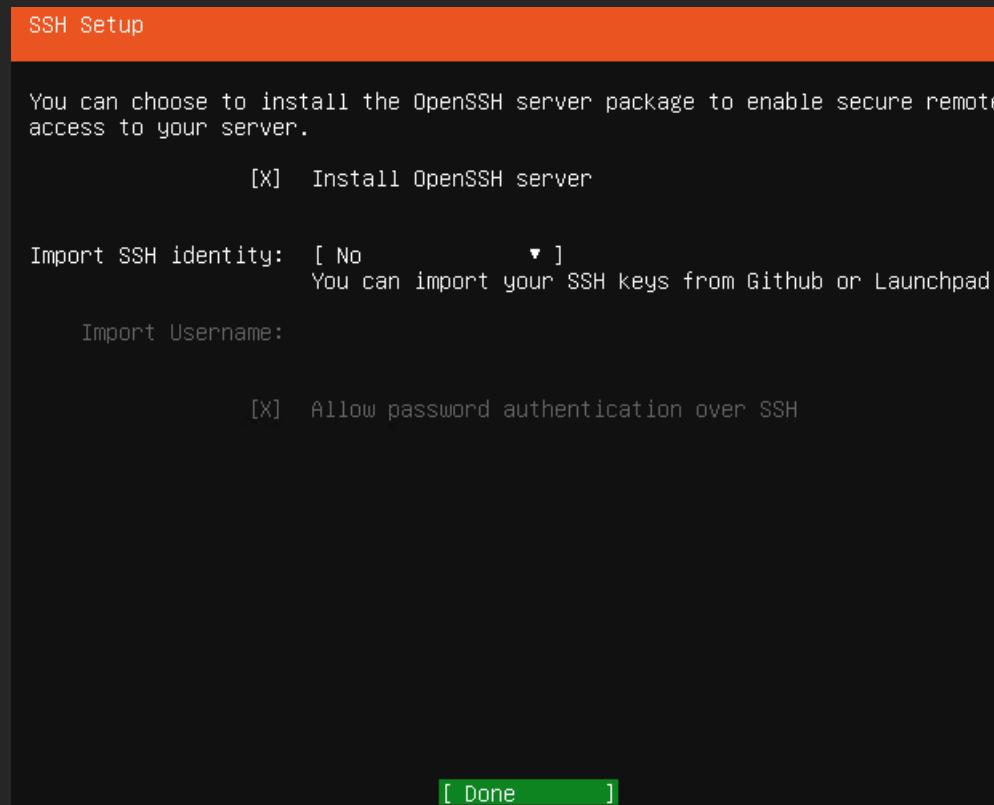
Installing Ubuntu 18.04 (cont'd)



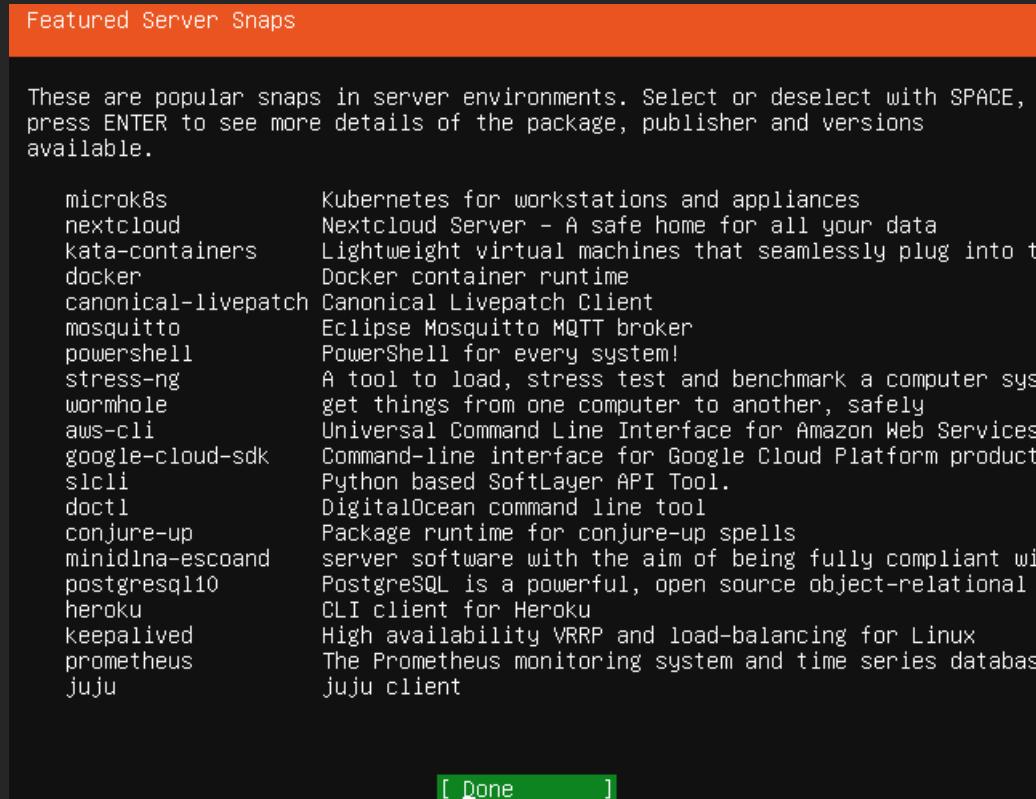
The screenshot shows the KeePass 'Add entry' dialog box with the following details:

- Title: SIEM VM login creds
- Username: ayy
- Password: [REDACTED]
- Repeat: [REDACTED]
- URL: [REDACTED]
- Expires: 4/1/2019 4:57 PM
- Notes: These are the user credentials for the SIEM VM Host-only Network/LAN 172.16.1.3 Ubuntu 18.04

Installing Ubuntu 18.04 (cont'd)

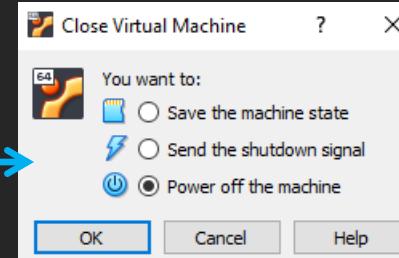


Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)

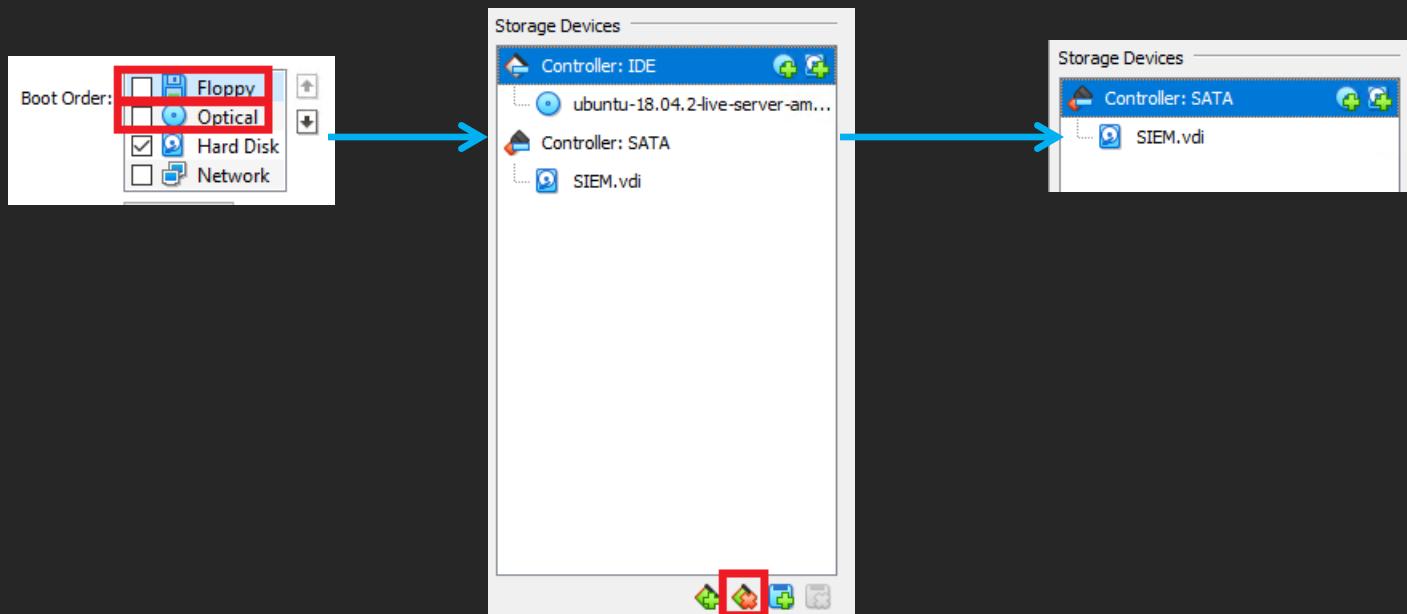
```
Installation complete!  
----- Finished install! -----  
running 'mount -t tmpfs tmpfs /target/run'  
running 'mkdir -p /target/run/cdrom'  
running 'mount --bind /cdrom /target/run/cdrom'  
running 'curtin curthooks'  
    curtin command curthooks  
        configuring apt configuring apt  
        installing missing packages  
        configuring iscsi service  
        configuring raid (mdadm) service  
        installing kernel  
        setting up swap  
        apply networking config  
        writing etc/fstab  
        configuring multipath  
        updating packages on target system  
        configuring pollinate user-agent on target  
finalizing installation  
    running 'curtin hook'  
    curtin command hook  
executing late commands  
final system configuration  
configuring cloud-init  
installing OpenSSH server  
cleaning up apt configuration  
  
[ View full log ]  
[ Reboot Now ]
```



Strip Remaining Excess Virtual Hardware

- SIEM VM Settings:
 - System: Uncheck Floppy and Optical checkboxes in Boot Order list
 - Storage: Remove Virtual CD/DVD drive

Strip Remaining Excess Virtual Hardware (cont'd)



Perform Connectivity Checks

- Log in to VM (username and password you set)
- Perform connectivity check commands
 - ping -c4 www.google.com
 - nslookup www.google.com
 - curl -I www.google.com
 - ifconfig -a (verify DHCP static map)
- Note: Ubuntu Server does NOT feature a desktop environment.
 - Hope you like /bin/bash

Perform Connectivity Checks (cont'd)

```
siem login: ayy
```

```
Password:
```

```
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-46-generic x86_64)
```

```
ayy@siem:~$ nslookup www.google.com
Server: 127.0.0.53
Address: 127.0.0.53#53
:
Non-authoritative answer:
Name: www.google.com
Address: 172.217.1.36
Name: www.google.com
Address: 2607:f8b0:4009:802::2004
```

```
ayy@siem:~$ ping -c4 www.google.com
PING www.google.com (172.217.1.36) 56(84) bytes of data.
64 bytes from ord37s07-in-f36.1e100.net (172.217.1.36): icmp_seq=1 ttl=53 time=24.7 ms
64 bytes from ord37s07-in-f36.1e100.net (172.217.1.36): icmp_seq=2 ttl=53 time=24.3 ms
64 bytes from ord37s07-in-f36.1e100.net (172.217.1.36): icmp_seq=3 ttl=53 time=21.7 ms
64 bytes from ord37s07-in-f36.1e100.net (172.217.1.36): icmp_seq=4 ttl=53 time=21.5 ms
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 21.509/23.115/24.799/1.498 ms
```

```
ayy@siem:~$ curl -I www.google.com
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2019 22:43:29 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-04-01-22; expires=Wed, 01-May-2019 22:43:29 GMT; path=/; domain=.google.com
Set-Cookie: NID=180=meyo1kuID5fAaaqLwGRhWT26QjhfK1_rtfIMd0kagd4LmtSSndx7NGuLUlUa11hwAN2xhiJt-K-txEff
fbI9Md8W-ULQ7L1tZybp0Tjcx9_uui8f2NY3bDzIqyVGXoMh6sxMLYQjaJWU1CHD9AMDWPxheFVm1tt3U9Vo2PzVHw; expires
=Tue, 01-Oct-2019 22:43:29 GMT; path=/; domain=.google.com; HttpOnly
Transfer-Encoding: chunked
Accept-Ranges: none
Vary: Accept-Encoding
```

```
ayy@siem:~$ ifconfig -a
enp0s17: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.1.3 netmask 255.255.255.0 broadcast 172.16.1.255
inet6 fe80::a00:27ff:fea1:4df6 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:a1:4d:f8 txqueuelen 1000 (Ethernet)
RX packets 759 bytes 583175 (583.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 202 bytes 22816 (22.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions
```

System Updates

- Note: Depending on how our connectivity is on-site, this may or may not fast...
- Log in to the SIEM VM
- Run the command `sudo su -`
 - Requires you to enter your password
 - Root is powerful. Use the power responsibly.
- Run the command(s):
 - `export DEBIAN_FRONTEND=noninteractive`
 - `apt-get update`
 - `apt-get -y dist-upgrade`
 - `init 6`
 - Updates the system, then reboots it
 - Note: If you have issues downloading updates, make sure that your connectivity checks were SUCCESSFUL. Verify that you configured the apt-get proxy correctly (<http://172.16.1.1:3128 -- /etc/apt/apt.conf>)

twitter:@da_667

email:deusexmachina667@gmail.com

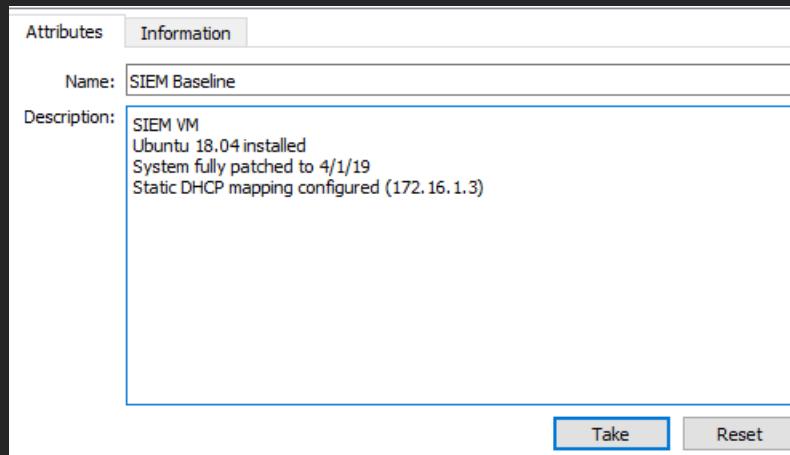
System Updates (cont'd)

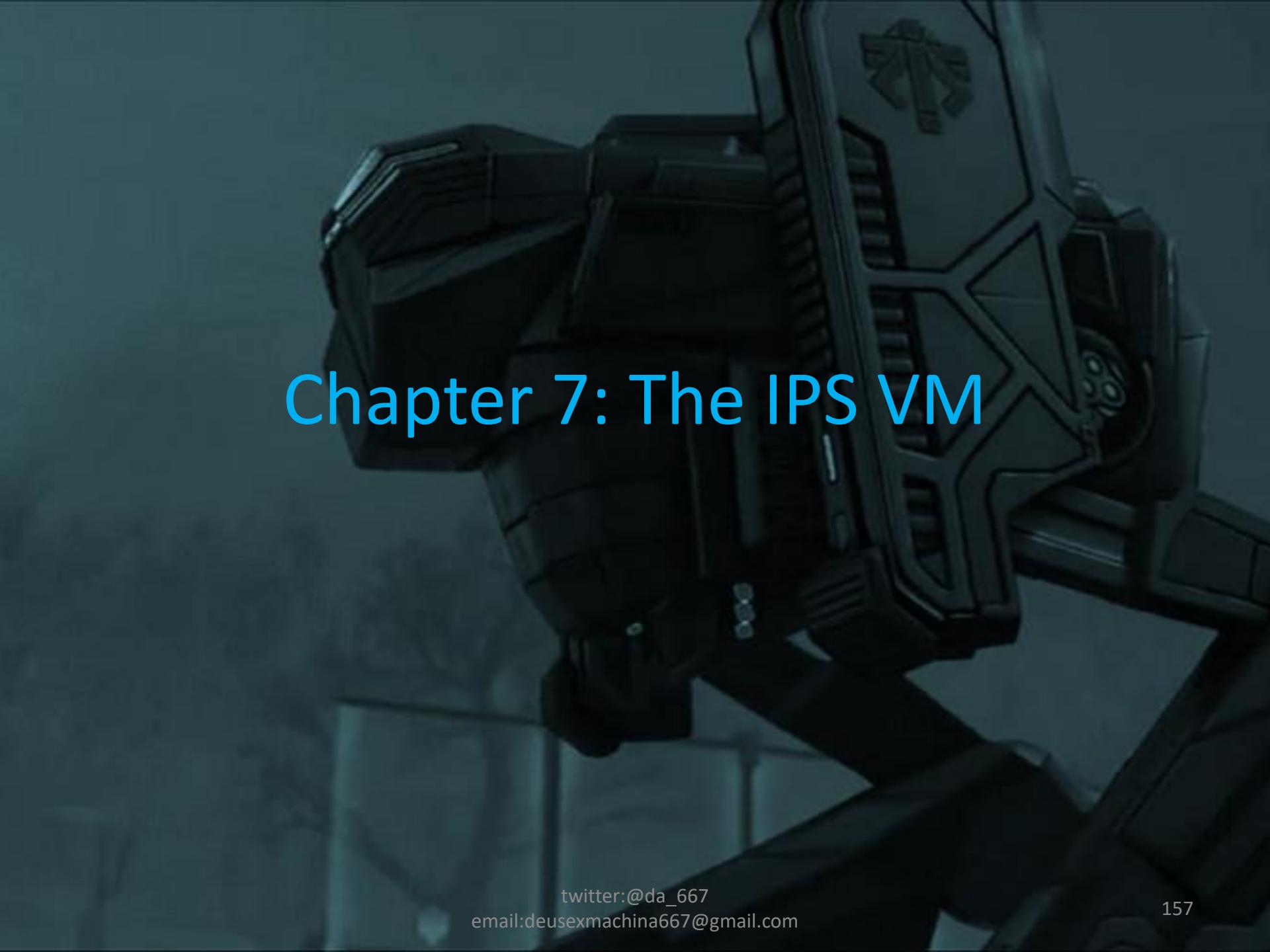
```
ayy@siem:~$ sudo su -  
[sudo] password for ayy:  
root@siem:~# whoami  
root  
  
root@siem:~# export DEBIAN_FRONTEND=noninteractive  
  
root@siem:~# apt-get update  
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease  
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]  
Get:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]  
Get:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]  
Fetched 252 kB in 1s (182 kB/s)  
Reading package lists... Done  
  
root@siem:~# apt-get -y dist-upgrade  
  
root@siem:~# init 6
```

Take Baseline Snapshot

- Meant to serve as a snapshot from BEFORE we install splunk (in case you want to upgrade in the future, try another SIEM, etc.)
- Literally the exact same steps as with the pfSense VM.
 - Virtualbox Manager -> Click bullet list icon -> Snapshots -> Take

Take Baseline Snapshot (cont'd)





Chapter 7: The IPS VM

IPS

- This system will be hosting our IDS/IPS Software
- OS: Ubuntu Server 18.04
- IDS/IPS Software: Snort or Suricata (user's choice)

What is (network) IDS/IPS?

- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- Software that analyzes network traffic for specific activity, and at a logs it for further analysis
 - IDS: Logs/generates alerts
 - IPS: Logs/generates alerts, PLUS can be configured to drop network traffic
- Most IDS/IPS are driven by signatures
 - Some people call these signatures “rules”
 - Rules are just another name for signatures. Don’t let anyone tell you otherwise
 - Notable examples: Snort, Suricata
- Some IDS/IPS are drive by anomalies
 - Notable example: Zeek (formerly known as BRO)
 - Bro is VERY different from traditional IDS/IPS

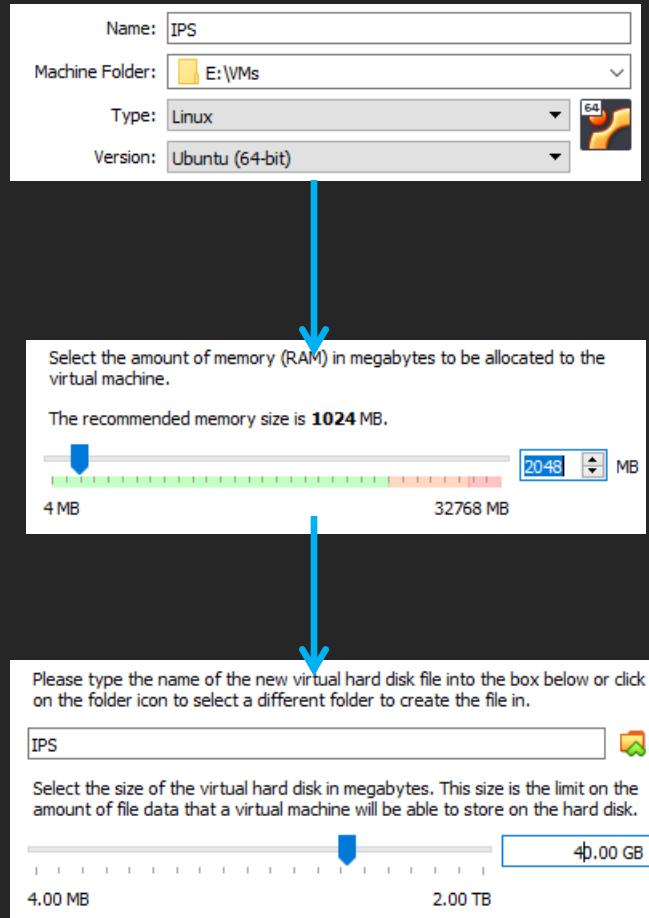
Tasks to Perform

- Create IPS VM
 - Create static DHCP mapping on pfSense LAN network for Network Adapter 1
- Strip away excess virtual hardware
- Install Ubuntu 18.04
- Strip remaining excess virtual hardware
- Perform connectivity checks
- Update VM
- Take baseline snapshot
- Process is nearly IDENTICAL to the SIEM VM
 - Except where noted

Create Virtual Machine Wizard:

- Screen 1:
 - Name: IPS
 - Machine Folder: Default
 - Type: Linux
 - Version: Ubuntu (64-bit)
- Screen 2:
 - Memory size: 2GB
- Screen 3:
 - Create virtual hard disk now
- Screen 4:
 - VDI (VirtualBox Disk Image)
- Screen 5:
 - Fixed size
- Screen 6:
 - Name: IPS
 - Size: 40.00GB

Create Virtual Machine Wizard (cont'd)



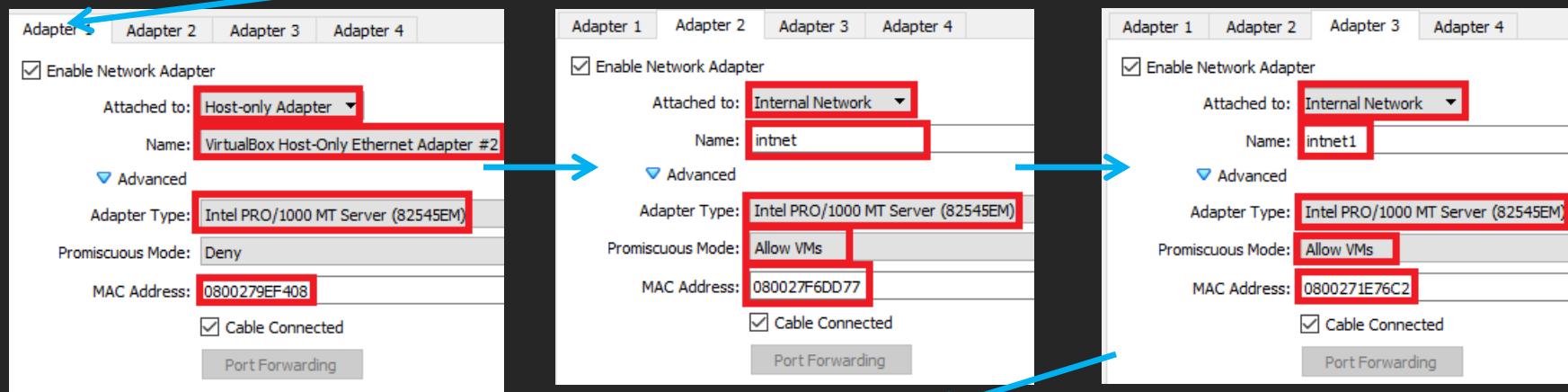
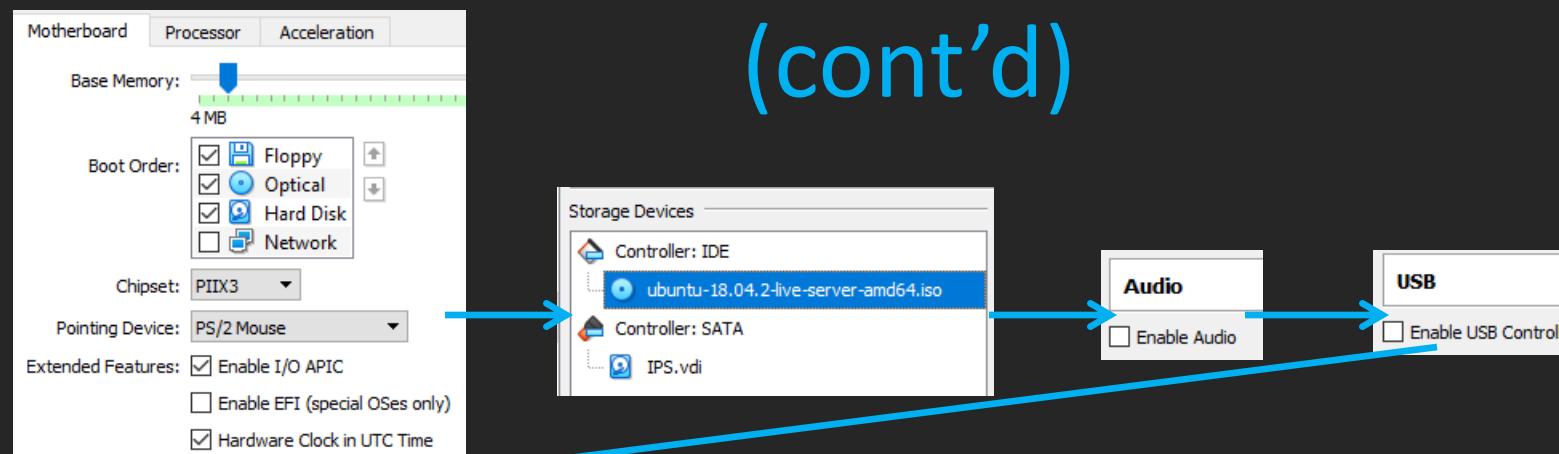
Strip away excess virtual hardware

- System:
 - Set Pointing Device drop-down to PS/2 Mouse
- Storage: Choose Virtual Optical Disk file
 - Ubuntu-18.04.X-live-server-amd64.iso
- Audio: Uncheck Enable Audio
 - Its PulseAudio and doesn't work half the time, anyhow.
- Serial Ports
 - Ensure no serial ports are enabled (should be default)
- USB: Uncheck Enable USB Controller
- Shared Folders
 - Ensure no shared folders are configured (should be default)

Strip away excess virtual hardware (cont'd)

- Network: Verify Enable Network Adapter checkbox is checked for Adapter 1, 2 and 3 ONLY
 - Network Adapter 1 attached to: Host-only Adapter
 - Network Adapter 2 attached to: intnet
 - Network Adapter 3 attached to: intnet1
 - Advanced Settings (All network adapters)
 - Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - Copy the MAC Address to your MAC address text file/document
 - Ensure Cable Connected is checked
 - Advanced Settings (network adapter 2 and 3)
 - Promiscuous mode – Set to Allow VMs (or Allow All)
 - Why: This is very very important for Snort/Suricata to work properly. DO NOT FORGET THIS STEP.

Strip away excess virtual hardware (cont'd)



Creating a Static DHCP Mapping

- Log in to pfSense webConfigurator (<https://172.16.1.1>)
- Navigate to Services > DHCP Server
 - LAN tab
 - DHCP Static Mappings for this Interface
- Input the MAC address for Network Adapter 1 (host-only) on the IPS VM
- Input 172.16.1.4 for the IP Address
- Optional: Enter “IPS” as the hostname and/or enter a description
 - Save, then Apply Changes
- Confirm the new DHCP Static Mapping

Creating a Static DHCP Mapping

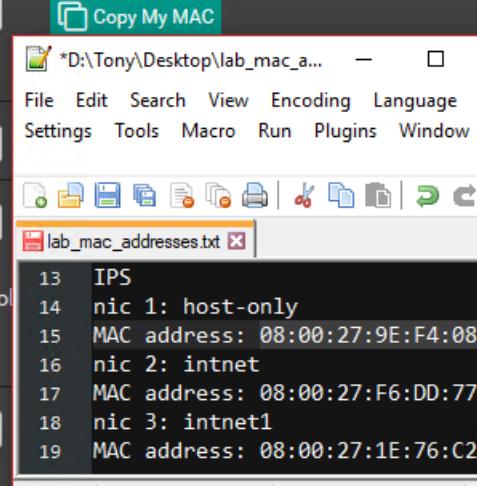
Services / DHCP Server / LAN / Edit Static Mapping

Static DHCP Mapping on LAN

MAC Address	08:00:27:9e:f4:08	<input type="button" value="Copy My MAC"/>
MAC address (6 hex octets separated by colons)		
Client Identifier		
IP Address	172.16.1.4	If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool.
The same IP address may be assigned to multiple mappings.		
Hostname	IPS	Name of the host, without domain part.

DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname
	08:00:27:a1:4d:f6	172.16.1.3	SIEM
	08:00:27:9e:f4:08	172.16.1.4	IPS



A blue arrow points from the 'IP Address' field in the configuration window down to the 'IP address' column in the 'DHCP Static Mappings for this Interface' table.

Installing Ubuntu 18.04

- Install process (Note: arrow keys to move, space bar to select things, Enter to confirm your selections):
 - Start the VM
 - Choose English as Preferred language, layout and variant
 - Install Ubuntu
 - On the Network Connections screen:
 - Match the MAC addresses – the MAC address for Network Adapter 1 should have an IP address of 172.16.1.4/24
 - All the other interfaces: Set them to “disabled”
 - Why: They should never have or acquire an IP address. AF_PACKET bridging doesn’t need IP addresses for these interfaces to work.
 - » Combined with some other customizations (NOARP, PROMISC flags on the interfaces), this makes the IDS very hard to detect

Installing Ubuntu 18.04 (cont'd)

- Set `http://172.16.1.1:3128` on the configure proxy page
 - Note: If you fail to do this, its okay! Check out:
<https://askubuntu.com/questions/257290/configure-proxy-for-apt>
 - TL;DR: as root, create `/etc/apt/apt.conf` and enter:
 - Acquire::http::Proxy “`http://172.16.1.1:3128`”;
- Hit enter on the next screen to use the default Ubuntu archive mirror

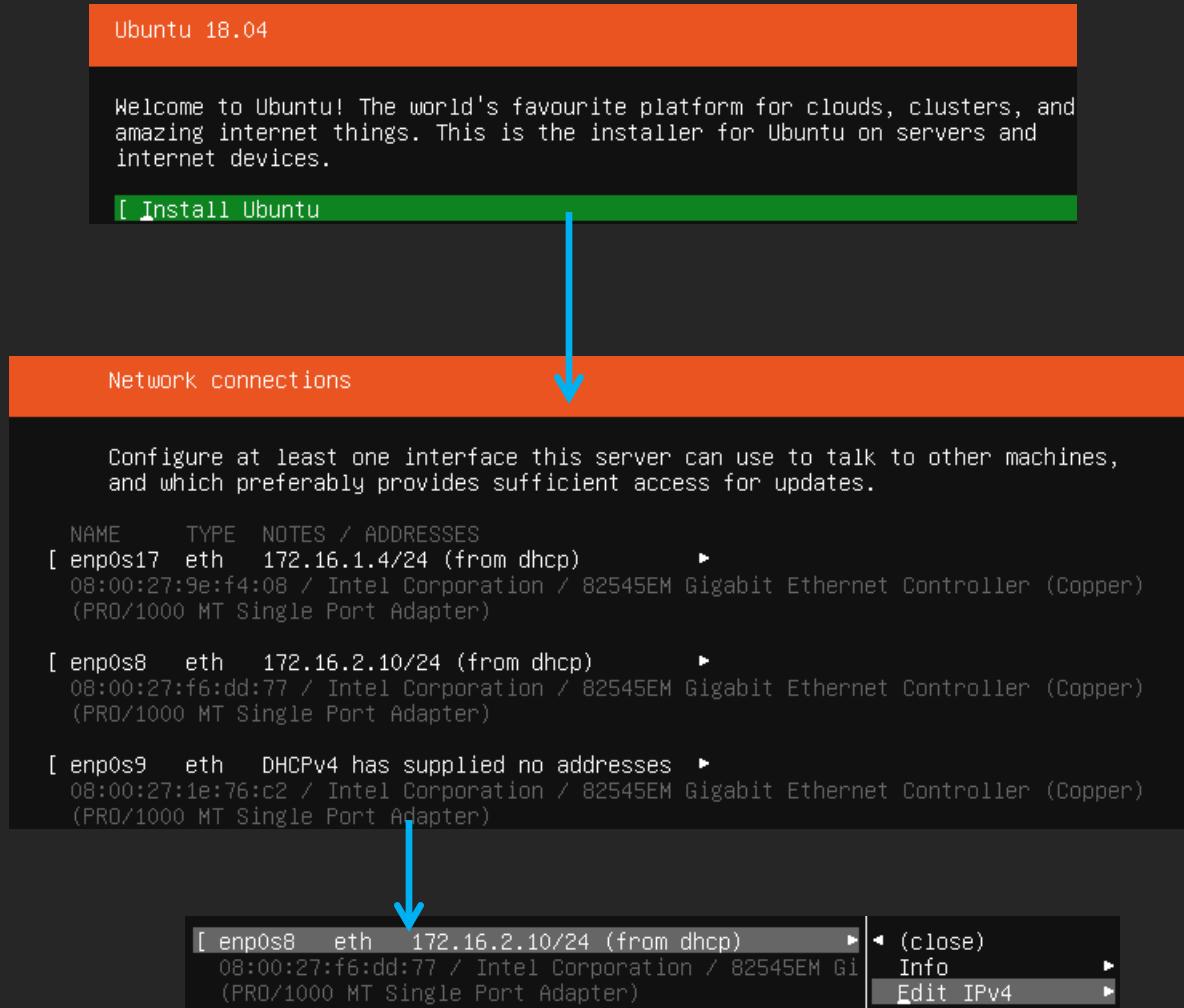
Installing Ubuntu 18.04 (cont'd)

- On Filesystem setup, select Use an Entire Disk
- Hit Enter to Choose the disk to install to (the only disk available)
- Select Done to begin formatting the disk
- Fill out the Profile setup screen
 - Your Name
 - Server name (optional)
 - Username
 - Password
 - Note: Be sure to enter the username and password into your password manager

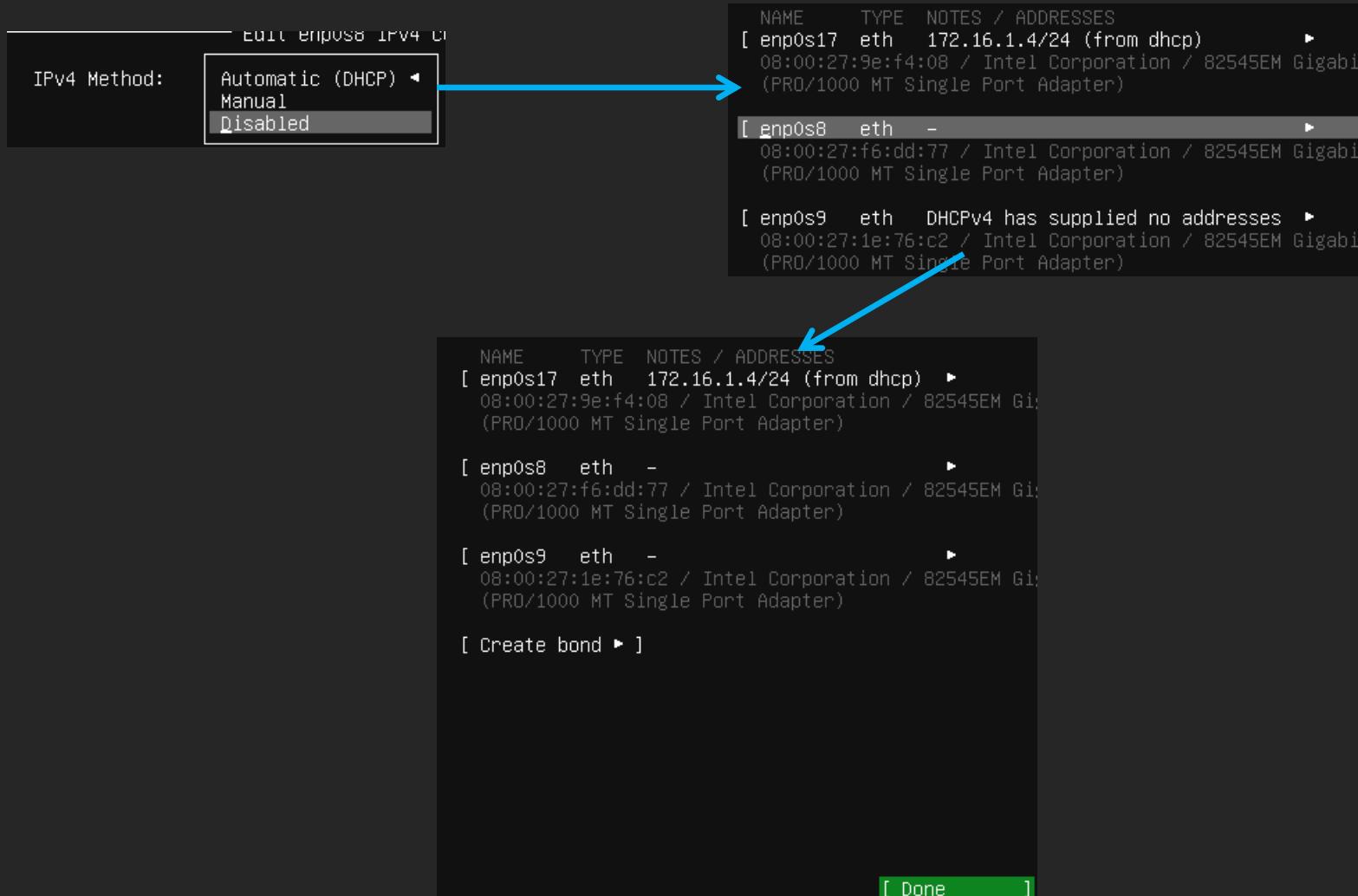
Installing Ubuntu 18.04 (cont'd)

- Install OpenSSH server
- On Featured Server Snaps, hit tab to highlight Done and hit enter
- After the installation process completes and Reboot Now is highlighted, close the virtual machine console to shut down the VM

Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)

The installer can guide you through partitioning an entire disk either directly or using LVM, or, if you prefer, you can do it manually.

If you choose to partition an entire disk you will still have a chance to review and modify the results.

