Networking

Michael Morgenthal, Ruben Ocana

Introduction

- Senior, Computer Engineering Major
- Took Systems Security last Semester (Spring 2020)
- This is my first time TA'ing for Syssec, but I've worked as a TA for the past 3 years for:
  - CSE 191 - Discrete Structures
  - CSE 199 - Freshmen Seminar

Michael Morgenthal

mmorgent@buffalo.edu
mmorgent (Mattermost)

Introduction

- Second Year MS MIS
- Took SysSec and NetSec 2019
- First time officially doing SecDev!
- Volunteered in multiple events (High School & UB Lockdown, GenCyber Camp)

rubenoca@buffalo.edu
ruben_ocana (Mattermost)

Welcome

Format of Tonight's Lecture:

- Why is this Week's Material Important?
- Overview of Homework Format
- Setup of Virtual Machine for Homework
- Introduction to Networking
  - Our Networking Infrastructure
- What is PfSense?

Why is this Week's Material Important?

Why is this Week's Material Important?

- Infrastructure designed in this homework will be used in **EVERY** future assignment
- You will be setting up the internet connection each virtual machine will link to.

Goal of this Week

- We want you to get **full credit** on this assignment, so that next week won't be "catch-up" work
- **Proper formatting** of the homework will is as important as the assignment itself
- Let's go over formatting...

Overview of Homework Format

Overview of Homework Format

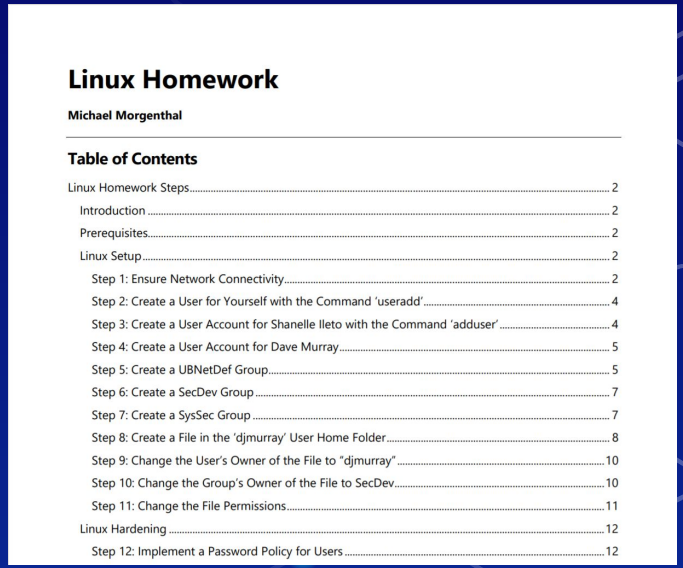
- Formatting of this week's assignment will be very important.
  - Its template will be followed for most future assignments.

Overview of Homework Format

- Table of Contents
- Short Introduction of Assignment
- Prerequisites
- Assignment Itself
  - Headers for Each HW Section
  - All Necessary Screenshots
  - Highlight Important Information
- Cite all Outside Sources Used

HW Format - Table of Contents

- Add each section of the homework to the TOC
- Include Page Numbers
- *Using Headers in Word makes creating a TOC much easier



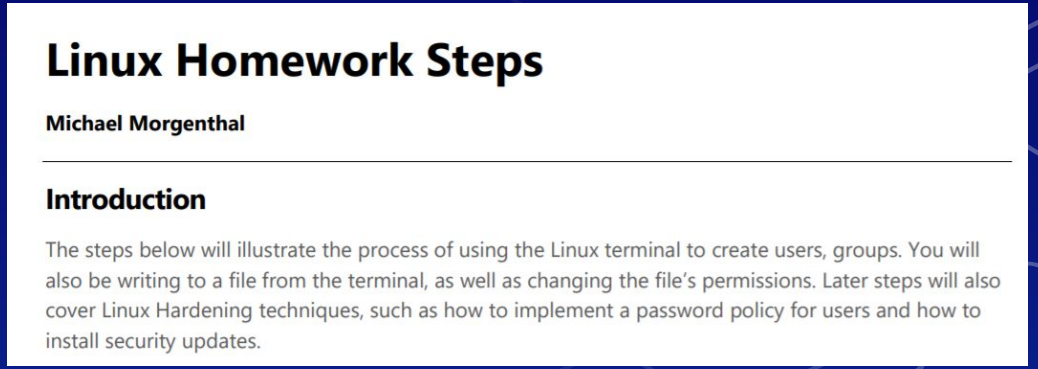
Linux Homework

Michael Morgenthal

Table of Contents

HW Format - Short Introduction

- Summarize the objective of the assignment in 3-5 sentences.



