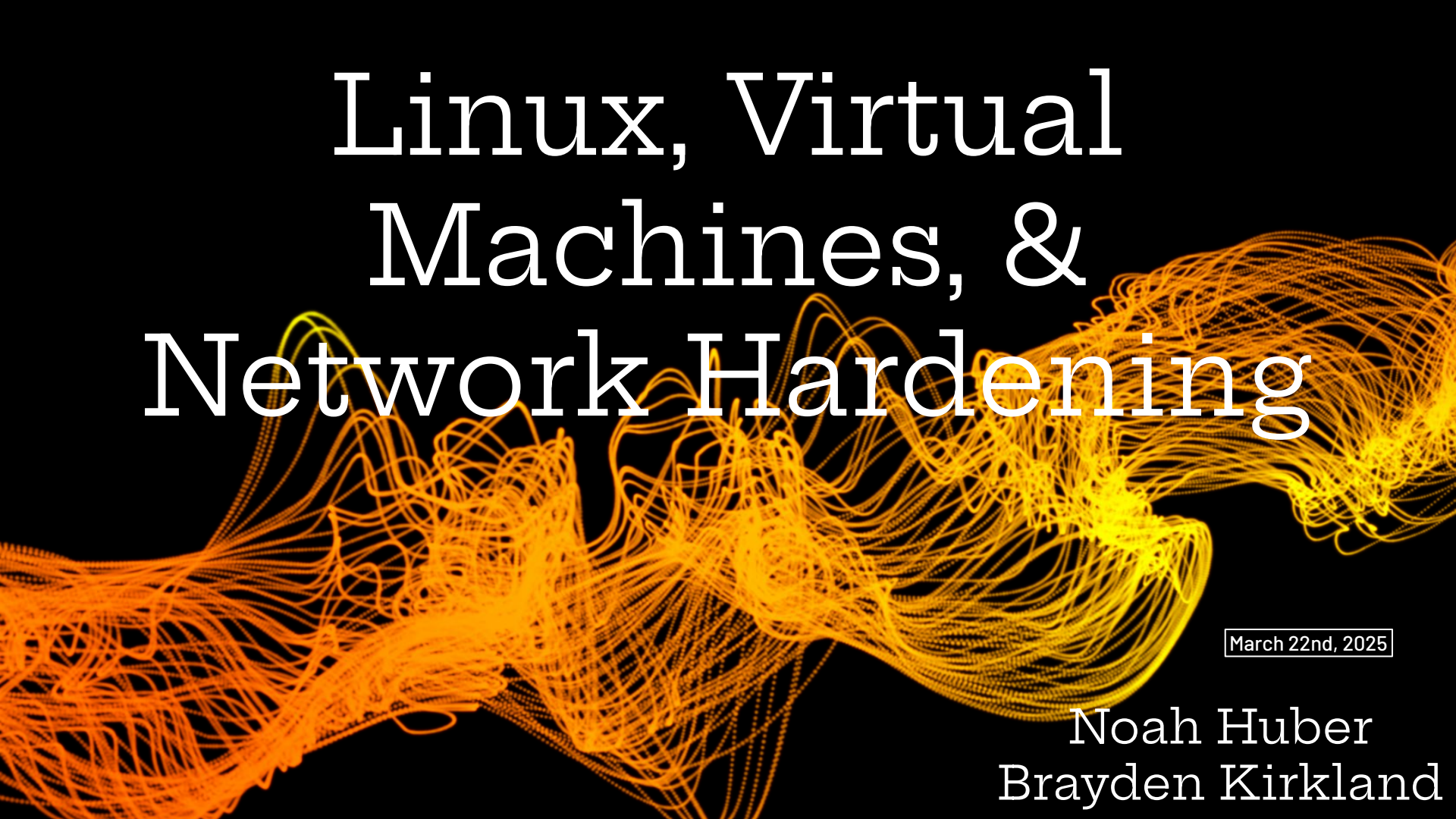
Linux, Virtual Machines, & Network Hardening



March 22nd, 2025

Noah Huber
Brayden Kirkland

Project Timeline

Presentation

History/Definition

What we are covering?

1st Section: Brief history of linux, ubuntu, and types of linux.
2nd Section: Types of virtual machines and what they do.
3rd Section: Network/Machine Hardening

Handout

Walkthrough

What is on the handout?

- Topic
- Setup
- Walkthrough
- Network Hardening Activity

Assignment

What is Due

What is the assignment?

Setting up and installing a Virtual Machine from scratch.
Installing ubuntu from scratch and understanding VM settings.
Network Hardening Activity and Deliverable

Looking Back

What we Learned?