[Use An Entire Disk]

Choose the disk to install to:

[VBOX_HARDDISK_VBd38b1ae4-af97a1e1 40.000G ▶]

FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
/	39.997G	ext4	partition of local disk ▶]

AVAILABLE DEVICES

No available devices

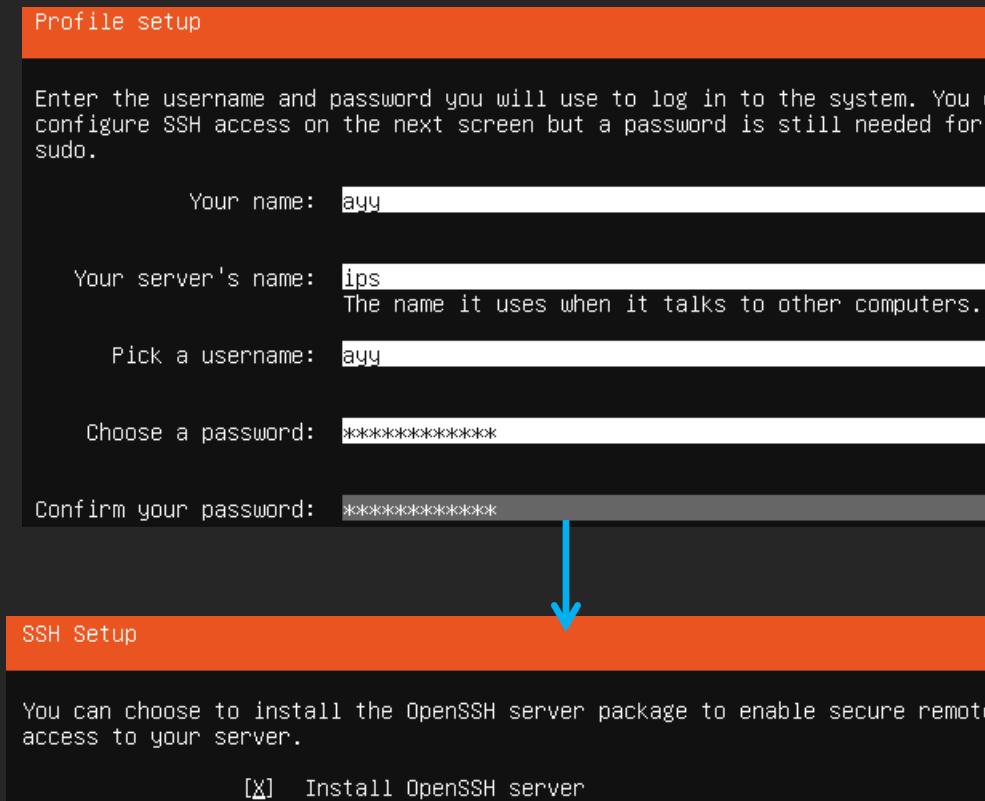
[Create software RAID (md) ▶]
[Create volume group (LVM) ▶]

USED DEVICES

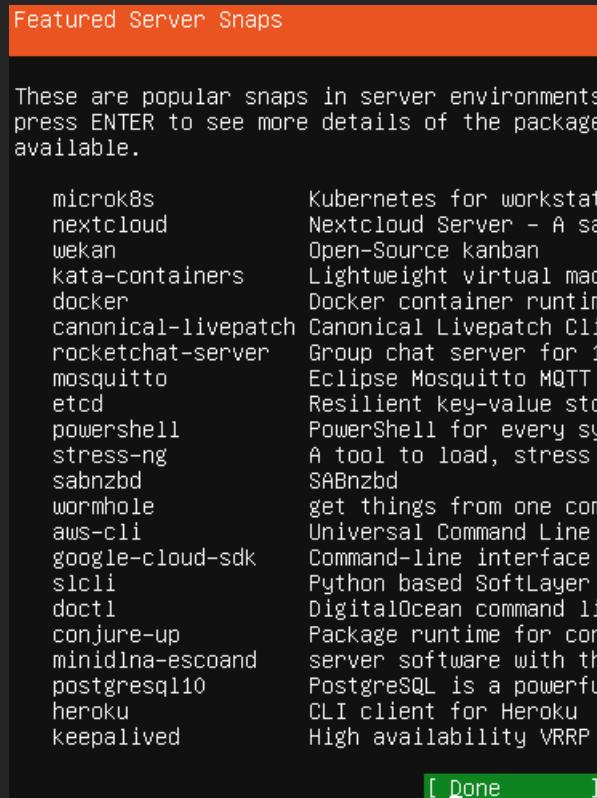
DEVICE	SIZE	TYPE
[VBOX_HARDDISK_VBd38b1ae4-af97a1e1	40.000G	local disk ▶]
[partition 1	1.000M (0%)	▶]
bios_grub		
[partition 2	39.997G (99%)	▶]
formatted as ext4, mounted at /		

[Done]

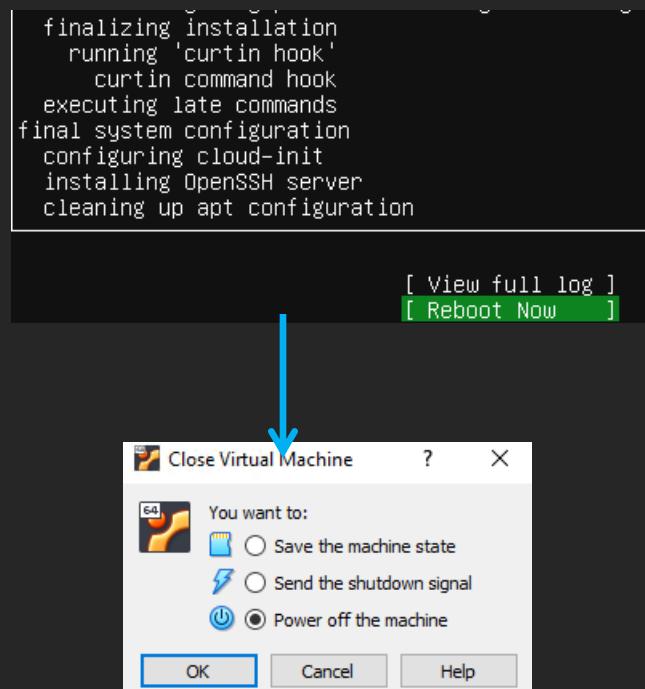
Installing Ubuntu 18.04 (cont'd)



Installing Ubuntu 18.04 (cont'd)



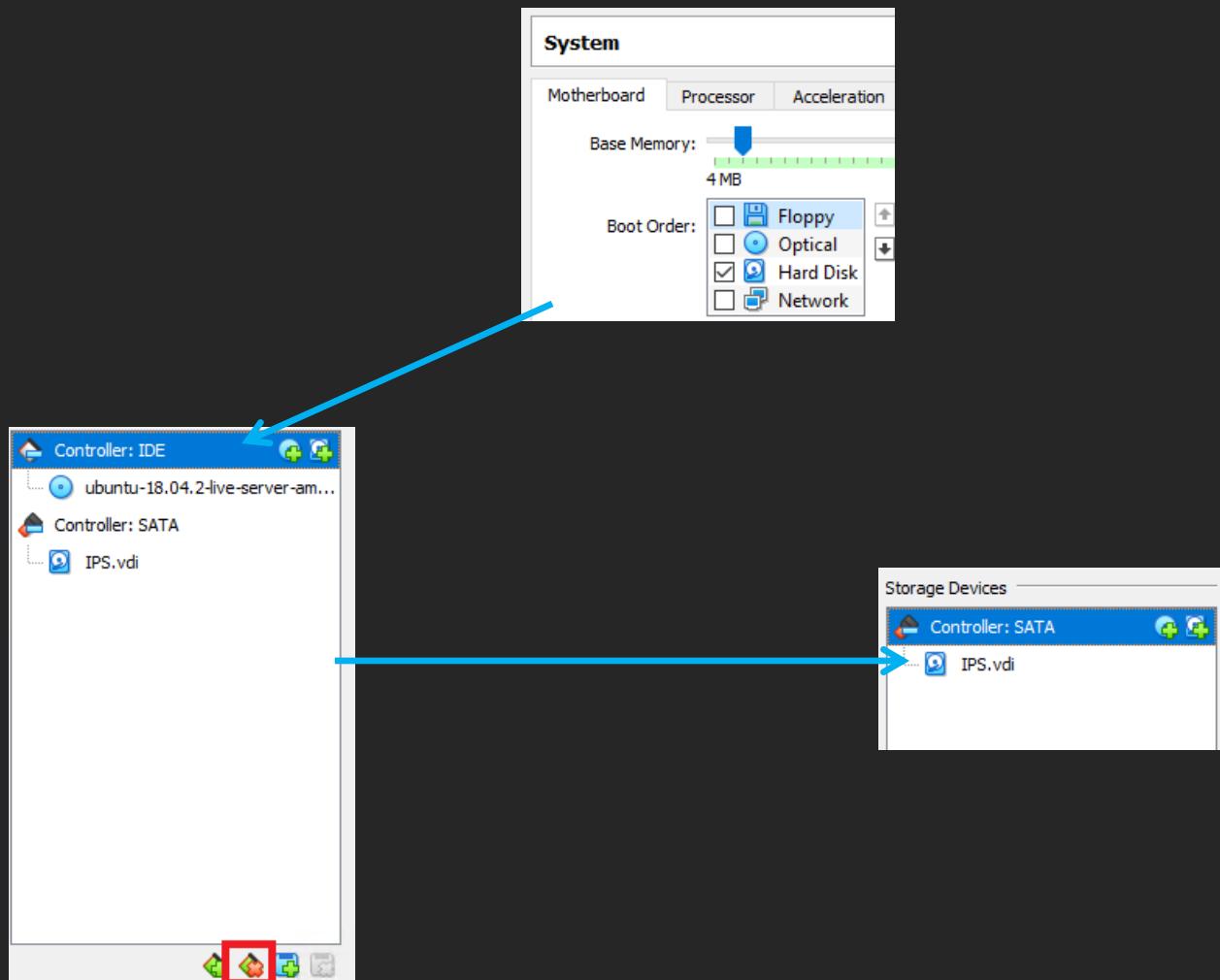
Installing Ubuntu 18.04 (cont'd)



Strip Remaining Excess Virtual Hardware

- IPS VM Settings:
 - System: Uncheck Floppy and Optical checkboxes in Boot Order list
 - Storage: Remove Virtual CD/DVD drive

Strip Remaining Excess Virtual Hardware (cont'd)



Perform Connectivity Checks

- Log in to VM (username and password you set)
- Perform connectivity check commands
 - ping -c4 www.google.com
 - nslookup www.google.com
 - curl -I www.google.com
 - ifconfig -a (verify DHCP static map for network adapter 1 and NO IP addresses for the other interfaces)

Perform Connectivity Checks (cont'd)

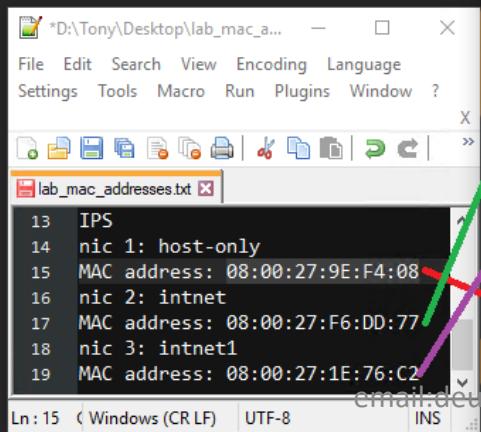
```
ayy@ips:~$ ping -c4 www.google.com
PING www.google.com (172.217.6.4) 56(84) bytes of data.
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=1 ttl=53 time=25.3 ms
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=2 ttl=53 time=23.7 ms
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=3 ttl=53 time=20.1 ms
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=4 ttl=53 time=20.4 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3064ms
rtt min/avg/max/mdev = 20.122/22.442/25.399/2.225 ms
```

```
ayy@ips:~$ nslookup www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.6.4
Name:   www.google.com
Address: 2607:f8b0:4009:811::2004
```

```
ayy@ips:~$ curl -I www.google.com
HTTP/1.1 200 OK
Date: Tue, 16 Apr 2019 18:46:17 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-04-16-18; expires=Thu, 16-May-2019 18:46:17 GMT; path=/; domain=.google.com
Set-Cookie: NID=181=ShfifyItzBt0-7mhbfp2ked--tBGjM8VDIn_ybeMt0h_GZ-d1YyXwTK3-HQ2n-vw5dhn1he0ccncF1GS
cM73RMG2g076INHB8f2KhtvLb2tNnpKkrM0-prPAst07nyk1MD1nk81AM7FF8V79AICgnRntxoCq4c82S9XP7F0Kzo; expires
=Wed, 16-Oct-2019 18:46:17 GMT; path=/; domain=.google.com; HttpOnly
Transfer-Encoding: chunked
Accept-Ranges: none
Vary: Accept-Encoding
```



```
ayy@ips:~$ ifconfig -a
enp0s8: flags=4098<Broadcast,Multicast> mtu 1500
ether 08:00:27:f6:dd:77 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=4098<Broadcast,Multicast> mtu 1500
ether 08:00:27:1e:76:c2 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s17: flags=4163<Up,Broadcast,Running,Multicast> mtu 1500
inet 172.16.1.4 netmask 255.255.255.0 broadcast 172.16.1.255
inet6 fe80::a00:27ff:fe9e:f408 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:9e:f4:08 txqueuelen 1000 (Ethernet)
RX packets 66755 bytes 560734 (560.7 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 281 bytes 24392 (24.3 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

email.deusexmachina667@gmail.com

System Updates

- Same as before, depending on network connectivity... This could be fast or slow
- Log in to the IPS VM
- Run the command sudo su –
 - Requires you to enter your password
- Run the command(s):
 - export DEBIAN_FRONTEND=noninteractive
 - apt-get update
 - apt-get -y dist-upgrade
 - init 6
 - Note: If you have issues downloading updates, make sure that your connectivity checks were SUCCESSFUL. Verify that you configured the apt-get proxy correctly (<http://172.16.1.1:3128> -- /etc/apt/apt.conf)
 - Tip: you run this group of commands all at once (after logging in as root):
 - export DEBIAN_FRONTEND=noninteractive && apt-get update && apt-get -y dist-upgrade && init 6
 - The “&&” between commands says “if and only if the previous command is successful, run the next command”

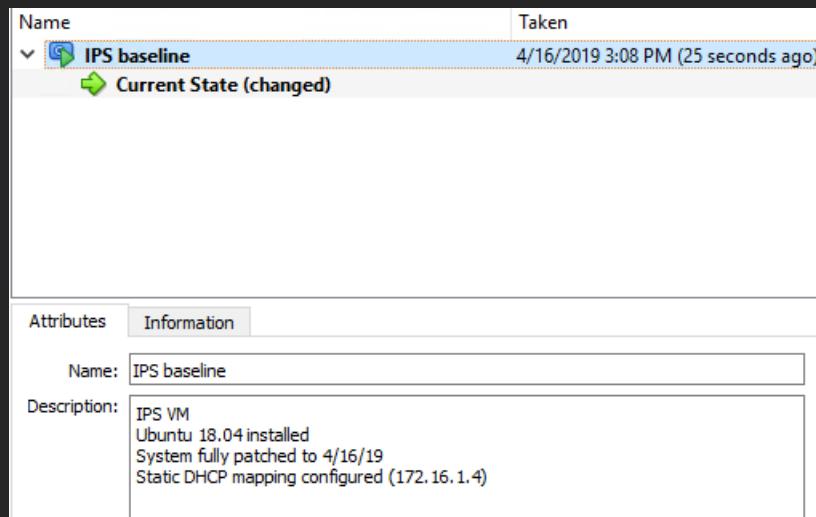
System Updates (cont'd)

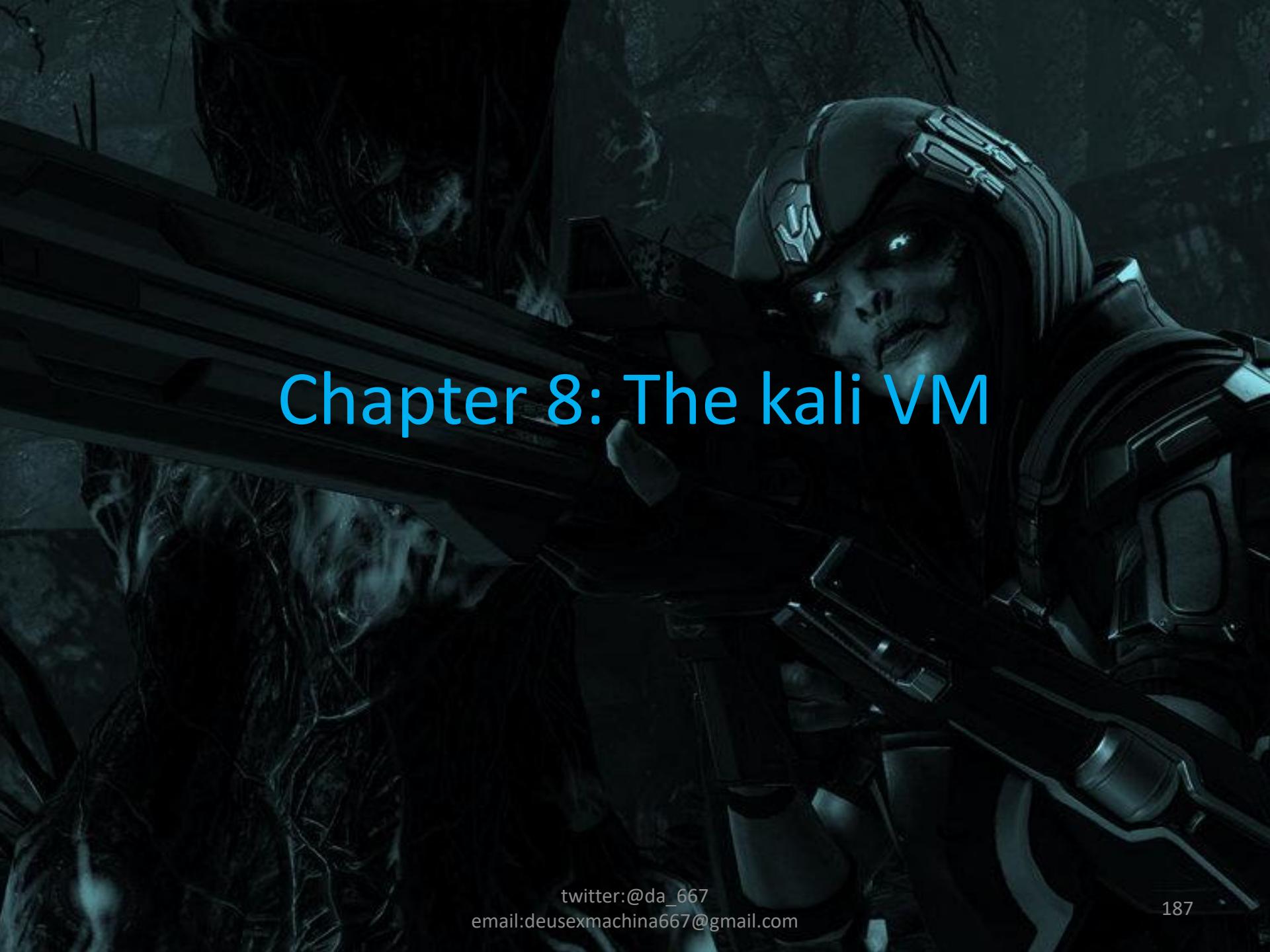
```
ayy@ips:~$ sudo su -  
[sudo] password for ayy:  
root@ips:~# whoami  
root  
  
root@ips:~# export DEBIAN_FRONTEND=noninteractive && apt-get update && apt-get -y dist-upgrade && in  
it 6  
  
Ubuntu 18.04.2 LTS ips tty1  
ips login:
```

Take Baseline Snapshot

- Meant to serve as a snapshot from BEFORE we install IPDS/IPS software (in case you want to upgrade in the future, try bridge-utils, etc.)
 - Virtualbox Manager -> Click bullet list icon -> Snapshots -> Take

Take Baseline Snapshot (cont'd)





Chapter 8: The kali VM

Kali Linux

- A Linux distribution to become an elite haxxor
 - Or join anonymous
 - Or become the baddest skid
 - Or spending hours a week downloading the entire metasploit framework for incremental updates.

Kali Linux (cont'd)

- “If you hate it so much, why are we using it?”
 - Because in spite of it having glaring design flaws, the alternatives are worse.
 - Kinda like Windows.
 - Its the de facto standard for most pentesters
 - Offsec marketing, best marketing
 - Guarantee some tryhard will say or has said to you “Try Harder”(tm) at some point.

Tasks to Perform

- Create kali VM
 - Create static DHCP mapping on pfSense LAN network
- Strip away excess virtual hardware
- Install Kali linux
- Strip remaining excess virtual hardware
- Perform connectivity checks
- Update VM
- Take baseline snapshot

Create Virtual Machine Wizard:

- Screen 1:
 - Name: kali
 - Machine Folder: Default
 - Type: Linux
 - Version: Debian (64-bit)
- Screen 2:
 - Memory size: 2GB
- Screen 3:
 - Create virtual hard disk now
- Screen 4:
 - VDI (VirtualBox Disk Image)
- Screen 5:
 - Fixed size
- Screen 6:
 - Name: kali
 - Size: 40.00GB

Strip away excess virtual hardware

- System:
 - Set Pointing Device drop-down to PS/2 Mouse
- Storage: Choose Virtual Optical Disk file
 - Ubuntu-18.04.X-live-server-amd64.iso
- Audio: Uncheck Enable Audio
- Serial Ports
 - Ensure no serial ports are enabled (should be default)
- USB: Uncheck Enable USB Controller
- Shared Folders
 - Ensure no shared folders are configured (should be default)
- Network: Verify Enable Network Adapter checkbox is checked for Adapter 1 ONLY
 - Attached to: internal network
 - Name: intnet
 - Advanced Settings
 - Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - Copy the MAC Address to your MAC address text file/document
 - Ensure Cable Connected is checked

Creating a Static DHCP Mapping

- Log in to pfSense webConfigurator (<https://172.16.1.1>)
- Navigate to Services > DHCP Server
 - OPT1 tab
 - DHCP Static Mappings for this Interface
- Input the MAC address for Network Adapter 1 (host-only) on the IPS VM
- Input 172.16.2.2 for the IP Address
- Optional: Enter “kali” as the hostname and/or enter a description
 - Save, then Apply Changes
- Confirm the new DHCP Static Mapping

Installing Kali

- Install process (Note: arrow keys to move, space bar to select things, Enter to confirm your selections):
 - Start the VM
 - On Boot menu, select Install
 - Select English as your language (default)
 - United States as your country
 - American English as your Keyboard's keymap
 - Installer then searches for an IP address for eth0 (the default network interface)

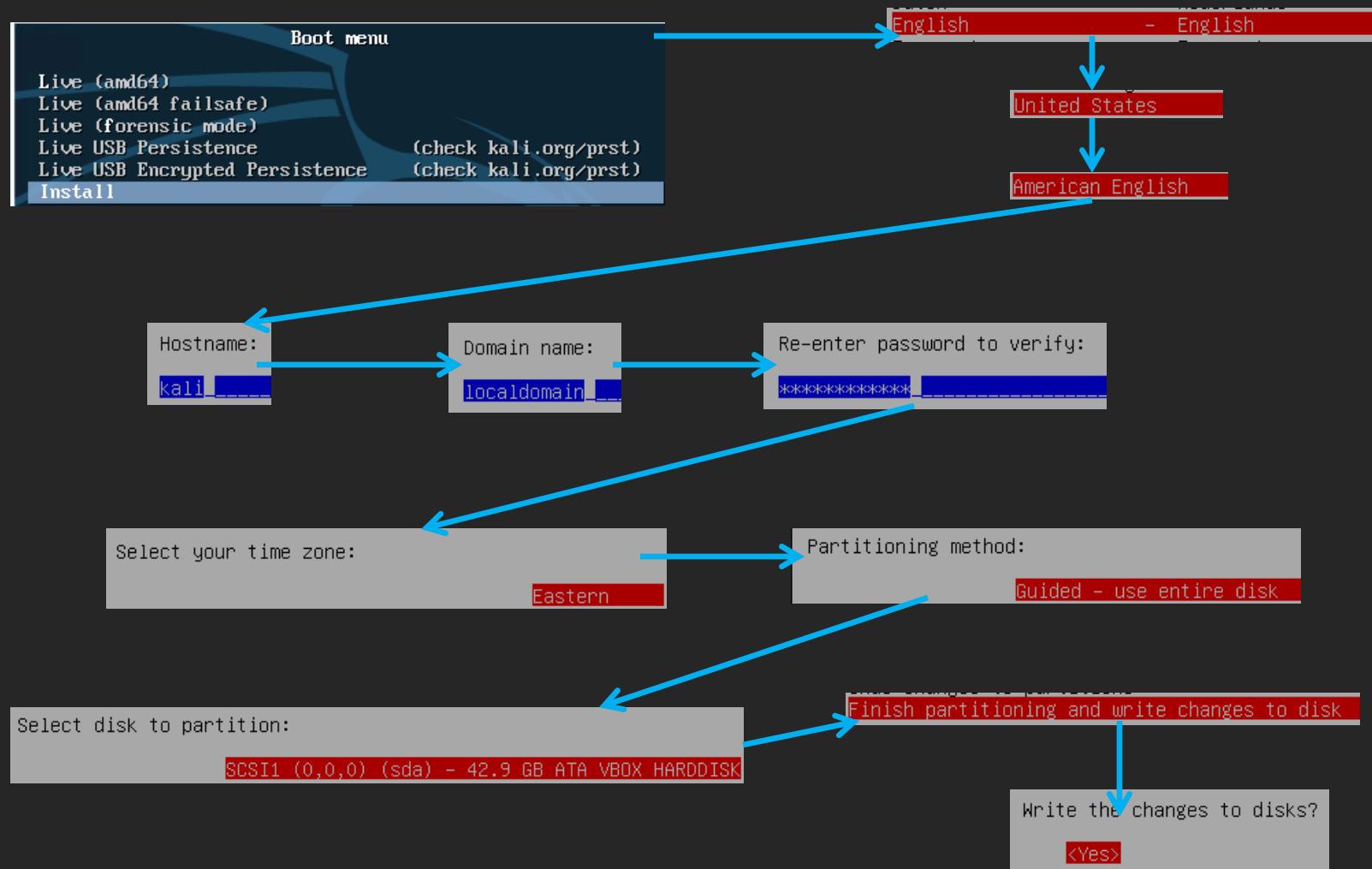
Installing Kali (cont'd)

- Set the hostname to “kali” (should be the default)
- Domain name “localdomain” should be fine
- Set, then confirm the root password
 - Consider putting the root user’s password in keepassXC
- Set your timezone to Eastern
 - Or for those at home/living in another timezone, your local timezone instead
- Set your Partitioning method to Guided – use entire disk
 - There should be only one disk to partition
 - Set the Partitioning scheme to All files in one partition
 - Select Finish partitioning and write changes to disk
 - Just kidding! Under Write changes to disks? Select Yes

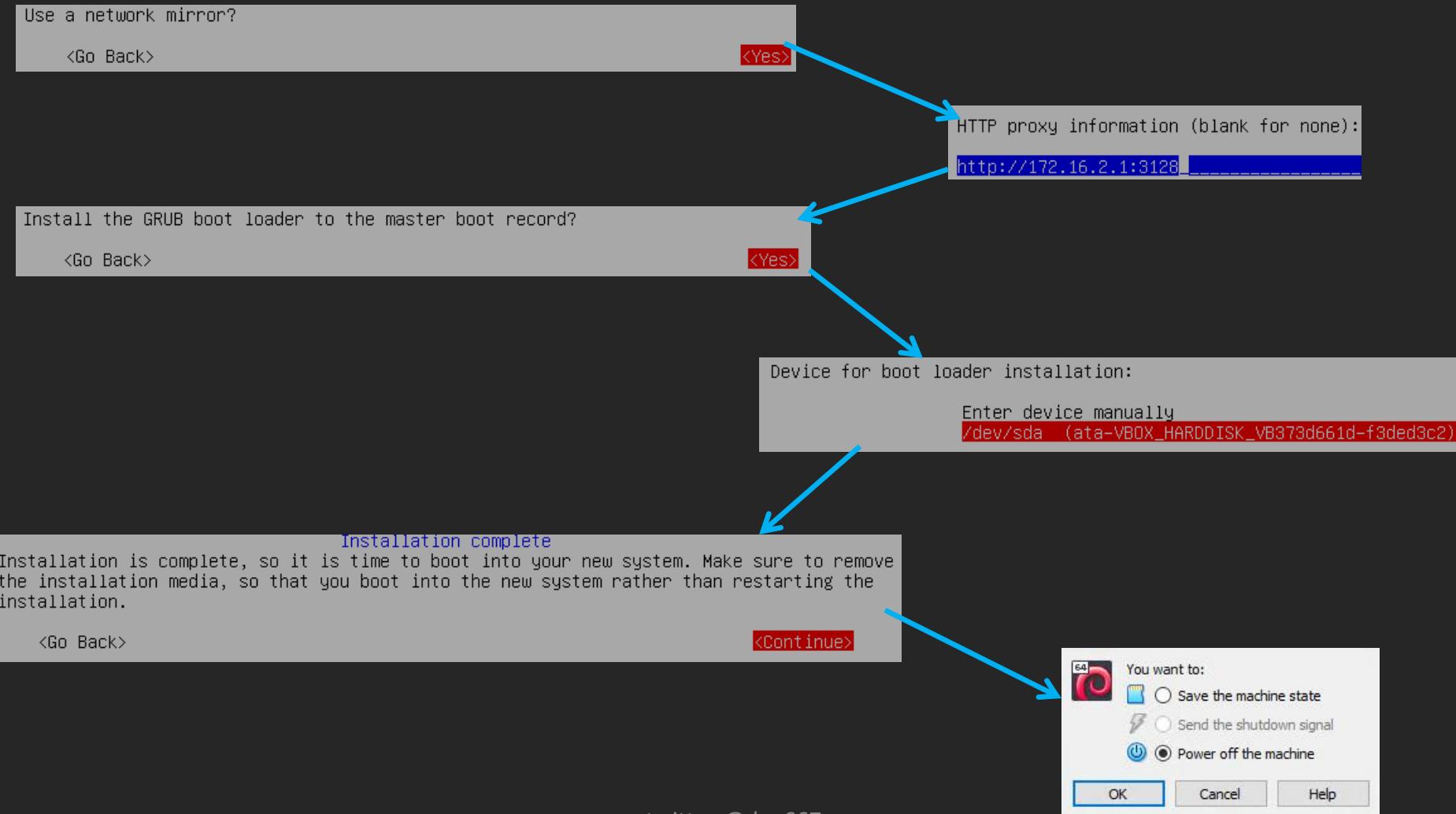
Installing Kali (cont'd)

- Grab some popcorn, take a smoke/bathroom break, set back and chill
 - This part takes a while. Even on SSD.
- Under Use a network mirror, select Yes
 - Under HTTP proxy information enter `http://172.16.2.1:3128`
- When asked to Install the GRUB boot loader to the master boot record, select Yes
 - Device for boot loader installation:
 - Select the option that starts with “/dev/sda”
 - » `/dev/sda (ata-VBOX_HARDDISK_uuid-uuid)`
- On the “Installation Complete” screen, hit enter.
 - System performs a bunch of cleanup tasks, then automatically tries to reboot
- While the system is rebooting, close the VM console, and select “Power off the Machine”

Installing Kali (cont'd)



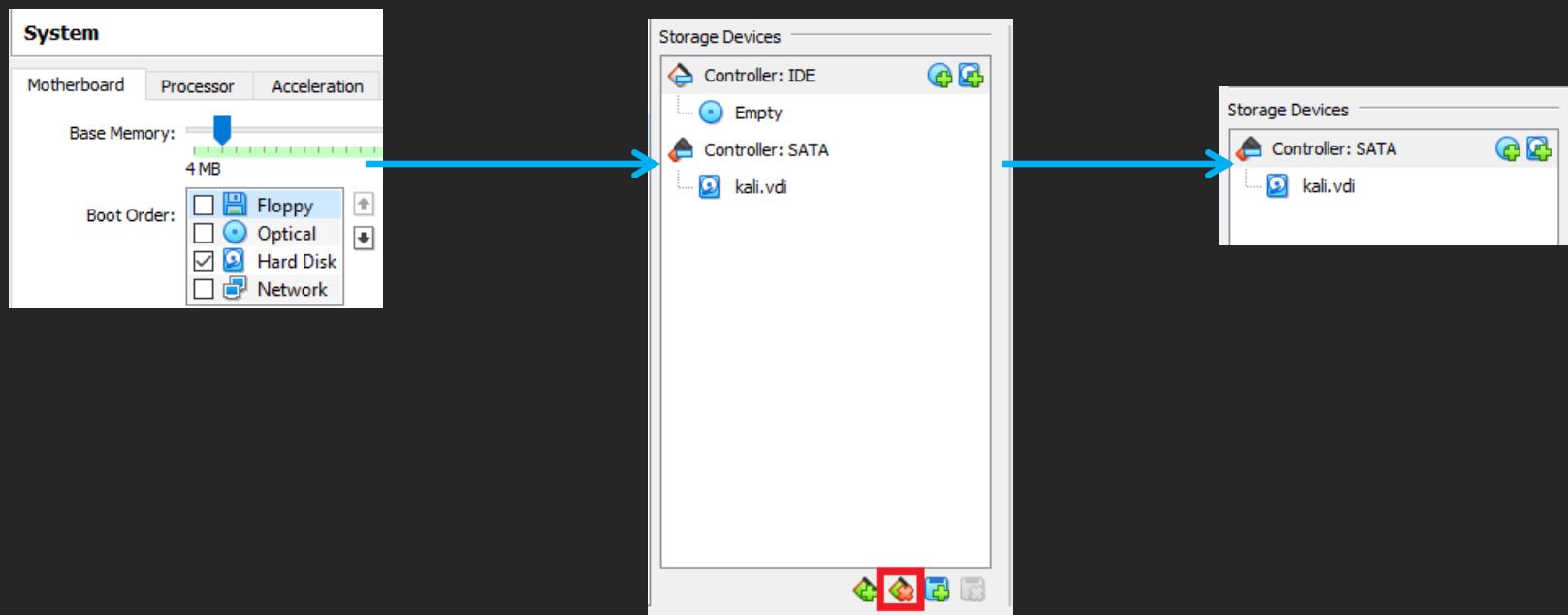
Installing Kali (cont'd)



Strip Remaining Excess Virtual Hardware

- kali VM Settings:
 - System: Uncheck Floppy and Optical checkboxes in Boot Order list
 - Storage: Remove Virtual CD/DVD drive

Strip Remaining Excess Virtual Hardware (cont'd)



Perform Connectivity Checks

- Log in to VM (username: root and password you set)
- Open terminal application
- Perform connectivity check commands
 - ping -c4 www.google.com
 - nslookup www.google.com
 - curl -I www.google.com
 - ifconfig -a (verify DHCP static map)

Perform Connectivity Checks (cont'd)

```
root@kali:~# ping -c4 www.google.com
PING www.google.com (172.217.6.4) 56(84) bytes of data.
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=1 ttl=53 time=24.
7 ms
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=2 ttl=53 time=24.
4 ms
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=3 ttl=53 time=21.
1 ms
64 bytes from ord38s01-in-f4.1e100.net (172.217.6.4): icmp_seq=4 ttl=53 time=20.
5 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 20.495/22.672/24.691/1.885 ms
```

```
root@kali:~# nslookup www.google.com
Server: 172.16.2.1
Address: 172.16.2.1#53

Non-authoritative answer:
Name: www.google.com
Address: 172.217.6.4
Name: www.google.com
Address: 2607:f8b0:4009:815::2004
```

```
root@kali:~# curl -I www.google.com
HTTP/1.1 200 OK
Date: Wed, 17 Apr 2019 17:52:58 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-04-17-17; expires=Fri, 17-May-2019 17:52:58 GMT; path=/;
domain=.google.com
Set-Cookie: NID=181=UOUxVntfx1L4XVXn2ocmaClIZveBdVM4peJVgj6PDFheamGMK7GZcqHtu002
NKv4uTtAhHwdV0TcQdaK8fT09l7kZQh4eK0ARS746udI0HCaKI9zFHY9f0wY5I7DPV90HFbeS-dw611B
2DYhlUdL8Pb53qsZLQWo29bHzafGMV0; expires=Thu, 17-Oct-2019 17:52:58 GMT; path=/;
domain=.google.com; HttpOnly
Transfer-Encoding: chunked
Accept-Ranges: none
Vary: Accept-Encoding
```

```
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 172.16.2.2 netmask 255.255.255.0 broadcast 172.16.2.255
            inet6 fe80::a00:27ff:fe6f:8be3 prefixlen 64 scopeid 0x20<link>
                  ether 08:00:27:6f:8b:e3 txqueuelen 1000 (Ethernet)
```

```
20
21 Kali
22 nic 1: Internal Network (intnet)
23 MAC address: 08:00:27:6F:8B:E3
```

System Updates

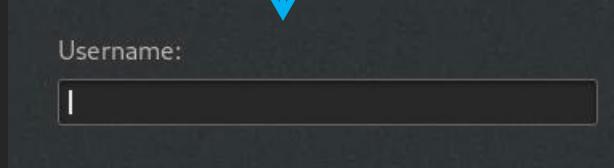
- Depending on network connectivity... This could be fast or slow
- Note: slight bug with performing system updates
 - Kali has an automatic update checker that:
 - Locks the update database (required for the system to actually update)
 - Doesn't actually identify all of the software packages available for update
 - Solution: Give Kali 5-10 minutes to tell you there are updates available, ignore the message then....

System Updates (cont'd)

- Run the command(s):
 - `export DEBIAN_FRONTEND=noninteractive`
 - `apt-get update`
 - `apt-get -y dist-upgrade`
 - `init 6`
 - No need to ‘`sudo su -`’, you’re already the root user.
 - Note: If you have issues downloading updates, make sure that your connectivity checks were **SUCCESSFUL**. Verify that you configured the `apt-get proxy` correctly (`http://172.16.2.1:3128 -- /etc/apt/apt.conf`)
 - Just like before, you can chain all of these commands together like this:
 - `export DEBIAN_FRONTEND=noninteractive && apt-get update && apt-get -y dist-upgrade && init 6`

System Updates (cont'd)

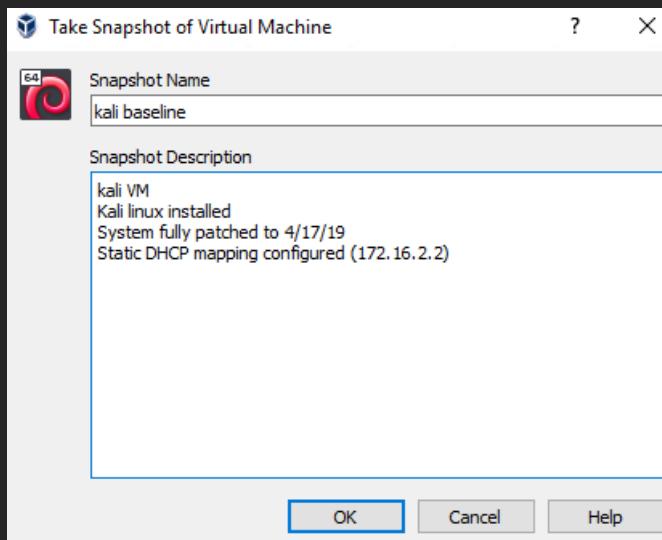
```
root@kali:~# export DEBIAN_FRONTEND=noninteractive && apt-get update && apt-get  
-y dist-upgrade && init 6
```



Take Baseline Snapshot

- Allows you to revert back to a known good state in case your leet exploits brick your VM.

Take Baseline Snapshot (cont'd)



Chapter 9: Metasploitable 2

Metasploitable 2

- A very, very old, very intentionally vulnerable virtual machine
 - Purpose: To serve as an exploitable pin cushion
 - Why are we using this: proof of concept
 - Kali VM attacks metasploitable 2
 - Has to traverse AFPACKET bridge (connectivity testing)
 - Alternatively: turn off IPS VM, no connectivity, demonstrates fail-close networking/emergency isolation
 - Generates alerts (IDS/IPS software testing)
 - Alerts get logged to Splunk (SIEM connectivity test)
 - Query Splunk to show IPS VM alerts (SIEM logging/testing)

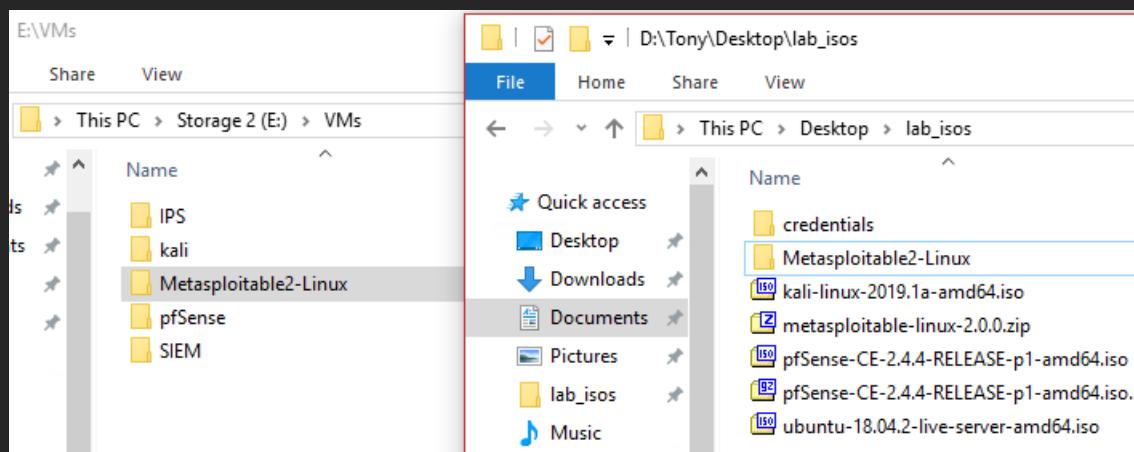
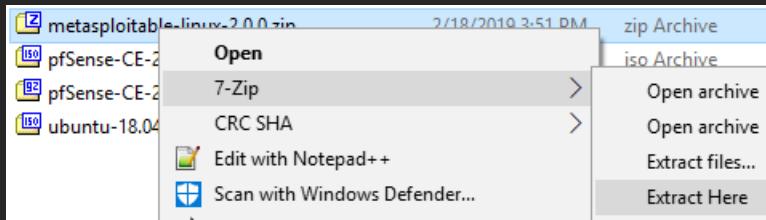
Tasks to Perform

- Decompress Metasploitable 2 VM
- Move to VM storage directory
- Add to Virtualbox Manager VM list
- Remove excess virtual hardware
- Add static DHCP map
- Power on VM
- Snapshot

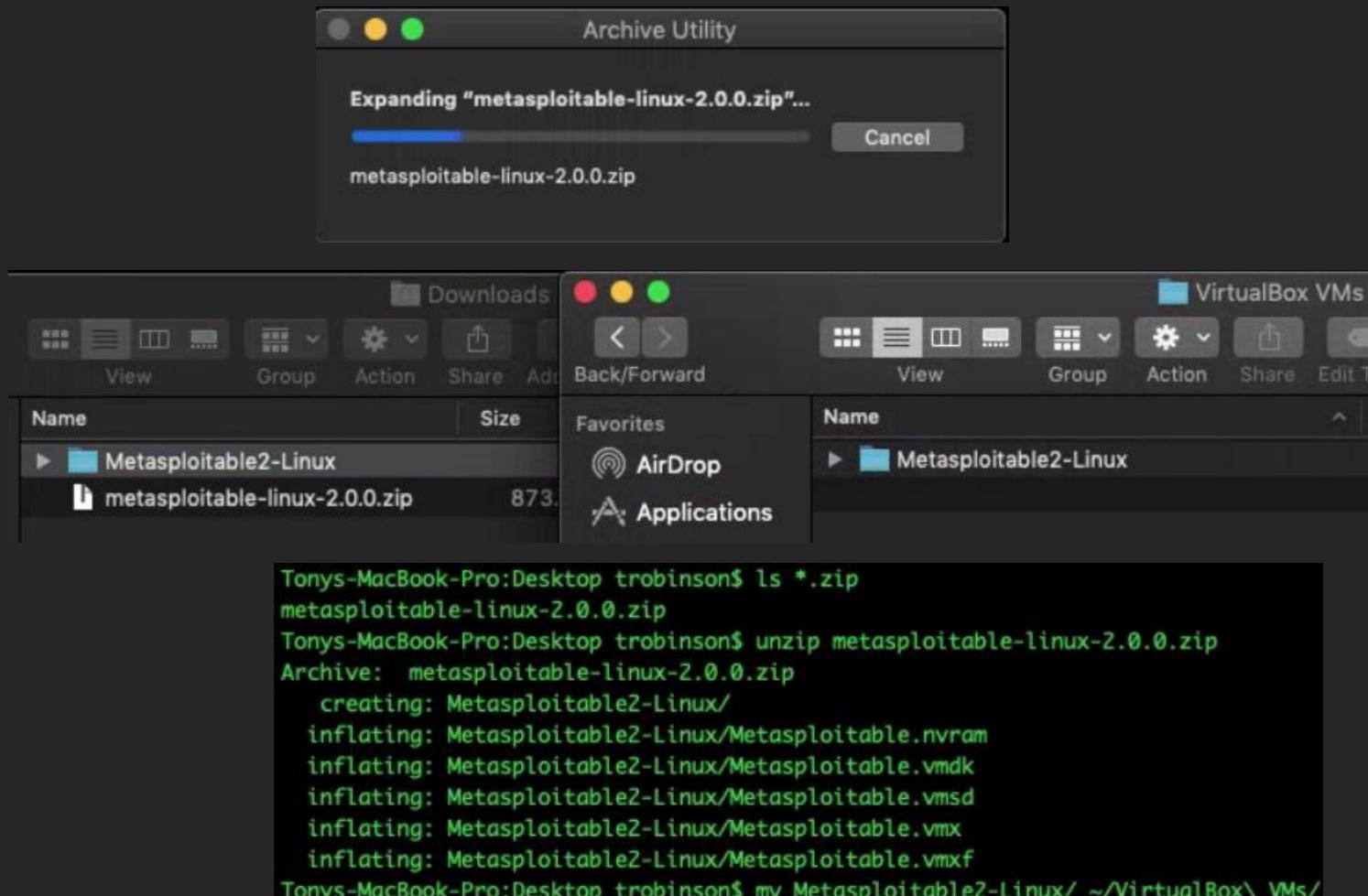
Decompress and Move Metasploitable 2

- Windows: Use 7-zip
 - Right Click `metasploitable-linux-2.0.0.zip` -> “Extract Here”
- Linux/OSX:
 - Option 1: Utilize your window manager’s filemanager and unzip the file with it
 - Linux: YMMV
 - OSX: Double click `metasploitable-linux-2.0.0.zip`
 - Automatically decompresses zip file.
 - Option 2: `unzip`
 - Open terminal
 - `cd /path/to/metasploitable-linux-2.0.0.zip`
 - `unzip metasploitable-linux-2.0.0.zip`
- Afterwards: Move the directory “Metasploitable2-Linux” to the default machine folder (e.g. On my system, this is E:\VMs)
 - Why: consistency is a good thing

Decompress and Move Metasploitable 2 (cont'd)



Decompress and Move Metasploitable 2 (cont'd)



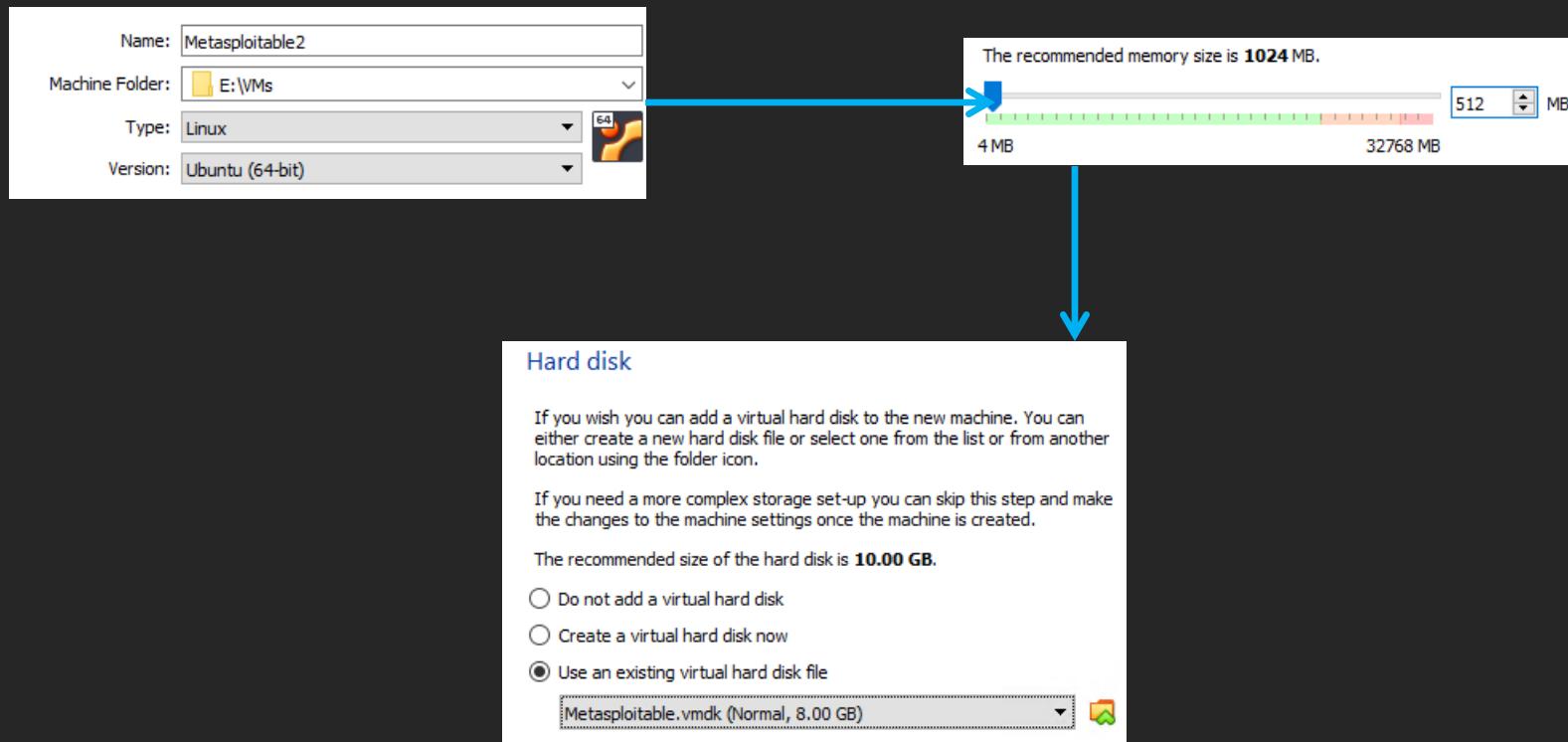
Adding Metasploitable 2 to the VirtualBox Manager

- This isn't exactly the same as adding a new VM, but its pretty close.
- Start the New VM wizard, same as normal. Here are the settings I recommend:
 - Name: Metasploitable2
 - Type: Linux
 - Version: Ubuntu (64-bit)
 - Note: Metasploitable2 is actually 32-bit, but this doesn't matter.
 - Memory Size: 512MB

Adding Metasploitable 2 to the VirtualBox Manager (cont'd)

- Hard disk (this is where things get a little different)
 - Select Use an existing virtual hard disk file, then click browse, and browse to your Machine Folder and the Metasploitable2-Linux subfolder. Select “Metasploitable.vmdk”
 - VMDK is a virtual disk file format. Its native to vmware, but virtualbox can read it.

Adding Metasploitable 2 to the VirtualBox Manager (cont'd)



Remove Excess Virtual Hardware

- The same song as dance as before, but this time, we do everything all at once
 - The Operating system is already installed, meaning we don't have to wait to nuke the virtual CD/DVD drive or modify the boot order.
- Metasploitable2 Settings:
 - System > Motherboard:
 - Uncheck Floppy and Optical from the Boot Order list
 - Change Pointing Device drop-down to PS/2 Mouse
 - Storage:
 - Remove the IDE controller (and Virtual CD/DVD drive)

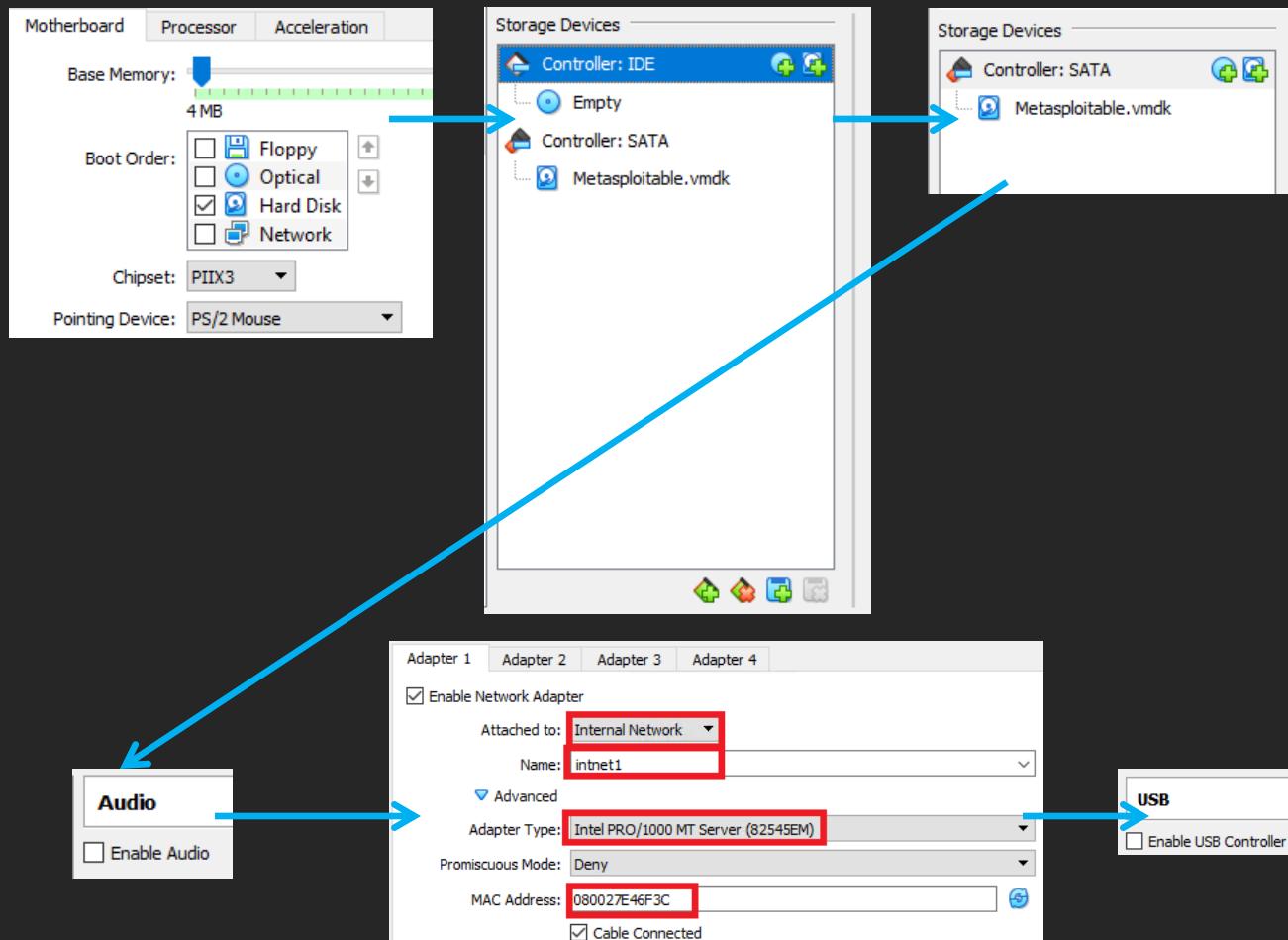
Remove Excess Virtual Hardware

- Audio
 - Uncheck Enable Audio
- Network
 - Ensure that Enable Network Adapter is checked for Adapter 1 ONLY
 - Attached to: Internal Network
 - » Name: intnet1
 - Advanced Settings:
 - » Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - » Record the MAC Address to create a static DHCP mapping on OPT1
 - » Ensure Cable Connected is checked
- USB
 - Uncheck Enable USB Controller

Remove Excess Virtual Hardware (cont'd)

- Audio
 - Uncheck Enable Audio
- Network
 - Ensure that Enable Network Adapter is checked for Adapter 1 ONLY
 - Attached to: Internal Network
 - » Name: intnet1
 - Advanced Settings:
 - » Adapter Type: Intel PRO/1000 MT Server (82545EM)
 - » Record the MAC Address to create a static DHCP mapping on OPT1
 - » Ensure Cable Connected is checked
- USB
 - Uncheck Enable USB Controller

Remove Excess Virtual Hardware (cont'd)



Creating a Static DHCP Mapping

- Log in to pfSense webConfigurator (<https://172.16.1.1>)
- Navigate to Services > DHCP Server
 - OPT1 tab
 - DHCP Static Mappings for this Interface
- Input the MAC address for Network Adapter 1 (host-only) on the IPS VM
- Input 172.16.2.3 for the IP Address
- Optional: Enter “Metasploitable2” as the hostname and/or enter a description
 - Save, then Apply Changes
- Confirm the new DHCP Static Mapping

Creating a Static DHCP Mapping (cont'd)

The screenshot shows a configuration interface for creating a static DHCP mapping on a device with the identifier 'OPT1'. The interface includes fields for MAC Address (08:00:27:E4:6F:3C), Client Identifier (empty), IP Address (172.16.2.3), and Hostname (metasploitable2). A note states: 'If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool.' Below this, it says: 'The same IP address may be assigned to multiple mappings.'

To the right, a terminal window titled 'lab_mac_addresses.txt' displays the following content:

```
25 metasploitable2
26 nic 1: Internal Network
(intnet1)
27 MAC Address: 08:00:27:E4:6F:3c
```

A blue arrow points from the 'Hostname' field in the configuration interface down to the 'metasploitable2' entry in the terminal window.

DHCP Static Mappings for this Interface			
Static ARP	MAC address	IP address	Hostname
	08:00:27:6f:8b:e3	172.16.2.2	kali
	08:00:27:e4:6f:3c	172.16.2.3	metasploitable2

Power on the VM

- Start up the metasploitable2 VM
- Log in
 - Username: msfadmin
 - Password: msfadmin
- We're only testing to make sure the VM boots up, and that you are able to successfully log in
 - As of right now, you won't have an IP address on the VM or any network connectivity
 - Why: the IPS VM isn't bridging intnet and intnet1 (yet)
- Close the VM console and power off the VM.

Power on the VM (cont'd)

```
Login with msfadmin/msfadmin to get started

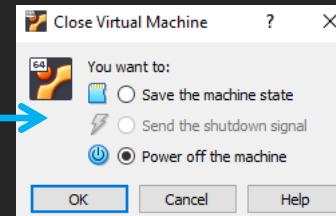
metasploitable login: msfadmin
Password:
Last login: Mon May 21 01:44:38 EDT 2012 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2012

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

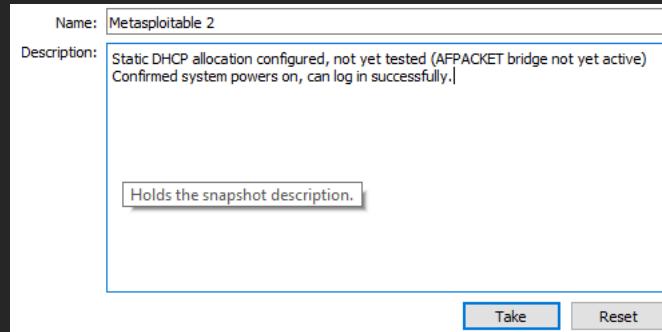
msfadmin@metasploitable:~$
```



Snapshot

- Same as before, make a baseline snapshot of the metasploitable2 VM
- It might not be fully functional (e.g. No network), but it powers on, and is in a good running state, so it gets a snapshot.

Snapshot (cont'd)



Chapter 10: Firewall Hardening and Customization



twitter:@da_667
email:deusexmachina667@gmail.com

Easy part is done. This is where the fun starts.

- You have (mostly) functional VMs
- You have basic network connectivity
- You have baseline snapshots
- This chapter will focus on pfSense (again)
 - pfSense is /mostly/ functional, but we're not 100% there yet.

pfSense Current Status:

- Patched pfSense to the latest version
- Installed, enabled, and configured squid
- Set up basic firewall rules to allow you to set up your VMs
- Disabled the default anti-lockout rule, and made a much more concise and strict anti-lockout rule
- Made a baseline snapshot
- Configured a bunch of Static DHCP allocations on LAN and OPT1

Tasks to Perform

- Learn about firewall aliases
 - Create an alias to represent all RFC1918 networks
- Learn about default deny and why firewall rule order matters
- Create an optimized firewall ruleset for WAN, LAN, and OPT1
 - Enforce network segmentation
- Enable and configure pfSense to serve time via NTP

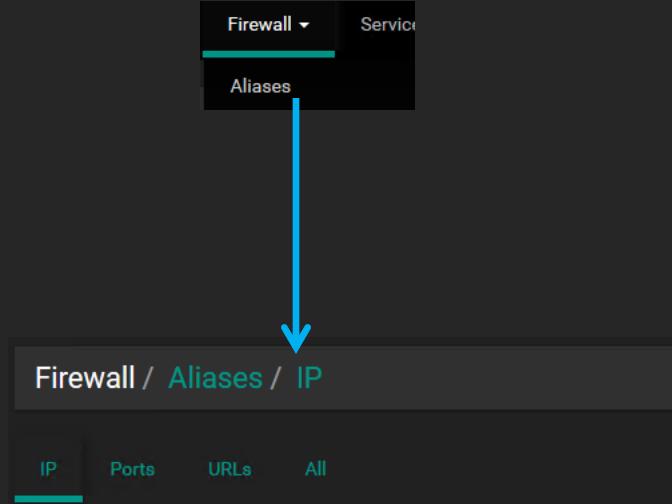
Firewall Aliases

- Allow pfSense to group together ports, IP addresses/networks and URLs under a single name
 - Think of firewall aliases as “variables” If you know programming/systems administration terminology
- pfSense has several aliases available by default
 - LAN net = network range of LAN IP addresses (e.g. 172.16.1.0/24)
 - LAN ip = IP address of LAN interface (e.g. 172.16.1.1)
 - Etc.

Firewall Aliases

- Where do I define aliases?
 - Firewall > Aliases
 - Can select from IP, Port, URL, or All

Firewall Aliases



What is RFC1918?

- RFC1918 are “local” networks
 - These networks are not routable on the public internet
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
 - Provided you’re not using IPv6(lol) your home or office network probably uses these networks for your LAN (local area network) to address your local systems
 - RFC1918 addresses are commonly used with:
 - NAT (Network Address Translation)
 - PAT (Port Address Translation)
 - NAT/PAT allow you to “share” a public IP address (or multiple public IP addresses) to allow multiple systems on your network access to the internet without all of them needing public IP addresses

Why do we care about RFC1918?

- We will be creating an alias that defines ALL RFC1918 networks
- This alias will be used to create firewall rules
 - Deny VMs on lab network segments the ability to connect to one another
 - Unless explicitly allowed
 - Deny other physical hosts on your local network from interacting with your lab VMs (or vice versa)
 - Prevent lab VMs from attacking other systems outside of their given network segment or the lab as a whole
 - Unless you explicitly allow it
 - Prevent other guests on the same physical network as your hypervisor from accessing your VMs
 - Again, unless you explicitly allow it

Why do we care about RFC1918? (cont'd)

- Network isolation is very important
 - Keep lab things in your lab
 - Limit exposure to or from external systems
 - Good housekeeping
 - An alias for RFC1918 networks will help enforce segmentation, while minimizing firewall rule list complexity

Creating the RFC1918 networks alias

- Navigate to Firewall > Aliases
 - Default tab should be IP, simply click Add.
- On the Firewall > Aliases > Edit page:
 - Name: RFC1918_Addresses
 - Description: Collection of RFC1918 Networks
 - Type: Network(s)
 - Click the Add Network button
 - Network 1: 10.0.0.0/8 Description: RFC1918 10.0.0.0/8 Networks
 - Network 2: 172.16.0.0/12 Description: RFC1918 172.16.0.0/12 Networks
 - Network 3: 192.168.0.0/16 Description: RFC1918 192.168.0.0/16 Networks
 - Click Save
- Back on Firewall > Aliases > IP
 - Click Apply Changes

Creating the RFC1918 networks alias (cont'd)

Firewall / Aliases / IP

IP Ports URLs All

Firewall Aliases IP

Name	Values	Description	Actions
			Add Import

Add Import

Firewall / Aliases / Edit

Properties

Name: RFC1918_Addresses
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description: Collection of RFC1918 Networks
A description may be entered here for administrative reference (not parsed).

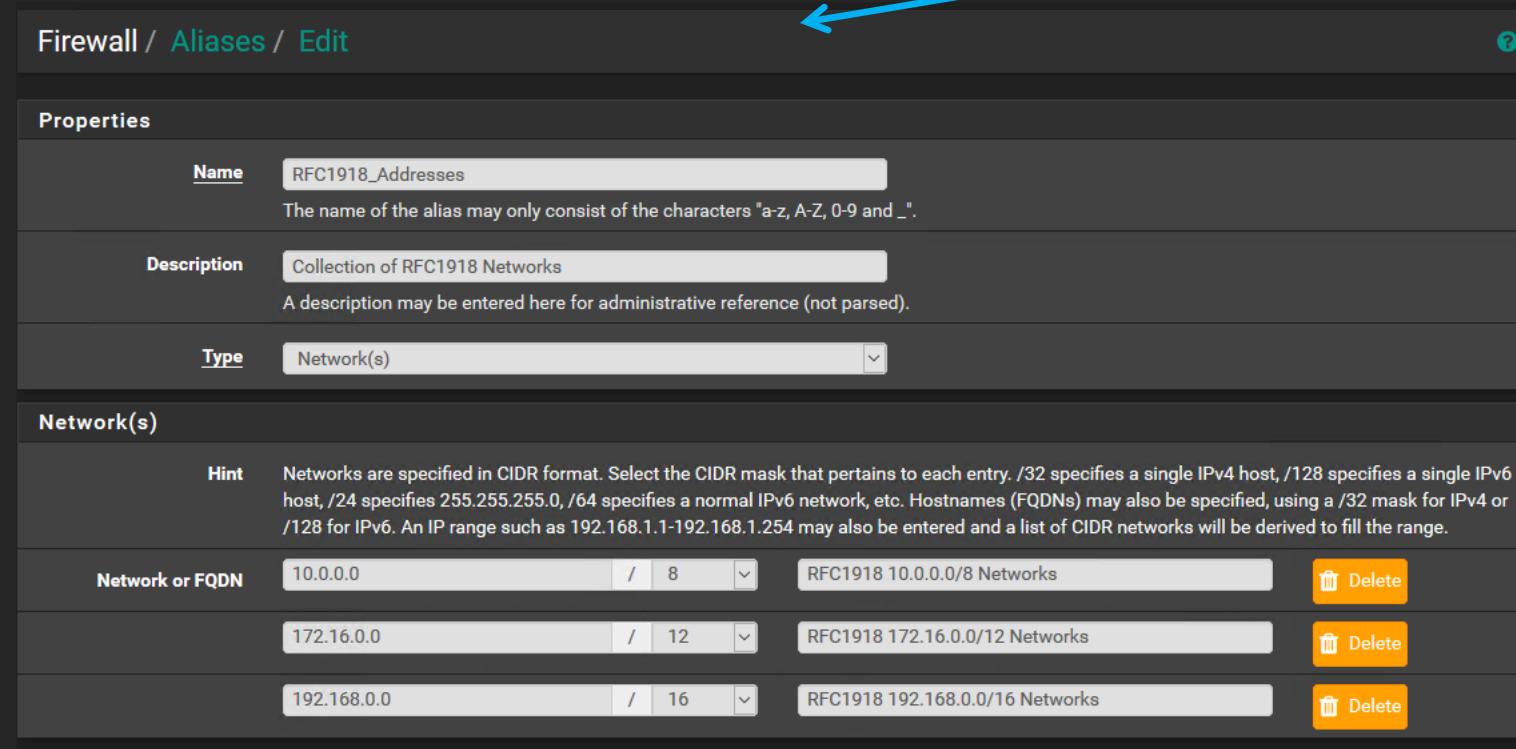
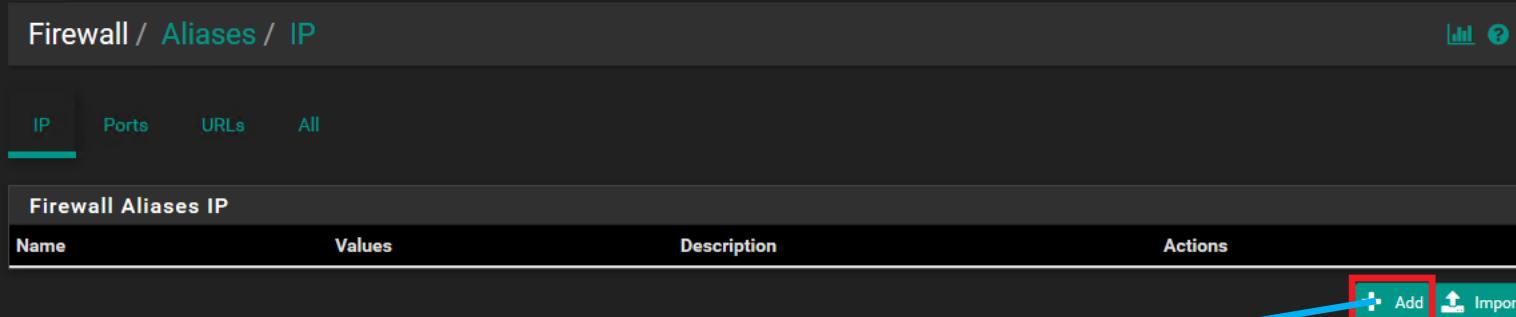
Type: Network(s)

Network(s)

Hint: Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN	/	8	RFC1918 10.0.0.0/8 Networks	Delete
10.0.0.0	/	8	RFC1918 10.0.0.0/8 Networks	Delete
172.16.0.0	/	12	RFC1918 172.16.0.0/12 Networks	Delete
192.168.0.0	/	16	RFC1918 192.168.0.0/16 Networks	Delete

Save Add Network



Creating the RFC1918 networks alias (cont'd)

Firewall Aliases IP			
Name	Values	Description	Actions
RFC1918_Addresses	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	Collection of RFC1918 Networks	
 Add Import			

Introduction to Firewall Rule logic – “Default Deny any/any”

- Default deny any/any
 - If there are no rules that explicitly allow a particular type of traffic, most modern firewalls have a feature called “default deny”
 - Invisible firewall rule that says “If traffic received doesn’t match any of the rules on this interface that are allowed, then drop it”

Introduction to Firewall Rule logic – “Default Deny any/any”

- Default deny any/any
 - If there are no rules that explicitly allow a particular type of traffic, most modern firewalls have a feature called “default deny”
 - Invisible firewall rule that says “If traffic received doesn’t match any of the rules on this interface that are allowed, then drop it”

Introduction to Firewall Rule logic – “Order of Rule Processing”

- Firewall rule order matters a lot
 - Most will process rules from top-most to bottom
- As it turns out, the order of Deny rules vs. Allow rules matters too

Introduction to Firewall Rule logic – “Order of Rule Processing”

- Example:
 - Two firewall rules:
 - Rule 1: Deny ICMP from source IP 10.0.0.1
 - Rule 2: Allow ICMP from source network 10.0.0.0/8
 - What happens when 10.0.0.1 tries to ping something that is NOT on the local network?
 - Deny rule gets evaluated first, any ICMP traffic from 10.0.0.1 to non-local hosts gets dropped
 - So what would happen if the rule order was switched?
 - All ICMP traffic from 10.0.0.0/8 source IP addresses would be allowed outbound, even traffic from 10.0.0.1
 - What happens when 10.0.0.1 tries to make an outbound connection on port 23/tcp to an external host?
 - Assuming the default deny any/any, and assuming this traffic is trying to reach a non-local network host, this traffic would be dropped by the firewall, because there is no rule explicitly allowing it

BEEF UP THEM FIREWALL RULES

- I'm going to show you a collection of screen caps of what your firewall rules should look like
 - One screen cap per interface – WAN, LAN and OPT1
- Configuring the interfaces with the proper firewall rules will be an exercise for you perform
 - Your firewall rules should be in the exact same order as presented. Drag and drop to change the processing order as needed

WAN

Firewall / Rules / WAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

#	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0 / 1.30 GiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
✗	0 / 418 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

LAN

Firewall / Rules / LAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✓ 1/9.57 MiB	IPv4 TCP	172.16.1.2	*	172.16.1.1	443 (HTTPS)	*	none		Better Anti-Lockout Rule	
■	✓ 0/0 B	IPv4 UDP	172.16.1.0/24	*	172.16.1.1	53 (DNS)	*	none		Allow DNS traffic to gateway	
■	✓ 0/0 B	IPv4 UDP	172.16.1.0/24	*	172.16.1.1	123 (NTP)	*	none		Allow NTP traffic to gateway	
■	✓ 0/0 B	IPv4 TCP	172.16.1.0/24	*	172.16.1.1	3128	*	none		Allow Squid proxy traffic to the gateway	
■	✓ 0/0 B	IPv4 TCP	172.16.1.2	*	172.16.2.2	22 (SSH)	*	none		Allow SSH access from hypervisor to kali VM	
■	✗ 0/0 B	IPv4+6	*	*	RFC1918 Addresses	*	*	none		Deny access to other RFC1918 networks	
■	✓ 0/0 B	IPv4 TCP	172.16.1.0/24	*	*	443 (HTTPS)	*	none		Allow HTTPS outbound	
■	✗ 0/0 B	IPv4+6	*	*	*	*	*	none		Explicit deny any/any	

OPT1

Firewall / Rules / OPT1

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✗ 0/0 B	IPv4 *	172.16.2.3	*	*	*	*	none		Deny Metasploitable 2 outbound	🔗 🖊️ 🗑️ 🗑️
■	✓ 0/0 B	IPv4 UDP	172.16.2.0/24	*	172.16.2.1	53 (DNS)	*	none		Allow DNS traffic to gateway	🔗 🖊️ 🗑️ 🗑️
■	✓ 0/0 B	IPv4 UDP	172.16.2.0/24	*	172.16.2.1	123 (NTP)	*	none		Allow NTP traffic to gateway	🔗 🖊️ 🗑️ 🗑️
■	✓ 0/0 B	IPv4 TCP	172.16.2.0/24	*	172.16.2.1	3128	*	none		Allow Squid proxy traffic to gateway	🔗 🖊️ 🗑️ 🗑️
■	✗ 0/0 B	IPv4+6 *	*	*	RFC1918 Addresses	*	*	none		Deny Access to other RFC1918 networks	🔗 🖊️ 🗑️ 🗑️
■	✗ 0/0 B	IPv4+6 TCP	*	*	*	80 (HTTP)	*	none		Deny HTTP out (force proxy use)	🔗 🖊️ 🗑️ 🗑️
■	✗ 0/0 B	IPv4+6 TCP	*	*	*	21 (FTP)	*	none		Deny FTP out (force proxy use)	🔗 🖊️ 🗑️ 🗑️
■	✓ 0/0 B	IPv4 *	*	*	*	*	*	none		Allow any/any out for custom C2/Malware	🔗 🖊️ 🗑️ 🗑️

Explanation

- WAN
 - Pretty self-explanitory – we don't want anything coming in to our lab network.
 - Tip: These are default rules. They can be disabled by clicking the gear option and unchecking block RFC1918 and/or Block Bogon Networks.
 - Tip2: Even if they weren't enabled, it wouldn't matter due to the default deny any/any. Ain't nothin' coming in
 - And that's how we want it.

Explanation (cont'd)

- LAN
 - First rule: Better anti-lockout rule. Allows hypervisor host-only network adapter access to webconfigurator.
 - No other systems on this network can access the webconfigurator
 - Next 3 rules: Allow VMs on LAN network to use pfSense for DNS, NTP, and HTTP/FTP proxy services
 - We'll be setting up NTP momentarily...
 - Fifth rule: Explicitly allows our hypervisor host-only interface to SSH to the kali linux VM
 - This is for a future chapter...
 - Sixth rule: Boundary enforcement – disallows LAN VMs from talking to systems on other network segments
 - Seventh rule: Allows LAN VMs outbound access over HTTPS for downloading updates, etc.
 - Specifically placed AFTER Rule 6. Takes advantage of order of firewall rule processing
 - Rule 8: Explicit deny any/any
 - Technically not needed, but created to serve as a reminder that the implicit deny any/any rule is a thing.

Explanation (cont'd)

- OPT1
 - Rule 1: Explicitly created to ensure Metasploitable 2 VM has ZERO outside network connectivity. Period.
 - Placed at the top to ensure it has the highest rule priority, order of rule processing
 - Rules 2-4: Same as LAN interface
 - Allow pfsense VM to be used for DNS, NTP, and proxy services
 - Rule 5: Same as LAN interface rule 6
 - Boundary enforcement, ensure OPT1 VMs cannot talk to other network segments without explicit permission
 - Rules 6,7: Explicitly deny HTTP and/or FTP outbound
 - We want to force all VMs in our lab network to use the squid proxy for HTTP and FTP traffic
 - Rule 8: Allow any/any outbound
 - Any traffic not explicitly defined/blocked above will be allowed out
 - Meant to make OPT1 serve as a “malware analysis” network
 - A lot of malware uses custom C2, custom ports, custom protocols, etc.
 - Rule setup protects local networks from malware attempting to connect, but allows outbound connectivity for additional malware (e.g. Second/third stage implants, C2, etc.)
 - Don’t plan on using OPT1 for malware analysis? Delete rules 6-8. Add allow HTTPS outbound as rule 6 (LAN interface rule 7), optionally add explicit deny any/any (LAN interface rule 8)

Note:

- Firewall rules, like Siths deal in absolutes
 - If there isn't a rule that explicitly allows your traffic outbound, then you will NOT have outbound access
 - Remember when we set up Ubuntu Server/Kali and you defined your http proxy server? That was kinda important
 - `http://172.16.1.1:3128` (LAN squid proxy address)
 - `http://172.16.2.1:3128` (OPT1 squid proxy address)
 - `/etc/apt/apt.conf` (apt/apt-get configuration file)
 - Without that configuration, and with these firewall rules, you will NOT be able to update your VMs.
 - If you have tools/applications that use HTTP for communication, **REMEMBER TO CONFIGURE THE APP TO USE YOUR PROXY**
 - Command line linux tools :
 - `export http_proxy=http://172.16.[12].1:3128`
 - Some linux/unix tools read the `http_proxy` variable to know what proxy server to use for HTTP comms.

NTP: Network Time Protocol

- Serving accurate time is pretty important for forensics and log management
- NTP is a service/protocol for serving time
 - Its not perfect by any means, but its what is usually used in most enterprise networks
 - Uses port 123/udp

Enabling NTP on pfSense

- Services > NTP
 - Interfaces: LAN and OPT1
 - Time Servers: the default of 0.pfsense.pool.ntp.org should be okay
 - Alternatively: visit www.ntppool.org for NTP pool options for your geographical location
 - Click Save, then apply changes.
 - You are now serving NTP
 - But none of the VMs are using it. We'll go into setting this up later...

Enabling NTP on pfSense (cont'd)

The changes have been applied successfully.

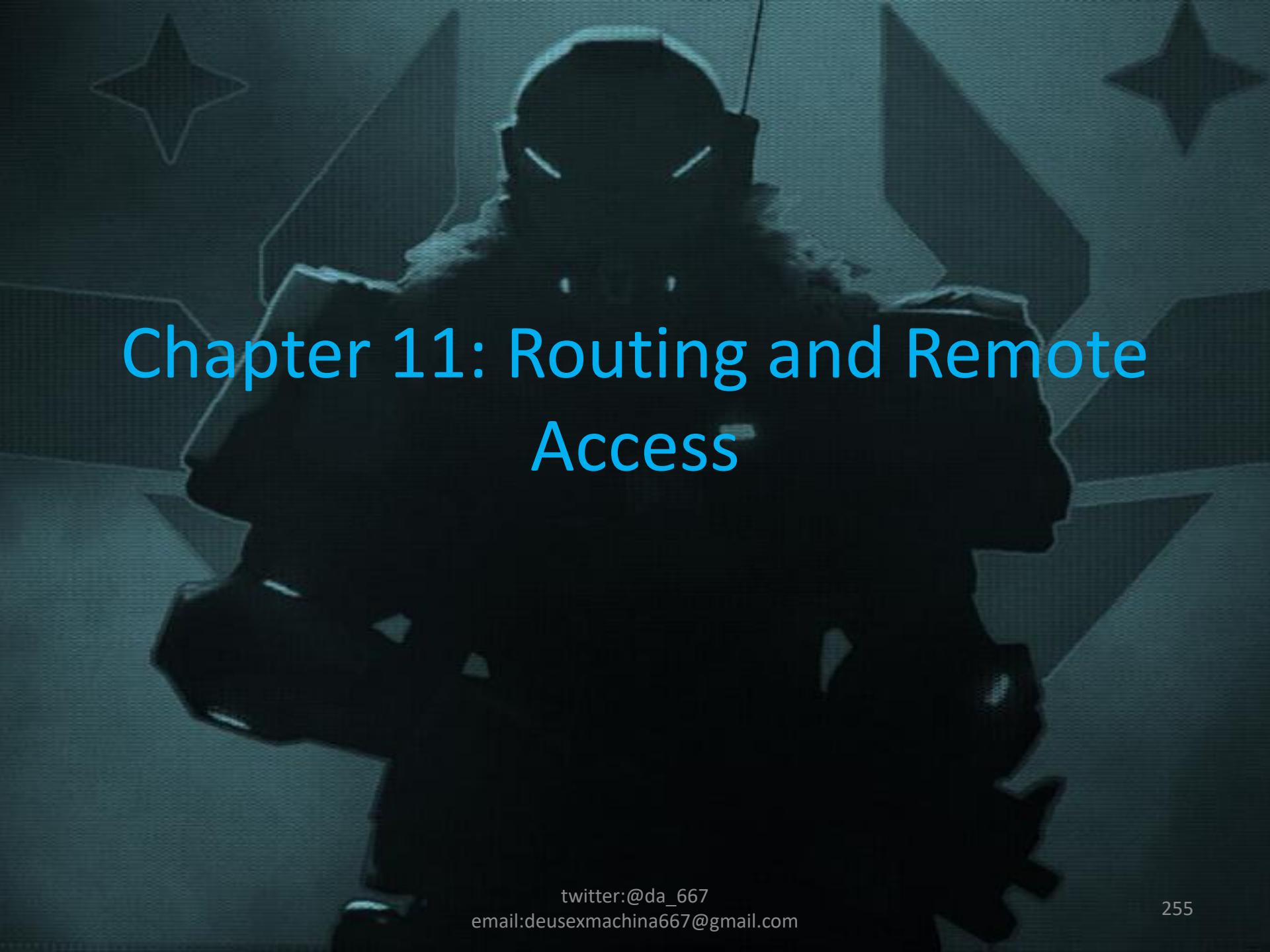
Settings ACLs Serial GPS PPS

NTP Server Configuration

Interface: WAN
LAN
OPT1

Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers: 0.pfsense.pool.ntp.org Prefer No Select Is a Pool



Chapter 11: Routing and Remote Access

Routing and remote access

- We're going to be setting up the kali, IPS, and SIEM virtual machines to be managed using the SSH protocol
 - Will be faster and easier to use than logging in through the console
 - Bonus: your mouse and keyboard input won't be eaten anymore, either
 - Note: This will be something of a long chapter, but you only need to pay attention to the sections that are relevant to you.

Tasks to Perform

- Configure a static route from your hypervisor host (Windows, Linux or OSX) to 172.16.2.0/24
 - Using OS tools, persist this static route to ensure consistent access to the kali VM over the network
- Windows Users:
 - Configure mremoteng to enable SSH access to SIEM, IPS, and kali VMs
 - Enable key-based authentication using puttygen, and various techniques to copy public keys to our VMs
- Linux/OSX Users:
 - Configure SSH connection aliases to SIEM, IPS, and kali VMs
 - Use ssh-keygen, and ssh-copy-id to configure key-based authentication to our VMs
- Windows/Linux/OSX Users:
 - Disabling password authentication via sshd_config
 - (optional) Enabling ssh as the root user

Static Routes

- Routing in a nutshell: Ensuring that your packets from point A (your system) reach point B (the destination host)
 - Routes are stored in a routing table
 - Table in your system's memory that contains a list of all the routes/networks your computer knows how to reach
 - By default, your system knows about networks they are attached to
 - E.g. Eth0 has IP address 172.16.1.1, netmask 255.255.255.0, then it is aware that network 172.16.1.0/24 is reachable from eth0
 - Usually your SOHO router/gateway provides something called a “default route” or “default gateway” via DHCP
 - “For all packets destined for a network you have no idea how to reach, send them to this address”
 - Static routes are routes that have been manually added to the routing table
 - Since the routing table is stored in memory, static routes don't normally persist beyond reboots

Static Routes (cont'd)

- Problem: We want our host-only network adapter on the hypervisor host (172.16.1.1) to be able to reach 172.16.2.0/24
- Solution add a static route
 - Windows, (most) Linux, and OSX all have a route command
 - The syntax is entirely different for Windows, Linux AND OSX
 - Note: newer linux systems may have the command “ip route” in place of, or in addition to the traditional route command
 - Note 2: modifying the routing table (adding or deleting routes) requires:
 - Root access (OSX/Linux)
 - Administrator access AND an elevated command prompt (Windows)

Adding a static route - Linux

- Step 1: confirm that vboxnet0 has an IP address of 172.16.1.2/24
 - Use either ifconfig or ip to check/set the IP address as necessary (we covered this earlier)
- Step 2: determine if you have the “ip” or “route” command
 - Open a terminal window and run “which route ip”
 - Command will return a filepath if the command is available on the system. If both commands exist, use whichever you prefer.
- Step 3: sudo su – (become the root user)
- Step 4.a : run the route command
 - route add –net 172.16.2.0 netmask 255.255.255.0 gw 172.16.1.1 dev vboxnet0
 - Then run the route command to confirm your route has been added.
- Step 4.b: run ip route add
 - ip route add 172.16.2.0/24 via 172.16.1.1 dev vboxnet0
 - Then run ip route to confirm your new route

Adding a static route – Linux (cont'd)

```
root@kali:~# whoami
root
root@kali:~# which route ip
/sbin/route
/sbin/ip
root@kali:~# ifconfig vboxnet0 172.16.1.2 netmask 255.255.255.0
root@kali:~# ifconfig vboxnet0
vboxnet0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 172.16.1.2 netmask 255.255.255.0 broadcast 172.16.1.255
                ether 0a:00:27:00:00:00 txqueuelen 1000 (Ethernet)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
root@kali:~# route add -net 172.16.2.0 netmask 255.255.255.0 gw 172.16.1.1 dev vboxnet0
root@kali:~# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref  Use Iface
default          _gateway        0.0.0.0        UG    100    0        0 eth0
172.16.1.0      0.0.0.0        255.255.255.0   U     0    0        0 vboxnet0
172.16.2.0      172.16.1.1    255.255.255.0   UG    0    0        0 vboxnet0
```

```
root@kali:~# whoami
root
root@kali:~# ifconfig vboxnet0
vboxnet0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 172.16.1.2 netmask 255.255.255.0 broadcast 172.16.1.255
                ether 0a:00:27:00:00:00 txqueuelen 1000 (Ethernet)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ip route add 172.16.2.0/24 via 172.16.1.1 dev vboxnet0
root@kali:~# ip route
172.16.2.0/24 via 172.16.1.1 dev vboxnet0
```

Adding a static route - OSX

- Step 1: confirm that vboxnet0 has an IP address of 172.16.1.2/24
 - Use ifconfig to view/set the ip address as necessary (this was covered earlier)
- Step 2: verify access to the “route” command
 - Open a terminal window and run “which route”
 - Command will return a filepath if the command is available
- Step 3: sudo su – (become the root user)
- Step 4 : run the route command
 - route add 172.16.2.0/24 172.16.1.1
 - Or, you can use “sudo” to run that one command as root
 - E.g. sudo route add 172.16.2.0/24 172.16.1.1
 - Then run netstat –nr –f inet | grep vboxnet to confirm your route has been added.

Adding a static route – OSX (cont'd)

```
Tony's-MacBook-Pro:~ trobinson$ ifconfig vboxnet0
vboxnet0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
      ether 0a:00:27:00:00:00
      inet 172.16.1.2 netmask 0xffffffff broadcast 172.16.1.255
Tony's-MacBook-Pro:~ trobinson$ sudo route add 172.16.2.0/24 172.16.1.1
Password:
add net 172.16.2.0: gateway 172.16.1.1
Tony's-MacBook-Pro:~ trobinson$ netstat -nr -f inet | grep vboxnet
172.16.1/24      link#13          UC            3      0 vboxnet      !
172.16.1.1       link#13          UHLWii        1      0 vboxnet      !
172.16.1.255     ff:ff:ff:ff:ff  UHLWbI        0      5 vboxnet      !
172.16.2/24      172.16.1.1     UGSc           0      0 vboxnet      !
Tony's-MacBook-Pro:~ trobinson$
```

Flightcheck.sh – Linux and OSX editions

- For the Linux and OSX users:
 - I wrote scripts – flightcheck-Linux.sh/flightcheck-OSX.sh
 - Checks for the existence of vmnet[1,2] (vmware workstation/fusion), or vboxnet0 (Virtualbox)
 - Assigns the IP address 172.16.1.2 netmask 255.255.255.0
 - Uses route (OSX), or ip route add (Linux) to add a route to 172.16.2.0/24 via 172.16.1.1
- This script can be used to reconfigure vboxnet0 and rebuild static routes to 172.16.2.0/24 after system reboots or crashes
 - Why: remember when I mentioned vboxnet0 doesn't exist after your system reboots?
 - That means static routes that reference networks/IP addresses associated with vboxnet0 and networks it is connected to won't work
 - That is why we can use built-in route persistence and have to use this janky script

Flightcheck.sh – Linux and OSX editions (cont'd)

- Installation/Usage:
 - Visit gist.github.com/da667
 - Click on flightcheck-Linux.sh OR flightcheck-OSX.sh
 - Choose “Download ZIP” or click “Raw” and right click -> Save target as -> flightcheck-Linux.sh
 - Navigate to your Downloads folder (usually ~/Downloads)
 - Unzip the zip file (if you downloaded the zip file)
 - sudo bash flightcheck-Linux.sh OR sudo bash flightcheck-OSX.sh
 - The script pauses and asks you to make sure that virtualbox is running, and that the pfSense VM is started. Once you have done both, hit enter to run the script.
 - Confirm vboxnet0 has ip address 172.16.1.2/24
 - Confirm routing table has route to 172.16.2.0/24 via 172.16.1.1

Flightcheck.sh – Linux and OSX editions (cont'd)

The screenshot shows a GitHub gist page with two code snippets. The top snippet is for the Linux edition and the bottom for the OSX edition. Both snippets are Bash scripts that check for the existence of vmnet1 or vboxnet0 interfaces and set their IP to 172.16.1.2/24, then create a static route to 172.16.2.0 via 172.16.1.1.

