Introduction to Linux

Cybersecurity

Linux 1 Day 1

Class Objectives

By the end of class, you will be able to:

- □ Name three of the most important Linux distributions.
- □ Navigate the Linux file structure using the command line.
- □ Manage processes with the `top`, `ps`, and `kill` commands.
- □ Install packages using `apt`.

So, Why Linux?

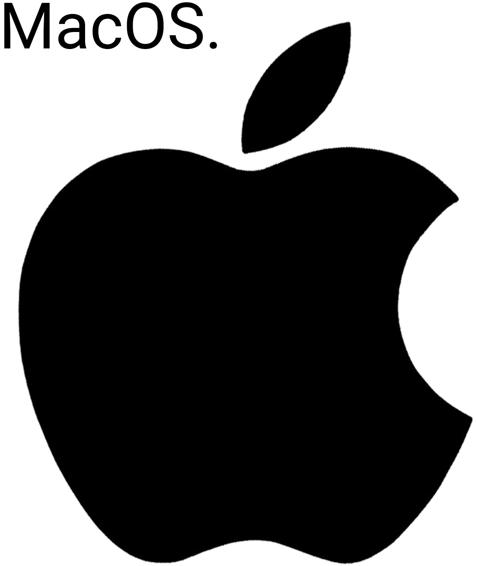
Why Linux

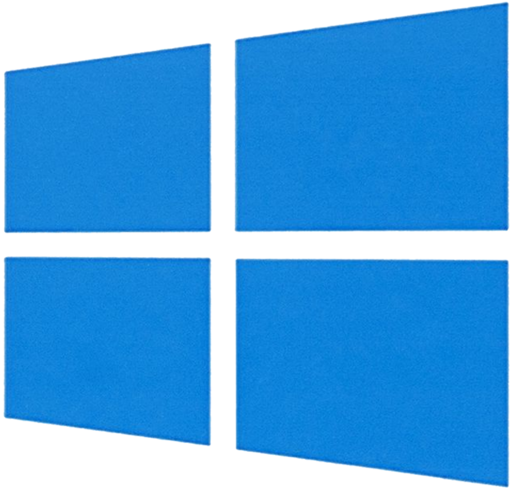
Over 70% of websites run some version of Unix.

w3techs.com

Why Linux

Unix refers to Unix and “Unix-like” operating systems. Unix-like operating systems include Linux, FreeBSD and MacOS.





Why Linux

The ubiquity of Linux machines on modern networks makes it a common target for attackers.

Familiarity with the operating system is crucial for cybersecurity professionals.

Linux in a Professional Context

Knowledge is essential for the following technical roles, among others:

- Help Desk / IT Support
- System Administration
- Penetration Testing
- Network Forensics

Activity Scenario

Throughout today's exercises, you will:

Investigate a malfunctioning Linux server reported to be running more slowly than usual.

Identify suspicious activity on the system and then contain it.

Methodology will include:

- Auditing files
- Auditing processes
- Installing security packages
- Configuring security services

Linux History and Distributions

A (very) Brief History of Linux

01 In 1969-1970, Dennis Ritchie, Kenneth Thompson and several others at AT&T Bell Labs began developing a small operating system called **Unix**.

02 Within the next two decades, different updates and distributions of Unix were created. Most were proprietary.

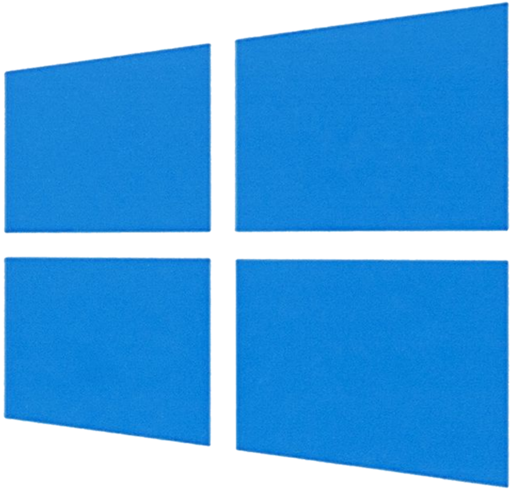
03 In 1984 Richard Stallman's Free Software Foundation (FSF) started the GNU project, which created a free distribution of the Unix operating system

04 In 1991, Linus Torvalds used many of the components from the GNU project to create a free, open source operating system, which is now known as **Linux**.