Linux Homework Steps

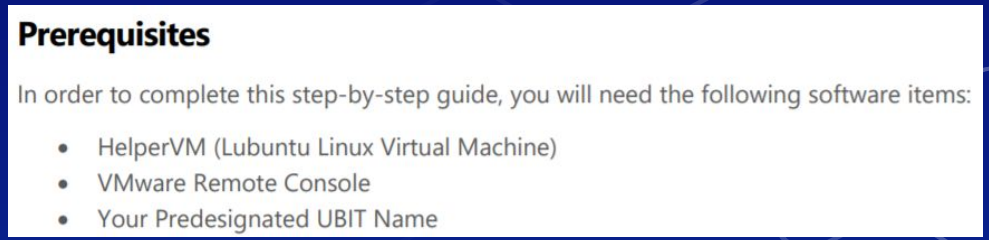
Michael Morgenthal

Introduction

The steps below will illustrate the process of using the Linux terminal to create users, groups. You will also be writing to a file from the terminal, as well as changing the file's permissions. Later steps will also cover Linux Hardening techniques, such as how to implement a password policy for users and how to install security updates.

HW Format - Prerequisites

- List everything used for the HW, including:
  - VMWare Remote Console
  - Virtual Machines
  - UBIT Names
  - *Etc.*



Prerequisites

In order to complete this step-by-step guide, you will need the following software items:

- HelperVM (Lubuntu Linux Virtual Machine)
- VMware Remote Console
- Your Predesignated UBIT Name

HW Format - Assignment Steps

- **Label each section and step** for completing the HW
- **Include ALL relevant screenshots**
  - Use judgement for relevance
- **Highlight credentials** and important information
- Include Page Numbers

Linux Setup

Step 1: Ensure Network Connectivity

Before starting this assignment, you first need to check if the virtual machine has internet access. We will check using both the terminal and Mozilla Firefox.

If prompted, login to the HelperVM with the following credentials:

User name: **sysadmin**

Password: **changeme**

1.1 Check Using the Terminal

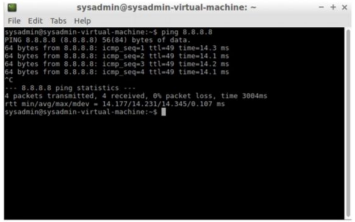
You will first need to open the terminal. You can find it by clicking the blue icon in the lower-left corner of the screen. Highlight the "System Tools" folder, and click the "LXTerminal" option that appears in the popup menu.

2

Type the following command into the terminal:

ping 8.8.8.8

This will continuously check if your virtual machine has a connection to the internet. To stop this process, hit the 'Control' key and the 'C' key simultaneously.



HW Format - Bibliography

- **Cite all outside sources** used to complete the assignment
  - APA Format
  - Internal Citations Needed
  - Attached Bibliography Needed

A virtual machine is "a software computer that, like a physical computer, runs an operating system and applications. (vSphere 5 Documentation Center, n.d.)" In this project, we will be setting up pfSense, "an

Bibliography

Merriam-Webster. (n.d.). *IP address*. Retrieved from Merriam-Webster.com dictionary: https://www.merriam-webster.com/dictionary/IP%20address

Merriam-Webster. (n.d.). *Local area network*. Retrieved from Merriam-Webster.com dictionary: https://www.merriam-webster.com/dictionary/local%20area%20network

Merriam-Webster. (n.d.). *Wide area network*. Retrieved from Merriam-Webster.com dictionary: https://www.merriam-webster.com/dictionary/wide%20area%20network

pfsense. (2020). Retrieved from pfsense: https://www.pfsense.org/

Rouse, M. (2019, November). *DMZ (networking)*. Retrieved from TechTarget.

vSphere 5 Documentation Center. (n.d.). Retrieved from vmware: https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-CEFF6D89-8C19-4143-8C26-4B6D6734D2CB.html

HW Format - Other Formatting Tips

- Not Required But May Help With Consistency
- Size 16-18 for Headers (Black Font)
- Size 12 for Regular Text (Dark Gray)
- Readable Font (i.e. Segoe UI)
- Smaller Screenshots so HW isn't 50+ pages