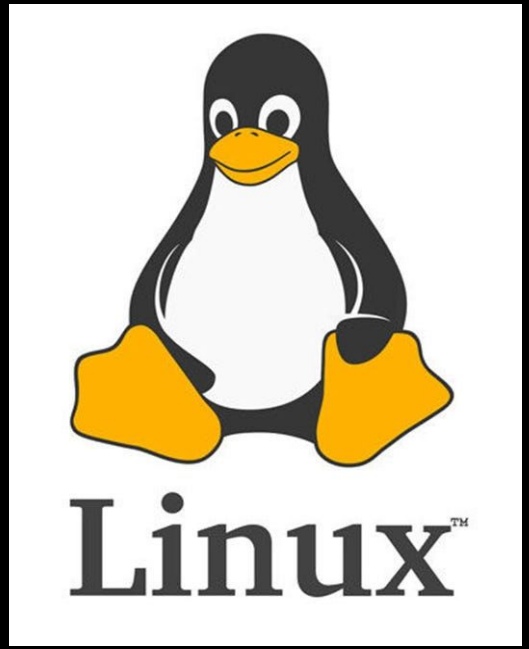
Answering Questions about what you have learned.

A brief section for questions to ensure completion.

Any questions on the assignment/ misunderstandings.

01

Linux (Ubuntu)



What is Linux

Linus Torvalds, born in 1969 in Finland. He created Linux in 1991 at the University of Helsinki. He wanted something open source with more adaptability and opened it to contributions, which sparked massive collaboration.

Linux is built on UNIX principles, emphasizing modularity, multitasking, and security. Today, Linux powers servers, cloud computing, Android devices, and supercomputers, making it one of the most influential software projects ever.

Interesting Fact About Linux

Your Smart Toaster Might Be Running Linux

Linux isn't just for computers; it powers smart fridges, toasters, washing machines, small electronics, and even traffic lights. If it's got a microprocessor, especially ARM, there's a good chance it's running Linux.

Different Types of Linux

Ubuntu

- One of the most popular and beginner-friendly Linux distributions.
- Based on **Debian** and used for **desktops, servers, and cloud computing**.
- Offers a smooth user experience with its **GNOME desktop**.
- Great support and regular updates.

Rocky Linux

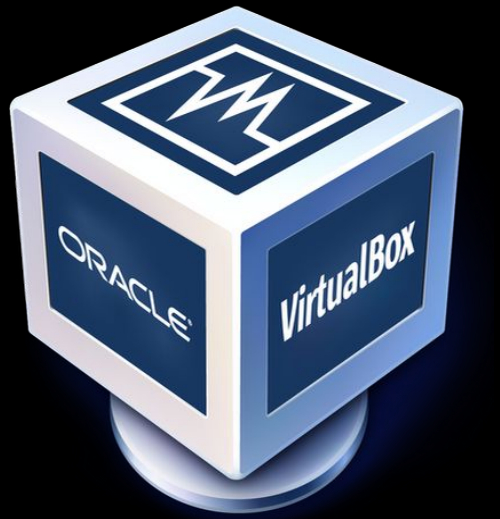
- Designed as a **CentOS replacement** for **enterprise and server environments**.
- Built to be **100% compatible with Red Hat Enterprise Linux (RHEL)**.
- Ideal for businesses needing a **stable, long-term support OS**.
- Heavy focus on reliability and security.

Linux Mint

- A user-friendly distro **based on Ubuntu**.
- Offers a familiar desktop experience with **Cinnamon, MATE, or XFCE**.
- Focuses on **simplicity and multimedia support**.
- Great for a **lightweight and hassle-free** Linux experience.

Kali Linux

- **Pen testing and ethical hacking** distro.
- Comes preloaded with **cybersecurity tools** for security professionals.
- Based on **Debian**, optimized for **offensive security tasks**.
- Used by hackers (both ethical and not), security researchers, and pentesters.



02
Virtual Machines

What are Virtual Machines?

A **Virtual Machine (VM)** is a software-based computer that runs inside another operating system. It **emulates** real hardware, allowing you to run multiple operating systems on a single physical machine.

VMs are incredibly useful for running Linux allowing users to test and run different Linux distros.
They provide a **safe**, **isolated environment** for development, cybersecurity testing, and software experimentation.

In an enterprise, many servers run on a linux distro, reducing costs and **improving efficiency**.

Different Types of Virtual Machines

VMware/VMplayer

- **Pro version is paid**, but **Player is free** for non-commercial use.
- **Better performance & graphics acceleration** than VirtualBox.
- **Enterprise & Cloud Computing Environments**
- **More Optimized** less Open-Source

Virtualbox (By Oracle)

- **Free & open-source**, cross-platform (Windows, macOS, Linux).
- **Beginner-friendly**
- Supports **snapshots** but needs extensions for advanced features.
- **Slower than VMware** in some cases.

UTM (for Apple M1/M2/M3 Macs)

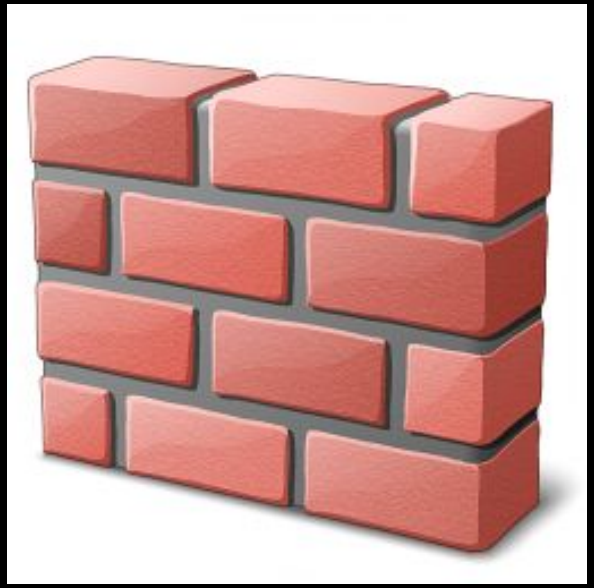
- **Built on QEMU**, optimized for Apple Silicon. (ARM-based Macs).
- **Best option for running Linux & Windows on macOS**
- **Easy to use**, but not as feature-rich as VMware.
- **Extremely Open-Source** to public.