```
1 #!/bin/bash
2 #This script is meant for VMware Workstation Professional, or Oracle Virtualbox users on mo
3 #Ensure that the Linux distro you will be running this on has both the ip and ifconfig comm
4 #This script checks for the existence of the interface vmnet1 (vmware workstation) or vboxn
5 #and will assign the IP address 172.16.1.2 to the first interface it finds. The script will
6 #if neither interface exists, the script will fail.
7 #after setting the IP address, the script attempts to add a static route to the 172.16.2.0
8
9 #Note: If you are using alternative networks for your lab other than 172.16.1.0/24, and 172
```

da667 / [flightcheck-Linux.sh](#)
Created Jun 15, 2018
equivalent of the flightcheck-OSX.sh script. Checks to see if vmnet1 (vmware workstation pro) or vboxnet0 (virtualbox) exists, sets its IP to 172.16.1.2/24, then creates a route to 172.16.2.0 via 172.16.1.1

1 file 0 forks 0 comments 0 stars

```
1 #!/bin/bash
2 #This script is meant for VMware Workstation Professional, or Oracle Virtualbox users on mo
3 #Ensure that the Linux distro you will be running this on has both the ip and ifconfig comm
4 #This script checks for the existence of the interface vmnet1 (vmware workstation) or vboxn
5 #and will assign the IP address 172.16.1.2 to the first interface it finds. The script will
6 #if neither interface exists, the script will fail.
7 #after setting the IP address, the script attempts to add a static route to the 172.16.2.0
8
9 #Note: If you are using alternative networks for your lab other than 172.16.1.0/24, and 172
```

da667 / [flightcheck-OSX.sh](#)
Last active Jun 15, 2018
This is an automation scripting for readers of Building Virtual Labs : A Hands-On Guide, or students of the upcoming Building Virtual Labs video training. This script will check to see if the interfaces vmnet2 or vboxnet0 exist. If either does, it configures the IP to 172.16.2.0 and the netmask to 255.255.255.0, then sets up a static route to 17...

Flightcheck.sh – Linux and OSX editions (cont'd)

da667 / **flightcheck-OSX.sh**

Last active Jun 15, 2018

Code Revisions 2

Embed <script src="https://gi: Download ZIP

This is an automation scripting for readers of Building Virtual Labs : A Hands-On Guide, or students of the upcoming Building Virtual Labs video training. This script will check to see if the interfaces vmnet2 or vboxnet0 exist. If either does, it configures the IP to 172.16.2.0 and the netmask to 255.255.255.0, then sets up a static route to 17...

flightcheck-OSX.sh Raw

```
1 #!/bin/bash
```

Save As: flightcheck-OSX.sh

Tags:

Where: Downloads

Format: Plain Text Document

Cancel Save

Flightcheck.sh – Linux and OSX editions (cont'd)

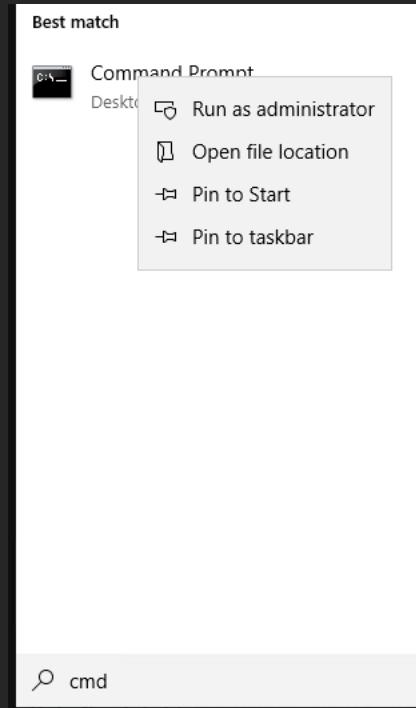
```
Tony's-MacBook-Pro:~ trobinson$ cd ~/Downloads/
Tony's-MacBook-Pro:Downloads trobinson$ ls *.sh
flightcheck-OSX.sh
Tony's-MacBook-Pro:Downloads trobinson$ sudo bash flightcheck-OSX.sh
Password:
Warning: Please make sure that all of your vmware fusion OR oracle virtualbox VMs are running. In particular, the pfSense VM MUST be running!
Once you have verified that your VMs are up and running, Press enter to continue
.
Checking for root privs..
We are root.
Checking to see if vmnet2 exists...
vmnet2 interface does not exist. Checking to see if vboxnet0 exists...
vboxnet0 interface exists. Setting IP to 172.16.1.2/24..
vboxnet0 interface IP set to 172.16.1.2
Adding static route to 172.16.2.0/24 via 172.16.1.1...
add net 172.16.2.0: gateway 172.16.1.1
added route to 172.16.2.0/24 via 172.16.1.1.

Tony's-MacBook-Pro:Downloads trobinson$ ifconfig vboxnet0; netstat -nr -f inet | grep vboxnet
vboxnet0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    ether 0a:00:27:00:00:00
        inet 172.16.1.2 netmask 0xffffffff broadcast 172.16.1.255
172.16.1.24      link#13          UC            3      0 vboxnet      !
172.16.1.1       link#13          UHLWII        1      0 vboxnet      !
172.16.1.255     ff:ff:ff:ff:ff:ff UHLWbI        0      2 vboxnet      !
172.16.2/24       172.16.1.1     UGSc           0      0 vboxnet      !
```

Adding a Static Route - Windows

- Start
 - Search for cmd
 - Right click -> run as administrator
 - route add -p 172.16.2.0 netmask 255.255.255.0 172.16.1.1
 - To view your routes: route print
 - That's it. Persists through reboots
 - Why: virtualbox host-only network adapter got registered with the windows network manager on creation.
 - Doesn't disappear on reboot like on OSX/Linux, doesn't lose its IP address
 - Route's “-p” option persists the route via the windows registry

Adding a Static Route – Windows (cont'd)



```
C:\WINDOWS\system32>route add -p 172.16.2.0 mask 255.255.255.0 172.16.1.1
OK!

C:\WINDOWS\system32>route print -4
=====
Interface List
  2...80 fa 5b 21 07 af .....Killer e2400 Gigabit Ethernet Controller
  21...0a 00 27 00 15 .....VirtualBox Host-Only Ethernet Adapter #2
  16...dc 53 60 cc a9 57 .....Intel(R) Dual Band Wireless-AC 7265
  13...dc 53 60 cc a9 58 .....Microsoft Wi-Fi Direct Virtual Adapter
  9...de 53 60 cc a9 57 .....Microsoft Wi-Fi Direct Virtual Adapter #2
  12...dc 53 60 cc a9 5b .....Bluetooth Device (Personal Area Network)
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0          0.0.0.0        10.0.0.1    10.0.0.11    25
          10.0.0.0    255.255.255.0        On-link       10.0.0.11    281
          10.0.0.11    255.255.255.255     On-link       10.0.0.11    281
          10.0.0.255   255.255.255.255     On-link       10.0.0.11    281
          127.0.0.0       255.0.0.0        On-link      127.0.0.1    331
          127.0.0.1       255.255.255.255     On-link      127.0.0.1    331
 127.255.255.255   255.255.255.255     On-link      127.0.0.1    331
          172.16.1.0       255.255.255.0        On-link     172.16.1.2    281
          172.16.1.2       255.255.255.255     On-link     172.16.1.2    281
 172.16.1.255   255.255.255.255     On-link     172.16.1.2    281
          172.16.2.0       255.255.255.0        On-link     172.16.1.2    26
          224.0.0.0        240.0.0.0        On-link      127.0.0.1    331
          224.0.0.0        240.0.0.0        On-link     172.16.1.2    281
          224.0.0.0        240.0.0.0        On-link      10.0.0.11    281
 255.255.255.255   255.255.255.255     On-link      127.0.0.1    331
 255.255.255.255   255.255.255.255     On-link     172.16.1.2    281
 255.255.255.255   255.255.255.255     On-link      10.0.0.11    281
=====
Persistent Routes:
Network Address      Netmask  Gateway Address Metric
  172.16.2.0    255.255.255.0      172.16.1.1     1
=====
```

Remote Access - Windows

- Have you downloaded/installed mremoteng, winscp and puttygen yet?
 - You'd best do so now.
 - Note: when asked, be sure to select the “commander” interface for winSCP.

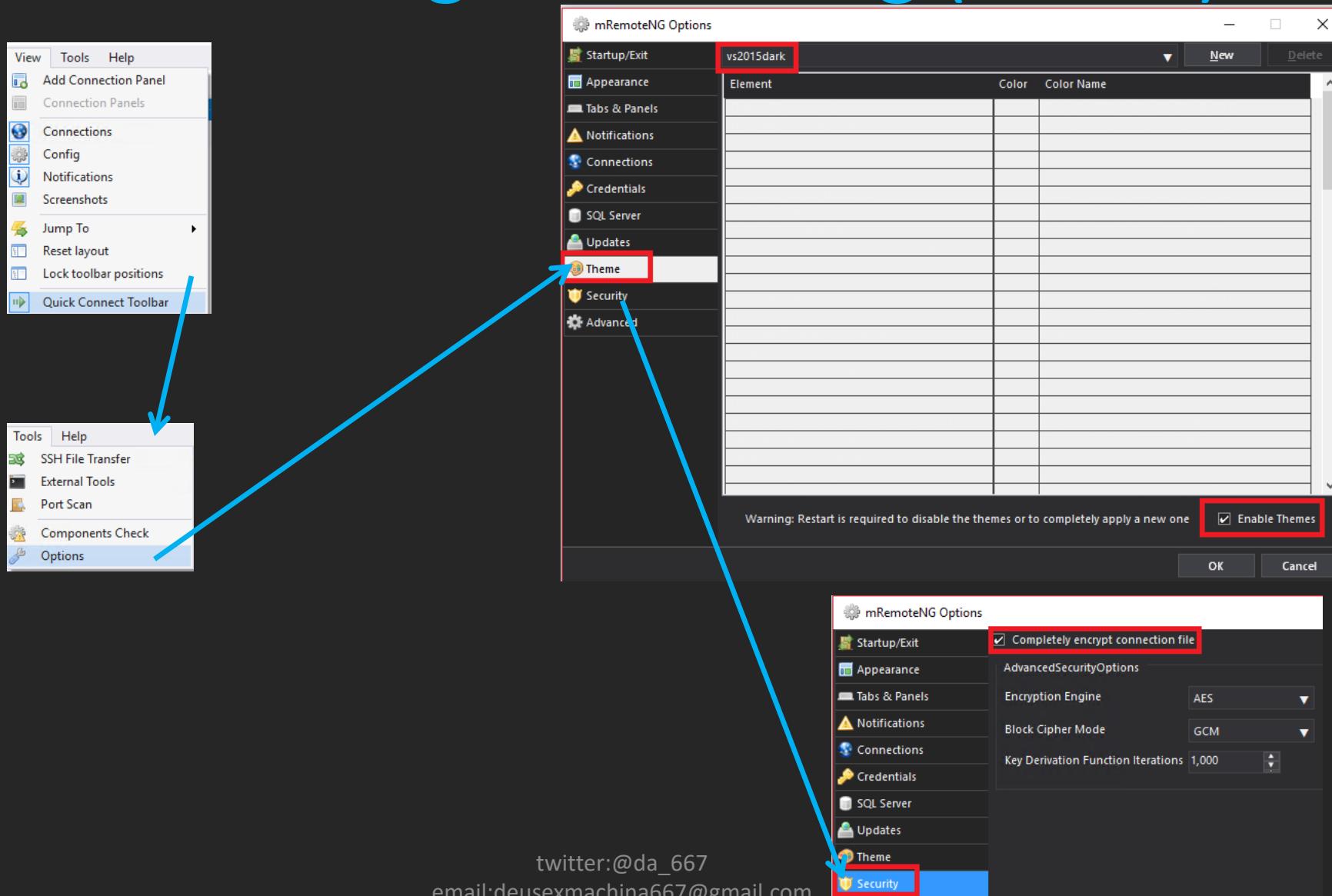
Goals

- Create mremoteng AND WinSCP connection profiles for SIEM, IPS, and kali
- Verify connectivity to the SIEM and IPS vms via SSH and SCP
- Discuss key-based authentication
- Generate SSH public/private key pair
- Format and transfer SSH public key and place it in to the user's `~/.ssh/authorized_keys` file with correct directory/file permissions
 - Display different methods of uploading/transferring the key
 - Show how to configure key-based auth in mremoteng AND WinSCP

Customizing mremoteng

- Fire up mremoteng.
 - Before we get started:
 - Remove the quick connect toolbar
 - View → Quick Connect Toolbar
 - Enable the dark theme so your eyes don't melt
 - Tools → Options → Theme → Enable Themes checkbox → Select a theme (e.g. vs2015dark)
 - Encrypt your connection files!
 - Tools → Options → Security → Completely encrypt connection file checkbox
 - Note: The Connections/Config panes panes are resizable (vertically and horizontally)
 - Resize the windows by hovering around the edges, and dragging/dropping.

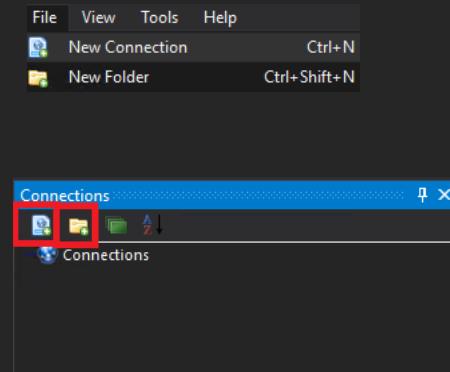
Customizing mremoteng (cont'd)



Creating mremoteng connection profiles

- Get familiar with creating new connection profiles and/or folders
 - Connection profiles: entries that have info on how to connect to a host (credentials, protocol to use, port, etc.)
 - Folders: can be used to organize connection profiles into categories. Folders can also contain other folders.
- Connection profiles can be created one of two ways:
 - Option 1: File menu option → New Connection/New Folder
 - Option 2: New connection or New Folder icons in the connections window pane

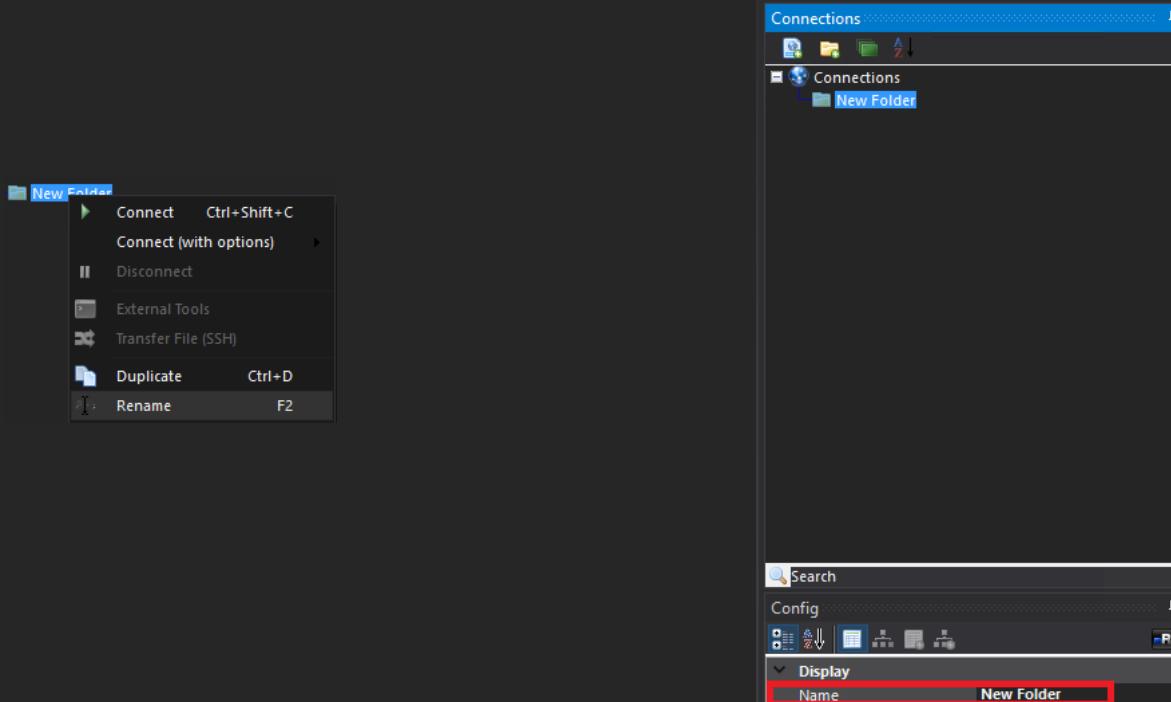
Creating mremoteng connection profiles (cont'd)



Creating mremoteng connection profiles (cont'd)

- First, lets create a folder
 - Create a folder, labeled “Virtual Machine Lab - Virtualbox”
 - Click the folder icon. A new folder is placed under “Connections”. The text is highlighted so you can rename it. Folder name is highlighted and ready for editing
 - What do I do if I mess up the name?
 - Option 1: Right click New Folder → Rename
 - Option 2: Left click New Folder to highlight, navigate to Config pane, double click on the text “New Folder” next to the name field

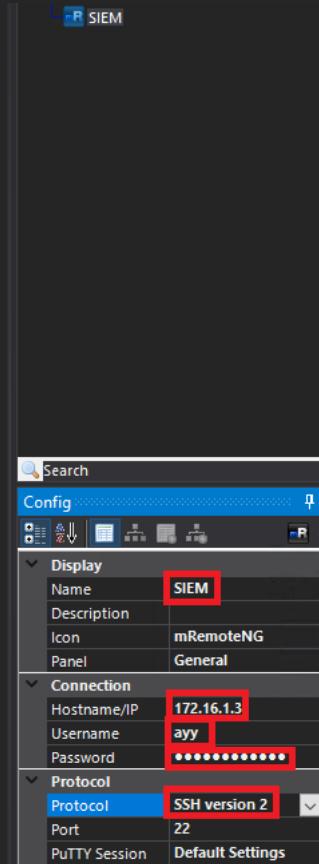
Creating mremoteng connection profiles



Creating mremoteng connection profiles (cont'd)

- Next, lets create our first connection profile.
 - Click the profile icon, or create a new one from the File menu.
 - Name: SIEM
 - Highlight the connection profile you made and in the config section, enter the following:
 - Protocol: SSH version 2
 - Hostname/IP: 172.16.1.3
 - Username: [username you created on OS install]
 - Password [password for the user you created]
 - Note: This connection profile WILL contain valid credentials for the SIEM VM. Make sure you checked the option to enable encryption for the connection file

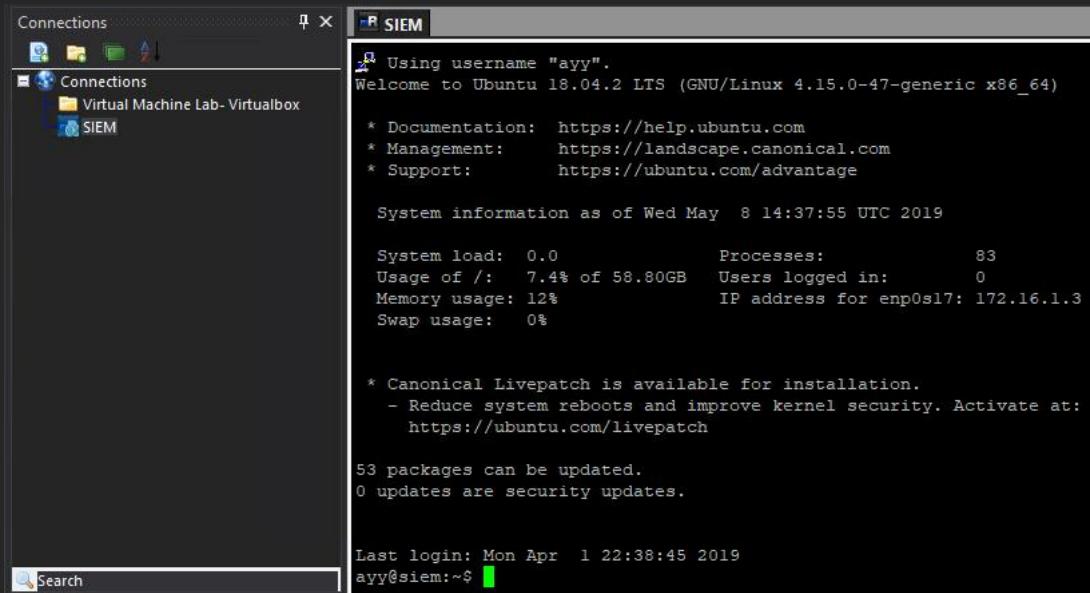
Creating mremoteng connection profiles (cont'd)



Creating mremoteng connection profiles (cont'd)

- Double click on SIEM on the Connections pane.
 - If everything is correct, you should have an SSH session on the SIEM VM.
 - Note: if you get a message “PuTTYNG Security Alert” – “WARNING – POTENTIAL SECURITY B REACH”, don’t panic.
 - SSH key fingerprints are a thing used to confirm the identity of an SSH host.
 - Select “Yes” to continue.

Creating mremoteng connection profiles (cont'd)



Creating mremoteng connection profiles (cont'd)

- Success! What now?
 - Right click on the SIEM tab and select disconnect (or type exit on the terminal) to disconnect your session.
 - Create two more connection profiles.
 - IPS
 - Protocol: SSH version 2
 - Hostname/IP: 172.16.1.4
 - Username: [username you created on OS install]
 - Password: [password you created for your user]
 - Kali
 - Protocol: SSH version 2
 - Hostname/IP: 172.16.2.2
 - Username: root
 - Password: [password you created for the root user on install]
 - Confirm SSH connectivity to the IPS VM, but don't bother with kali just yet. We'll be fixing this in a moment..
 - Drag and drop the SIEM, IPS and kali connection profiles into the “Virtual Machine Lab – Virtualbox” folder
 - Save your Connection File via File → Save Connection File

Creating mremoteng connection profiles (cont'd)

The image consists of three side-by-side screenshots. The left screenshot shows the 'Config' window for a connection named 'IPS'. It includes sections for Display (Name: IPS, Description: , Icon: mRemoteNG, Panel: General), Connection (Hostname/IP: 172.16.1.4, Username: ayy, Password: masked), and Protocol (Protocol: SSH version 2, Port: 22, PutTY Session: Default Settings). The middle screenshot shows a similar 'Config' window for a connection named 'kali', with identical settings. The right screenshot shows a terminal session titled 'IPS' with the command 'ssh root@172.16.2.2'. The session displays system information for Ubuntu 18.04.2 LTS, including system load, memory usage, swap usage, and package updates. It ends with a prompt 'ayy@ips:~\$'.

Config

Name	IPS
Description	
Icon	mRemoteNG
Panel	General

Connection

Hostname/IP	172.16.1.4
Username	ayy
Password	*****

Protocol

Protocol	SSH version 2
Port	22
PutTY Session	Default Settings

Config

Name	kali
Description	
Icon	mRemoteNG
Panel	General

Connection

Hostname/IP	172.16.2.2
Username	root
Password	*****

Protocol

Protocol	SSH version 2
Port	22
PutTY Session	Default Settings

IPS

```
* Using username "ayy".
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-47-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Wed May  8 15:45:17 UTC 2019

System load:  0.0          Processes:           84
Usage of /:  10.3% of 39.12GB   Users logged in:    0
Memory usage: 11%          IP address for enp0s17: 172.16.1.4
Swap usage:  0%

* Ubuntu's Kubernetes 1.14 distributions can bypass Docker and use containerd
directly, see https://bit.ly/ubuntu-containerd or try it now with

  snap install microk8s --classic

* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch

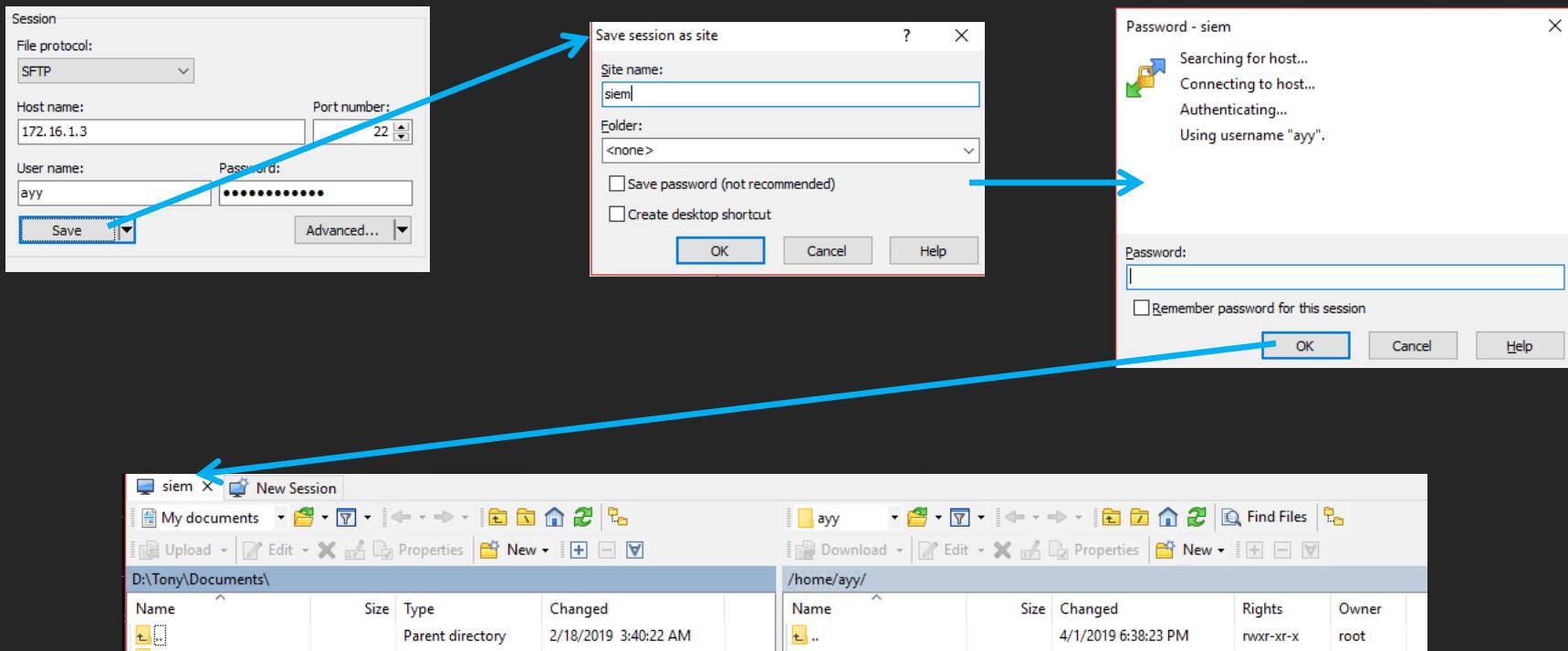
41 packages can be updated.
0 updates are security updates.

Last login: Fri Apr 26 19:28:30 2019
ayy@ips:~$
```

Creating winSCP connection profiles

- Open up winSCP
 - If you didn't select the commander UI or never got the option, navigate to Tools → Preferences → Interface → Commander radio button
 - Highlight “New Site”
 - File Protocol: SFTP (default)
 - Hostname: 172.16.1.3
 - Username: [username for SIEM user created at install]
 - Click Save, enter “siem” as the site name, and click OK
 - Double click the siem connection profile, enter the password for your user, and verify you can connect successfully.
 - Note: you may get a “potential security breach” warning (similar to mremoteng. Select “Update” to continue.

Creating winSCP connection profiles



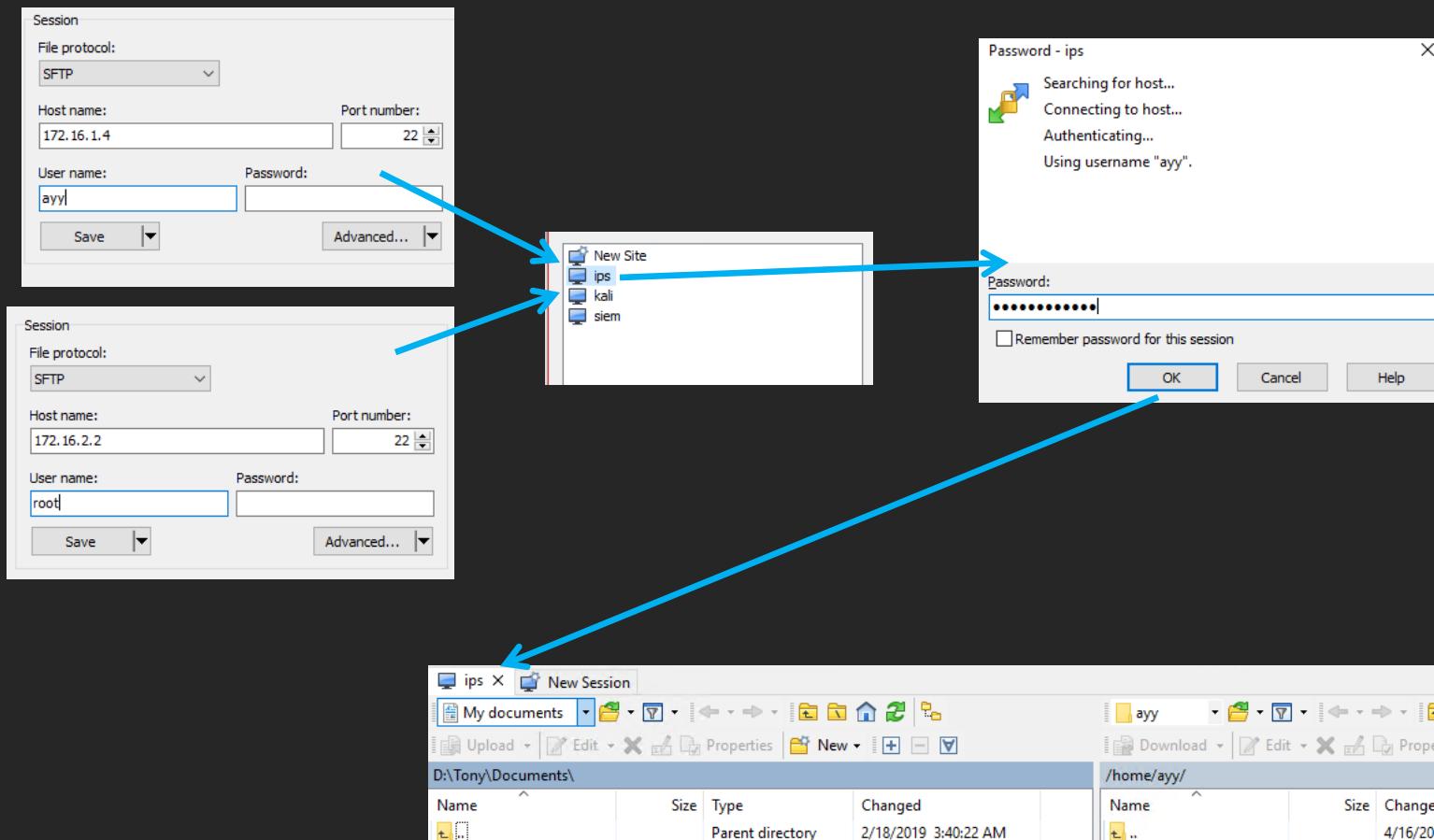
Creating winSCP connection profiles

- Success! What do?
 - Create two more connection profiles
 - IPS
 - File Protocol: SFTP
 - Hostname: 172.16.1.4
 - Username: [username assigned on install]
 - Save site name: ips
 - Kali
 - File Protocol: SFTP
 - Hostname: 172.16.2.2
 - Username: root
 - Save site name: kali
 - Confirm successful connectivity to IPS vm
 - Again, don't bother with the kali VM just yet.

Creating winSCP connection profiles

- Success! What do?
 - Create two more connection profiles
 - IPS
 - File Protocol: SFTP
 - Hostname: 172.16.1.4
 - Username: [username assigned on install]
 - Save site name: ips
 - Kali
 - File Protocol: SFTP
 - Hostname: 172.16.2.2
 - Username: root
 - Save site name: kali
 - Confirm successful connectivity to IPS vm
 - Again, don't bother with the kali VM just yet.

Creating winSCP connection profiles



Generating an SSH key with puttygen (cont'd)

- Double click puttygen.exe to run puttygen
- Select “ED25519” radio button under Parameters
- Click “Generate” under Actions
 - You’ll be asked to move your mouse around to generate “randomness” (entropy) for the key.
- Window changes a bit as new fields and information appear.

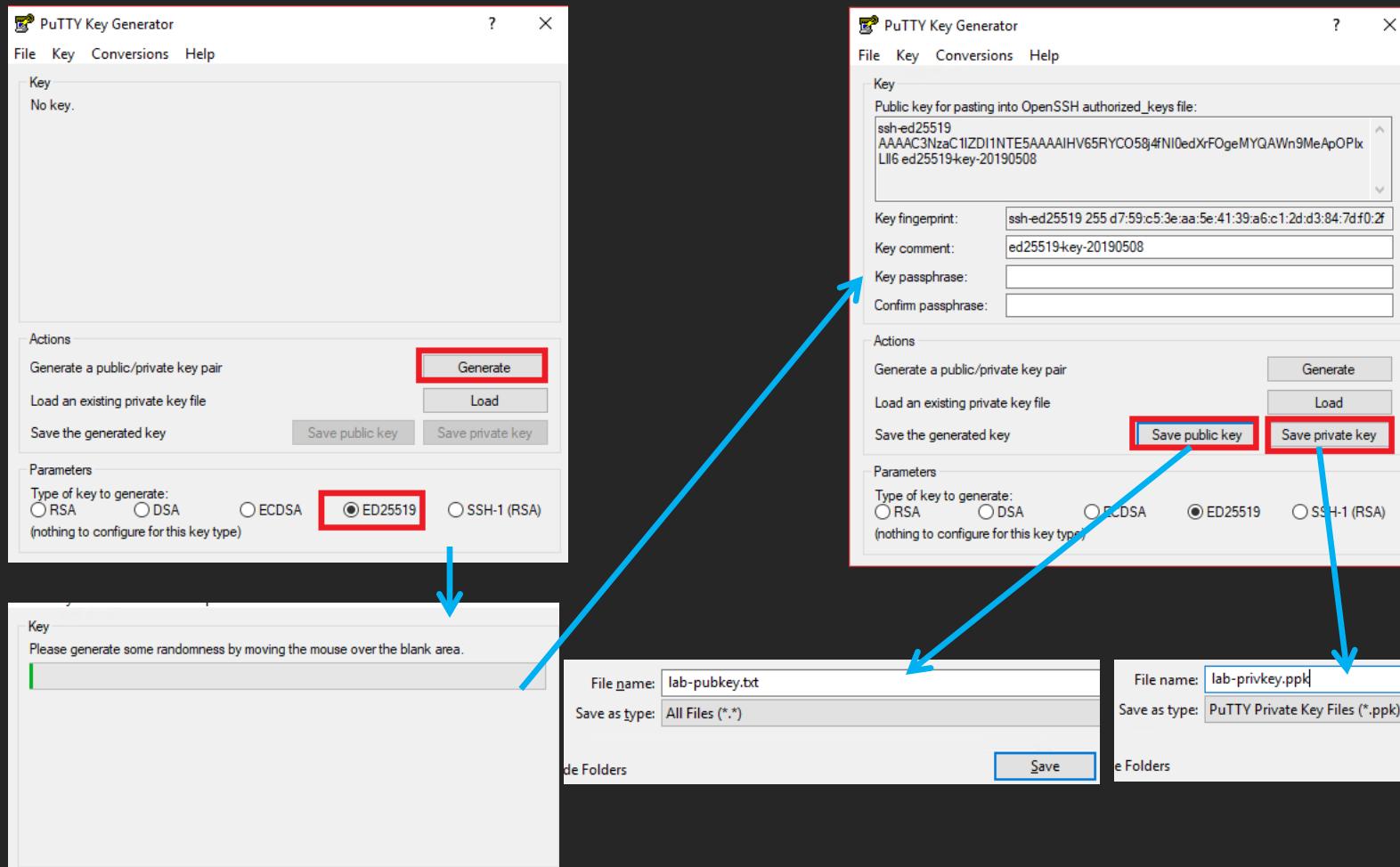
Generating an SSH key with puttygen (cont'd)

- Key passphrase/Confirm passphrase
 - Very important fields. Sets password to encrypt your private key file.
 - If encrypted, means you need both the private key file AND the password for the key to use key-based auth.
 - Two-factor Authentication: something you have (private key) + something you know (password to decrypt key)
 - If you leave the fields blank: no password required to use your SSH key.
 - Fast Access, but anyone who acquires your private key and knows the correct username can log in as you.
 - Recommendation:
 - Personal lab? Can probably get away with no password protection.
 - Shared lab environment? Lab hosted on a shared/enterprise network? Encrypt your SSH key.

Generating an SSH key with puttygen (cont'd)

- Click “Save public key”
 - Save As prompt comes up. Name the file lab-pubkey.txt
- Click “Save private key”
 - Save As prompt comes up again. Name the file lab-privkey.ppk
 - Note: if you save the key without a password, puttygen will warn you. Click Yes to continue.
 - Recommend saving in the same directory as the public key

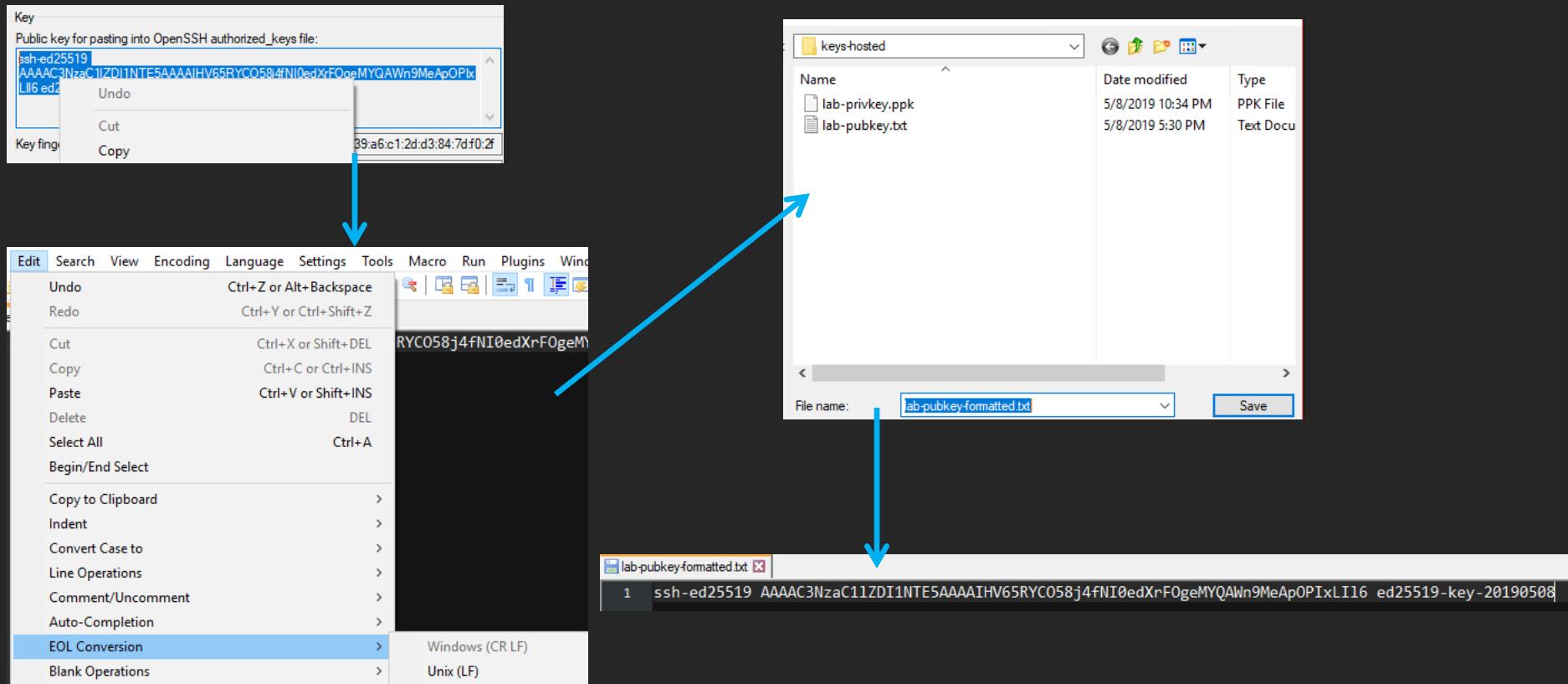
Generating an SSH key with puttygen



Generating an SSH key with puttygen (cont'd)

- Need to format our public key
- If you haven't installed notepad++, do so now.
 - If you try to use the public key puttygen creates, most OpenSSH servers will laugh at you. Or vomit. Maybe both.
 - Public key contents need to be squeezed on to a single line
 - [Key Type] [Key itself] [comment/note (optional)]
 - ssh-ed25519 AAAAC3NzaC1iZDI1NTE5AAAAIHV65RYC058j4fNI0edXrFOgeMYQAWn9MeApOPIxLII6 ed25519-key-20190508
 - Two options:
 - take the existing SSH public we saved, and reformat it to look something like the line above, configure EOL Conversion for Unix (LF) and save as "lab-pubkey-formatted.txt"
 - Copy the content from "Public key for pasting into OpenSSH authorized_keys file:" into notepad++, configure EOL Conversion for Unix (LF) and save as "lab-pubkey-formatted.txt"

Generating an SSH key with puttygen (cont'd)



Transferring the public key to our VMs

- We need to get the formatted public key to the IPS and SIEM vms.
 - Because this is Windows (and Windows is pain) we have to get creative.
 - Method 1: SCP the formatted key file to the system, SSH on to the system, and configure the system to use the public key
 - Method 2: Copy/Paste the contents of the formatted key file into the terminal, the configure the system to write the key to a file for use
 - Method 3: Similar to method 2, but involves using “vi”
 - Needs to be renamed to “authorized_keys”
 - Needs to be placed in the user’s home directory in a subdirectory called “.ssh” (aka ~/.ssh)
 - The authorized_keys file and .ssh directory need to be owned by the user/group you want to login as and need to have specific file permissions

Method 1:

- Open up winSCP to either SIEM or IPS
- Copy lab-pubkey-formatted.txt to the VM (drag and drop from the directory on your computer, to the /home/[username] directory)
- Run the following commands in order:
 - mkdir ~/.ssh
 - mv ~/lab-pubkey-formatted.txt ~/.ssh/authorized_keys
 - chown –R username:group ~/.ssh
 - Note: the username and group for your first user are usually the same (e.g. Username:ayy group:ayy, so chown –R ayy:ayy ~/ssh)
 - chmod 700 ~/.ssh
 - chmod 600 ~/.ssh/authorized_keys
 - Note: Can chain these commands together using “&&” to run them one after the other

Method 1:

Name	Size	Type	Changed
..		Parent directory	5/8/2019 10:48:49 PM
lab-privkey.ppk	1 KB	PPK File	5/8/2019 10:34:30 PM
lab-pubkey.txt	1 KB	Text Document	5/8/2019 5:30:06 PM
lab-pubkey-formatted.txt	1 KB	Text Document	5/8/2019 10:48:49 PM

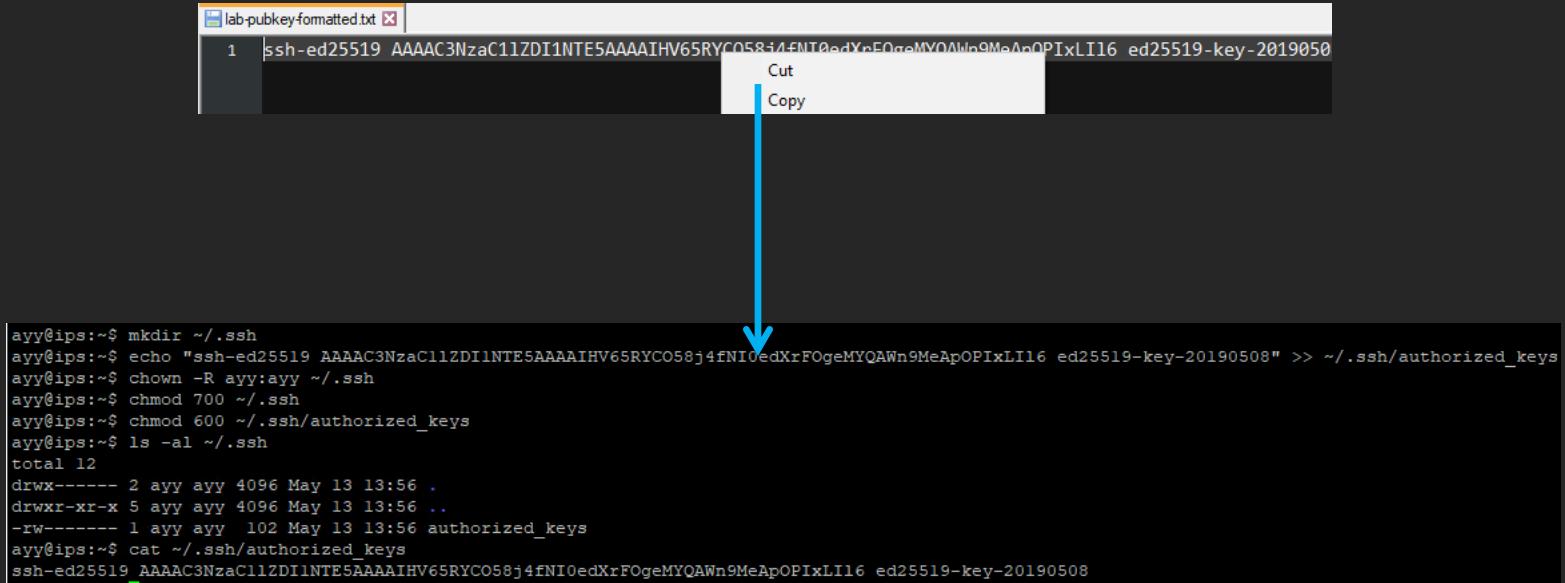
Name	Size	Changed	Rights	Owner
..		4/16/2019 2:43:11 PM	rxr-xr-x	root
lab-pubkey-formatted.txt	1 KB	5/8/2019 10:48:49 PM	rw-rw-r--	ayy