An **operating system (OS)** is the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals

An Introduction to Linux

Windows, Mac OS X, and Linux are all examples of operating systems.



> By W3Cook's analysis of Alexa's data, 96.3% of the top one million web servers are running Linux. The remainder is split between Windows, 1.9%, and FreeBSD, 1.8%.
>
> *—Steven J. Vaughan-Nichols*

zdnet.com

Most enterprise networks feature at least one Linux machine.

Unlike Windows and OS X, Linux is **free, open source software** (FOSS).

Anyone can modify the source code.

Most tools in the hacker / security community are still published as open-source.

Free software and information is prevalent in the industry. Almost all the tools we'll use in class are open source.

Distributions

Distributions are special-purpose variants of the operating system

Linux Distributions

In this course, we'll use two distributions: Ubuntu and Kali Linux.

01 Ubuntu

Ubuntu is geared towards general-purpose users.

02 Kali Linux

Kali is designed specifically for security professionals.

Linux Distributions

Ubuntu and Kali Linux are both specialized distributions of Debian, which is itself a distribution.

Linux Servers

In order to conserve as many resources as possible, most production Linux servers don’t offer a graphical interface. They also don’t have a keyboard or mouse.

Therefore knowledge of the command-line is essential for understanding Linux.

These command-line only machines are called headless servers.

Activity: Distribution Research

You are a system administrator at *X Corp*, which has recently experienced a number of breaches involving servers running outdated Linux distributions.

- In response, the IT Department has decided to upgrade the affected servers with newer distributions of Linux.
- You must conduct research to determine which distribution is most appropriate for each machine.

Suggested Time:
15 Minutes

Times Up! Let’s Review.

Distribution Research Review

Identify which distribution(s) is most appropriate for each situation.

Central Data Server	
Public Web Server	
IT Audit Workstation	
User Workstation	

Which distribution is most flexible and best suited for day-to-day and administrative tasks?

Which distribution is built specifically for penetration testers?

Which distribution would you use to set up a web or data server?

What is the most widely-used Linux desktop environment?

What is a headless server?

Does Ubuntu have a headless server type? Does Fedora? CentOS?

Which distribution is Ubuntu based on?
What about Kali?

Which distribution is CentOS based on?
What about Fedora?

What is SELinux?

You are deciding between versions of Ubuntu Servers. If you want a version that will remain stable over time, which version do you choose?

What are some security implications of using free and open source software or forks of popular Linux distributions?

As demonstrated in the Mint OS article, open source means that anyone can contribute. Therefore, a hacker with programming skills will be able to attack somewhat easily. **You must be vigilant of where you download your software.**

Linux File System Structure

Linux File System Structure

Each OS maintains certain conventions for where and how they store different kinds of files. For example, Windows and Mac machines typically place images in a ~/Pictures folder.

Linux also has a conventional file system structure.

These conventions are consistent across distributions. For example, user applications are typically stored in /usr/bin, and this will always be the case across distributions.

Therefore, we can apply what they learn today to other distributions we encounter, since each distribution will have the files and directories that we will learn about today.

In addition, all popular Linux distributions use the bash shell by default. This means we can use the command line tools they learn here on other distros, as well.