Setup HW Virtual Machines

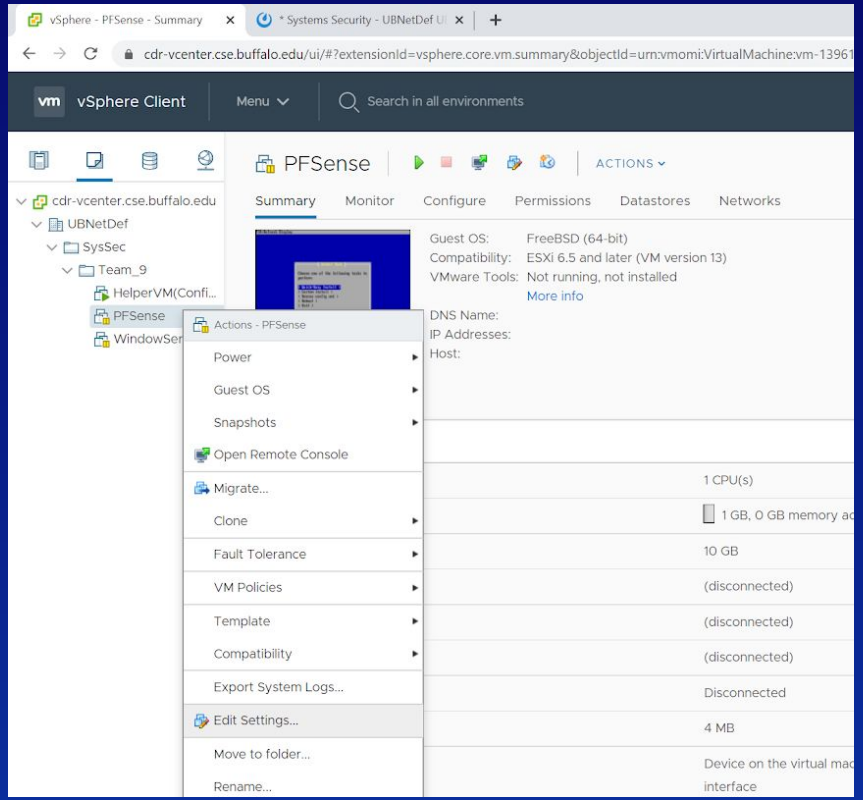
Setup HW Virtual Machines

- We will be using 2 virtual machines in this HW:
  - **PfSense**
  - **StudentVM**
- The following setup might be initially confusing, but we'll explain everything step-by-step and in the proceeding slides

Setup HW Virtual Machines

- Visit “**cdr-vcenter.cse.buffalo.edu**”
- **Login with your credentials** as you had done last class.

Setup HW Virtual Machines



NEXT,

Find the list item within the popup that says “CD/DVD drive 1”.

Check the box that says “Connect at Power On”.

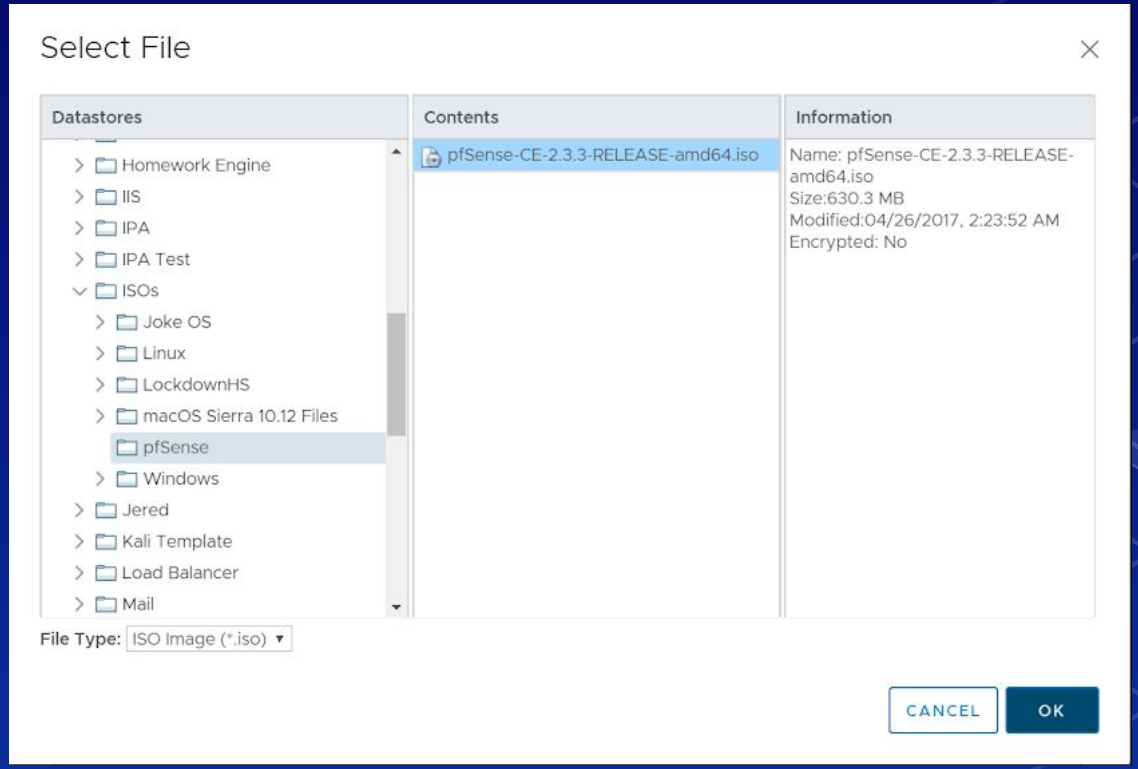
Click the dropdown menu and select “Datastore ISO File”, then click the “Browse…” button beneath it.