```
ayy@ips:~$ pwd
/home/ayy
ayy@ips:~$ ls -al *.txt
-rw-rw-r-- 1 ayy ayy 101 May  9 02:48 lab-pubkey-formatted.txt
ayy@ips:~$ mkdir ~/.ssh
ayy@ips:~$ mv ~/lab-pubkey-formatted.txt ~/.ssh/authorized_keys
ayy@ips:~$ chown -R ayy:ayy ~/.ssh
ayy@ips:~$ chmod 700 ~/.ssh
ayy@ips:~$ chmod 600 ~/.ssh/authorized_keys
ayy@ips:~$ ls -al ~/.ssh
total 12
drwx----- 2 ayy ayy 4096 May 13 13:43 .
drwxr-xr-x 5 ayy ayy 4096 May 13 13:43 ..
-rw----- 1 ayy ayy 101 May  9 02:48 authorized_keys
ayy@ips:~$ cat ~/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAIHV65RYC058j4fNI0edXrFOgeMYQAWn9MeApOPIxLI16 ed25519-key-20190508
```

Method 2:

- Open up lab-pubkey-formatted.txt in notepad++
- Ctrl+A (highlight everything), Ctrl-C (Copy to clipboard)
- SSH to SIEM or IPS VM, run the following commands:
 - mkdir ~/.ssh
 - echo “[right-click to paste clipboard contents here]” >> ~/.ssh/authorized_keys
 - Note: right click to paste doesn’t seem to work on Kali (like most things) hit the “Insert” key on your keyboard if right click to paste isn’t working properly
 - chown –R username:group ~/.ssh
 - Note: the username and group for your first user are usually the same (e.g. Username:ayy group:ayy, so chown –R ayy:ayy ~/.ssh)
 - chmod 700 ~/.ssh
 - chmod 600 ~/.ssh/authorized_keys
- This method can be used to add more than 1 key to the authorized_keys file
 - “>>” shell redirect.
 - “If this file doesn’t exist create it, and write the contents from the previous command to the file I specify. If the file DOES exist, APPEND the contents to the end of the file.”

Method 2:



```
lab-pubkey-formatted.txt
1 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHV65RYC058j4fNI0edXrFOgeMYQAWn9MeApOPIxLI16 ed25519-key-20190508

ayy@ips:~$ mkdir ~/.ssh
ayy@ips:~$ echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHV65RYC058j4fNI0edXrFOgeMYQAWn9MeApOPIxLI16 ed25519-key-20190508" >> ~/.ssh/authorized_keys
ayy@ips:~$ chown -R ayy:ayy ~/.ssh
ayy@ips:~$ chmod 700 ~/.ssh
ayy@ips:~$ chmod 600 ~/.ssh/authorized_keys
ayy@ips:~$ ls -al ~/.ssh
total 12
drwx----- 2 ayy ayy 4096 May 13 13:56 .
drwxr-xr-x 5 ayy ayy 4096 May 13 13:56 ..
-rw----- 1 ayy ayy 102 May 13 13:56 authorized_keys
ayy@ips:~$ cat ~/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHV65RYC058j4fNI0edXrFOgeMYQAWn9MeApOPIxLI16 ed25519-key-20190508
```

Method 3:

- Open up lab-pubkey-formatted.txt in notepad++
- Ctrl+A (highlight everything), Ctrl-C (Copy to clipboard)
- SSH to SIEM or IPS VM, run the following commands:
 - mkdir ~/.ssh
 - vi ~/.ssh/authorized_keys
 - Hit ‘i’ for insert mode
 - [right-click to paste contents into text editor]
 - Hit ESC
 - Type “:wq!”>> ~/.ssh/authorized_keys
 - chown –R username:group ~/.ssh
 - Note: the username and group for your first user are usually the same (e.g. Username:ayy group:ayy, so chown –R ayy:ayy ~/.ssh)
 - chmod 700 ~/.ssh
 - chmod 600 ~/.ssh/authorized_keys
- This method can also be used to add more than 1 key to the authorized_keys file
 - Open file in vi
 - Shift+G = sends you to last line of the file
 - Shift +A = sends you to end of the line, and puts you into insert mode
 - Hit enter, paste in new key
 - Esc, “:wq!”

Method 3:

The diagram illustrates a workflow for copying a public key from a file to an SSH configuration directory. It consists of several windows and terminal sessions:

- File Explorer Window:** Shows a file named "lab-pubkey-formatted.txt" containing a single line of text:

```
1 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIHV65RYC058j4fNI0edXrFOgeMYQAWn9MeApOPIxLI16 ed25519-key-2019050
```

A context menu is open over the file, with "Copy" selected.
- Terminal Session 1:** Shows the user navigating to their home directory and opening a new file for editing:

```
ayy@ips:~$ mkdir ~/.ssh  
ayy@ips:~$ vi ~/.ssh/authorized_keys
```
- Terminal Session 2:** Shows the user pasting the copied public key into the file:

```
-- INSERT --
```

A blue arrow points from the "Copy" menu in the first window to the "INSERT" indicator in the second window.
- Terminal Session 3:** Shows the user saving the changes and exiting the editor:

```
:wq!
```

A blue arrow points from the "wq!" command in the second window to the "wq!" command in the third window.
- Terminal Session 4:** Shows the user confirming the file was created and listing its contents:

```
ayy@ips:~$ ls -al ~/.ssh  
total 12  
drwx----- 2 ayy ayy 4096 May 13 14:17 .  
drwxr-xr-x 5 ayy ayy 4096 May 13 14:17 ..  
-rw----- 1 ayy ayy 102 May 13 14:17 authorized_keys
```
- File Explorer Window:** Shows the final state of the "lab-pubkey-formatted.txt" file, which now contains the copied public key text.

Testing your key-based auth

- At this point SIEM and IPS should have your public key
 - Located in `/home/[username]/.ssh/authorized keys`
 - The file ownership and permissions should be all set to go
- So, how do we actually do key-based auth?
 - We have to create a puttyNG SSH profile in mRemoteNG.

Creating a puttyNG connection profile

- In mRemoteNG navigate to: Tools → Options → Advanced
 - Click the “Launch PuTTY” button.
- In the PuTTYNG Configuration window:
 - Click the “+” Next to SSH in the Category pane
 - Click on the text labeled “Auth”. “Options controlling SSH authentication” appears.
 - Click the Browse button under “Authentication Parameters”
 - Labeled “Private key file for authentication”
 - » Browse to the directory where you saved your private SSH key (the ppk file) and select it.
 - Scroll up on the “Category” pane, and click on “Session”.
 - Click on the input box labeled “Saved Sessions” under “Load, save or delete a stored session”
 - Type in something like “vbox_lab_keyauth”, then click the Save button.
 - Your putty session settings should be in the list along with “Default Settings”
 - Click the Close button, then click OK to close mRemoteNG options.

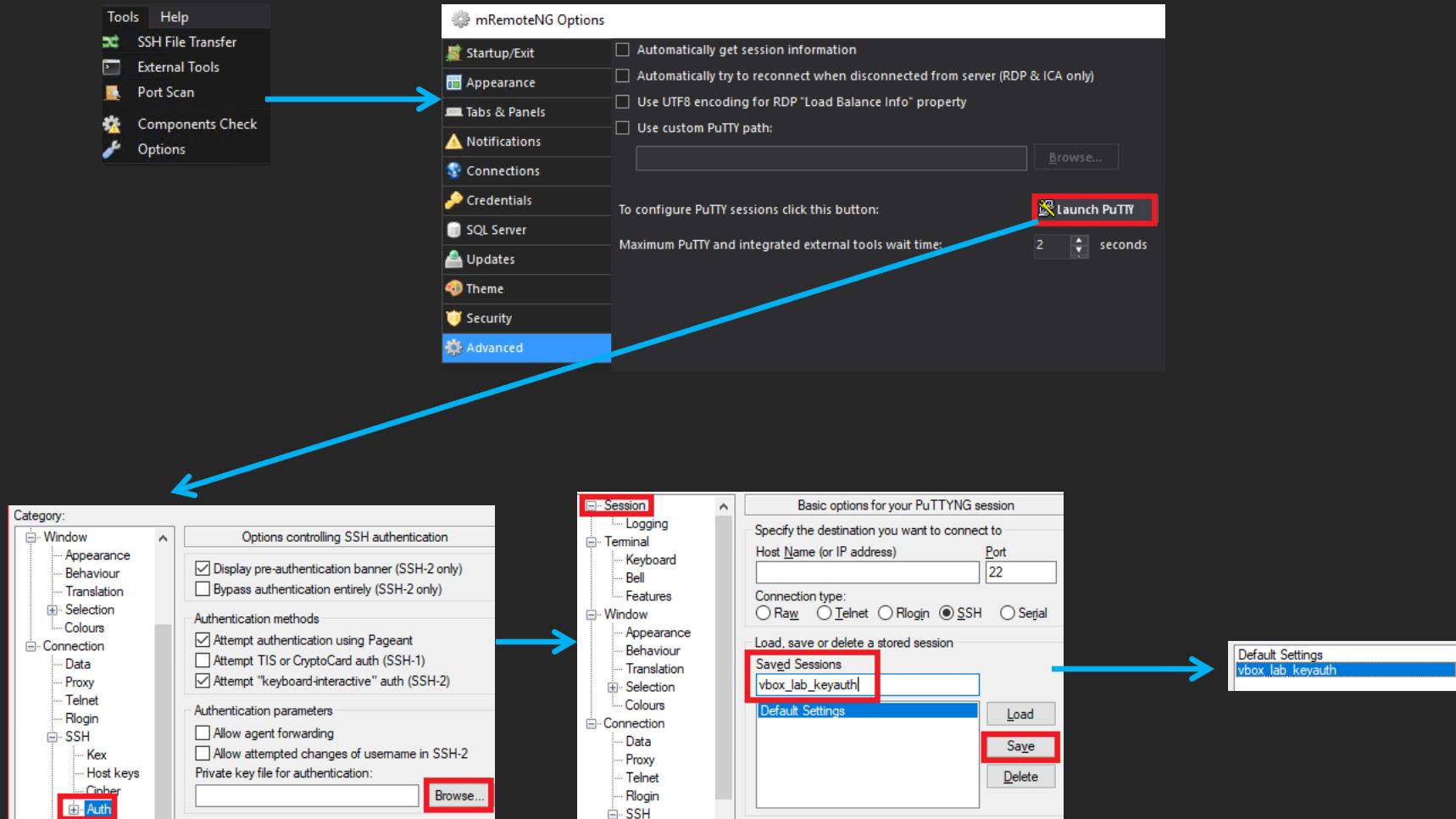
Creating a puttyNG connection profile (cont'd)

- Under the mRemoteNG Connections pane, select one of your SSH connection profiles.
 - In the Config pane, navigate to the “Protocol” section → PuTTY Session. Click on the text “Default Settings” and a dropdown icon appears next to it.
 - Click on `vbox_lab_keyauth`
- Repeat this process for your other SSH connection profiles.
 - All three connecton profiles should be using your “`vbox_lab_keyauth`” connection profile.
 - No, this won’t fix Kali. (nothing can)
 - We’ll get to that. I promise.

Creating a puttyNG connection profile (cont'd)

- Under the mRemoteNG Connections pane, select one of your SSH connection profiles.
 - In the Config pane, navigate to the “Protocol” section → PuTTY Session. Click on the text “Default Settings” and a dropdown icon appears next to it.
 - Click on vbox_lab_keyauth
 - Under the Connection pane, delete the contents of the “Password” field (except for the kali connection profile)
- Repeat this process for your other SSH connection profiles.
 - All three connecton profiles should be using your “vbox_lab_keyauth” connection profile.
 - No, this won’t fix Kali. (nothing can)
 - We’ll get to that. I promise.
- File → Save Connection File (save your changes)
- Test time
 - Double click on the SIEM and IPS connection profiles
 - If you made your SSH key without a password, you should have a connection.
 - If you made your SSH key with a password, you’ll be prompted for that password now.
 - If its not working, you’ve got troubleshooting to do! Go back through the previous slides and make sure you followed the steps in order.

Creating a puttyNG connection profile (cont'd)



Creating a puttyNG connection profile (cont'd)

The image shows the mRemoteNG application interface. At the top left is a tree view of connections under 'Virtual Machine Lab- Virtualbox'. Below it are three connection profiles: 'SIEM' (selected), 'IPS', and 'kali'. To the right are three detailed configuration tables for each profile. Arrows point from the 'PuTTY Session' field in the 'Protocol' section of the 'SIEM' and 'IPS' tables to the 'External Tool' field in the 'Miscellaneous' section of their respective connection configuration panes. The 'kali' profile is shown separately.

Name	SIEM
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	172.16.1.3
Username	ayy
Password	*****
Protocol	
Protocol	SSH version 2
Port	22
PuTTY Session	vbox_lab_keyauth

Name	IPS
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	172.16.1.4
Username	ayy
Password	*****
Protocol	
Protocol	SSH version 2
Port	22
PuTTY Session	vbox_lab_keyauth

Name	kali
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	172.16.2.2
Username	root
Password	*****
Protocol	
Protocol	SSH version 2
Port	22
PuTTY Session	vbox_lab_keyauth

Config	
Display	
Name	SIEM
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	172.16.1.3
Username	ayy
Password	*****
Protocol	
Protocol	SSH version 2
Port	22
PuTTY Session	Default Settings
Miscellaneous	
External Tool	vbox_lab_keyauth

Config	
Display	
Name	IPS
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	172.16.1.4
Username	ayy
Password	*****
Protocol	
Protocol	SSH version 2
Port	22
PuTTY Session	Default Settings
Miscellaneous	
External Tool	vbox_lab_keyauth

SIEM Session Log:

```
Using username "ayy".
Authenticating with public key "ed25519-key-20190508"
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-47-generic x86_64)
```

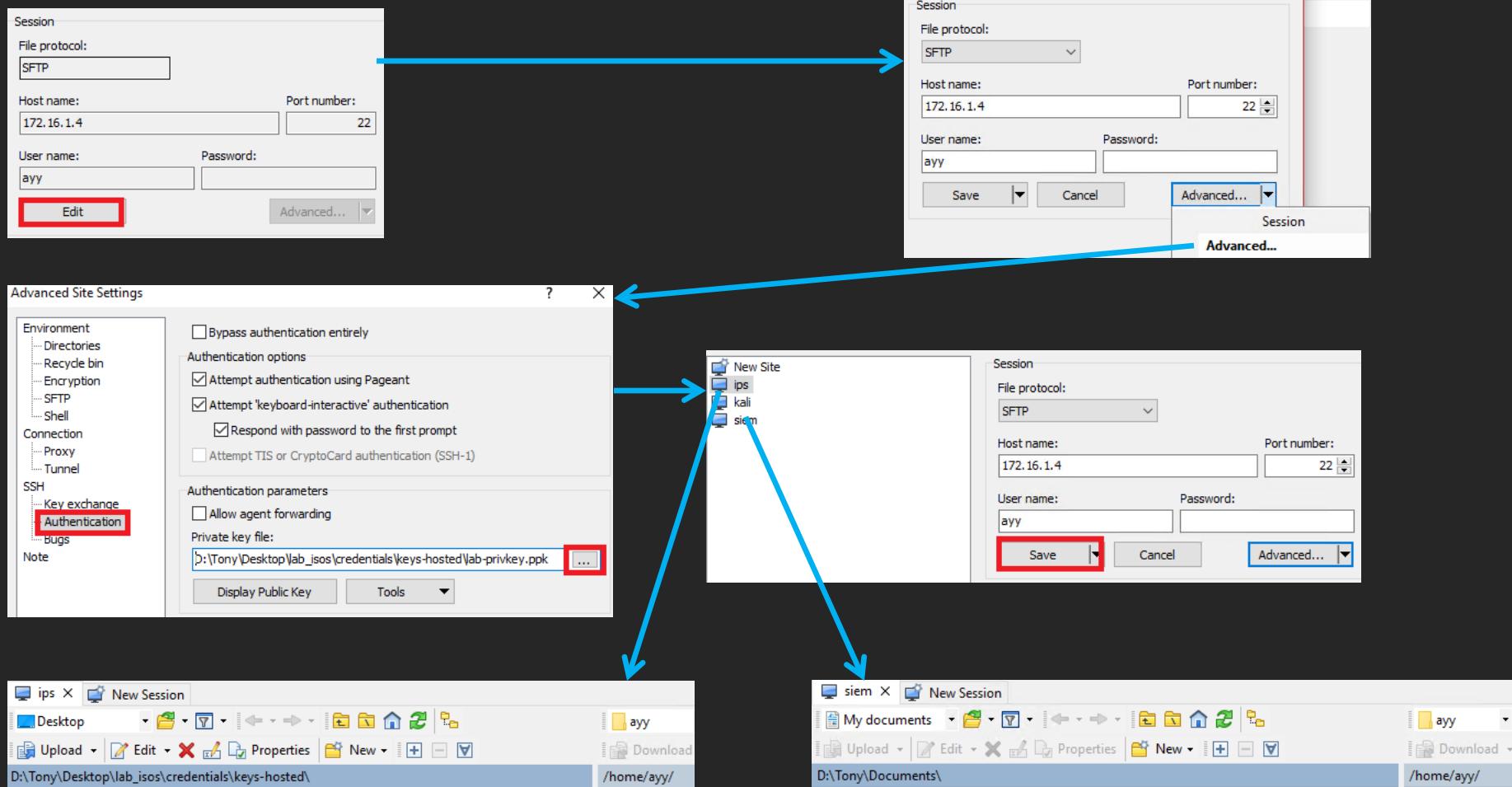
IPS Session Log:

```
Using username "ayy".
Authenticating with public key "ed25519-key-20190508"
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-47-generic x86_64)
```

Configuring key-based auth for winSCP

- Select an existing profile
- Click the Edit button
- Click the “Advanced...” button
 - Select “Advanced...” in the drop-down menu (if necessary)
- “Advanced Site Settings” window pops up.
 - Click on “Authentication” under SSH
 - “Private key file:” Under “Authentication parameters”, click “...” to browse to your private key PPK file, and select it.
 - Click OK to exit this sub-menu
 - Click Save to save these details to the current connection profile
- Repeat these steps until all 3 winSCP profiles are configured to use your private key for SSH auth.
- Test connectivity with the IPS and SIEM SCP profiles. Same as with mremoteng, if you were logged into the VM automatically, you’re good to go.

Configuring key-based auth for winSCP (cont'd)



Remote Access – Linux/OSX

- Verify that you have a terminal application installed
 - Linux: iTerm, iTerm2
 - OSX: Konsole, Gnome Terminal, Terminator, etc.
- Confirm that you have access to the following commands:
 - ssh, scp, ssh-keygen, ssh-copy-id, alias, vi/vim
 - Reminder: The which command can help you confirm these commands are available for use
 - Optional: a graphical text editor
 - Linux: kwrite, leafpad, etc.
 - OSX: BBEdit, etc.

Goals

- Create persistent ssh aliases for SIEM, IPS, and kali
- Verify connectivity to the SIEM and IPS vms via SSH and SCP
- Discuss key-based authentication
- Generate SSH public/private key pair
- Format and transfer SSH public key and place it in to the user's `~/.ssh/authorized_keys` file with correct directory/file permissions
 - Primarily using `ssh-copy-id`, but also demonstrate that the windows techniques work here, too.
- Test to confirm key-based auth works for both SSH and SCP.

The alias command

- Alias command allows you to say “when I type this, execute this”
 - Example: `alias siem='ssh ayy@172.16.1.3'`
 - Everytime you type `siem` into the terminal, the `ssh` command runs
 - Connects as the user “ayy”
 - To the ip address “172.16.1.3” (the SIEM vm)

The alias command (cont'd)

- Problem: aliases are not persistent
- Solution: `~/.bashrc`, `~/.bash_profile`, or `~/.profile`
 - Special configuration files that set up the BASH shell (command line environment) settings for the user you are running as.
 - We'll place our aliases here, and every time you use the terminal application, the aliases for our lab VMs will be loaded automatically
 - Note: Most linux distros read user BASH settings from `~/.bashrc`
 - In fact, this is the only bash config file that Kali linux seems to want to actually read.
 - Note: OSX users will have to create the file `~/.bash_profile`
 - `touch ~/.bash_profile; chmod 744 ~/.bash_profile`

The alias command (cont'd)

- Perform the following tasks:
 - OSX:
 - echo "alias siem='ssh [username]@172.16.1.3'" >> ~/.bash_profile
 - echo "alias ips='ssh [username]@172.16.1.4'" >> ~/.bash_profile
 - echo "alias kali='ssh root@172.16.2.2'" >> ~/.bash_profile
 - If you messed up your aliases: rm -rf ~/.bash_profile, then try again
 - Remember: use touch and chmod to create the file and set permissions
 - Linux
 - cp ~/.bashrc ~/.bashrc_backup
 - We're making a backup, just in case there are typos or you need to try again
 - echo "alias siem='ssh [username]@172.16.1.3'" >> ~/.bashrc
 - echo "alias ips='ssh [username]@172.16.1.4'" >> ~/.bashrc
 - echo "alias kali='ssh root@172.16.2.2'" >> ~/.bashrc
 - If you messed up your aliases: rm -rf ~/.bashrc; mv ~/.bashrc_backup ~/.bashrc
- Test to see if your aliases are working
 - Linux: source ~/.bashrc
 - OSX: source ~/.bash_profile
 - Type in "siem" and/or "ips" in the terminal
 - If you get prompted for a password, the alias is working correctly.
 - Enter the SIEM or IPS user's password. Confirm you can log in
 - Note: SSH to Kali is broken. We'll be fixing this soon

The alias command (cont'd)

```
ayy@potato:~$ ls -al
total 36
drwxr-xr-x 5 ayy ayy 4096 May 16 15:09 .
drwxr-xr-x 3 root root 4096 May 14 16:39 ..
-rw-r--r-- 1 ayy ayy 220 Apr  4 2018 .bash_logout
-rw-r--r-- 1 ayy ayy 3771 May 16 15:09 .bashrc
drwx----- 2 ayy ayy 4096 May 14 16:39 .cache
drwx----- 3 ayy ayy 4096 May 14 16:39 .groups
-rw-r--r-- 1 ayy ayy 807 Apr  4 2018 .profile
drwx----- 2 ayy ayy 4096 May 16 01:19 .ssh
-rw-r--r-- 1 ayy ayy 0 May 14 16:43 .sudo_as_admin_successful
-rw----- 1 ayy ayy 1838 May 16 15:09 .viminfo
ayy@potato:~$ cp ~/.bashrc ~/.bashrc_backup
ayy@potato:~$ echo "alias siem='ssh ayy@172.16.1.3'" >> ~/.bashrc
ayy@potato:~$ echo "alias ips='ssh ayy@172.16.1.4'" >> ~/.bashrc
ayy@potato:~$ echo "alias kali='ssh root@172.16.2.2'" >> ~/.bashrc
ayy@potato:~$ source ~/.bashrc
ayy@potato:~$ alias | grep ssh
alias ips='ssh ayy@172.16.1.4'
alias kali='ssh root@172.16.2.2'
alias siem='ssh ayy@172.16.1.3'
```

```
ayy@potato:~$ siem
The authenticity of host '172.16.1.3 (172.16.1.3)' can't be established.
ECDSA key fingerprint is SHA256:G4DCOHm/n8v2U0Y0Wpb+M4Y44Jk14rfMffNYmVgCWKO.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.1.3' (ECDSA) to the list of known hosts.
ayy@172.16.1.3's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

```
ayy@potato:~$ ips
The authenticity of host '172.16.1.4 (172.16.1.4)' can't be established.
ECDSA key fingerprint is SHA256:+yB1Fbxr7PBz0nAfa22siSEif+pKkpjiCsZwDPHIyho.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.1.4' (ECDSA) to the list of known hosts.
ayy@172.16.1.4's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

The alias command (cont'd)

```
Tony's-MacBook-Pro:~ trobinson$ touch ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ chmod 744 ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ echo "alias siem='ssh ayy@172.16.1.3'" >> ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ echo "alias ips='ssh ayy@172.16.1.4'" >> ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ echo "alias kali='ssh root@172.16.2.2'" >> ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ source ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ alias | grep ssh
alias ips='ssh ayy@172.16.1.4'
alias kali='ssh root@172.16.2.2'
alias siem='ssh ayy@172.16.1.3'
```

```
Tony's-MacBook-Pro:~ trobinson$ siem
The authenticity of host '172.16.1.3 (172.16.1.3)' can't be established.
ECDSA key fingerprint is SHA256:G4DCOHm/n8vZU0Y0Wpb+M4Y44Jk14rfMfFNYmVgCWk0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.1.3' (ECDSA) to the list of known hosts.
ayy@172.16.1.3's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

```
Tony's-MacBook-Pro:~ trobinson$ ips
The authenticity of host '172.16.1.4 (172.16.1.4)' can't be established.
ECDSA key fingerprint is SHA256:+yBlFbxr7PBz0nAfaZZsiSEif+pKkpjiCsZwDPHIyho.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.1.4' (ECDSA) to the list of known hosts.
ayy@172.16.1.4's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

Key-based Auth

- Allows you to use a public/private key pair to auth/login to SSH.
- Private key can be encrypted/password protected to provide two-factor auth
 - Something you have (private key)
 - Something you know (decryption password)
- Or, you can leave the private key unprotected
 - So long as you have the private key, you can log in as the user you configured key-based auth for
 - But so can anyone else who has your key
- Recommendation:
 - Personal lab environment: Probably no need to password protect your key
 - Shared lab environment and/or Lab on an enterprise network: Password protect your key to limit your liabilities

Key-based Auth (cont'd)

- What Do?
 - Run `ssh-keygen -t ed25519`
 - Hit enter to save the key to `/home/[username]/.ssh/id_ed25519`
 - Input a password or just hit enter to not set a password
 - Command finishes, and creates `id_ed25519` and `id_ed25519.pub`
 - `id_ed25519` = private key. Keep it secret, keep it safe(tm)
 - `id_ed25519.pub` = public key. We need to get this on to the SIEM, IPS and (eventually) kali VMs.

Key-based Auth (cont'd)

```
ayy@potato:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/ayy/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ayy/.ssh/id_ed25519.
Your public key has been saved in /home/ayy/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:23w802wHOwiPhIGALcs86R2XuZ1nVeFAkLRmRM5hIk ayy@potato
The key's randomart image is:
+--[ED25519 256]--+
| o.o.E+B+o .. |
| o . + *+o o. |
| oo. +*o ... |
| .= . +o. * + = |
| . o o + S * @ . |
| . . + o o . = |
| . . . . . . . . |
| . . . . . . . . |
+----[SHA256]----+
ayy@potato:~$ ls ~/.ssh
id_ed25519  id_ed25519.pub  known_hosts
```

Transferring your public key

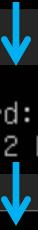
- Much like Windows, there are tons of ways to do this
 - Method 1: ssh-copy-id
 - If you have SSH access to a remote system, ssh-copy-id handles all of the dirty work for you
 - Method 2: copy your public key to the remote system manually via SCP
 - ssh to the system, run:
 - mkdir ~/.ssh
 - mv ~/id_ed25519.pub ~/.ssh/authorized_keys
 - chown -R [user]:[group] ~/.ssh
 - chmod 700 ~/.ssh
 - chmod 600 ~/.ssh/authorized_keys
 - Method 3: copy your public key to the clipboard, SSH to the system, then use output redirection to dump your key
 - ssh to the system, run:
 - mkdir ~/.ssh
 - echo “[right click → paste]” >> ~/.ssh/authorized_keys
 - chown -R [user]:[group] ~/.ssh
 - chmod 700 ~/.ssh
 - chmod 600 ~/.ssh/authorized_keys
 - Bonus: This method can append additional keys to the authorized_keys file

Method 1

```
ayy@potato:~$ ssh-copy-id ayy@172.16.1.3
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/ayy/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install all the new keys
ayy@172.16.1.3's password:
Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'ayy@172.16.1.3'"
and check to make sure that only the key(s) you wanted were added.
```

Method 2

```
ayy@potato:~$ cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIE9R54qHaDfbx1FQjQCGhAkwOf9xn7X6KvnN17sRECW6 ayy@potato
ayy@potato:~$ scp ~/.ssh/id_ed25519.pub ayy@172.16.1.3:~
ayy@172.16.1.3's password:
id_ed25519.pub                                         100%   92     77.6KB/s  00:00
  

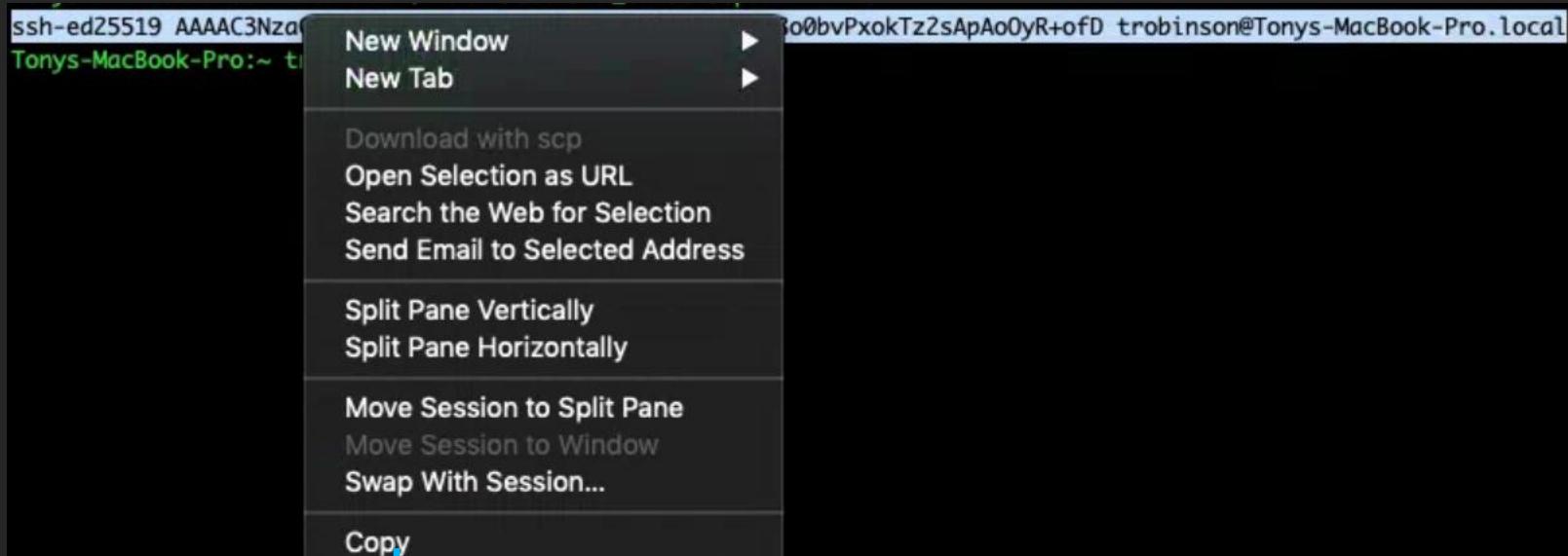

```
ayy@potato:~$ siem
ayy@172.16.1.3's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```


```
ayy@siem:~$ ls -al *.pub
-rw-r--r-- 1 ayy ayy 92 May 15 15:21 id_ed25519.pub
ayy@siem:~$ cat id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIE9R54qHaDfbx1FQjQCGhAkwOf9xn7X6KvnN17sRECW6 ayy@potato
ayy@siem:~$ mkdir ~/.ssh
ayy@siem:~$ mv id_ed25519.pub ~/.ssh/authorized_keys
ayy@siem:~$ chown -R ayy:ayy ~/.ssh
ayy@siem:~$ chmod 700 ~/.ssh
ayy@siem:~$ chmod 600 ~/.ssh/authorized_keys
ayy@siem:~$ ls -al ~/.ssh
total 12
drwx----- 2 ayy ayy 4096 May 15 15:42 .
drwxr-xr-x 5 ayy ayy 4096 May 15 15:42 ..
-rw----- 1 ayy ayy 92 May 15 15:21 authorized_keys
ayy@siem:~$ exit
```


```

Method 3



ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMA/JzeD7FE5tK+8ai4a8o0bvPxokTz2sApAo0yR+ofD trobinson@Tonys-MacBook-Pro.local
Tonys-MacBook-Pro:~ trobinson\$ ssh ayy@172.16.1.3
ayy@172.16.1.3's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
ayy@siem:~\$ mkdir ~/.ssh
ayy@siem:~\$ echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMA/JzeD7FE5tK+8ai4a8o0bvPxokTz2sApAo0yR+ofD trobinson@Tonys-MacBook-Pro.local" >> ~/.ssh/authorized_keys
ayy@siem:~\$ chown -R ayy:ayy ~/.ssh
ayy@siem:~\$ chmod 700 ~/.ssh
ayy@siem:~\$ chmod 600 ~/.ssh/authorized_keys
ayy@siem:~\$ ls -al ~/.ssh
total 12
drwx----- 2 ayy ayy 4096 May 16 00:28 .
drwxr-xr-x 5 ayy ayy 4096 May 16 00:28 ..
-rw----- 1 ayy ayy 115 May 16 00:28 authorized_keys

Testing key-based auth

- After transferring your key to IPS and SIEM, test your SSH aliases
 - If you didn't password protect your private key, should connect with no password prompt
 - If you're still getting prompted for a password, something is wrong. Go back through the previous slides, take your time and try again.
 - If you did password protect your private key, you'll be prompted for the password to your SSH key
- Fun fact: SSH keys work for the scp command as well
 - This means passwordless SCP transfers
 - This will come in handy in the coming sections.

Testing key-based auth (cont'd)

```
Tony's-MacBook-Pro:~ trobinson$ siem  
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

```
Tony's-MacBook-Pro:~ trobinson$ ips  
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

```
Tony's-MacBook-Pro:~ trobinson$ scp ubuntu-18.04.2-live-server-amd64.iso ayy@172.16.1.3:~/  
ubuntu-18.04.2-live-server-amd64.iso
```

51% 432MB 75.8MB/s 00:05 ETA

Enabling SSH on Kali Linux

- So we created connection profiles for SIEM, IPS /and/ kali, but we haven't tried to connect to kali
 - Why:
 - the ssh service is disabled (in spite of being installed)
 - `/etc/ssh/sshd_config`'s `PermitRootLogin` directive is restricting access as the root user to key-based authentication only
 - Seeing as we don't have our pubkey in the authorized keys file, we're kinda screwed.