Other/Older

- **Microsoft Virtual PC** – Discontinued, was used for Windows XP mode.
- **Parallels** – Paid, optimized for macOS, better macOS guest OS support.
- **Xen & KVM** – Used for **server and enterprise virtualization** (not desktop-friendly).


VMware Workstation Player
Parallels
Parallels Desktop
QEMU
QEMU
VirtualBox
citrix
Citrix

03



Network/System Observation

What is Network Hardening?

Network Hardening is the process of strengthening a network to reduce vulnerabilities and protect against cyber threats. Firewalls, intrusion detection/prevention systems **(IDS/IPS)**, and access controls can prevent unauthorized access and data breaches.

Securing a system or **System Hardening** means applying best practices to protect an individual computer or server. This includes keeping software updated, **disabling unnecessary services**, and enforcing strong passwords. Both network and system hardening work together to create a strong defense against cyber threats. We will be performing a security audit using Lynis (Open/Source)

Network/System Scanning and Testing

Network Scanning with **Nmap or Nessus** is essential for identifying vulnerabilities and securing systems. Both scanning methods are typically for remote use.
Nmap (Network Mapper) is a powerful open-source tool used for network discovery, allowing administrators to scan hosts, **detect open ports**, identify running services, and even determine operating systems.
It is widely used for **penetration testing** and **reconnaissance**, with commands like nmap -A <IP> performing aggressive scans for detailed insights.

On the other hand, **Nessus** is a commercial vulnerability scanner designed for **in-depth security assessments**. Nessus scans systems for known vulnerabilities, outdated software, and misconfigurations, providing **risk ratings** and remediation recommendations. This can help companies develop **mitigation strategies** and enhance overall security.

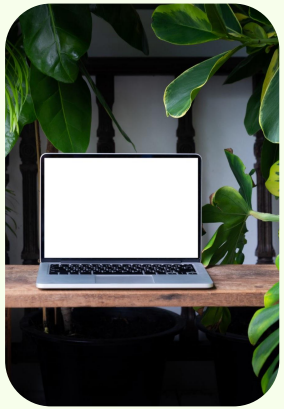
Lynis Security Audit Tool

Lynis is an **open-source security auditing tool** designed for **Linux, macOS, and Unix-based systems**. It helps assess system security, **detect vulnerabilities, and provide hardening suggestions**. It is widely used by system administrators, security professionals, and compliance auditors to ensure system integrity.

When you run a security audit, Lynis:
Checks System Information – OS, kernel version, hardware, etc.
Scans Installed Software – Identifies outdated or vulnerable software.
Analyzes Security Configurations – Examines firewall settings, permissions, and encryption protocols.
Generates a Report – Provides findings with risk levels and suggestions.

Topics Covered

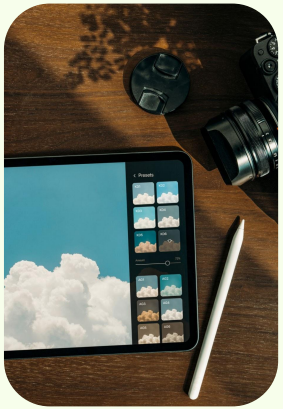
01



Linux/Ubuntu

Operating System we are using for this assignment.

02



Virtual Machines

Setting up and operating a virtual machine for this assignment.

03

Network & System Observation

Learning and understanding how to detect and perform network & system tasks.

04

Walkthrough & Assignment

Walkthrough/Assignment

01 Virtual Machine Setup

- Setup Virtual Machine either **VirtualBox or UTM.**
- Understand the different settings and network types.

02 Ubuntu Installation

- Use the most recent **Ubuntu ISO.**
- Setup and install Ubuntu Linux from scratch.
- Change wallpaper

03 Network/System Obs.

- Perform **nmap port scan**, **ip a**, or **ss -tulnp** for open ports on the network.
- Can perform **nmap -A** scan for more details on remote systems

04 Lightweight Security Assessment

- Find and understand services running on the Linux machine.
- Enable UFW.
- Disable unused or unnecessary services
- Run security audit using **Lynis**

05 Deliverable

1. **Screenshot of the virtual machine software open and ready to install a .iso.**
2. **Screenshot of successful installation of Ubuntu and changed wallpaper.**
3. **Screenshot of nmap Port Scan, ip a, or ss -tulnp to show o/c ports or netstats.**
4. **Screenshot of security audit performed using Lynis.**

THANK YOU

March 22nd, 2025