Locate the menu item “ISOs” within the vertical panel on the left-most side of the popup window.

Expand the folder and click the contained folder “pfSense”. A single item should now appear in the “Contents” panel shown in the center vertical column. Click this item and press “OK”.

(Image of these steps shown on next slide.)

Setup HW Virtual Machines



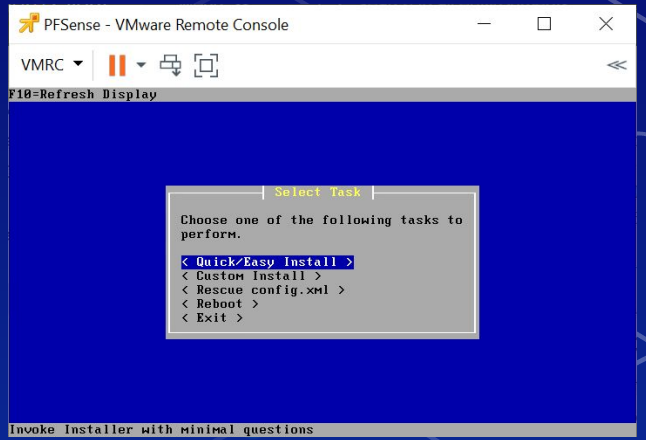
Setup HW Virtual Machines - Review

- The PfSense VM in vCenter originally had nothing attached to it
  - If opened, you would have seen a black screen
- To fix this problem, we adjusted the settings of this VM by adding a PfSense iso file to it

Setup HW Virtual Machines - Next Steps

- Click the **green play-shaped button** to run the PFSense virtual machine.
- Press the “**Launch Web Console**” button
  - Or if you have VMware installed:

    Press the “Launch Remote Console” button, and click the popup option titled “Open VMware Remote Console”.

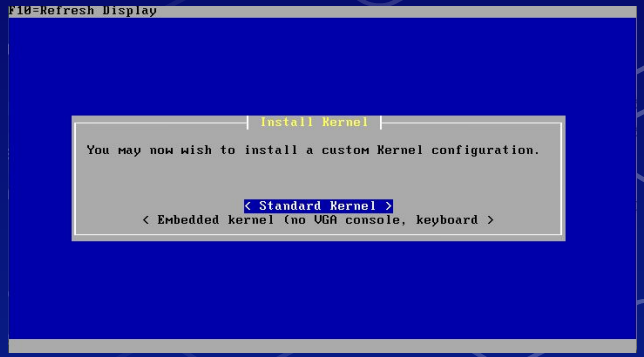


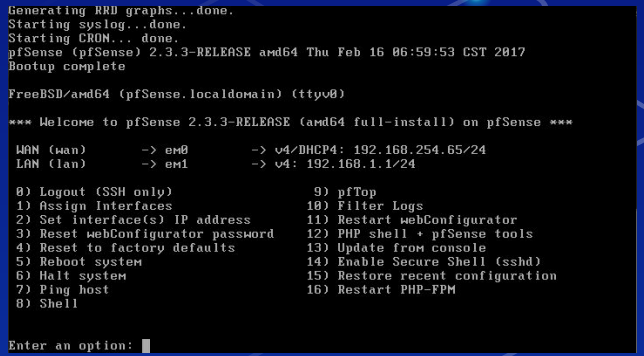
Setup HW Virtual Machines - Next Steps

- ** To make your mouse reappear, press **Ctrl** + **Alt** keys **
- Press the **Enter** key while highlighting the “**Quick/Easy Install**” option
- Next, choose the “**Standard Kernel**” option

Setup HW Virtual Machines - Next Steps

- Wait for the load screen to finish
  - Do **NOT** press cancel
- Let the VM reboot on its own
  - Do **NOT** press anything until you are presented with a black screen like the following:





Introduction to Networking

What is Networking?

- The connection between two or more devices
- This connection involves both the sending and receiving of data (packets)

The Internet

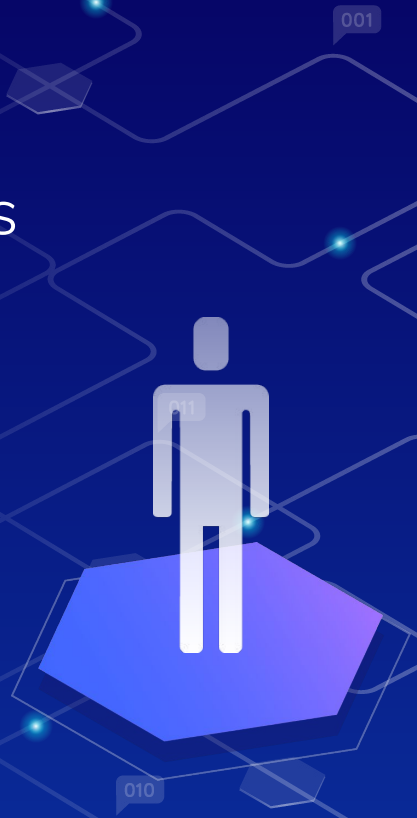
- Governed by a series of protocols that together form the laws for communication between devices
- In other words, it's a vast network comprised of billions of other smaller networks
- Devices communicate over the internet by sending one packet of information from one section of the internet to another