Enabling SSH on Kali Linux (cont'd)

- Solution:
 - Backup `/etc/ssh/sshd_config`
 - Set `PermitRootLogin "yes"` temporarily
 - Enable the ssh service to start on boot, and start it
 - Copy our public key to `/root/.ssh/authorized_keys` (using whatever methods available to you AND with the right file/directory permissions)
 - Note: If you use the copy/paste methods for transferring your key, and right-click to paste isn't working, trying hitting the Insert (Ins) key
 - Confirm key-based SSH works
 - Reconfigure the `sshd_config` `PermitRootLogin` back to "without-password"
 - Restart SSH service
 - mRemoteNG users: Remove the root user's password from the kali connection profile then File → Save connection file

Enabling SSH on Kali Linux (cont'd)

```
root@kali:~# cp /etc/ssh/sshd_config /etc/ssh/sshd_config_backup  
root@kali:~# vi /etc/ssh/sshd_config
```



```
32 #PermitRootLogin prohibit-password
```



```
32 PermitRootLogin yes
```



```
root@kali:~# systemctl enable ssh  
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sysvinit-defaults.  
Executing: /lib/systemd/systemctl enable ssh  
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.  
root@kali:~# service ssh start
```



```
1 Using username "root".  
2 Server refused our key  
Linux kali 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2kali1 (2019-03-18) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
root@kali:~#
```

Enabling SSH on Kali Linux (cont'd)

```
# Using username "root".
# Server refused our key
Linux kali 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2kali1 (2019-03-18) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 16 10:48:30 2019 from 172.16.1.2
root@kali:~# mkdir ~/.ssh
root@kali:~# echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIEHV65RYCO58j4fNI0edXrFOgeMYQAWn9MeApOPIxLI16 ed25519-key-20190508" >> ~/.ssh/authorized_keys
root@kali:~# chown -R root:root ~/.ssh
root@kali:~# chmod 700 ~/.ssh
root@kali:~# chmod 600 ~/.ssh/authorized_keys
root@kali:~# mv /etc/ssh/sshd_config_backup /etc/ssh/sshd_config
root@kali:~# service ssh restart
```



```
# Using username "root".
# Authenticating with public key "ed25519-key-20190508"
Linux kali 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2kali1 (2019-03-18) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 16 10:54:25 2019 from 172.16.1.2
root@kali:~# 
```

Enabling SSH on Kali Linux (cont'd)

```
Tony's-MacBook-Pro:~ trobinson$ ssh-copy-id root@172.16.2.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/Users/trobinson/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@172.16.2.2's password:

Number of key(s) added:      1

Now try logging into the machine, with:  "ssh 'root@172.16.2.2'"
and check to make sure that only the key(s) you wanted were added.

Tony's-MacBook-Pro:~ trobinson$ kali
Linux kali 4.19.0-kali3-amd64 #1 SMP Debian 4.19.20-1kali1 (2019-02-14) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# mv /etc/ssh/sshd_config_backup /etc/ssh/sshd_config
root@kali:~# service ssh restart
```

Enabling SSH as root to the IPS and SIEM VMs

- Remember what we just did with the Kali VM?
 - We can do that with the IPS and SIEM VMs, except its even easier to enable SSH as the root user:
 - SSH in as your regular user account
 - sudo su – (become root)
 - cp –r /home/[username]/.ssh /root
 - chown –R root:root /root/.ssh
 - Create new connection aliases and/or mremote/winSCP profiles
 - Connect to SIEM and IPS as the root user

Enabling SSH as root to the IPS and SIEM VMs (cont'd)

```
ayy@siem:~$ sudo su -
[sudo] password for ayy:
root@siem:~# cp -r /home/ayy/.ssh/ ~/
root@siem:~# chown -R root:root ~/.ssh/
root@siem:~# ls -al ~/.ssh
total 12
drwx----- 2 root root 4096 May 14 15:28 .
drwx----- 3 root root 4096 May 14 15:28 ..
-rw----- 1 root root 207 May 16 16:01 authorized_keys
```



```
Tony's-MacBook-Pro:~ trobinson$ echo "alias siemroot='ssh root@172.16.1.3'" >> ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ source ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ siemroot
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

```
ayy@ips:~$ sudo su -
[sudo] password for ayy:
root@ips:~# cp -r /home/ayy/.ssh/ ~/
root@ips:~# chown -R root:root ~/.ssh/
root@ips:~# ls -al ~/.ssh
total 12
drwx----- 2 root root 4096 May 14 15:34 .
drwx----- 3 root root 4096 May 14 15:34 ..
-rw----- 1 root root 207 May 16 16:21 authorized_keys
```



```
Tony's-MacBook-Pro:~ trobinson$ echo "alias ipsroot='ssh root@172.16.1.4'" >> ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ source ~/.bash_profile
Tony's-MacBook-Pro:~ trobinson$ ipsroot
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-48-generic x86_64)
```

Enabling SSH as root to the IPS and SIEM VMs (cont'd)

Name	siem(root)
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	172.16.1.3
Username	root
Password	
Protocol	
Protocol	SSH version 2
Port	22
PutTY Session	vbox_lab_keyauth

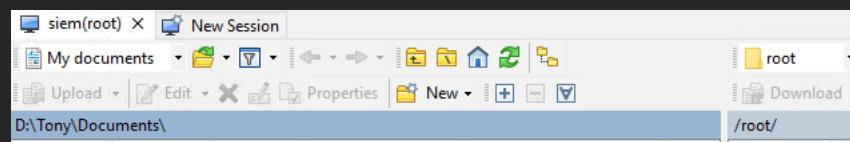
Name	ips(root)
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	172.16.1.4
Username	root
Password	
Protocol	
Protocol	SSH version 2
Port	22
PutTY Session	vbox_lab_keyauth

```
R SIEM
ayy@siem:~$ sudo su -
[sudo] password for ayy:
root@siem:~# cp -r /home/ayy/.ssh/ ~/
root@siem:~# chown -R root:root ~/.ssh/
root@siem:~# ls -al .ssh/
total 12
drwx----- 2 root root 4096 Apr  1 22:38 .
drwx----- 3 root root 4096 Apr  1 23:11 ..
-rw----- 1 root root 102 May 16 19:15 authorized_keys
```

```
ayy@ips:~$ sudo su -
[sudo] password for ayy:
root@ips:~# cp -r /home/ayy/.ssh/ ~/
root@ips:~# chown -R root:root ~/.ssh/
root@ips:~# ls -al ~/.ssh/
total 12
drwx----- 2 root root 4096 May 16 19:28 .
drwx----- 3 root root 4096 May 16 19:28 ..
-rw----- 1 root root 102 May 16 19:28 authorized_keys
```

```
R SIEM [R] siem(root)
Using username "root".
Authenticating with public key "ed25519-key-20190508"
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-47-generic x86_64)
```

```
R IPS [R] ips(root)
Using username "root".
Authenticating with public key "ed25519-key-20190508"
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-47-generic x86_64)
```



Enabling SSH as root to the IPS and SIEM VMs (cont'd)

- Warning: a lot of people say that enabling SSH/SCP as the root user is bad practice and in bad form
 - But it *is* extremely convenient
 - Things to think about:
 - If its your home or personal lab environment, its probably fine to enable SSH as root with key-based auth (with or without an encrypted private key)
 - If its an enterprise/shared lab environment, make sure your SSH key is password protected if you're gonna do this
 - You should probably not be enable SSH as the root user at all for anything production, or anything that touches production (not only for CYA/typos/change control, but for the express purpose of auditing who became the root user, and when)

Disabling password authentication over SSH

- Remember `/etc/ssh/sshd_config`?
 - All sorts of cool config options here.
 - One of them controls whether or not your SSH server will accept passwords at all.
 - Why: Makes remote access to your VMs over SSH tons more secure
 - Anyone who tries to connect without your key (and/or key password, if you did that) gets the boot immediately.
 - `PermitRootLogin prohibit-password` does this for the root user already, but disabling password auth protects your user-level accounts as well.

Disabling password authentication over SSH (cont'd)

- Solution:
 - Make a backup of /etc/ssh/sshd_config (`cp /etc/ssh/sshd_config /etc/ssh/sshd_config_backup`)
 - Open /etc/ssh/sshd_config
 - Find the line “PasswordAuthentication”
 - Set that line to “no”
 - Save changes
 - Restart SSH service
 - Test to see if it works
 - (tip: leave your current SSH session up, create a new SSH session to test)
 - Repeat process until all SSH enabled VMs are reconfigured
 - Yes, even the kali VM
 - Yes, I'm well aware that PermitRootLogin kinda makes this a moot point. Do it anyhow.

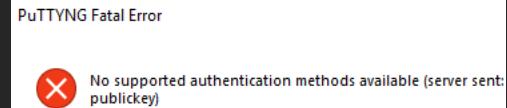
Disabling password authentication over SSH (cont'd)

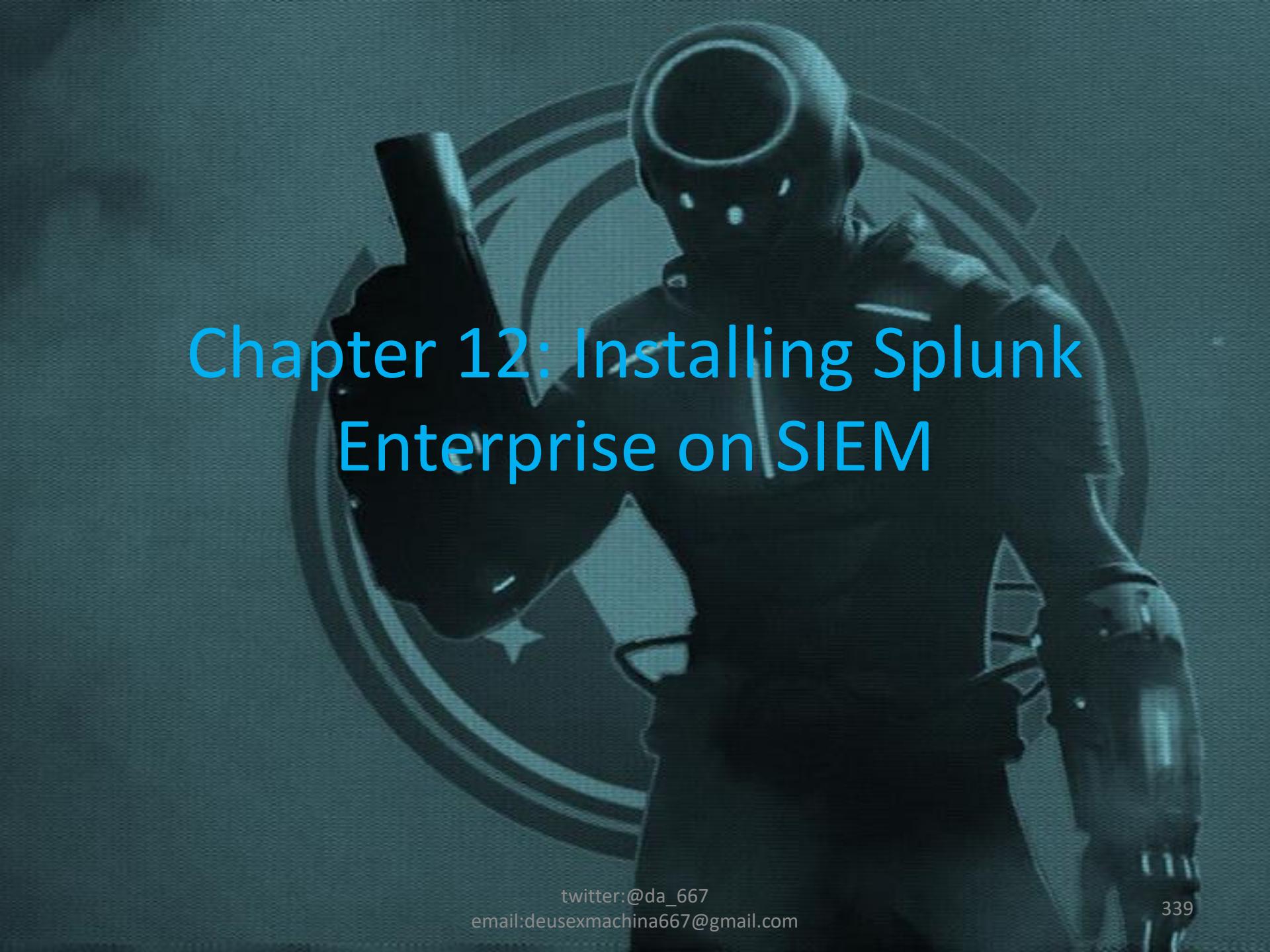
```
root@siem:~# cp /etc/ssh/sshd_config /etc/ssh/sshd_config_backup  
root@siem:~# vi /etc/ssh/sshd_config
```

56 #**PasswordAuthentication yes**

56 **PasswordAuthentication no**

```
Tony's-MacBook-Pro:~ trobinson$ siem  
ayy@172.16.1.3: Permission denied (publickey).
```





Chapter 12: Installing Splunk Enterprise on SIEM

Before we continue..

- Recommend taking snapshots of all of your VMs.
 - We just got done patching them, setting up key-based authentication, and hardening remote access
 - This is a really good baseline to have
 - We're about to install software that gets updated pretty frequently. Having a snapshot to revert to pre software installation makes installing new(er) versions much easier.

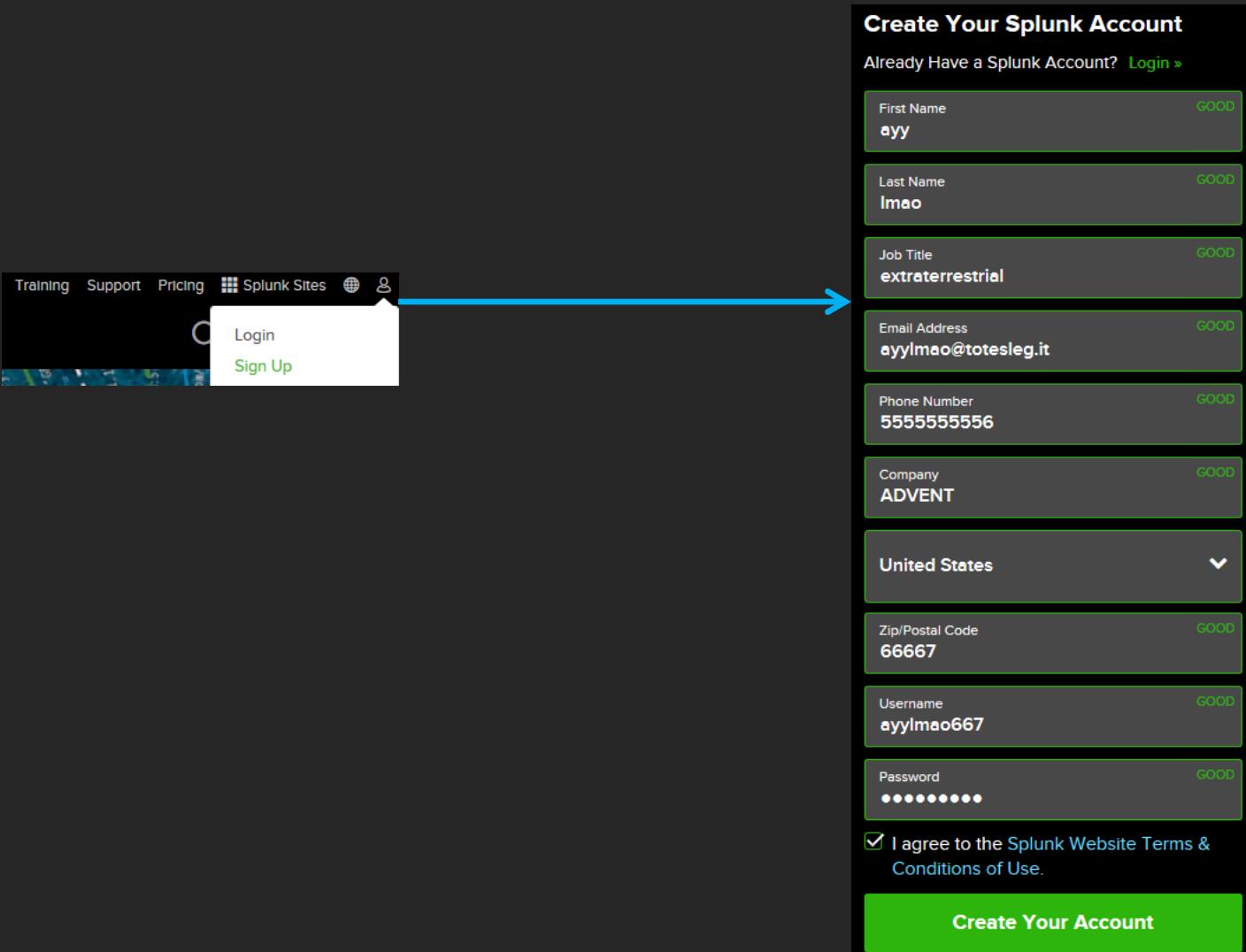
Splunk Enterprise

- Splunk: A very powerful log management platform
 - Its where we'll be send our IDS/IPS logs
 - Its not freeware, but it /is/ awesome
- Splunk Enterprise allows you to log 500MB of data per day for free
 - 10GB if you get a dev license approved/installed.

Tasks to Perform

- You created a splunk.com account, right?
- Did you request a splunk dev license? (optional)
- Login to splunk.com, download Splunk Enterprise for Linux (x86_64) .deb package
- Install Splunk Enterprise (dpkg -i)
- Go through install process, configure boot persistence, and HTTPS web UI
- Log in to <https://172.16.1.3:8000>
 - Learn how to change your password
 - Learn how to change the default HTTPS listener to port 443
 - Learn how to apply your developer license (optional)
 - Learn how to configure a listener so we can receive logs from the IPS VM

Splunk.com account



Create Your Splunk Account

Already Have a Splunk Account? [Login >](#)

First Name	ayy	GOOD
Last Name	lmao	GOOD
Job Title	extraterrestrial	GOOD
Email Address	ayylmao@totesleg.it	GOOD
Phone Number	5555555556	GOOD
Company	ADVENT	GOOD
United States	▼	
Zip/Postal Code	66667	GOOD
Username	ayylmao667	GOOD
Password	••••••••••	GOOD

I agree to the [Splunk Website Terms & Conditions of Use](#).

Create Your Account

twitter:@da_667
email:deusexmachina667@gmail.com

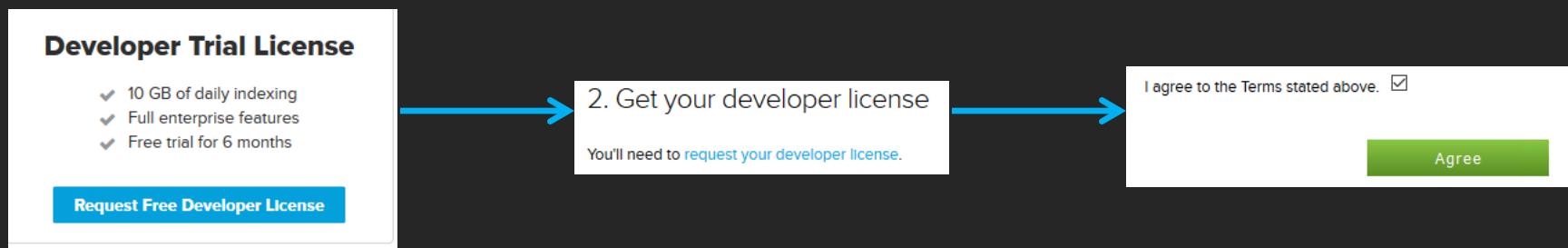
Splunk.com account

- You'll probably get some sort of a confirmation email you have to respond to in order to create your account
- Reminder: I recommended downloading and installing a password manager for a reason.
Save your creds

Requesting a developer license

- Visit <https://splunkbase.splunk.com/develop>
- Log in with your splunk.com account
- Click “Request Free Developer License”
 - On the next page, click “request your developer license” under 2. Get your developer license
 - On the next page, check out the terms of your dev license, click the “I agree to the Terms stated above” checkbox then the big green Agree button
 - Request pending
 - Usually takes 1-3 business days for splunk to review your request
 - This is why I told you to request one before the class.

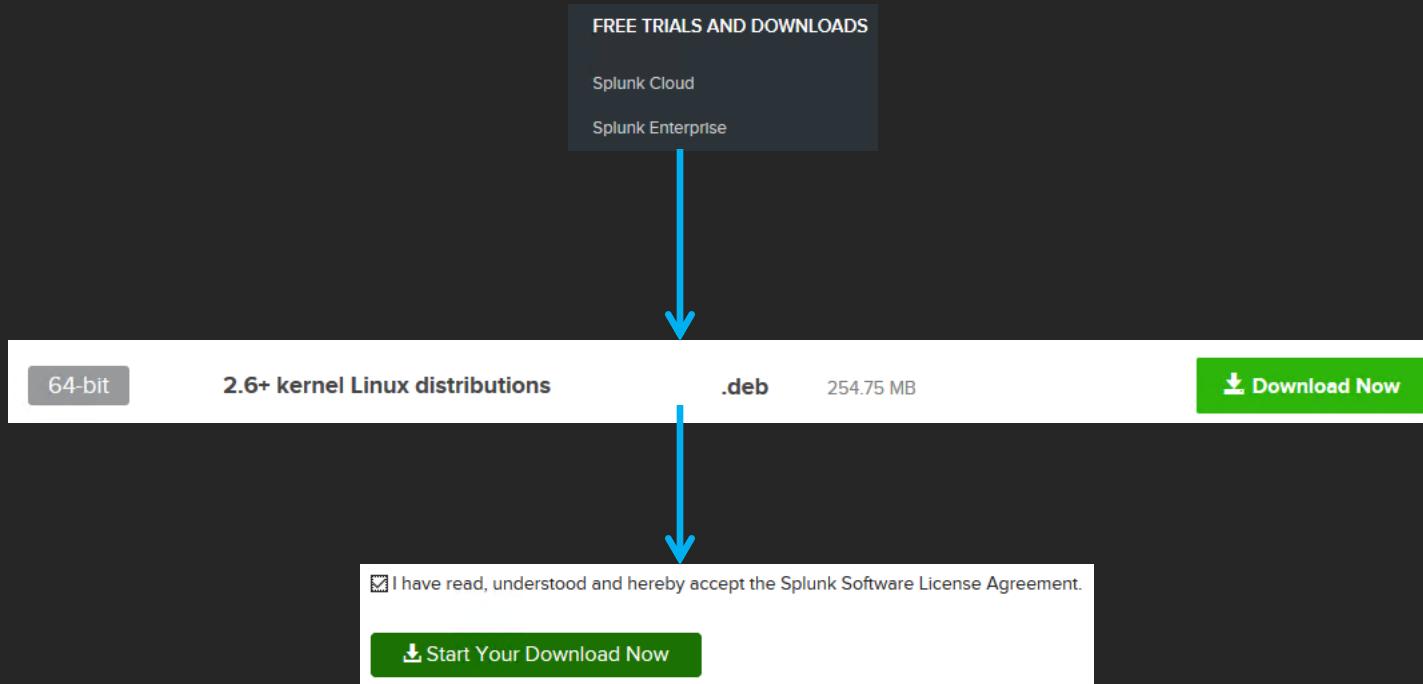
Requesting a developer license



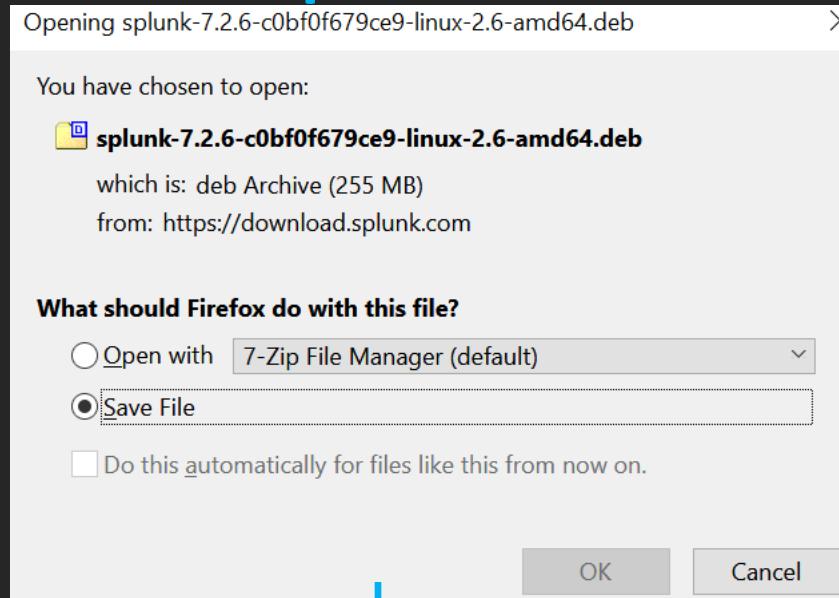
Downloading and Installing Splunk Enterprise

- Go to splunk.com and log in
- Scroll to the bottom of the page and click “Splunk Enterprise” under “Free Trials and Downloads”
- On the next page, under the section labeled “Choose your Installation Package”, select Linux, 64-bit, 2.6+ kernel Linux distributions, .deb
- On the next page, read/submit to the license agreement by clicking the checkbox “I have read, understand and hereby accept the Splunk Software License Agreement” (Even though you clearly haven’t)
- The next page opens a dialogue prompt
 - Option 1: Download the software to your hypervisor host OS and SCP it over to the SIEM VM
 - Note: If you opted to download Splunk Enterprise in Advance, or from the USB drives I provided, You’ll be doing this.
 - Option2: Cancel the download prompt and select the option that gives you a wget command to download the software package DIRECTLY to the SIEM vm. Copy the command, open an SSH session to SIEM, paste the command in, and let wget handle all the dirty work.

Downloading and Installing Splunk Enterprise (cont'd)



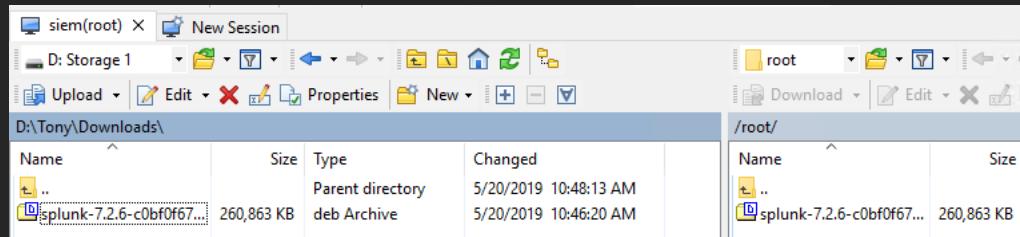
Option 1:



A screenshot of a Windows File Explorer window showing the "Downloads" folder. The file "splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb" is listed in the file list. The file is highlighted with a blue border. The table has columns for Name, Date modified, Type, and Size. The file details are: Name = "splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb", Date modified = "5/20/2019 10:46 AM", Type = "deb Archive", Size = "260,863 KB".

Name	Date modified	Type	Size
splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb	5/20/2019 10:46 AM	deb Archive	260,863 KB

Option 1 (cont'd):



```
Tony's-MacBook-Pro:~ trobinson$ scp splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb root@172.16.1.3:~/  
splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
```



```
root@siem:~# ls -al ~/*.deb  
-rw-r--r-- 1 root root 267123024 May 20 14:52 /root/splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
```

Option 2:

USEFUL TOOLS

- Download via **Command Line (wget)**

We've got ampersands in the URL  and they're all escaped and ready for wget. This URL won't work in your browser. Click [here](#) to select the entire command.

```
wget -O splunk-7.2.6-
c0bf0f679ce9-linux-2.6-
amd64.deb
'https://www.splunk.com
/bin/splunk
/DownloadActivityServlet?archit
```

```
root@siem:~# wget -O splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.2.6&product=splunk&filename=splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb&wget=true'
--2019-05-20 15:04:50-- https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.2.6&product=splunk&filename=splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb&wget=true
Resolving www.splunk.com (www.splunk.com) ... 23.47.79.225, 23.47.79.202
Connecting to www.splunk.com (www.splunk.com)|23.47.79.225|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://download.splunk.com/products/splunk/releases/7.2.6/linux/splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb [following]
--2019-05-20 15:04:53-- https://download.splunk.com/products/splunk/releases/7.2.6/linux/splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com) ... 13.249.87.74, 13.249.87.55, 13.249.87.58, ...
Connecting to download.splunk.com (download.splunk.com)|13.249.87.74|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 267123024 (255M) [application/octet-stream]
Saving to: 'splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb'

splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.d 100%[=====] 254.75M 34.8MB/s   in 7.3s

2019-05-20 15:05:01 (34.8 MB/s) - 'splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb' saved [267123024/267123024]

root@siem:~# ls *.deb
splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
```

Downloading and Installing Splunk Enterprise (cont'd)

- Once downloaded, become root (either via sudo su -, or an SSH session as root) and run dpkg –i /path/to/splunk_enterprise.deb
 - Installs to /opt/splunk
- Cd /opt/splunk/bin
- ./splunk start --accept-license
 - You'll be requested to enter a username and password for administering the splunk server.
 - Remember to save this password to your password manager
- ./splunk enable boot-start
 - Enables splunk to start automatically when the system is rebooted
- ./splunk enable web-ssl
 - Serves the splunk web UI over SSL
 - You'll need to enter the admin username and password here
- ./splunk restart

Logging in to the searchhead (webUI)

- In your web browser, enter
<https://172.16.1.3:8000>
 - Your web browser will complain about self-signed SSL. Continue.
- To log in, enter the credentials you entered at the command line when you installed Splunk.

Things to do while you're here

- Not happy with the admin password? Click Administrator → Account Settings
 - Remember to save your changes to your password manager.
- Don't want to remember to add “:8000” every time you connect to the searchhead? Click Settings → Server Settings
 - On the Server Settings, select “General Settings”
 - Under the “Splunk Web” section, change the input box labeled “Web Port” from 8000 to 443. Scroll to the bottom of the page, hit Save.
 - Please note that you will either need to reboot the server or restart the splunk server (like we did during the installation phase)

Things to do while you're here (cont'd)

- Add your dev license
 - Did you get a dev license? Download the `splunk.license` attachment from your email. Click Settings → Licensing
 - Click Add License
 - Browse to the `splunk.license` file, select it, then click Install
 - You'll need to restart the Splunk services to get your license limits updated
 - Navigate back to Settings → Licensing and confirm your Developer license was applied

Things to do while you're here (cont'd)

- Add a listener, so the IPS VM's log forwarder can send its logs to Splunk and the SIEM VM.
 - Settings → Forwarding and Receiving
 - Click on “Add New” to the right of “Configure Receiving”
 - Input “9997” on the input box labeled “Listen on this port”, then click Save

Things to do while you're here (cont'd)

The screenshot shows a user interface for account management. At the top right, there is a dropdown menu labeled "Administrator" with options: "Account Settings" (which is highlighted with a blue border), "Preferences", and "Logout".

The main area is titled "Personal" and contains the following fields:

- Full name: Administrator
- Email address: changeme@example.com
- Old password: Old password
- Set password: New password
- Confirm password: Confirm new password

Below these fields, there is a note: "Password must contain at least ?" followed by "8 characters".

A green "Save" button is located at the bottom right of the form.

Things to do while you're here (cont'd)

The screenshot shows the Splunk Web interface with a sidebar and a main configuration page.

Sidebar:

- Add Data
- Explore Data
- Monitoring Console

Main Configuration Page:

General settings (highlighted by a blue arrow pointing from the sidebar menu.)

Server settings (highlighted by a red box in the sidebar menu.)

Run Splunk Web: Yes (radio button selected)

Enable SSL (HTTPS) in Splunk Web?: Yes (radio button selected)

Web port *: 443 (highlighted by a blue box)

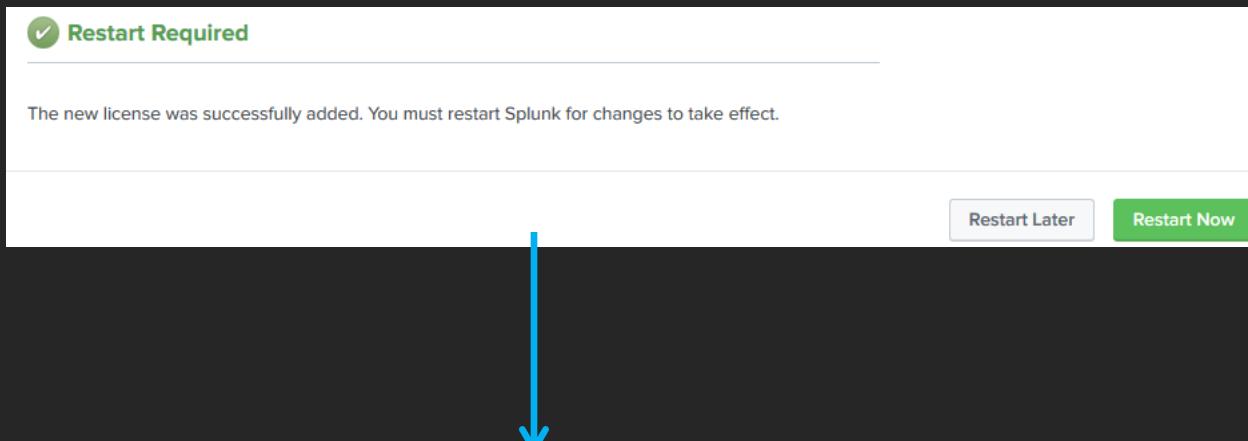
Things to do while you're here (cont'd)

The screenshot illustrates the steps to add a license to a Splunk instance. It consists of three main panels:

- Top Panel:** Shows the main navigation bar with "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". Below the navigation are several links categorized into sections: KNOWLEDGE, DATA, EXPLORE DATA, DISTRIBUTED ENVIRONMENT, SYSTEM, and USERS AND AUTHENTICATION. The "Licensing" link under the SYSTEM section is highlighted with a red box.
- Middle Panel:** A modal window titled "Add new license". It contains instructions to learn more about license options at [splunk.com](#) and to upload a license file. It features a "Browse..." button followed by the file name "Splunk.License". An alternative method is provided: "Or, copy & paste the license XML directly...". At the bottom right are "Cancel" and "Install" buttons.
- Bottom Panel:** A sidebar on the left side of the main interface, titled "License Details". It displays the following information:
 - Product: Splunk Developer Personal License NOT FOR RESALE
 - Size: 10 GB
 - Expiration Date: November 13, 2019 11:59 PMA file icon labeled "Splunk.License" is shown below this information.

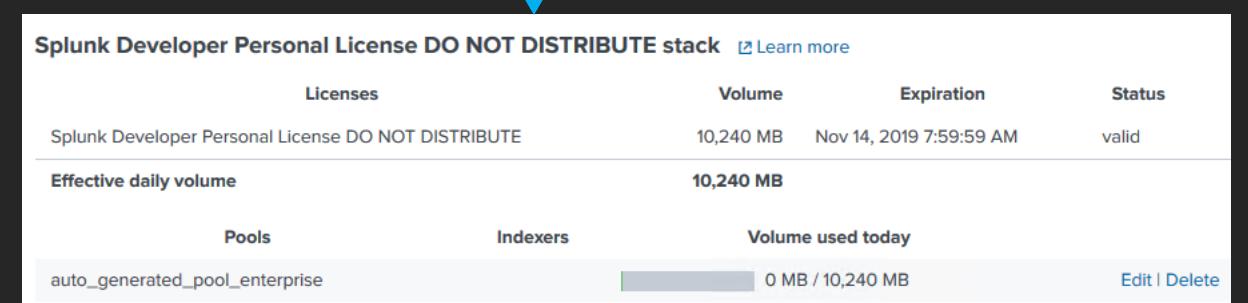
Blue arrows indicate the flow of the process: one arrow points from the "Add Data" link in the top navigation to the "Add new license" modal; another arrow points from the "Add license" button in the bottom sidebar to the "Browse..." field in the modal; and a third arrow points from the "Splunk.License" file in the bottom sidebar to the "Browse..." field in the modal.

Things to do while you're here (cont'd)



The new license was successfully added. You must restart Splunk for changes to take effect.

[Restart Later](#) [Restart Now](#)



Splunk Developer Personal License DO NOT DISTRIBUTE stack [Learn more](#)

Licenses	Volume	Expiration	Status
Splunk Developer Personal License DO NOT DISTRIBUTE	10,240 MB	Nov 14, 2019 7:59:59 AM	valid
Effective daily volume	10,240 MB		
Pools	Indexers	Volume used today	
auto_generated_pool_enterprise		0 MB / 10,240 MB	Edit Delete

Things to do while you're here (cont'd)

The screenshot shows the Splunk web interface with a dark theme. The top navigation bar includes links for Administrator, Messages, Settings, Activity, Help, and Find. A red box highlights the "Forwarding and receiving" link under the DATA category in the main menu.

Add Data (highlighted in blue box)

Monitoring Console

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

SYSTEM

- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management

DATA

- Data inputs
- Forwarding and receiving** (highlighted with a red box)
- Indexes
- Report acceleration summaries
- Virtual indexes
- Source types

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Distributed search

USERS AND AUTHENTICATION

- Access controls

Receive data

Configure this instance to receive data forwarded from other instances.

Configure receiving

+ Add new (highlighted with a red box)

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

For example, 9997 will receive data on TCP port 9997.

Cancel Save

Things to do while you're here (cont'd)

- SIEM vm is fully configured
- Recommend holding off on snapshot until we test/confirm logs from the IPS VM

Chapter 13: Installing Universal Forwarder, and Snort or Suricata on IPS

Tasks to Perform

- Login to splunk.com, download Splunk Universal Forwarder for Linux (x86_64) .deb package
 - Alternatively: you can use the universal forwarder package provided on my USB drive(s)
- Install Splunk UF (universal forwarder) (`dpkg -i`)
- Go through install process, configure boot persistence
- Connect to Splunk Instance on SIEM
- Install Snort via Autosnort, and Hurricane Labs add-on for unified2
 - Or –
- Install Suricata via Autosuricata and Splunk TA for Suricata
- Test functionality of SIEM (logged alerts) and IPS VM (afpacket, and IDS alerts)
- TAKE SNAPSHOTS OF YOUR LAB VMS IN A KNOWN GOOD STATE.

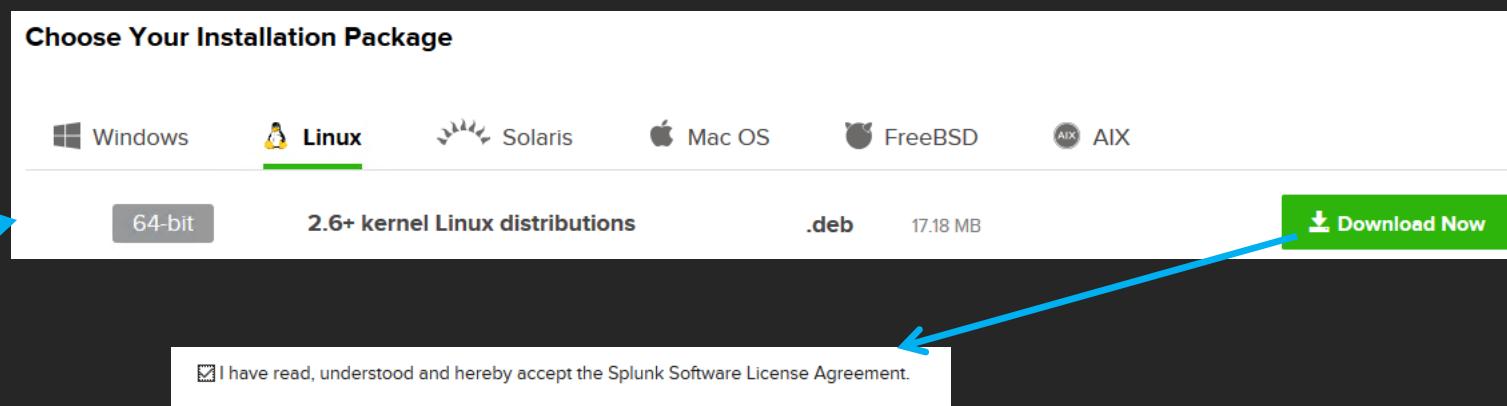
Installing the Universal Forwarder (cont'd)

- Log in to splunk.com
 - Navigate to the bottom of the main page → Free Trials and Downloads → Click Splunk Universal Forwarder
 - Next page: Select Linux, 64-bit, 2.6+ kernel, click the download now button next to the “.deb” package.
 - Next page: Accept the Splunk Software License Agreement, check the box that says you submit to your log management overlords. Then click “Start your Download now”
 - Next page: Just like with the splunk enterprise installer, you have two options for getting it on to the IPS VM:
 - Option 1: Download to your hypervisor host (or copy the installer I included on the thumbdrive(s)), then SCP to the IPS VM
 - Option 2: Use wget to download directly to the IPS VM

Option 1:

FREE TRIALS AND DOWNLOADS

- Splunk Cloud
- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence
- Splunk Insights for Infrastructure
- Splunk Universal Forwarder**
- Splunk Apps & Add-Ons
- All Trials and Downloads



Opening splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb

You have chosen to open:

[splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb](#)
which is: deb Archive (17.18 MB)
from: <https://download.splunk.com>

What should Firefox do with this file?

Open with 7-Zip File Manager (default)

Save File

Do this automatically for files like this from now on.

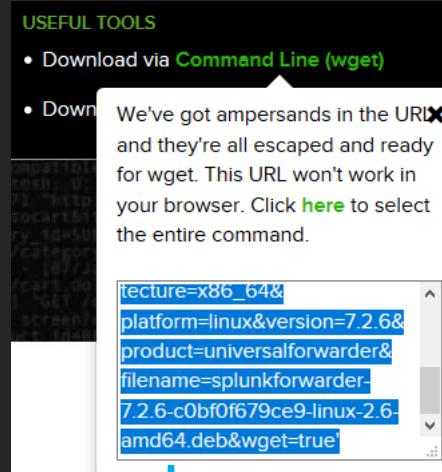
OK

Cancel

Name	Size	Type
..	2 KB	Parent directory
Splunk.License	2 KB	LICENSE File
splunk-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb	260,863 KB	deb Archive
splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb	17,588 KB	deb Archive

```
Tony's-MacBook-Pro:~ trobinson$ scp splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb root@172.16.1.4:~/  
splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
```

Option 2:



```
root@ips:~# wget -O splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.2.6&product=universalforwarder&filename=splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb&wget=true'
--2019-05-21 16:32:20-- https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.2.6&product=universalforwarder&filename=splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb&wget=true
Resolving www.splunk.com (www.splunk.com) ... 23.47.79.225, 23.47.79.202
Connecting to www.splunk.com (www.splunk.com) |23.47.79.225|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://download.splunk.com/products/universalforwarder/releases/7.2.6/linux/splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb [following]
--2019-05-21 16:32:22-- https://download.splunk.com/products/universalforwarder/releases/7.2.6/linux/splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com) ... 99.84.254.93, 99.84.254.39, 99.84.254.119, ...
Connecting to download.splunk.com (download.splunk.com) |99.84.254.93|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18009700 (17M) [application/octet-stream]
Saving to: 'splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb'

splunkforwarder-7.2.6-c0bf0f679ce9-linux-2. 100%[=====] 17.17M 24.6MB/s in 0.7s

2019-05-21 16:32:23 (24.6 MB/s) - 'splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb' saved [18009700/18009700]
```

Installing the Universal Forwarder (cont'd)

- Once downloaded, become root (either via sudo su -, or an SSH session as root) and run dpkg –i /path/to/splunkforwarder.deb
 - Installs to /opt/splunkforwarder
- Cd /opt/splunkforwarder/bin
- ./splunk start --accept-license
 - You'll be requested to enter a username and password for administering the splunk server.
 - Remember to save this password to your password manager
- ./splunk stop
 - Need to stop the service for the next command
- ./splunk add forward-server 172.16.1.3:9997
 - Enables splunk to start automatically when the system is rebooted
- ./splunk enable boot-start
 - Allows the universal forwarder to start automatically on reboots
- ./splunk start
 - Start the UF again

Installing the Universal Forwarder (cont'd)

- Once downloaded, become root (either via sudo su -, or an SSH session as root) and run dpkg –i /path/to/splunkforwarder.deb
 - Installs to /opt/splunkforwarder
- cd /opt/splunkforwarder/bin
- ./splunk start --accept-license
 - You'll be requested to enter a username and password for administering the splunk server.
 - Remember to save this password to your password manager
- ./splunk stop
 - Need to stop the service for the next command
- ./splunk add forward-server 172.16.1.3:9997
 - Enables splunk to start automatically when the system is rebooted
- ./splunk enable boot-start
 - Allows the universal forwarder to start automatically on reboots
- ./splunk start
 - Start the UF again

Installing the Universal Forwarder (cont'd)

```
root@ips:~# ls *.deb
splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
root@ips:~# dpkg -i splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 102591 files and directories currently installed.)
Preparing to unpack splunkforwarder-7.2.6-c0bf0f679ce9-linux-2.6-amd64.deb ...
Unpacking splunkforwarder (7.2.6) ...
Setting up splunkforwarder (7.2.6) ...
complete
root@ips:~# cd /opt/splunkforwarder/bin/
root@ips:/opt/splunkforwarder/bin# ./splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
 * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

Y

Title:	splunk UF admin credentials
Username:	admin
Password:	*****
Repeat:	*****

```
root@ips:/opt/splunkforwarder/bin# ./splunk stop
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
root@ips:/opt/splunkforwarder/bin# ./splunk add forward-server 172.16.1.3:9997
Added forwarding to: 172.16.1.3:9997.
root@ips:/opt/splunkforwarder/bin# ./splunk enable boot-start
Init script installed at /etc/systemd/system/.
Init script is configured to run at boot.
root@ips:/opt/splunkforwarder/bin# ./splunk start

Splunk> Winning the War on Error

Checking prerequisites...
    Checking mgmt port [8089]: open
    Checking conf files for problems...
    Done
    Checking default conf files for edits...
    Validating installed files against hashes from '/opt/splunkforwarder/splunkf
All installed files intact.
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

Installing Snort or Suricata

- Time to make a decision
 - For the purposes of our lab environment, both serve an identical role:
 - Bridge IPS1 and IPS2 via AFPACKET bridging
 - Generate alerts on bad traffic between IPS1 and IPS2
 - Personal preference?
 - Suricata, hands down.
 - Whole host of features that Snort simply doesn't have.
 - We'll cover how to install Snort and the Hurricane Labs add-on for Unified2, Then Suricata, and the SuricataTA
 - After covering installation of both NSM platforms, we'll go over how to test functionality on both platforms

Installing Snort

- Installing Snort via Autosnort, AVATAR edition
 - Script that automates all of the hard stuff
 - Installing prerequisite software packages
 - Compiling Snort and the DAQ (data acquisition) library
 - Setting up directories for config files and logs to live
 - Installing pulledpork (rule manager) as well as download/installing rules
 - Setting up interfaces for bridging between IPS1 and IPS2
 - Installing a service to allow the Snort to auto-start on system reboots, and control start/stopping/restarting snort

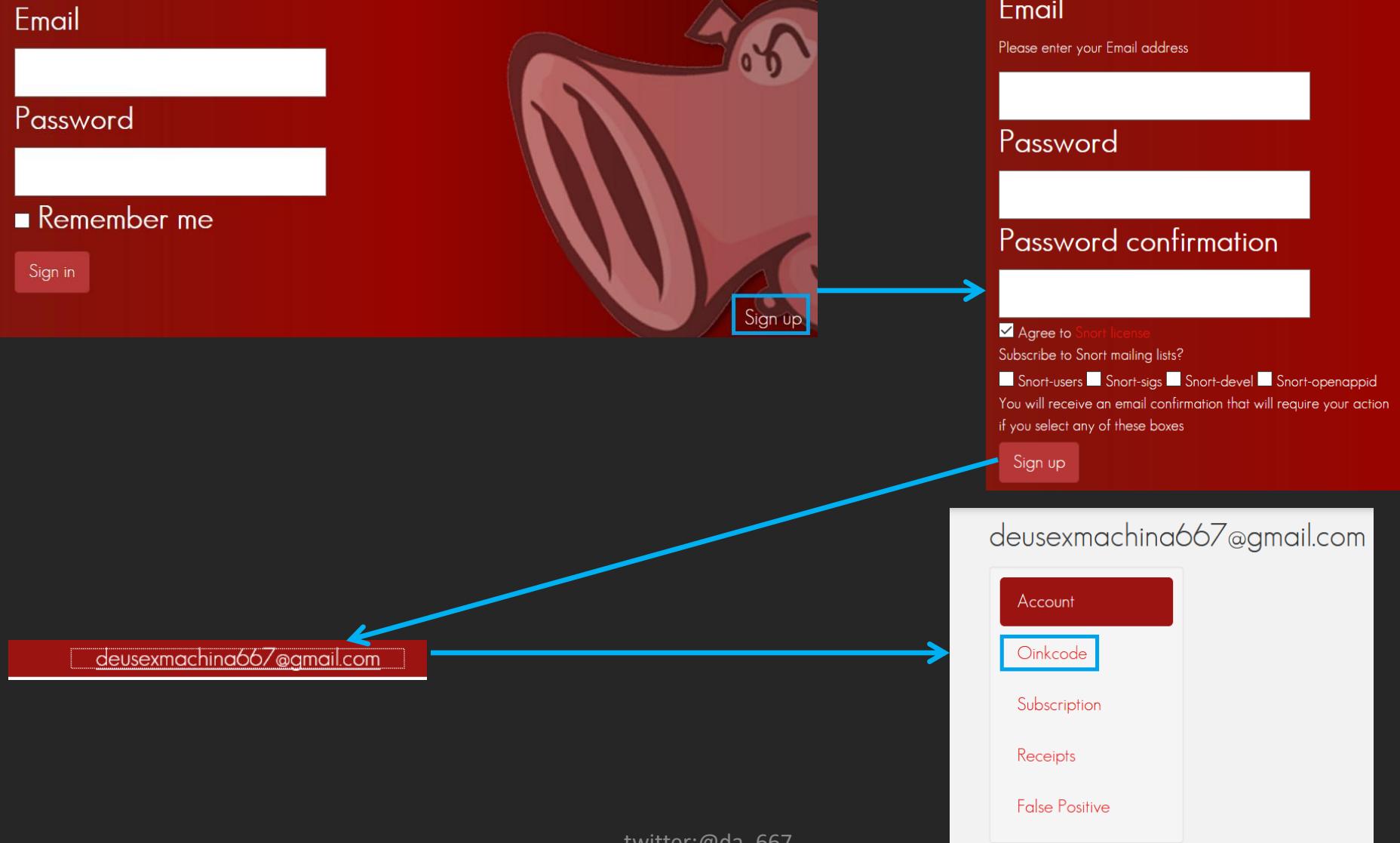
Installing Snort (cont'd)

- But before we continue....
 - Did you register an account on snort.org?
 - You absolutely need to. You need an “Oink Code” to run autosnort
- Visit https://snort.org/users/sign_in
 - Click Sign up
 - Next page, enter your e-mail, password (twice)
 - Click the checkbox agreeing to the Snort License, then click Sign Up
 - Optional: if you want spam, click the checkboxes for snort-users, snort-sigs, snort-devel, snort-openappid to get on the mailing list(s)
 - Check your e-mail, click the confirmation link, and log in to your new snort.org account

Installing Snort (cont'd)

- Click on your e-mail address in the upper-right
- Click on the link labeled Oinkcode
 - Copy the long alphanumeric string
 - Hint: Save your snort.org credentials to your password manager. Put the oink code in the comment section for the entry for easy access.

Installing Snort (cont'd)



twitter:@da_667

email:deusexmachina667@gmail.com

Installing Snort (cont'd)

- How to run the script:
 - Recommend logging in as root, or using sudo su – to become root
 - git clone <https://github.com/da667/Autosnort>
 - cd ~/Autosnort/Autosnort-Ubuntu/AVATAR/
 - You will need to configure full_autosnort.conf and enter the name of the network interface cards connected to IPS1 and IPS 2, and your oink code
 - Hint: ifconfig –a
 - Look for interfaces with no IP/inet address
 - Put them in the snort_iface_1 and snort_iface_2 field
 - Oink code goes into the o_code field
 - This is why you created a snort.org account
 - export http_proxy=http://172.16.1.1:3128
 - export https_proxy=
 - These export statements are important. YOU HAVE TO RUN THEM.
 - bash autosnort-ubuntu-avatar.sh
 - The script MUST be ran as root (log in as root, or use “sudo bash autosnort-ubuntu-avatar.sh”)
 - Let the script run
 - System will reboot automatically when the script finishes

Installing Snort (cont'd)