Servers

- Computers or programs that can manage access to a centralized resource or service on a network.
- Their purpose is to store information and manage network resources
- Used for websites, SQL databases, virtualization, AD, emailing, remote printing, etc.

Clients / Endpoints

- Computers or programs that send requests for data to another device/program (i.e. servers)
  - Smartphones, Tablets, PCs
- These clients are connected to a network (LAN/WAN)



Common Network Devices

Network Switches

Routers

Wireless Access Points

Firewalls

Networking Switches

- Networking features that are used to connect devices on a computer network
- Two basic types of switches:
  - Unmanaged - plug-and-play, immutable
  - Managed - Can be configured locally or remotely

Routers

- Act as dispatchers, are responsible for sending and receiving packets to and from the internet
  - Analyzes necessary traffic
  - Chooses best route for traffic
  - Sends necessary data
- Routers allow all networked computers to share a single internet connection
- Some include features such as firewalls and VPNs

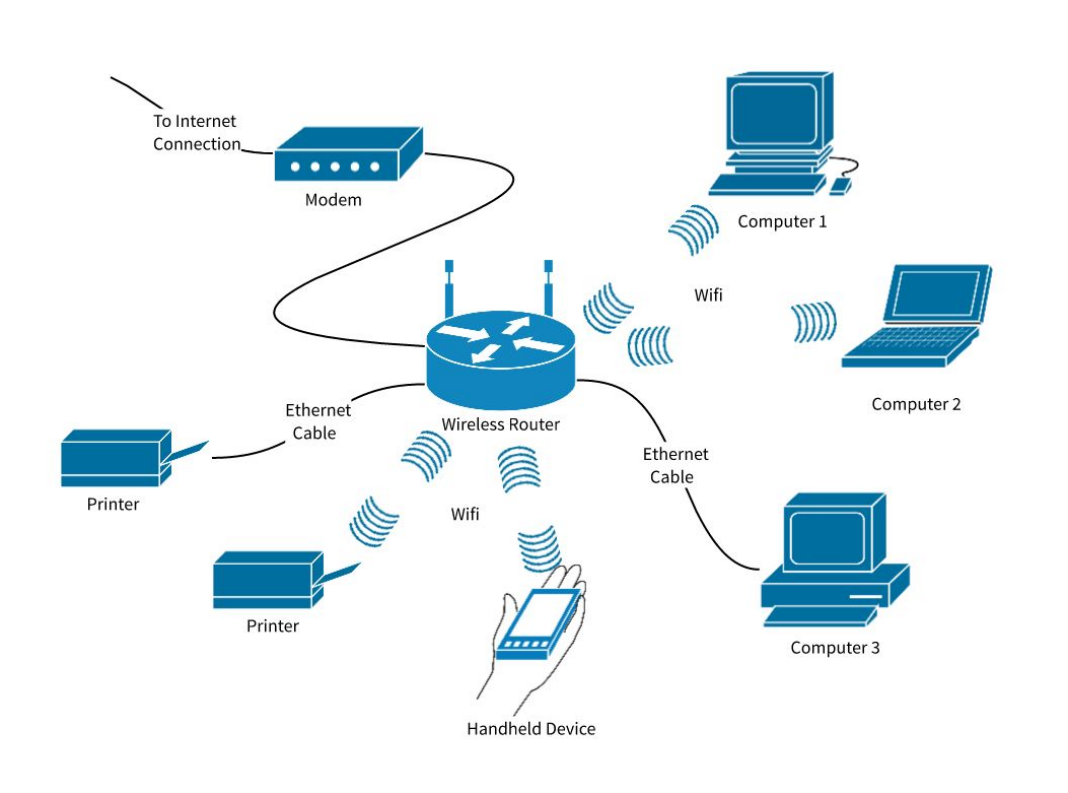
Wireless Access Points

- Include a radio transmitter capable of connecting devices wirelessly
- Removes the need for manual wired connections
- Expands the bandwidth a router provides
- Note: they are different from routers, merely additional points of contact for devices

Firewalls

- Used to secure traffic sent, and restricts traffic entering the network
- Only permits authorized traffic to pass through the network
- Can potentially alarm users of suspicious or unusual behavior
- Cannot be used to protect against internal threats (i.e. employees)