```
root@ips:~# git clone https://github.com/da667/Autosnort
Cloning into 'Autosnort'...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 863 (delta 0), reused 7 (delta 0), pack-reused 856
Receiving objects: 100% (863/863), 2.23 MiB | 8.91 MiB/s, done.
Resolving deltas: 100% (482/482), done.
root@ips:~# cd Autosnort/Autosnort-Ubuntu/AVATAR/
root@ips:~/Autosnort/Autosnort-Ubuntu/AVATAR# ifconfig -a
enp0s8: flags=4098<Broadcast,Multicast> mtu 1500
      ether 08:00:27:f6:dd:77  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

enp0s9: flags=4098<Broadcast,Multicast> mtu 1500
      ether 08:00:27:le:76:c2  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

enp0s17: flags=4163<UP,Broadcast,Running,Multicast> mtu 1500
      inet 172.16.1.4  netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::a00:27ff:fe9e:f408  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:9e:f4:08  txqueuelen 1000  (Ethernet)
            RX packets 594091  bytes 335497084 (335.4 MB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 47911  bytes 6121510 (6.1 MB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,Loopback,Running> mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
            RX packets 1306  bytes 120606 (120.6 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 1306  bytes 120606 (120.6 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@ips:~/Autosnort/Autosnort-Ubuntu/AVATAR# vi full_autosnort.conf
```

```
##snort_iface_1##
# This is the name of the first interface you will use.
# This option MUST be set.
# Example:
# snort_iface_1=eth1
#Default setting: snort_iface_1=eth1
snort_iface_1=enp0s8

##snort_iface_2##
# This is the name of the second interface you will use.
# This option MUST be set.
# Example:
# snort_iface_2=eth2
#Default setting: snort_iface_2=eth2
snort_iface_2=enp0s9

##o_code##
# This setting is the sink code that will be used by Snort.
# You MUST input a valid sink code for the script to work.
# This can be a registered user sink code, or VRT sink code.
# If you have no idea what an oink code is, or how to get one,
# After registering your account, and logging in you can find it under "My Account".
# Example:
# o_code=2426170067b2e110c1f3fdee444118fcc15180f0
# the above is not a valid oink code, do not use it.
o_code=2426170067b2e110c1f3fdee444118fcc15180f0
```

```
root@ips:~/Autosnort/Autosnort-Ubuntu/AVATAR# export http_proxy=http://172.16.1.1:3128
root@ips:~/Autosnort/Autosnort-Ubuntu/AVATAR# export https_proxy=
root@ips:~/Autosnort/Autosnort-Ubuntu/AVATAR# bash autosnort-ubuntu-AVATAR.sh
```

Installing Snort (cont'd)

- On reboot, reconnect to the IPS VM. Run the following commands:
 - Service snortd status
 - Check the status of the snortd service. This will tell you if snort is running and the last logs out of the log file
 - If it's not running, it may provide hints as to why
 - Note: the snortd service supports status, start, stop, and restart arguments.
 - Ifconfig –a
 - If the script ran correctly, the interfaces in full_autosnort.conf should have the flags: UP, BROADCAST, RUNNING, NOARP, PROMISC
 - Ps -ef | grep snort
 - Shows you the process id for snort, and its command line arguments
 - -D: daemonize
 - -u: snort (drop privileges to the snort user)
 - -g: snort (drop privileges to the snort group)
 - -c /opt/snort/etc/snort.conf (this is where the snort config file lives)
 - -Q operating in inline mode
 - --daq afpacket (specifically use the AFPACKET data acquisition libraries)
 - --daq-mode inline (specifically run the AFPACKET daq for inline operation)
 - -i interface1:interface2 (what interfaces should snort run on? Inline interfaces separated by the colon (:) symbol)

Installing Snort (cont'd)

```
root@ips:~# service snortd status
● snortd.service - LSB: start and stop snort
   Loaded: loaded (/etc/init.d/snortd; generated)
   Active: active (running) since Tue 2019-05-21 18:55:54 UTC; 27s ago
     Docs: man:systemd-sysv-generator(8)
 Process: 1709 ExecStop=/etc/init.d/snortd stop (code=exited, status=0/SUCCESS)
 Process: 1796 ExecStart=/etc/init.d/snortd start (code=exited, status=0/SUCCESS)
   Tasks: 2 (limit: 2319)
  CGroup: /system.slice/snortd.service
          └─1800 /opt/snort/bin/snort -D -u snort -c /opt/snort/etc/snort.conf -Q --daq afpacket --daq-mode inline -i enp0s8:enp0s9

May 21 18:55:54 ips snort[1800]:      Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
May 21 18:55:54 ips snort[1800]:      Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
May 21 18:55:54 ips snort[1800]:      Preprocessor Object: SF_DNS Version 1.1 <Build 4>
May 21 18:55:54 ips snort[1800]:      Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
May 21 18:55:54 ips snort[1800]:      Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
May 21 18:55:54 ips snort[1800]:      Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
May 21 18:55:54 ips snort[1800]: Commencing packet processing (pid=1800)
May 21 18:55:54 ips snort[1800]: Decoding Ethernet
May 21 18:55:54 ips root[1801]: Snort Started!
May 21 18:55:54 ips systemd[1]: Started LSB: start and stop snort.
```

Installing Snort (cont'd)

```
root@ips:~# ps -ef | grep snort
snort      1800      1  0 18:55 ?        00:00:00 /opt/snort/bin/snort -D -u snort -g snort -c /opt/snort/etc/snort.conf -Q --daq afpacket --daq-mode inline -i enp0s8:enp0s9
```

```
root@ips:~# ifconfig -a
enp0s8: flags=451 <UP,BROADCAST,RUNNING,NOARP,PROMISC>    mtu 1500
          inet6 fe80::a00:27ff:fe00:77 txqueuelen 1000  (Ethernet)
          ether 08:00:27:f6:dd:77  txqueuelen 1000  (Ethernet)
          RX packets 144 bytes 9776 (9.7 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 64 bytes 9091 (9.0 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=45 <UP,BROADCAST,RUNNING,NOARP,PROMISC>    mtu 1500
          inet6 fe80::a00:27ff:fe00:76 txqueuelen 1000  (Ethernet)
          ether 08:00:27:1e:76:c2  txqueuelen 1000  (Ethernet)
          RX packets 973 bytes 324049 (324.0 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 28 bytes 3112 (3.1 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s17: flags=4163 <UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
          inet 172.16.1.4 netmask 255.255.255.0 broadcast 172.16.1.255
          inet6 fe80::a00:27ff:fe9e:f408 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:9e:f4:08  txqueuelen 1000  (Ethernet)
          RX packets 85738 bytes 119108866 (119.1 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 18746 bytes 2272022 (2.2 MB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73 <UP,LOOPBACK,RUNNING>  mtu 65536
          inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1  prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000  (Local Loopback)
          RX packets 168 bytes 14240 (14.2 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 168 bytes 14240 (14.2 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Quick Troubleshooting (Snort)

- Is suricatad not running?
 - service suricatad start
- Still not running? Check /usr/local/var/run for suricata.pid
 - “Stale” pid files
 - Usually happens when the process/system crashes (or wasn’t shut down properly)
 - rm -rf /usr/local/var/run/*.pid*
 - service suricatad start
- Still not running?
 - grep suricata /var/log/syslog | less
- Wanna update your rules?
 - export http_proxy=http://172.16.1.1:3128
 - export https_proxy=
 - suricata-update -D /usr/local/etc/suricata --no-merge
 - -D: look at this directory for config files, and also where I want rules to be dumped
 - --no-merge: do not merge all the rules into a single file; use separate rule categories/files

Hurricane Labs Add-On for Unified2

- Unified2: The preferred logging format for Snort
 - Pros: Its fast
 - Cons: Its binary. Requires a parser to make human readable
 - See also: Barnyard2
- Hurricane Labs Add-On for Unified2
 - Splunk Forwarder add-on
 - Parses Unified2, dumps as JSON, gets ingested by Splunk

Hurricane Labs Add-On for Unified2(cont'd)

- How to install:
 - <https://splunkbase.splunk.com/app/1858/>
 - Note: you'll need to log in with your splunk.com creds
 - Click Download, and then click the checkbox to agree to license terms and conditions, then click Agree to Download
 - You'll need to transfer from your hypervisor host to your IPS VM via SCP.

Hurricane Labs Add-On for Unified2 (cont'd)

The Hurricane Labs Add-On for Unified2 is a Splunk Technology Add-On by Hurricane Labs for parsing data stored by Snort or Suricata in the Unified2 binary format into a Splunk-compatible JSON format. This optionally includes packet capture data.

Accept License Agreements

This app is provided by a third party and your right to use the app is in accordance with the license provided by that third-party licensor. Splunk is not responsible for any third-party apps does not provide any warranty or support. If you have any questions, complaints or claims with respect to this app, please contact the licensor directly.

MIT License
[Splunk Websites Terms and Conditions of Use](#)

I have read the terms and conditions of this license and agree to be bound by them.
 I consent to Splunk sharing my contact information with the publisher of this app so I receive more information about the app directly from the publisher.

Agree to Download

Opening hurricane-labs-add-on-for-unified2_105.tgz

You have chosen to open:
hurricane-labs-add-on-for-unified2_105.tgz
which is: tar Archive (7.8 KB)
from: https://cdn.apps.splunk.com

What should Firefox do with this file?
 Open with 7-Zip File Manager (default)
 Save File
 Do this automatically for files like this from now on.

OK Cancel

ips(root) X New Session

D:\ Storage 1 Upload Edit Properties New +

D:\Tony\Downloads\ Name Size Type Parent directory

.. 8 KB tgz Archive

hurricane-labs-add-on-for-unified2_105.tgz 2 KB LICENSE File

Download Edit Properties

/root/ Name

.. 5 Autosnort 5 hurricane-labs-add-on-for-unified2_105.tgz

```
Tonys-MacBook-Pro:~ tr Robinson$ scp hurricane-labs-add-on-for-unified2_105.tgz root@172.16.1.4:~/hurricane-labs-add-on-for-unified2_105.tgz
```

100% 7936 9.0MB/s 00:00

twitter:@da_667
email:deusexmachina667@gmail.com

Hurricane Labs Add-On for Unified2 (cont'd)

- How to install (cont'd):
 - SSH to IPS (preferably as root, or use sudo su – to become root)
 - apt-get –y install python
 - Yes, you need python 2.x to run this. For now.
 - cp /path/to/hurricane-labs-add-on-for-unified2_105.tgz /opt/splunkforwarder/etc/apps
 - cd /opt/splunkforwarder/etc/apps
 - tar –xzvf hurricane-labs-add-on-for-unified2_105.tgz
 - cd TA-unified2/default
 - Modify the unified2.conf file to point to the sid-msg.map, gen-msg.map and classification.config in /opt/snort/etc
 - Modify inputs.conf, and change the disabled field from 1 to 0
 - cd /opt/splunkforwarder/bin
 - ./splunk restart

Hurricane Labs Add-On for Unified2 (cont'd)

```
root@ips:~# ls *.tgz
hurricane-labs-add-on-for-unified2_105.tgz
root@ips:# cp ~/hurricane-labs-add-on-for-unified2_105.tgz /opt/splunkforwarder/etc/apps/
root@ips:~# cd /opt/splunkforwarder/etc/apps/
root@ips:/opt/splunkforwarder/etc/apps# tar -xzvf hurricane-labs-add-on-for-unified2_105.tgz
```

```
root@ips:/opt/splunkforwarder/etc/apps# cd TA-unified2/default/
root@ips:/opt/splunkforwarder/etc/apps/TA-unified2/default# vi unified2.conf
```

```
[output]
pretty = false
pcap = true

[unified2]
checkpoint_file = /var/log/snort/alert_json.checkpoint
input_u2 = /var/log/snort/snort.u2
sid_msg_map = /opt/snort/etc/sid-msg.map
gen_msg_map = /opt/snort/etc/gen-msg.map
classifications = /opt/snort/etc/classification.config
```

```
root@ips:/opt/splunkforwarder/etc/apps/TA-unified2/default# vi inputs.conf
```

```
[script:///bin/alert_json.sh]
disabled = 0
interval = 30
sourcetype = snort_json
```

```
root@ips:/opt/splunkforwarder/etc/apps/TA-unified2/default# cd /opt/splunkforwarder/bin/
root@ips:/opt/splunkforwarder/bin# ./splunk restart
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
```

Installing Suricata

- Installing Suricata via Autosuricata
 - Same process as Snort, but even simpler
 - No websites to register to
 - Script automates the tedious bits
 - Downloading apt-get prerequisites
 - Downloading suricata + compiling
 - Downloading rules
 - Configuring AFPACKET bridging
 - Configuring service persistence

Installing Suricata (cont'd)

- How to run the script:
 - Recommend logging in as root, or using sudo su – to become root
 - git clone <https://github.com/da667/Autosuricata>
 - cd ~/Autosuricata/AutoSuricata-Deb/AVATAR/
 - You will need to configure full_autosuricata.conf and enter the name of the network interface cards connected to IPS1 and IPS 2
 - Hint: ifconfig –a
 - Look for interfaces with no IP/inet address
 - Put them in the suricata_iface_1 and suricata_iface_2 field
 - export http_proxy=http://172.16.1.1:3128
 - export https_proxy=
 - These export statements are important. YOU HAVE TO RUN THEM.
 - bash autosuricata-deb-AVATAR.sh
 - The script MUST be ran as root (log in as root, or use “sudo bash autosnort-ubuntu-avatar.sh”)
 - Let the script run
 - System will reboot automatically when the script finishes

Installing Suricata (cont'd)

```
root@ips:~# git clone https://github.com/da667/Autosuricata
Cloning into 'Autosuricata'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 71 (delta 3), reused 8 (delta 3), pack-reused 59
Unpacking objects: 100% (71/71), done.
root@ips:~# cd Autosuricata/AutoSuricata-Deb/AVATAR/
root@ips:~/Autosuricata/AutoSuricata-Deb/AVATAR# ifconfig -a
enp0s8: flags=4098<Broadcast,Multicast> mtu 1500
      ether 08:00:27:f6:dd:77 txqueuelen 1000  (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=4098<Broadcast,Multicast> mtu 1500
      ether 08:00:27:le:76:c2 txqueuelen 1000  (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s17: flags=4163<Up,Broadcast,Running,Multicast> mtu 1500
      inet 172.16.1.4 netmask 255.255.255.0 broadcast 172.16.1.255
      inet6 fe80::a00:27ff:fe9e:f408 prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:9e:f4:08 txqueuelen 1000  (Ethernet)
      RX packets 267342 bytes 246883043 (246.8 MB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 49137 bytes 7270424 (7.2 MB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<Up,Loopback,Running> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000  (Local Loopback)
      RX packets 599 bytes 50553 (50.5 KB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 599 bytes 50553 (50.5 KB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ips:~/Autosuricata/AutoSuricata-Deb/AVATAR# vi full_autosuricata.conf
```

The diagram illustrates a workflow for setting up Suricata. It starts with a terminal session on the left, which then points to a configuration file on the right. A final command is shown at the bottom.

Terminal Session (Left):

```
root@ips:~# git clone https://github.com/da667/Autosuricata
Cloning into 'Autosuricata'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 71 (delta 3), reused 8 (delta 3), pack-reused 59
Unpacking objects: 100% (71/71), done.
root@ips:~# cd Autosuricata/AutoSuricata-Deb/AVATAR/
root@ips:~/Autosuricata/AutoSuricata-Deb/AVATAR# ifconfig -a
enp0s8: flags=4098<Broadcast,Multicast> mtu 1500
      ether 08:00:27:f6:dd:77 txqueuelen 1000  (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=4098<Broadcast,Multicast> mtu 1500
      ether 08:00:27:le:76:c2 txqueuelen 1000  (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s17: flags=4163<Up,Broadcast,Running,Multicast> mtu 1500
      inet 172.16.1.4 netmask 255.255.255.0 broadcast 172.16.1.255
      inet6 fe80::a00:27ff:fe9e:f408 prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:9e:f4:08 txqueuelen 1000  (Ethernet)
      RX packets 267342 bytes 246883043 (246.8 MB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 49137 bytes 7270424 (7.2 MB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<Up,Loopback,Running> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000  (Local Loopback)
      RX packets 599 bytes 50553 (50.5 KB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 599 bytes 50553 (50.5 KB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ips:~/Autosuricata/AutoSuricata-Deb/AVATAR# vi full_autosuricata.conf
```

Configuration File (Right):

```
##suricata_iface_1##
# This is the name of the first interface
# This option MUST be set.
# Example:
# suricata_iface_1=eth1
#default setting: suricata_iface_1=suricata_iface_1=suricata_iface_1=enp0s8

##suricata_iface_2##
# This is the name of the second interface
# This option MUST be set.
# Example:
# suricata_iface_2=eth2
#default setting: suricata_iface_2=enp0s9
```

Proxy Configuration (Bottom):

```
root@ips:~# export http_proxy=http://172.16.1.1:3128
root@ips:~# export https_proxy=
root@ips:~# bash autosuricata-deb-AVATAR.sh
```

Installing Suricata (cont'd)

- On reboot, reconnect to the IPS VM. Run the following commands:
 - service suricatad status
 - Check the status of the suricatad service. This will tell you if suricata is running and the last logs out of the log file
 - If its not running, it may provide hints as to why
 - Note: the suricatad service supports status, start, stop, and restart arguments.
 - ifconfig -a
 - If the script ran correctly, the interfaces in full_autosnort.conf should have the flags: UP, BROADCAST, RUNNING, NOARP, PROMISC
 - ps -ef | grep suricata
 - Shows you the process id for snort, and its command line arguments
 - -D: daemonize
 - -c /usr/local/etc/suricata/suricata.yaml (this is where the suricata config file lives)
 - --af-packet tells suricata to run specifically in AF_PACKET mode

Installing Suricata (cont'd)

```
root@ips:~# service suricatad status
● suricatad.service - LSB: start and stop suricata
  Loaded: loaded (/etc/init.d/suricatad; generated)
  Active: active (running) since Wed 2019-05-22 17:43:30 UTC; 7min ago
    Docs: man:systemd-sysv-generator(8)
 Process: 739 ExecStart=/etc/init.d/suricatad start (code=exited, status=0/SUCCESS)
   Tasks: 8 (limit: 2319)
  CGroup: /system.slice/suricatad.service
          └─849 /usr/local/bin/suricata -D -c /usr/local/etc/suricata/suricata.yaml --af-packet

May 22 17:43:29 ips systemd[1]: Starting LSB: start and stop suricata...
May 22 17:43:29 ips suricatad[739]: Starting Suricata
May 22 17:43:29 ips suricatad[739]: 22/5/2019 -- 17:43:29 - <Info> - Including configuration file af-packet.yaml.
May 22 17:43:29 ips suricatad[739]: 22/5/2019 -- 17:43:29 - <Notice> - This is Suricata version 4.1.4 RELEASE
May 22 17:43:30 ips suricatad[739]: Suricata successfully started.
May 22 17:43:30 ips systemd[1]: Started LSB: start and stop suricata.
```

```
root@ips:~# ifconfig -a
enp0s8: flags=451<UP,BROADCAST,RUNNING,NOARP,PROMISC> mtu 1500
inet6 fe80::a00:27ff:fe6:dd77 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:f6:dd:77 txqueuelen 1000 (Ethernet)
RX packets 14 bytes 2826 (2.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 2486 (2.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=451<UP,BROADCAST,RUNNING,NOARP,PROMISC> mtu 1500
inet6 fe80::a00:27ff:fe1e:76c2 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:1e:76:c2 txqueuelen 1000 (Ethernet)
RX packets 4 bytes 1086 (1.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 39 bytes 4672 (4.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s17: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.1.4 netmask 255.255.255.0 broadcast 172.16.1.255
inet6 fe80::a00:27ff:fe9:f408 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:9e:f4:08 txqueuelen 1000 (Ethernet)
RX packets 7984 bytes 2011114 (2.0 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 2891 bytes 3222308 (3.2 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 124 bytes 10156 (10.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 124 bytes 10156 (10.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@ips:~# ps -ef | grep suricata
root      849      1  0 17:43 ?        00:00:24 /usr/local/bin/suricata -D -c /usr/local/etc/suricata/suricata.yaml --af-packet
```

email:deusexmachina667@gmail.com

Quick Troubleshooting (Suricata)

- On reboot, reconnect to the IPS VM. Run the following commands:
 - service suricatad status
 - Check the status of the suricatad service. This will tell you if suricata is running and the last logs out of the log file
 - If its not running, it may provide hints as to why
 - Note: the suricatad service supports status, start, stop, and restart arguments.
 - ifconfig -a
 - If the script ran correctly, the interfaces in full_autosnort.conf should have the flags: UP, BROADCAST, RUNNING, NOARP, PROMISC
 - ps -ef | grep suricata
 - Shows you the process id for snort, and its command line arguments
 - -D: daemonize
 - -c /usr/local/etc/suricata/suricata.yaml (this is where the suricata config file lives)
 - --af-packet tells suricata to run specifically in AF_PACKET mode

Splunk TA for Suricata

- Add-on for the universal forwarder
- Gathers suricata's eve.json logs to be ingested into splunk

Splunk TA for Suricata (cont'd)

- How to install:
 - Login to [splunk.com](https://splunkbase.splunk.com)
 - <https://splunkbase.splunk.com/app/2760/>
 - Click download, Accept the License checkbox, Click Agree to download
 - You'll need to SCP this tgz file to the IPS VM.

Splunk TA for Suricata (cont'd)

This TA will parse Suricata data into Splunk CIM format. The parsed events will also trigger notables in Enterprise Security.

Download

Accept License Agreements

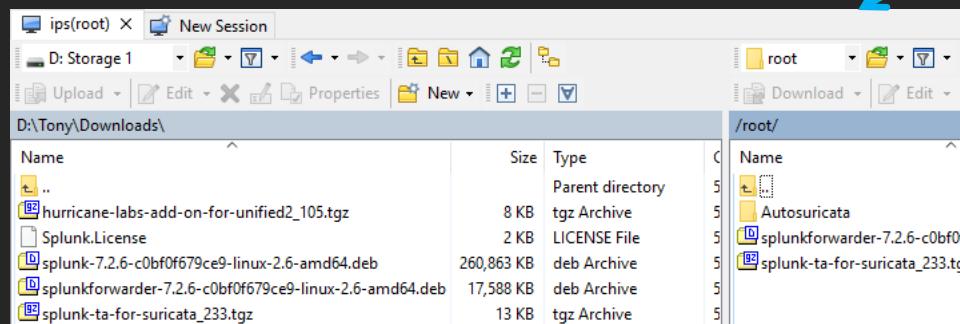
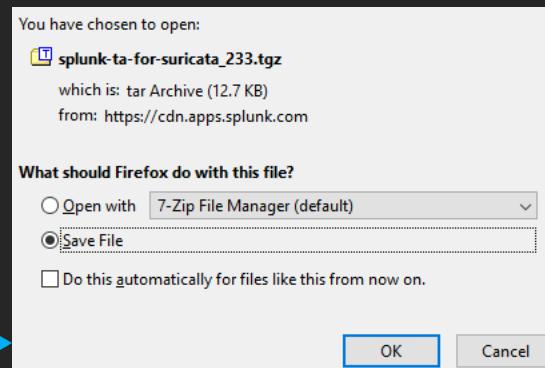
This app is provided by a third party and your right to use the app is in accordance with the license provided by that third-party licensor. Splunk is not responsible for any third-party apps and does not provide any warranty or support. If you have any questions, complaints or claims with respect to this app, please contact the licensor directly.

GNU GENERAL PUBLIC LICENSE

[Splunk Websites Terms and Conditions of Use](#)

- I have read the terms and conditions of this license and agree to be bound by them.
- I consent to Splunk sharing my contact information with the publisher of this app so I can receive more information about the app directly from the publisher.

Agree to Download



```
Tonys-MacBook-Pro:~ trobinson$ scp splunk-ta-for-suricata_233.tgz root@172.16.1.4:~/
```

email:deusexmachina667@gmail.com

100% 13KB 12.5MB/s 00:00

395

Splunk TA for Suricata (cont'd)

- How to install (cont'd):
 - SSH to the IPS VM (preferably as root, or sudo su –)
 - cp /path/to/splunk-ta-for-suricata_233.tgz /opt/splunkforwarder/etc/apps
 - cd /opt/splunkforwarder/etc/apps
 - tar -xzvf splunk-ta-for-suricata_233.tgz
 - cd TA-Suricata/default
 - Need to modify inputs.conf. Change the index from “suricata” to “main”
 - Change the host field to “ips-vm”
 - cd /opt/splunkforwarder/bin
 - ./splunk restart

Splunk TA for Suricata (cont'd)

```
root@ips:~# ls *.tgz
splunk-ta-for-suricata_233.tgz
root@ips:# cp splunk-ta-for-suricata_233.tgz /opt/splunkforwarder/etc/apps/
root@ips:# cd /opt/splunkforwarder/etc/apps/
root@ips:/opt/splunkforwarder/etc/apps# tar -xzvf splunk-ta-for-suricata_233.tgz
TA-Suricata/
TA-Suricata/static/
TA-Suricata/static/appIconAlt.png
TA-Suricata/static/appicon_2x.png
TA-Suricata/static/appiconAlt 2x.png
TA-Suricata/static/appicon.png
TA-Suricata/metadata/
TA-Suricata/metadata/default.meta
TA-Suricata/README.md
TA-Suricata/lookups/
TA-Suricata/lookups/suricata_tcp_flag.csv
TA-Suricata/lookups/suricata_vendor_info.csv
TA-Suricata/lookups/suricata_severity.csv
TA-Suricata/appserver/
TA-Suricata/appserver/static/
TA-Suricata/appserver/static/appIconAlt.png
TA-Suricata/appserver/static/appicon_2x.png
TA-Suricata/appserver/static/appiconAlt_2x.png
TA-Suricata/appserver/static/docs/
TA-Suricata/appserver/static/docs/Install_Suricata.md
TA-Suricata/appserver/static/appicon.png
TA-Suricata/default/
TA-Suricata/default/transforms.conf
TA-Suricata/default/props.conf
TA-Suricata/default/app.conf
TA-Suricata/default/inputs.conf
TA-Suricata/default/eventtypes.conf
TA-Suricata/default/tags.conf
TA-Suricata/default/inputs.conf.example
root@ips:/opt/splunkforwarder/etc/apps# cd TA-Suricata/default/
root@ips:/opt/splunkforwarder/etc/apps/TA-Suricata/default# vi inputs.conf
```



```
[monitor:///var/log/suricata/eve.json]
host = ips-vm
sourcetype = suricata
index = main
```



```
root@ips:/opt/splunkforwarder/etc/apps/TA-Suricata/default# cd /opt/splunkforwarder/bin/
root@ips:/opt/splunkforwarder/bin# ./splunk restart
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
```

What now?

- If Suricata/Snort is running, and you picked the correct interfaces connected to the right networks...
 - IPS1 and IPS2 should be bridged by the IPS VM. How to test:
 - Restart the metasploitable2 VM then log in (msfadmin/msfadmin)
 - Run ifconfig -a
 - Does the network interface have an IP address? Is that IP address 172.16.2.3?
 - Log into the kali VM
 - Open up terminal and enter:
 - » ping -c 4 172.16.2.3
 - You should get 4 ICMP echo replies
 - » curl 172.16.2.3
 - This command should return output/links from the webserver on metasploitable2
 - » msfdb init
 - This is to initialize the metasploit database
 - » Service postgresql start
 - Metasploit uses postgres for hosting its database info. We need this service to be running for the next step...

What now?

```
msfadmin@metasploitable:~$ ifconfig -a
eth0      Link encap:Ethernet HWaddr 08:00:27:e4:6f:3c
          inet addr:172.16.2.3 Bcast:172.16.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4:6f3c/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:5 errors:0 dropped:0 overruns:0 frame:0
             TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:892 (892.0 B) TX bytes:5378 (5.2 KB)
             Base address:0xd070 Memory:f1820000-f1840000
```

```
root@kali:~# ping -c 4 172.16.2.3
PING 172.16.2.3 (172.16.2.3) 56(84) bytes of data.
64 bytes from 172.16.2.3: icmp_seq=1 ttl=64 time=1.24 ms
64 bytes from 172.16.2.3: icmp_seq=2 ttl=64 time=0.737 ms
64 bytes from 172.16.2.3: icmp_seq=3 ttl=64 time=0.497 ms
64 bytes from 172.16.2.3: icmp_seq=4 ttl=64 time=0.656 ms

--- 172.16.2.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 35ms
rtt min/avg/max/mdev = 0.497/0.782/1.238/0.277 ms
root@kali:~# curl 172.16.2.3
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

Warning: Never expose this VM to an untrusted network!



```
root@kali:~# msfdb init
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali:~# service postgresql start
```

What now (cont'd)?

- Now, we're gonna pepper Metasploitable2 with exploits like drunken hillbillies.
 - We want to make sure the IDS is logging right? Best way to do that is to generate IDS alerts.
 - Option 1: Armitage
 - Target: 172.16.2.3
 - Option2: curl with custom user-agents to 172.16.2.3
 - Option3: tcpreplay-edit
 - I supplied pcaps on the USB drives earlier. Transfer them to kali VM, and use tcpreplay-edit to trigger IDS alerts

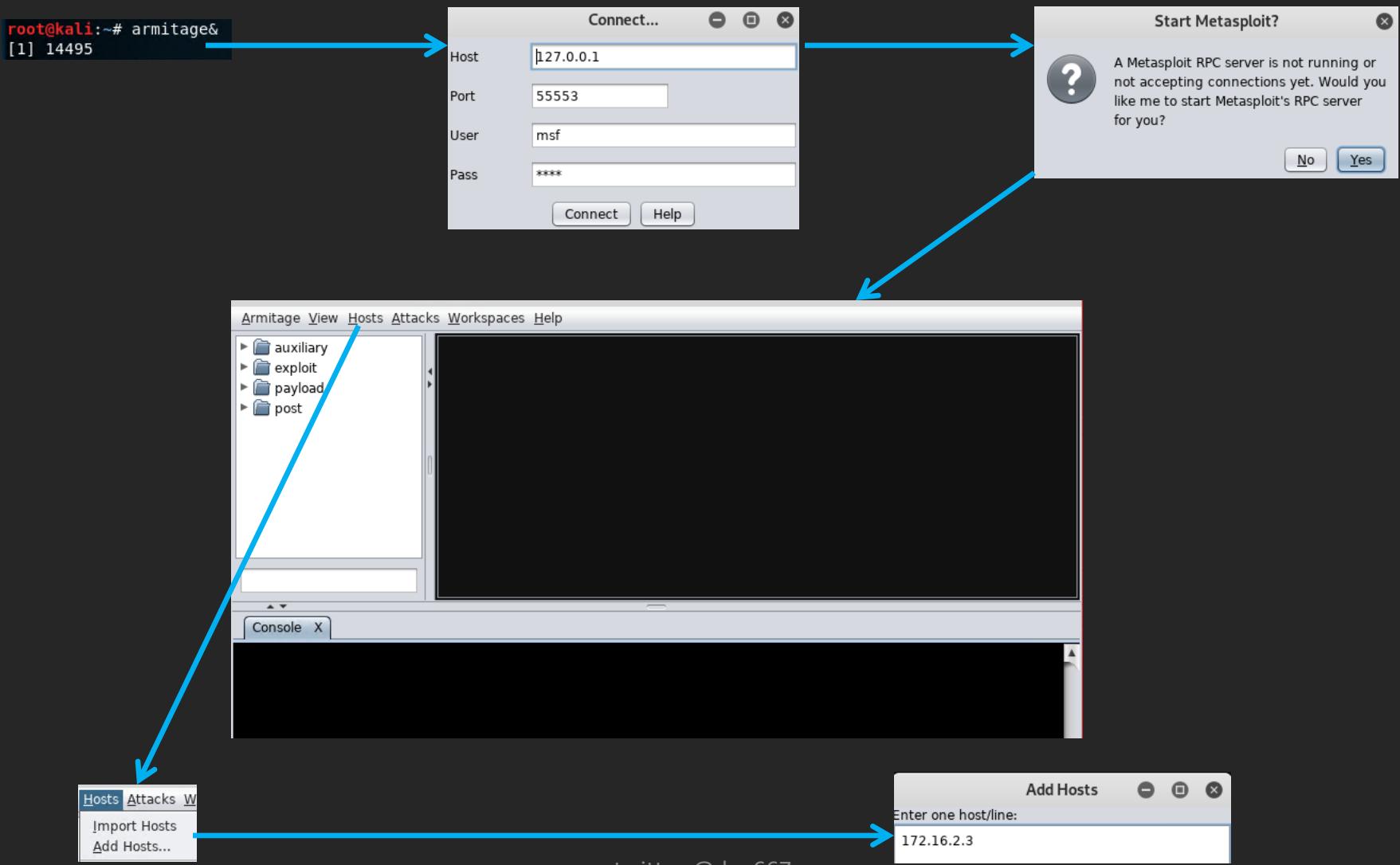
What now (cont'd)?

- Now, we're gonna pepper Metasploitable2 with exploits like drunken hillbillies.
 - We want to make sure the IDS is logging right?
Best way to do that is to generate IDS alerts.
 - Option 1: Armitage
 - Option 2: for loop and curl with custom user-agents
 - Option 3: pregenerated pcaps and tcpreplay-edit
 - These are on the USB drives

Option 1

- Open a terminal on the kali linux VM console
 - Armitage&
 - Starts the armitage program and backgrounds it (in case you need to do other things on the terminal)
 - Click Connect to accept the defaults on the connection window
 - Click yes to have armitage start the metasploit RPC server for you (msfrpcd)
 - Left Pane: Metasploit modules pane.
 - Select metasploit modules to run against targets. Features a search bar for finding particular modules/exploits
 - Center pane: the “workspace”. Representation of systems you are targeting
 - Bottom pane: the console pane. Allows CLI access to the metasploit framework via the console. Generates new tabs for each metasploit module launched.
 - Once the GUI is loaded, select Hosts → Add Hosts... → 172.16.2.3

Option 1



Option 1 (cont'd)

- In the metasploit console, enter:
 - set -g RHOSTS 172.16.2.3
 - In the metasploit modules pane, search for ‘eternalblue’
 - Double click ms17_010_eternalblue → click the big Launch button to launch a tac nuke at Metasploitable2
 - Lets try throwing some more exploits. Search for and launch the following:
 - pureftpd_bash_env_exec
 - usermap_script
 - unreal ircd_3281_backdoor
 - vsftpd_234_backdoor

Option 1 (cont'd)

The image shows two windows from the Metasploit Framework interface. A blue arrow points from the left window to the right window.

Left Window (File Explorer):

- exploit
- windows
- smb
- ms17_010_etalblue**

Right Window (Attack Module):

MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt. with mathematical

Option	Value
LHOST	172.16.2.2
LPORT	1532
RHOSTS +	
RPORT	445
SMBDomain	

Targets: 0 => Windows 7 and Server 2008 R2 (x64) All Service Packs

Use a reverse connection
 Show advanced options

Launch

pureftpd_bash_env_exec

Pure-FTPD External Authentication Bash Environment Variable Code Injection (Shellshock)

This module exploits the Shellshock vulnerability, a flaw in how the Bash shell handles external environment variables. This module targets the Pure-FTPD FTP server when it has been compiled with the --with-extauth flag and an external Bash script is used for

Option	Value
EXE::Custom +	
LHOST	172.16.2.2
LPORT	5582
RHOSTS +	
RPATH	/bin

Targets: 0 => Linux x86

Use a reverse connection
 Show advanced options

Launch

Option 2

- We're gonna use a bash for-loop and curl to spam metasploitable with HTTP requests with user-agents that Snort/Suricata don't like.
 - Open a terminal session on kali. Enter the following:

Option 2

- We're gonna use a bash for-loop and curl to spam metasploitable with HTTP requests with user-agents that Snort/Suricata don't like.
 - Open a terminal session on kali. Enter the following:
 - For i in '(); Nmap ' sme32 Havij 'sleep('; do curl –user-agent "\$i" 172.16.2.3
 - Runs the curl command with 4 different user-agents.

Option 2 (cont'd)

```
root@kali:~/Downloads# for i in '(); Nmap ' Havij 'sleep(' Sme32; do curl --user-agent "$i" 172.16.2.3; done
```

Option 3

- Two pcaps:
 - exploit_traffic.pcap
 - user-agents.pcap
- Use SCP to transfer them to the kali VM
 - winSCP or the scp command (scp [filename] root@172.16.2.2:~/
- Open a terminal on the kali VM
 - cd ~/
 - tcpreplay-edit –C –t –i eth0 exploit_traffic.pcap
 - tcpreplay-edit –C –t –i eth0 user-agents.pcap
 - Tcpreplay-edit: replays packet captures out of a specified interface.
Allows you to edit packets replayed on-the-fly
 - -C: fix packet checksums. Sometimes, IDS/IPS will just /drop/ packets quietly if the checksums/CRCs don't match
 - -t: replay at maximum speed
 - -i eth0: replay out of the eth0 interface

Option 3 (cont'd)