Network Diagram



Types of Networks (Interfaces)

LAN

WAN

DMZ

LAN

- Local Area Network
- LANs are the most fundamental type of network
- All devices on a shared LAN communicate directly across a switch
- These small basic networks are the building blocks of the internet

WAN

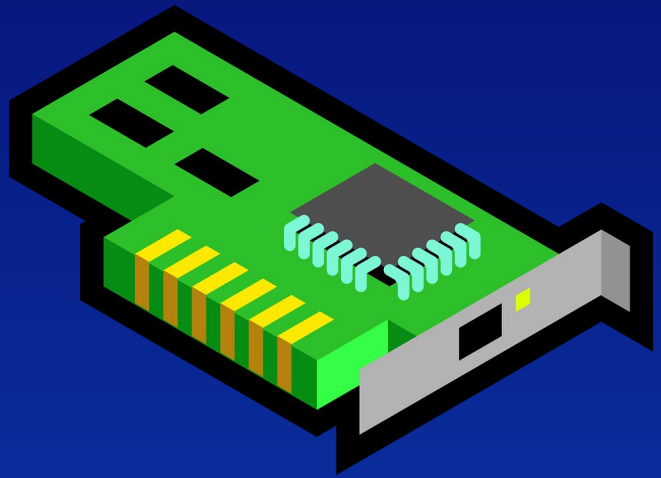
- Wide Area Network
- Consists of LANs that are all connected together
- Span a much larger area than LANs
  - The internet can be considered a WAN
- These LANs are connected together through the use of routers

DMZ

- Demilitarized Zone
- Physical or logical subnetwork that separates an internal LAN
- Allows specific resources to be accessible from the internet while the rest of the devices on the LAN are inaccessible

Network Interface Cards (NIC)

- Computers speak with each other through NICs (act as the mouth and ears)



MAC Addresses

- Act as the computer's name
- Encoded on the Network Interface Card (NIC)
- 48 bit addresses
  - Each character represents 4 bits (0 or 1)

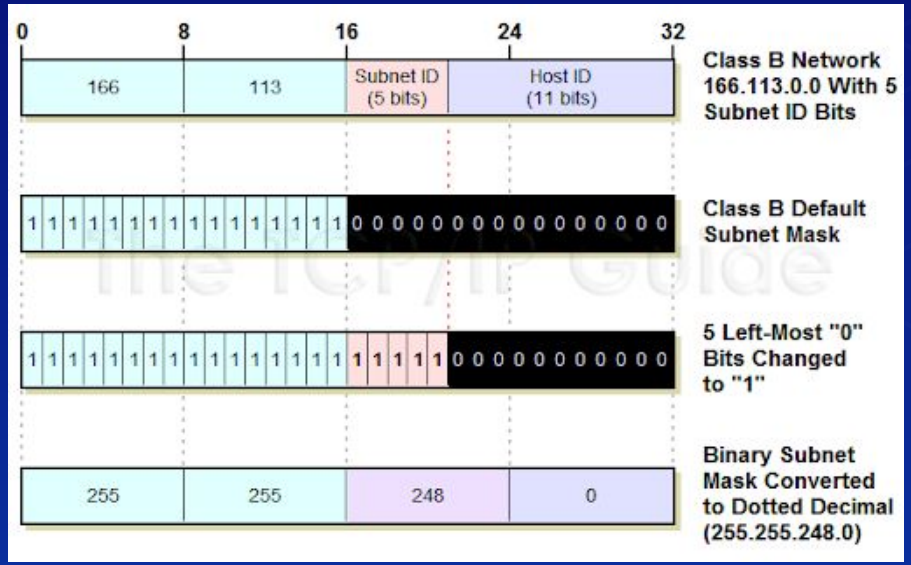
```
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . : tecad.fsu.edu.
Description . . . . . . . . . . . : Intel(R) Ethernet Connection (7) I219-LM
Physical Address. . . . . . . . . : C8-F7-50-6F-48-9F
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

IP Address

- Internet Protocol Address
- Unique identifier separated by 4 periods
  - 192.168.10.10 (LAN Address)
- Uses Subnet mask to specify a part of the address
  - Determines the boundaries of LAN
  - Determines how many IP addresses are allotted to a network

Subnet Masks

- Determines which part of a large network is used by the IP address.



Ports

- Logical, not physical
- Associated with a protocol type
- Common ports:
  - HTTPS: 443
  - HTTP: 80, 8080
  - FTP: 21
  - SSH: 22
  - DNS: 53

Ports

- Well-known ports: 0-1023
- Registered ports continue from 1024-49151
  - Registered by Internet Assigned Numbers Authority (IANA), an American non-profit responsible for global IP address allocation
- Dynamic ports: 49152-65535
  - Contain either dynamic or private ports that cannot be registered with IANA

Domain Name Systems (DNS)

- Translates an IP address to a name
  - 8.8.8.8 translates to **google.com**
  - 128.205.201.57 translate to **buffalo.edu**
- Created to help alleviate the need to remember these long IP addresses

TCP/IP

- Transmission Control Protocol / Internet Protocol
- Suite of protocols used to interconnect network devices on the internet
  - Specifies how much data is transferred over the internet
    - How it's broken-up
    - How it's transmitted

OSI Model

- Open Systems Interconnection Model
- Used for data network design, operation specifications and troubleshooting
- More advanced than the TCP/IP Model
  - 7 layers as opposed to 4 on the TCP/IP

Transport Layer

TCP vs UDP

- TCP (Transmission Control Protocol)
  - Reliable
  - Connection Oriented
  - 3 way handshake (SYS, SYN-ACK, ACK)
  - Best for applications that require high reliability but not time sensitive
  - Packets get organized in order specified, guaranteed data transfer in correct order

Transport Layer

TCP vs **UDP**

- UDP (User Datagram Protocol)
  - Not reliable
  - Connectionless, relationship between programs ends after packets are sent
  - Best for applications that require fast, efficient transmission
    - Streaming, Gaming, etc.
  - Packets are independent of each other so there is no order
    - No guarantee that the packets will be received

Network Protocols

- Routers use these protocols to communicate with each other
  - Read messages to each other
  - Establish communication
  - Establish routing tables
- Examples:
  - BGP: Border Gateway Protocol
  - RIP: Routing Information Protocol

Packets

- Contain 2 IP addresses:
  - Source IP Address: IP of the Sending Device
  - Destination IP Address: IP of the Receiver
  - Source MAC Address (Yours)
  - Destination MAC Address
- Frame Check Sequence (FCS)
  - Checks for errors to make sure ones with errors are dropped before reaching the Destination IP

Flow of Data and Packets

- IP Layer determines the location of the client you are sending packets to through the…
  - Client's IP Address
  - Client's Subnet Mask
  - Destination IP Address
- LAN traffic is passed through switches (Layer 2 Devices)
  - Handled through MAC address

Flow of Data and Packets