```
root@kali:~# ls -al *.pcap
-rw-r--r-- 1 root root 68326 May 26 14:06 exploit_traffic.pcap
-rw-r--r-- 1 root root 7912 May 26 15:15 user-agents.pcap
root@kali:~# tcpreplay-edit -C -t -i eth0 exploit_traffic.pcap
Warning in replay.c:replay_file() line 138:
exploit_traffic.pcap was captured using a snaplen of 1518 bytes. This may mean you have truncated packets.
Warning in send_packets.c:send_packets() line 644:
Unable to send packet: Error with PF_PACKET send() [63]: Message too long (errno = 90)
Actual: 62 packets (6696 bytes) sent in 0.002390 seconds
Rated: 2801673.6 Bps, 22.41 Mbps, 25941.42 pps
Statistics for network device: eth0
    Successful packets:      62
    Failed packets:         1
    Truncated packets:     0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
root@kali:~# tcpreplay-edit -C -t -i eth0 user-agents.pcap
Warning in replay.c:replay_file() line 138:
user-agents.pcap was captured using a snaplen of 1518 bytes. This may mean you have truncated packets.
Actual: 40 packets (7248 bytes) sent in 0.001052 seconds
Rated: 6889733.8 Bps, 55.11 Mbps, 38022.81 pps
Statistics for network device: eth0
    Successful packets:      40
    Failed packets:          0
    Truncated packets:      0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
```

How do we know the IDS triggered any alerts?

- Suricata: /var/log/suricata/
 - eve.json
 - Massive JSON file that logs a boatload of stuff. Just not IDS events.
 - fast.log
 - Plaintext log file that contains just IDS alerts triggered. If this file is NOT 0 bytes in size, 99% chance you successfully triggered IDS events.
- Snort: /var/log/snort
 - Snort.u2.[epochtimestamp]
 - Unified2 files are binary.
 - Not human readable
 - Doesn't really matter. So long as the file is greater than 0 bytes in size, it saw SOMETHING.
 - Tip: /usr/src/snort*/tools/u2spewfoo
 - » U2spewfoo /var/log/snort/snort.u2.[epochTS]: read the contents of a unified2 file

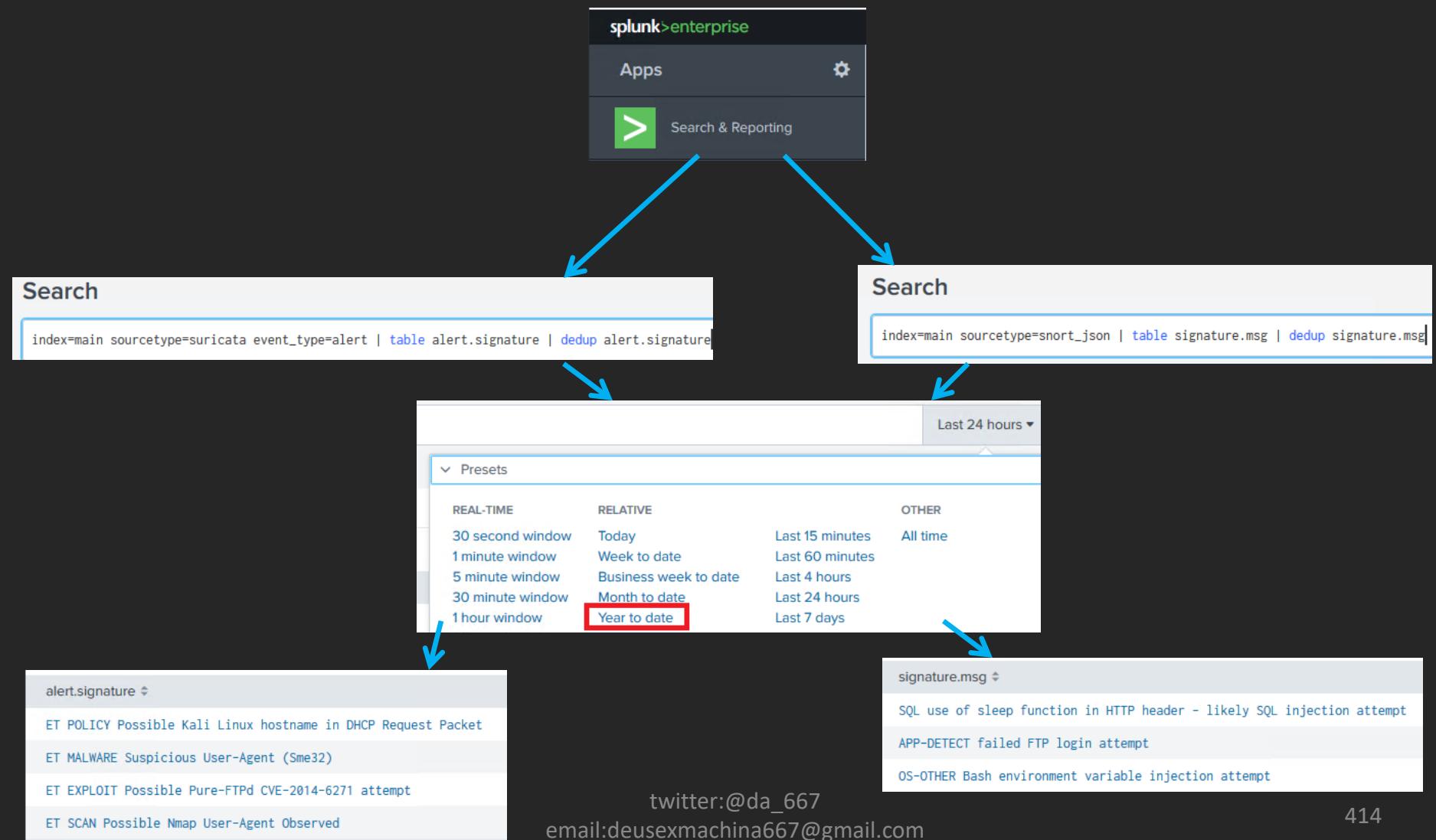
What if the IDS isn't triggering alerts?

- Start with the basics. Is snort/suricata even running?
 - We went over the commands to confirm this:
 - service snortd/suricatad status
 - ps -ef |grep snort, ps -ef | grep suricata
 - grep snort /var/log/syslog | less, grep suricata /var/log/syslog | less
 - Double check your virtual networking setup
 - Remember when I had you document what MAC addresses belonged to which VMs, and what virtual network segments they were connected to?
 - Verify that the interfaces you bridged on the IPS VM are connected to ‘intnet’ and ‘intnet1’
 - Verify that you configured promiscuous mode on the advanced virtual network adapter settings for the IPS VM (Either “allow all” or “allow VMs”)
 - Verify kali is connected to ‘intnet’
 - Verify metasploitable2 is connected to ‘intnet1’

How do I actually view IDS alerts on Splunk?

- On the hypervisor host, open a web browser and log into the SIEM vm on <https://172.16.1.3>
- Click on “Search & Reporting”
 - Snort: “index=main sourcetype=snort_json |table signature.msg | dedup signature.msg
 - Suricata: “index=main sourcetype=suricata event_type=alert | table alert.signature | dedup alert.signature
 - Not getting any data? Try changing the time period you are looking at. Change from “Last 24 hours” (default) to “Year to date”
 - Break-down of the query:
 - Index= Tells splunk what data index to look at. By default, Splunk provides the “main” index
 - Sourcetype= Tells splunk what data source we want to query specifically
 - “| table [field name]” = “take all of this output, and create a table with just these extracted field names
 - “| dedup [field name]” = “remove all duplicate data from the field name I specify”

How do I actually view IDS alerts on Splunk?



What do I do if there are no logs/results in Splunk?

- Did you open a TCP listener on the SIEM VM?
 - Should have opened a listener on port 9997/tcp
 - Open an SSH session to SIEM. Become root. Run:
 - Netstat –natp | grep 9997
 - Should be at least two entries one with state LISTEN and another with state ESTABLISHED from 172.16.1.4
 - Can also run this command on the IPS vm. Should be at least one entry with state ESTABLISHED to 172.16.1.3
 - If you see these entries, then at the very least, you configured the listener on SIEM correctly and added the forward-server on the IPS vm correctly
- Check /opt/splunk[forwarder]/var/log/splunk/splunkd.log
 - If theres an issue, its probably mentioned in this log
- Snort users: /opt/splunkforwarder/etc/apps/TA-unified2/default/inputs.conf and unfied2.conf should be doubled checked
 - inputs.conf needs disabled set to 0
 - unified2.conf needs to be pointing at the sid-msg.map gen-msg.map and classification.config in /opt/snort/etc
 - Make sure you specified the FULL, correct directory path
- Suricata users: /opt/splunkforwarder/etc/apps/TA-Suricata/default/inputs.conf should be double checked
 - The index should be main. If you have anything else here, the TA won't log anything

Chapter 14: Final Touches, Extra Content, and Ideas

Everything appears to be working...

- If everything seems to be working...
 - Snapshot all your VMs. A known/good baseline is very important.

What was the point of all this?

- This training was meant to provide you with a starting point.
 - Now you know how to:
 - Create VMs
 - Harden them
 - Perform proper network segmentation
 - Configure secure remote access
 - Configure baseline snapshots
- “Give a man a fish, he eats for a day. Teach a man to fish, and he can sustain himself for a lifetime.”
- You have the knowledge and power to modify your lab however you see fit now.
 - Don’t like Ubuntu? Use whatever distro you like.
 - Don’t like Linux at all? Run BSD (Or Solaris for all I care).
 - Don’t like pfSense? OPNSense, Vyatta, Ipfire, etc. Are all alternatives.
 - Don’t want to use an IDS/IPS? Try bridge-utils.
 - Don’t like Splunk? Try out ELK, Graylog, etc.

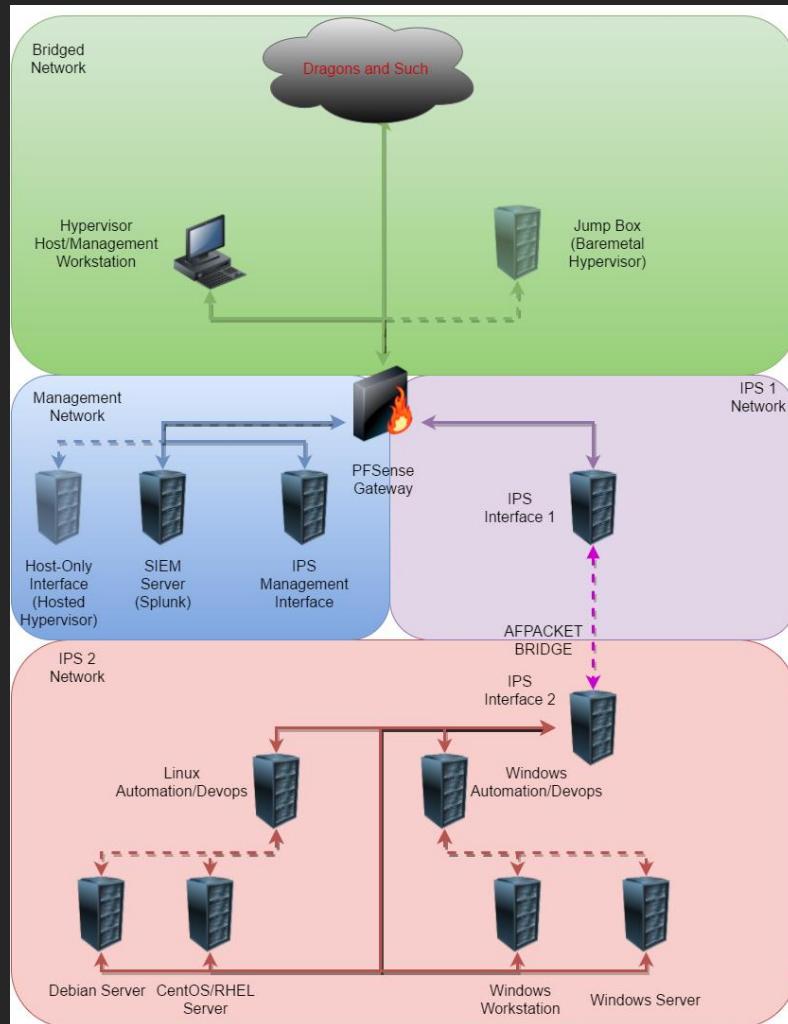
Tasks to Perform

- Alternate network diagrams
 - To suit your learning needs
- Study/Training materials
 - TONS of free resources you can use to shore up your knowledge.
- Extra Credit: Little things you can do to improve your lab
 - NTP
 - We set up an NTP server on our pfSense server. How can we configure our lab VMs to use it? How do I fix apt-get errors after reverting to a snapshot (ntp/ntpdate)
 - Update automation
 - /etc/cron.[hourly/daily/weekly], /etc/crontab, and the updater script for SIEM, IPS and kali
 - Snort users: idstools-u2json
 - TA-unified2 is written in python2.7. Python 2.7 is EOL in 2020. Lets look at deploying an alternative
 - Using Windows Firewall or IPTABLES to enforce network segmentation between the hypervisor host and VM lab
 - With the right firewall rules, you can configure your host-only NIC to only allow outbound connects to your lab environment but deny ALL inbound connections to the host-only NIC/172.16.1.2
 - Sorry OSX users, but your firewall sucks.

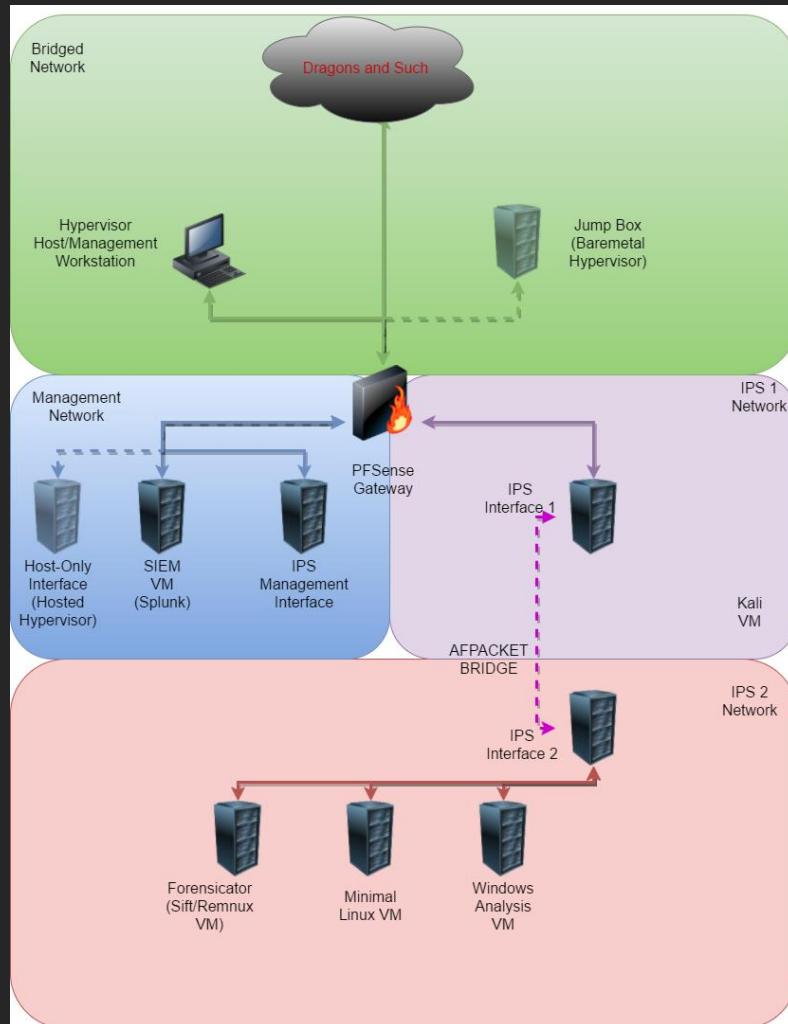
Alternate Network Diagrams

- Where do you go from here?
 - Wherever you want.
- Feel like adding vulnerable VMs and practicing redteam things? Cool
 - Check out vulhub.com for various “boot2root” vms with write-ups to follow
 - Check out modern.ie for free windows (7-10) VMs
 - Microsoft literally tells you to snapshot the VM on install, and revert it for unlimited trial periods on any of the VMs.
 - <https://www.microsoft.com/en-us/evalcenter/>
 - Need Windows Server VMs? Download an Eval here. Snapshot on install/revert the VM if you need more trial time.
- Feel like doing malware analysis things? Awesome
 - Check out Remnux and/or SIFT for a boatload of malware analysis and forensic tools.
- Feel like learning more about automation and devops things?
 - Run whatever VMs you feel like. Learn more about WSUS, SCCM, Ansible, Hashicorp tools, Docker/Kubernetes, etc.
- Here are some network diagrams to give you some ideas.
 - Wanna make your own network diagrams?
 - Draw.io

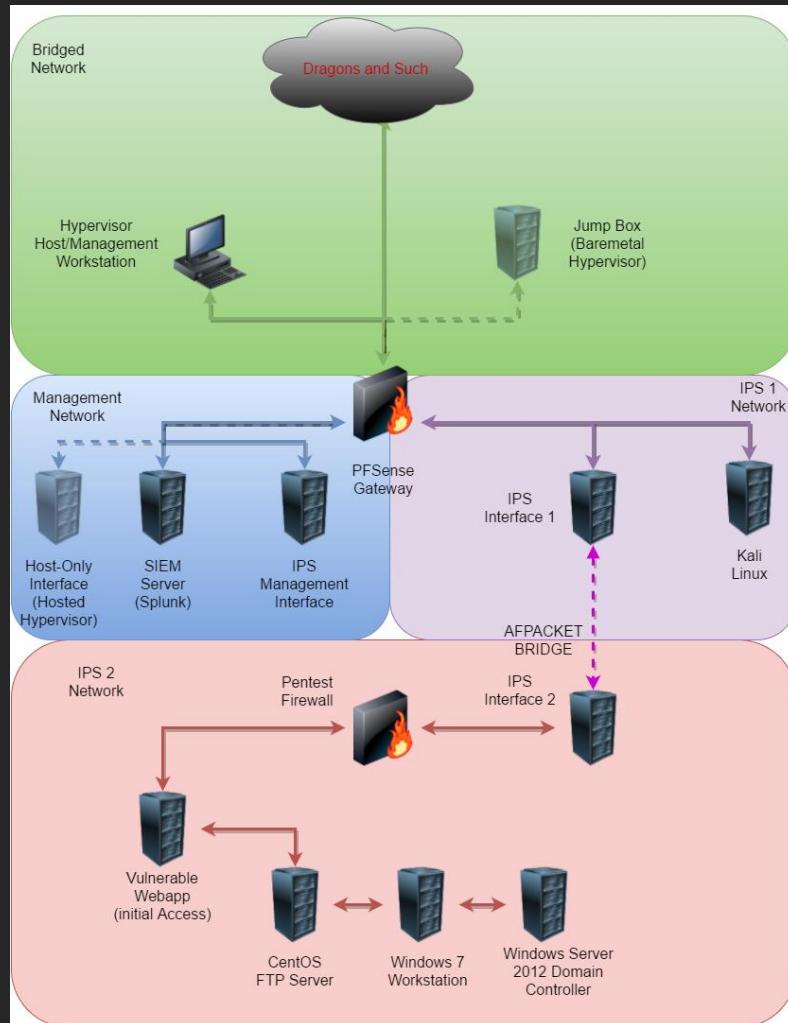
Alternate Network Diagrams (cont'd)



Alternate Network Diagrams (cont'd)



Alternate Network Diagrams (cont'd)



Study/Training Materials

- I wrote a thing:
 - <https://medium.com/@deusexmachina667/the-big-blog-post-of-information-security-training-materials-ad9572223fcd>
 - https://github.com/da667/Training_Materials_Bookmarks
 - Collection of free/freemium training materials broken into subcategories

Extra Credit - NTP

- Remember how we set up an NTP server on pfSense?
 - None of our Linux VMs are actually using it
- ntp: service can be pointed at pfSense to keep time synchronized.
- ntpdate: command that can be used to force the system clock to synchronize immediately with an NTP source

Extra Credit – NTP (cont'd)

- Install process: Identical for SIEM, IPS and Kali:
 - SSH/console session
 - Become root
 - apt-get –y install ntp ntpdate
 - Use a text editor to modify ntp.conf and change the “pool” entries to a single:
 - server 172.16.1.1 (IPS, SIEM)
 - server 172.16.2.1 (kali)
 - Save ntp.conf, run service ntp start

Extra Credit – NTP (cont'd)

- How to use ntpdate:
 - Login to SIEM/IPS/Kali
 - Become root
 - If ntp is running: service ntp stop
 - ntpdate 172.16.1.1 (SIEM/IPS)
 - ntpdate 172.16.2.1 (kali)
 - service ntp start
- Note: you don't have to install ntp, you can just use ntpdate to force a clock sync. Simply apt-get -y install ntpdate
- What do I do if I had to revert pfSense and its time is off?
 - Wait for the ntp service to eventually correct it

Extra Credit - NTP



Extra Credit – Update Automation

- Wouldn't it be neat if your Linux VMs kept themselves up to date?
 - <https://gist.github.com/da667/20f1c67c264f7823c7139f5c835a7026>
 - updater: Runs apt-get update and upgrade with no user interaction required, logs that the script ran to /var/log/syslog, reboots the system after running (to apply kernel updates, if any)
 - We'll be using run-parts (/etc/cron.[daily,weekly,monthly]) and /etc/crontab to run this script on regular intervals.
 - IPS and SIEM: we'll be using run-parts
 - Kali: like with most things, kali has to be difficult and we'll be using /etc/crontab
 - Recommendation: configure to run once weekly, but if you wanna go daily or monthly, that's up to you.

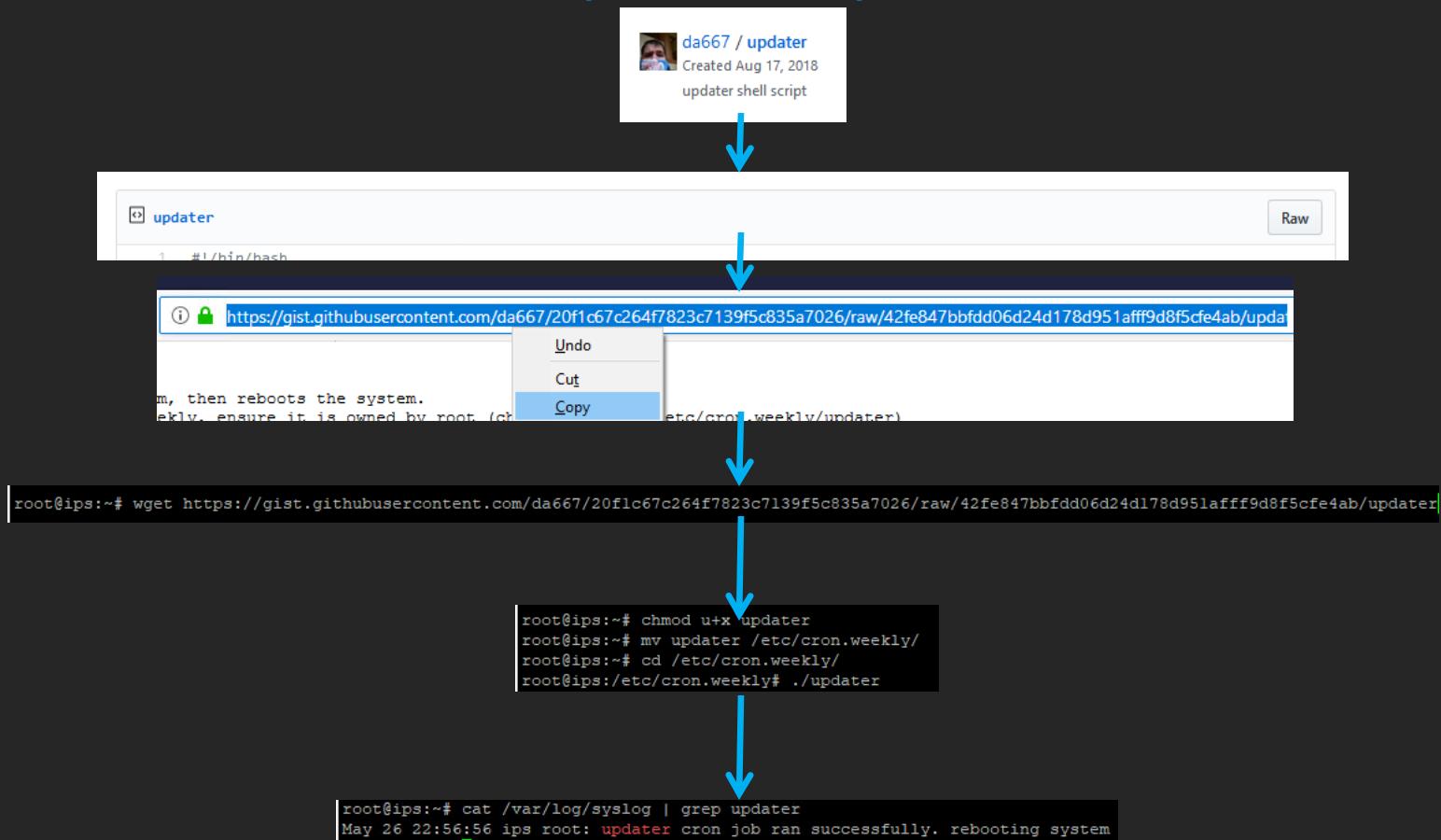
Extra Credit – Update Automation (cont'd)

- How to configure:
 - On hypervisor host, open your web browser, visit <https://gist.github.com/da667/20f1c67c264f7823c7139f5c835a7026>
 - Click the button labeled “Raw”
 - On the raw script page, click/highlight the entire browser URL → right click → copy
 - Open an SSH session to SIEM, IPS, or Kali
 - Become root (if you aren't root already)
 - wget [paste url here]

Extra Credit – Update Automation (cont'd)

- Chmod u+x ~ updater
- IPS, SIEM: mv ~ updater /etc/cron.weekly
- Kali:
 - mkdir ~ systemscripts
 - mv ~ updater ~ systemscripts
 - vi /etc/crontab
 - Tip: crontab.guru
 - Use this website to help you validate your cron jobs
 - We'll be adding a job to run the script once weekly on Monday at 9am
 - » 9am on Monday doesn't work for you? Use crontab.guru to choose another time.
 - 09 * * 1 root /root/systemscripts/updater
- Tip: wanna see when cron.weekly is going to run?
 - cat /etc/crontab. Look for "run-parts –report /etc/cron.weekly"
 - Don't want updater to run at that time?
 - You can install a cron job on SIEM and/or IPS just like you did on kali if you don't like when cron.[daily/weekly/monthly] runs its scripts

Extra Credit – Update Automation (cont'd)



Extra Credit – Update Automation (cont'd)

“At 09:00 on Monday.”

next at 2019-05-27 09:00:00

0 9 * * 1

minute hour day month day
(month) (month) (week)

- * any value
- ,
- range of values
- / step values
- @yearly (non-standard)
- @annually (non-standard)
- @monthly (non-standard)
- @weekly (non-standard)
- @daily (non-standard)
- @hourly (non-standard)
- @reboot (non-standard)

```
root@kali:~# mkdir ~/systemscripts
root@kali:~# chmod u+x updater
root@kali:~# mv ~/updater ~/systemscripts/
root@kali:~# vi /etc/crontab
```



```
0 9 * * 1 root /root/systemscripts/updater
```

Extra Credit – u2json

- This exercise is for those who chose to run Snort.
- Remember how I mentioned python2 is EOL in 2020?
 - TA-unified2 runs on python2. So this is a problem
- Idstools-u2json
 - More or less the same thing, just not in a pretty pre-packaged splunk app.

Extra Credit – u2json

- How to install:
 - SSH to the IPS VM and become root
 - Apt-get –y install python3-pip
 - Pip3 install idstools

Extra Credit – u2json

```
root@ips:~# apt-get -y install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
```



```
root@ips:~# pip3 install idstools
Collecting idstools
  Downloading https://files.pythonhosted.org/packages/
    100% |████████████████████████████████| 71kB 1.5s
Building wheels for collected packages: idstools
  Running setup.py bdist_wheel for idstools ... done
  Stored in directory: /root/.cache/pip/wheels/49/2a/
Successfully built idstools
Installing collected packages: idstools
Successfully _installed idstools-0.6.3
```

Extra Credit – u2json

- Okay, so we installed this, now how do we actually use it?
 - By committing a mortal sin: creating a systemd service
 - vi /etc/systemd/system/u2json.service
 - [Unit]
 - Description=Daemonizing idstools-u2json to parse unified2 files for SIEM integration
 - [Service]
 - ExecStart=/usr/local/bin/idstools-u2json --snort-conf /opt/snort/etc/snort.conf --directory /var/log/snort --prefix snort.u2 --follow -bookmark /var/log/snort/u2json.bookmark --delete --output /var/log/snort/alerts.json
 - [Install]
 - WantedBy=multi-user.target
 - chmod 700 /etc/systemd/system/u2json.service
 - systemctl daemon-reload
 - systemctl enable u2json.service
 - service u2json start
 - service u2json status

Extra Credit – u2json

```
root@ips:~# cd /etc/systemd/system/  
root@ips:/etc/systemd/system# vi u2json.service
```



```
[Unit]  
Description=Daemonizing idstools-u2json to parse unified2 files for SIEM integration  
  
[Service]  
ExecStart=/usr/local/bin/idstools-u2json --snort-conf /opt/snort/etc/snort.conf --directory /var/log/snort --prefix snort.u2 --follow --bookmark /var/log/snort/u2json.bookmark  
--delete --output /var/log/snort/alerts.json  
  
[Install]  
WantedBy=multi-user.target
```



```
root@ips:/etc/systemd/system# chmod 700 /etc/systemd/system/u2json.service  
root@ips:/etc/systemd/system# systemctl daemon-reload  
root@ips:/etc/systemd/system# systemctl enable u2json.service  
Created symlink /etc/systemd/system/multi-user.target.wants/u2json.service → /etc/systemd/system/u2json.service.  
root@ips:/etc/systemd/system# service u2json start  
root@ips:/etc/systemd/system# service u2json status  
● u2json.service - Daemonizing idstools-u2json to parse unified2 files for SIEM integration  
  Loaded: loaded (/etc/systemd/system/u2json.service; enabled; vendor preset: enabled)  
  Active: active (running) since Tue 2019-05-28 02:31:41 UTC; 5s ago  
    Main PID: 2242 (idstools-u2json)  
      Tasks: 1 (limit: 2319)  
     CGroup: /system.slice/u2json.service  
             └─2242 /usr/bin/python3 /usr/local/bin/idstools-u2json --snort-conf /opt/snort/etc/snort.conf --directory  
  
May 28 02:31:41 ips systemd[1]: Started Daemonizing idstools-u2json to parse unified2 files for SIEM integration.  
May 28 02:31:41 ips idstools-u2json[2242]: INFO: Loaded 37696 rule message map entries.  
May 28 02:31:41 ips idstools-u2json[2242]: INFO: Loaded 38 classifications.
```

twitter:@da_667

email:deusexmachina667@gmail.com

Extra Credit – u2json

- Okay, what the hell was all of that?
 - We created u2json.service
 - Describe the service ([Unit] - Description)
 - Tell me what command and options to run when you want me to start it ([Service] - ExecStart)
 - When should I run it ([Install] - WantedBy)
 - /usr/local/bin/idstools-u2json --snort-conf /opt/snort/etc/snort.conf --directory /var/log/snort --prefix snort.u2 --follow --bookmark /var/log/snort/u2json.bookmark --delete --output /var/log/snort/alerts.json
 - --snort-conf: where can I find the snort.conf file? Assumes that the sid-msg.map, gen-msg.map and classification.config are in the same directory.
 - --directory: “look in this directory for unified2 files”
 - --prefix: “The unified2 files should start with this in their filename”
 - --follow: run continuously (e.g. Daemonize)
 - --bookmark: “This file contains the last event I processed, and where I should leave off when I begin processing again later”
 - --delete: delete old unified2 files
 - --output: where should I dump the processed JSON file?

Extra Credit – u2json

- We're generating JSON files, now how do I get them to the SIEM VM?
- You still have a root shell on the IPS VM, right?
- First, let's nuke the TA-unified2 install. We're done with it.
 - `rm -rf /opt/splunkforwarder/etc/apps/TA-unified2`
- Next, we have to create an inputs.conf file in
`/opt/splunkforwarder/etc/system/local`
 - `vi /opt/splunkforwarder/etc/system/local/inputs.conf`
 - [default]
 - host = ips
 - [monitor:///var/log/snort/*.json]
 - disabled = false
 - sourcetype = u2json_log
 - index = main
- Now, restart the forwarder.
 - `cd /opt/splunkforwarder/bin`
 - `./splunk restart`

Extra Credit – u2json

```
root@ips:~# rm -rf /opt/splunkforwarder/etc/apps/TA-unified2  
root@ips:~# vi /opt/splunkforwarder/etc/system/local/inputs.conf
```



```
[default]  
host = ips  
  
[monitor:///var/log/snort/*.json]  
disabled = false  
sourcetype = u2json_log  
index = main
```



```
root@ips:~# cd /opt/splunkforwarder/bin/  
root@ips:/opt/splunkforwarder/bin# ./splunk restart  
Stopping splunkd...  
Shutting down. Please wait, as this may take a few minutes.  
  
Stopping splunk helpers...  
  
Done.
```

Extra Credit – u2json

- Now to test things.
- Take a moment and generate some alerts from the kali VM
 - Use any of the methods we talked about earlier.
- Come back to the IPS VM
 - ls –al /var/log/snort/*.json
 - Does alerts.json exist? Is it larger than 0bytes?
 - If so, then we know that u2json is doing its job. If not..
 - Check to see if the service is running
 - Confirm all of the command options are correct
 - » Note: if you have to modify the u2json.service file, you have to run:
 - systemctl daemon-reload
 - service u2json stop
 - service u2json start
 - Login to the search head on the SIEM VM (<https://172.16.1.3>)
 - Search & Reporting
 - index=main sourcetype=u2json_log
 - index=main sourcetype=u2json_log type=event | table event.msg | dedup event.msg
 - You can use this query once it extracts fields for the data it has processed.

Extra Credit – u2json

```
root@ips:~# ls -al /var/log/snort/*.json  
-rw-r--r-- 1 root root 373308 May 28 03:16 /var/log/snort/alerts.json
```



```
index=main sourcetype=u2json_log type=event | table event.msg | dedup event.msg
```



```
event.msg ♦  
  
MALWARE-TOOLS Havij advanced SQL injection tool user-agent string  
SQL use of sleep function in HTTP header - likely SQL injection attempt  
ftp_pp: FTP parameter length overflow  
OS-OTHER Bash environment variable injection attempt  
OS-WINDOWS Microsoft Windows SMB remote code execution attempt  
APP-DETECT failed FTP login attempt
```

Extra Credit – u2json

- What do I do if splunk isn't seeing events?
 - Check
`/opt/splunkforwarder/etc/system/local/inputs.conf`
 - Make sure you input everything EXACTLY as demonstrated
 - Check
`/opt/splunkforwarder/var/log/splunk/splunkd.log`
 - Adjust the timeframe from 24 hours to Year to date

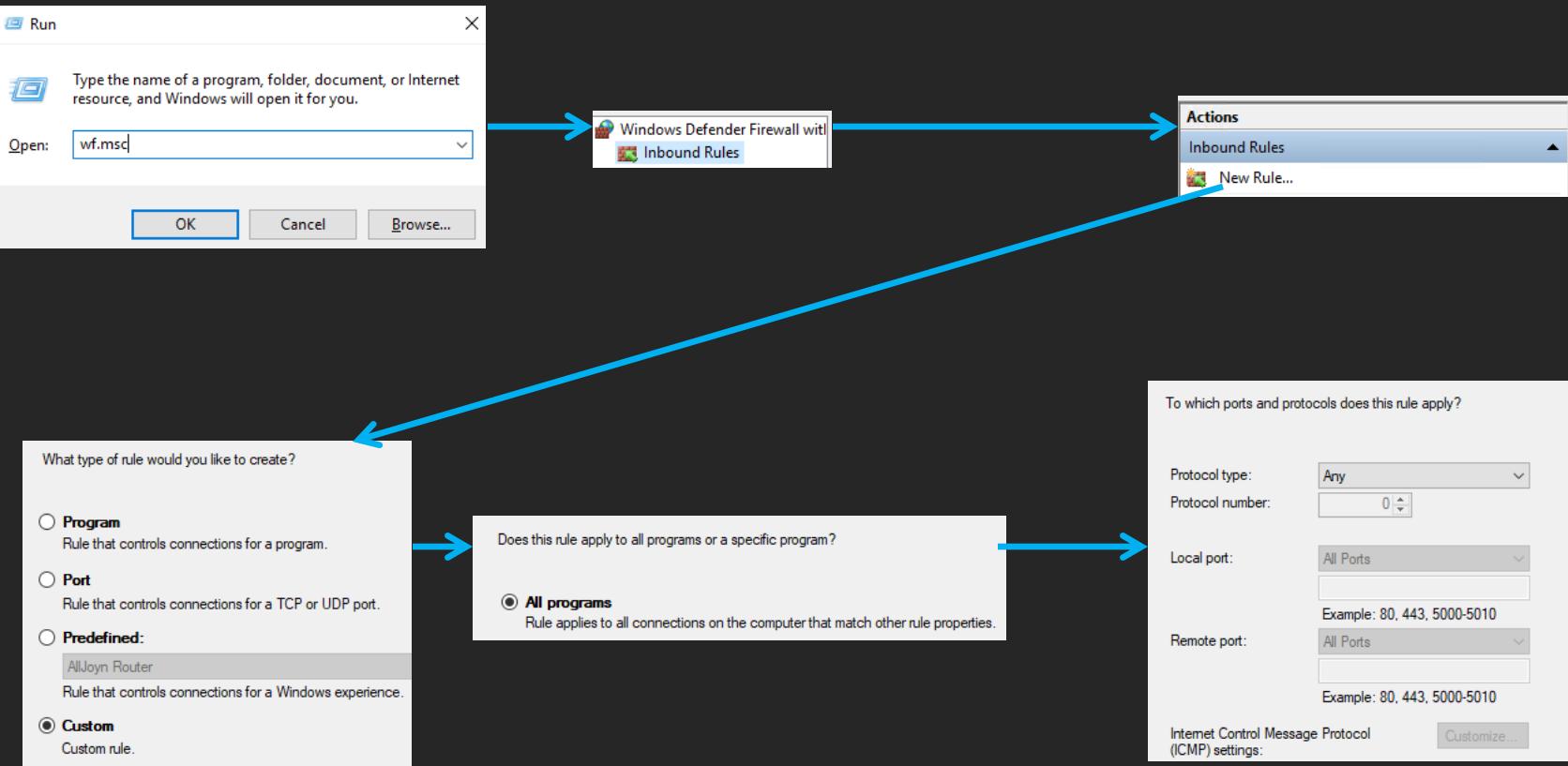
Extra Credit – Hypervisor host firewall

- pfSense provides network segmentation and security, but having another layer of defense doesn't hurt
 - What we'll be doing:
 - Creating firewall rules that deny all traffic inbound from 172.16.1.0/24 and 172.16.2.0/24
 - Windows : Windows Firewall with Advanced Security (wf.msc)
 - Linux: iptables-persistent
 - OSX: You guys are boned
 - » Technically, /etc/pf.conf is there
 - Even if enabled, on reboot, the firewall is gone
 - Need to set up a launchd service to persist it.
 - /etc/pf.conf will be overwritten on new OSX releases.
 - Buy commercial firewall software. Pray for Apple's swift demise.
 - murusfirewall.com
 - Little Snitch
 - Allegedly ESET firewall is good

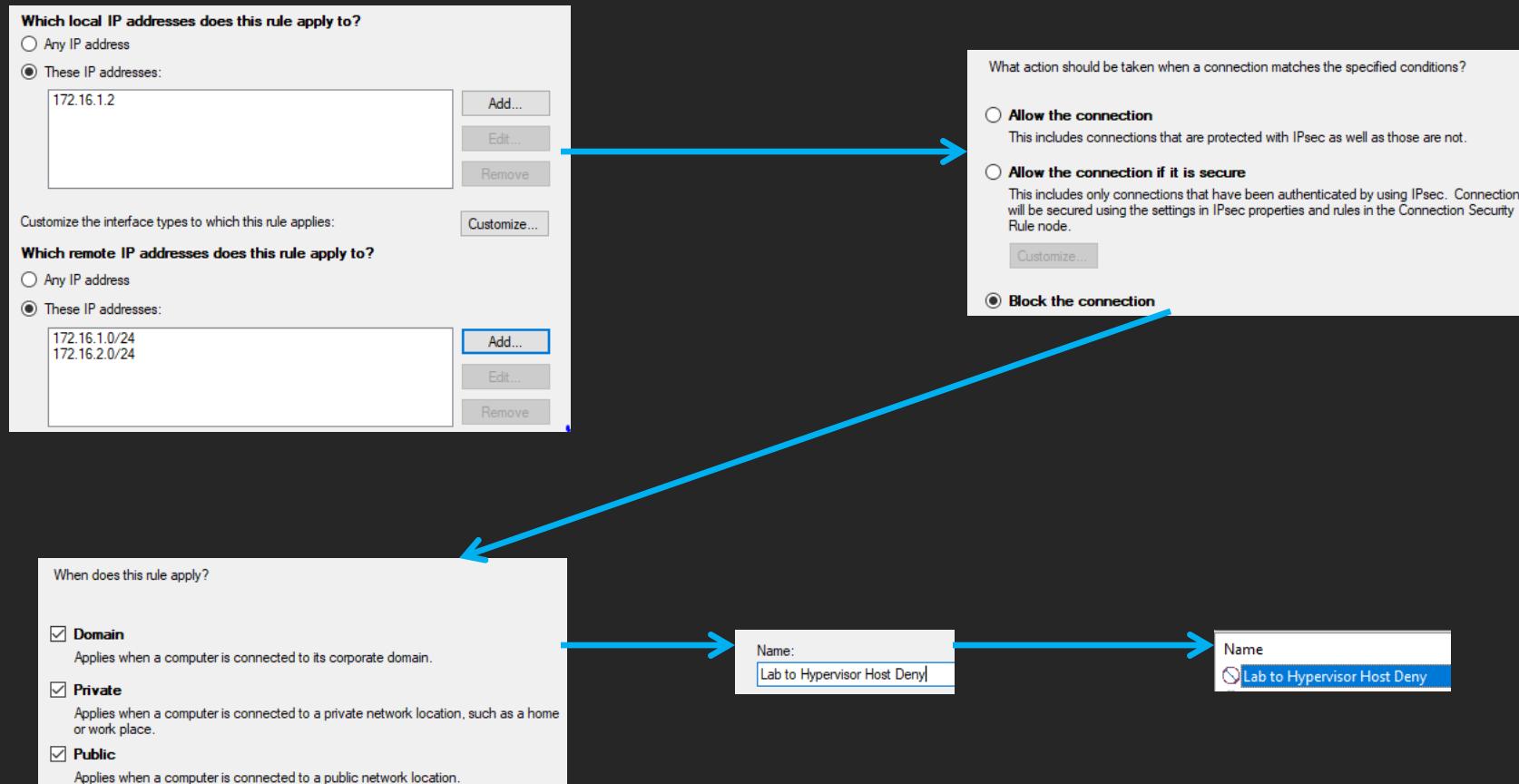
Extra Credit – Hypervisor host firewall (cont'd)

- Windows:
 - Start → Run → wf.msc → Inbound Rules → New Rule... (under Actions)
 - Rule Type: Custom
 - All Programs
 - Protocol Type: Any
 - Which local IP addresses does this rule apply to?
 - These IP addresses:
 - » 172.16.1.2
 - Which remote IP addresses does this rule apply to?
 - These IP addresses:
 - » 172.16.1.0/24
 - » 172.16.2.0/24
 - Block the connection
 - When does this rule apply?
 - Domain
 - Private
 - Public
 - Name: Lab to Hypervisor Host Deny

Extra Credit – Hypervisor host firewall (cont'd)



Extra Credit – Hypervisor host firewall (cont'd)



Extra Credit – Hypervisor host firewall (cont'd)

- Linux:
 - Login as root or sudo to root on your hypervisor host.
 - apt-get install iptables-persistent
 - The installer asks if you want to save your current firewall rules (if you have any)
 - Note: If you use firewalld or ufw, then god help you. I'm only covering iptables.
 - Note: If you use a distro that is not debian-based, you need to determine how to install/enable iptables for your distro
 - E.g. CentOS/RHEL: <https://serverfault.com/questions/626521/centos-7-save-iptables-settings>
 - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
 - “Allow packets from ESTABLISHED connections”
 - iptables -A INPUT -s 172.16.1.0/24 -j DROP
 - Drop connections from source network 172.16.1.0/24
 - iptables -A INPUT -s 172.16.2.0/24 -j DROP
 - Drop connections from source network 172.16.2.0/24
 - iptables-save > /etc/iptables/rules.v4
 - Save the current iptables rules to /etc/iptables/rules.v4

Extra Credit – Hypervisor host firewall (cont'd)

```
root@potato:~# apt-get -y install iptables-persistent
```



```
root@potato:~# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
root@potato:~# iptables -A INPUT -s 172.16.1.0/24 -j DROP
root@potato:~# iptables -A INPUT -s 172.16.2.0/24 -j DROP
root@potato:~# iptables -n -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source          destination
      0     0 ACCEPT     all  --  *       *       0.0.0.0/0        0.0.0.0/0          ctstate RELATED,ESTABLISHED
      0     0 DROP       all  --  *       *       172.16.1.0/24   0.0.0.0/0
      0     0 DROP       all  --  *       *       172.16.2.0/24   0.0.0.0/0
```



```
root@potato:~# siem
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-50-generic x86_64)
```

```
ayy@siem:~$ ssh ayy@172.16.1.11
```



```
12    804 DROP      all  --  *       *       172.16.1.0/24   0.0.0.0/0
```



```
root@potato:~# iptables-save >/etc/iptables/rules.v4
```

WE DONE HERE.

- Wanna tell me how much my class sucked?
 - Fill out this google form. I want your feedback:
 - <https://forms.gle/ALVYgqwogN5jCjyc8>
- Wanna give me money?
 - paypal.me/da667
 - Will probably go towards my cocaine coffee addiction

Just kidding...

- With thanks to:
 - @munin, for saying “you should submit something for CCC.”
 - Circle City Con, for organizing this event and hosting me. This con gets better every year.
 - Hurricane Labs, my employer.
 - This is the only company name-drop in this slide deck.
 - You want an MSSP that does kick-ass things with Splunk? Hire us, or at least check out our blog to learn a bunch of cool shit.
 - YOU! If you hadn’t registered for this class, I would’ve been drinking mead.
 - Not such a bad fate, really.