- Address Resolution Protocol (ARP) request
  - What IP goes to which MAC address?
    - If not in the ARP table, forward to router or default gateway

DHCP vs Static Addressing

- Static
  - Assign each address manually
  - IP Address does not change (i.e. Printers)
- DHCP
  - Preferred method for IPv4 assignments to host on large networks
  - Dynamically assigned addresses throughout the network

IPv6

- IPv6 was created to replace IPv4
- This was due to no more IPv4 addresses left to give out
- IPv4 Limit: $2^{32} = 4,296,967,296$
- IPv6 Limit: $2^{128} =$ 340,282,366,920,938,463,463,374,607,431,768,211,456 (340 Undecillion)

Public Addresses vs. Private Addresses

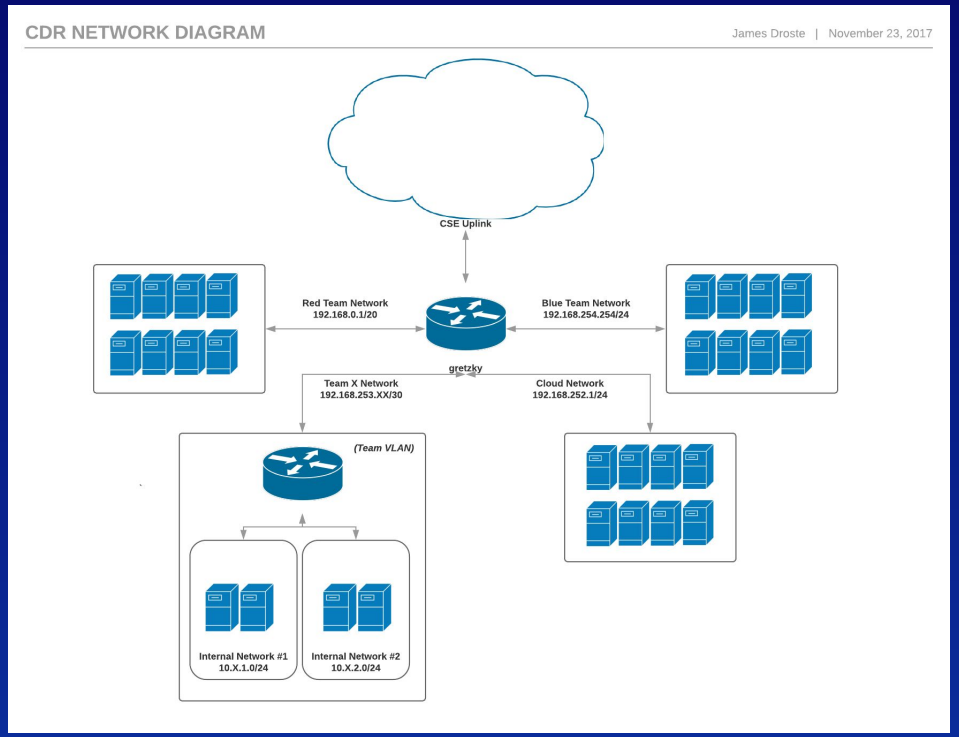
- Public Addresses
  - Used for intranet communication
  - UB is publicly addressed
- Private Addresses
  - Mainly home networks or company networks
  - Usually starting with 192.168... or 10.0...

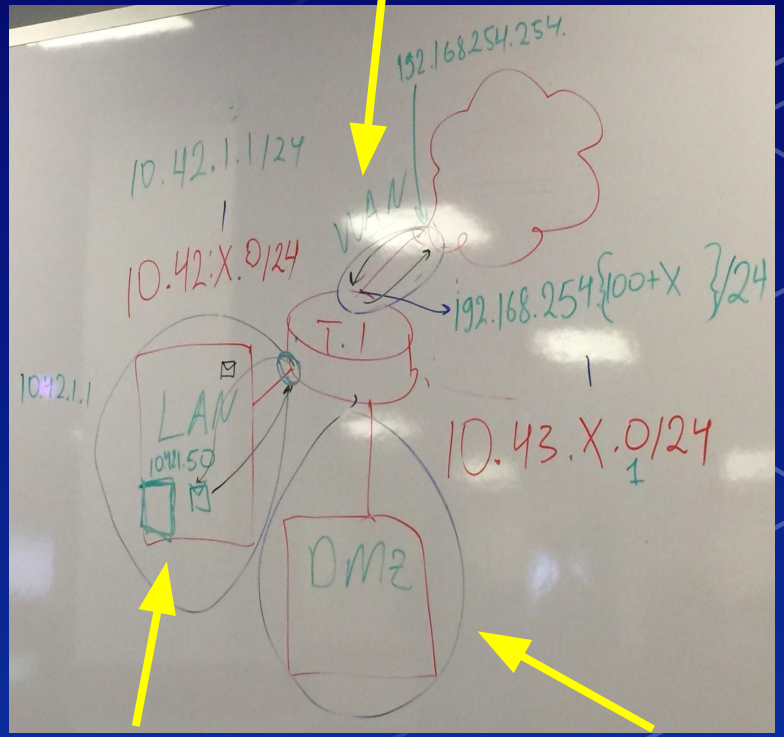
Commands

- ping: check your network connection
  - **ping 10.0.0.20** - will check if a device with this IP address is connected to the LAN network
- **ipconfig**: shows IP address information on Windows
  - Use the **ifconfig** command on Linux
- nslookup: display DNS server information
  - **nslookup 8.8.8.8** ➜ dns.google

Our Networking Infrastructure

Our Networking Infrastructure





(X = Your Team #)

10.42.X.0/24

10.43.X.0/24

What is PfSense?

What is PfSense?

- PfSense is a firewall and router that runs within its own virtual machine
- It will act as a gateway to the internet for all the VMs you use in future assignments

Homework Overview

Homework Overview

- In this HW, you will be setting up the following in PfSense:
  - LAN
  - WAN
  - DMZ
- Connect your StudentVM to PfSense
- Display proof that your StudentVM connects to the Internet

Remaining Parts of HW Not Discussed

Email to Employer

Topology

Email to Employer

- Write an email to your boss about the pros and cons of implementing virtualization within your company Netdef Incorporated
- Between ¾ and a full page in length (more is fine)
  - No larger than size 12 font and 1.15 spacing.
- Explain in detail all technical language used

Topology

- Diagram of your network that contain information specific to each device and connection on a network
- Use either **LucidChart** or **Draw.io** to design the topology on your HW

Topology

- Things to include:
  - Gateway
  - PFSense
  - Client (StudentVM)
- Also include:
  - IP Addresses of Machines
  - All interfaces associated with PfSense

Submission

- Please submit the following in one PDF document to UBLearns:
  - Email to Employer
  - PfSense & Client Machine Steps
  - Topology

- Only typed submissions will be accepted

Homework Points Breakdown

- Part 1 - Email to Employer
  - **15%**
- Part 2 - PfSense & Client Machine
  - Successful setup of PfSense: **40%**
  - Successful setup of Client: **20%**
  - Clean Runbook Submission: **10%**
- Part 3 - Topology
  - **15%**

Expectations

- This course is largely self-driven
- Before reaching out to Michael and Ruben on Mattermost, please first:
  - Research! Google Search the issue you're facing
    - Most times, someone else will have encountered the same problem you're having
  - Ask each other, but do not provide a step-by-step solution if you have the answer
    - Academic Integrity policies will be upheld