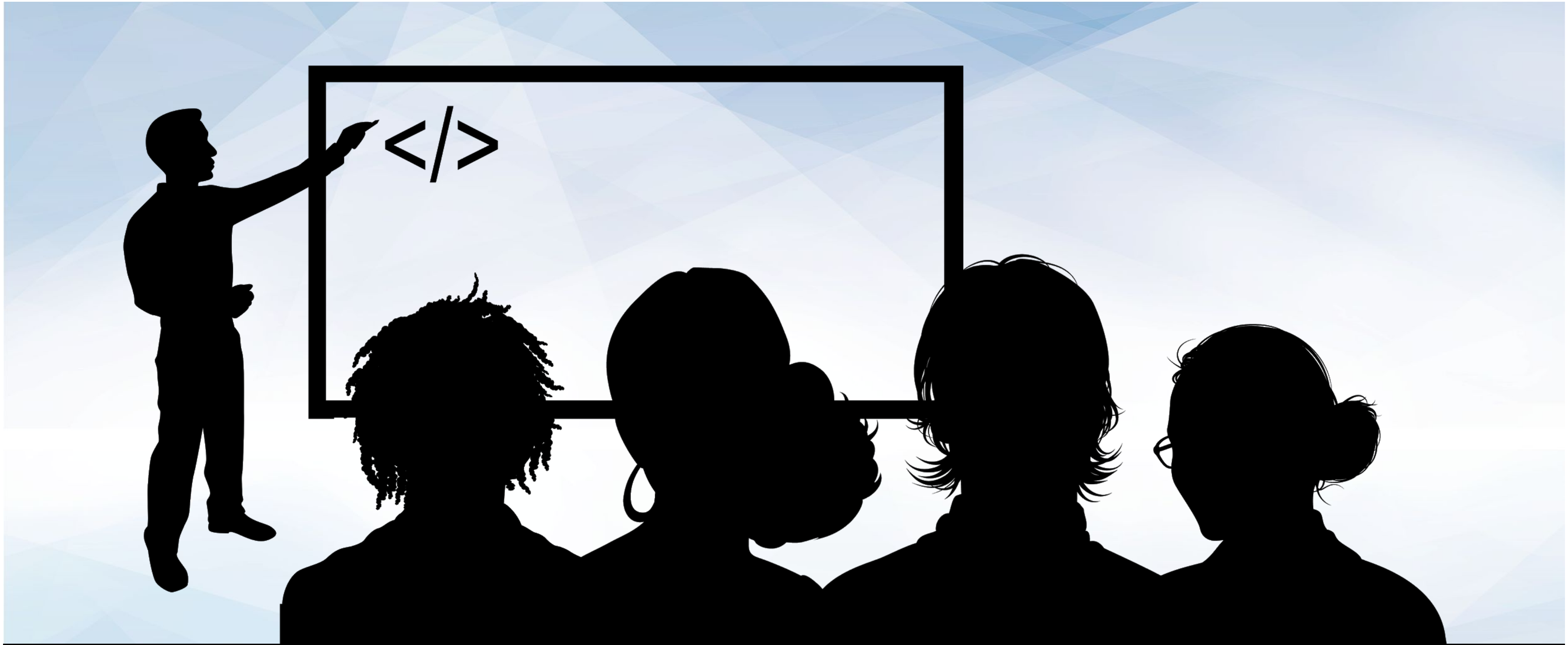
File Systems

Linux maintains certain conventions for storing files:

`/ (root)`	The root directory that contains every other directory.
`/home`	Contains users’ private file. Users should not be able to save files elsewhere.
`/etc`	Contains configuration files, defining how a machine runs and who can use it.
`/bin, /sbin`	Contain applications such as web browsers and commands like `ls`.
`/var`	Contains files that change over time.
`/tmp`	Contains files that are only needed for a short period of time.

Demo Scenario

Let’s launch a terminal an walk through the Linux file system, starting at the top of the directory structure, the Root Directory.



Instructor Demonstration

Navigating Linux File Structures

Demo Takeaways

The audit took us to the following directories:

`/etc`	Stores specific, system-wide configuration files, as well as the most sensitive files on a Linux system.
`/var`	Stores files that are continually updated.
`/home`	Stores user home directories.
`/tmp`	Where applications write temporary files that can be deleted on reboot.
`/bin` and `/sbin`	Where the system keeps its main binary or program files.

Activity: Linux Landmarks

Most technical roles in cybersecurity require comfort with the command line and familiarity with the structure of a Linux file system.

You will use this knowledge to navigate file systems when looking for suspicious activity or administering the machine.

The next exercise will give you an opportunity to explore the file system and practice using the command-line.

Suggested Time:
30 Minutes

Times Up! Let’s Review.

Break

Resources and Processes

Introduction to Processes

When a program runs, it must process data and potentially make changes to the file system. This is why we call a running program a **process**.

When these programs process, save and modify data, they consume a computer’s resources.

Let’s take a look at two of the most important resources: **memory** and the **CPU**.

Memory is the space used by a process to save and manipulate data.

Memory

Memory comes in two forms:

01 RAM

Random Access Memory (RAM) is used to run the program’s code. RAM is only used while the program is running.

The more work a process does, the more RAM it needs.

02 Disk Space

Disk space is used to save data permanently.

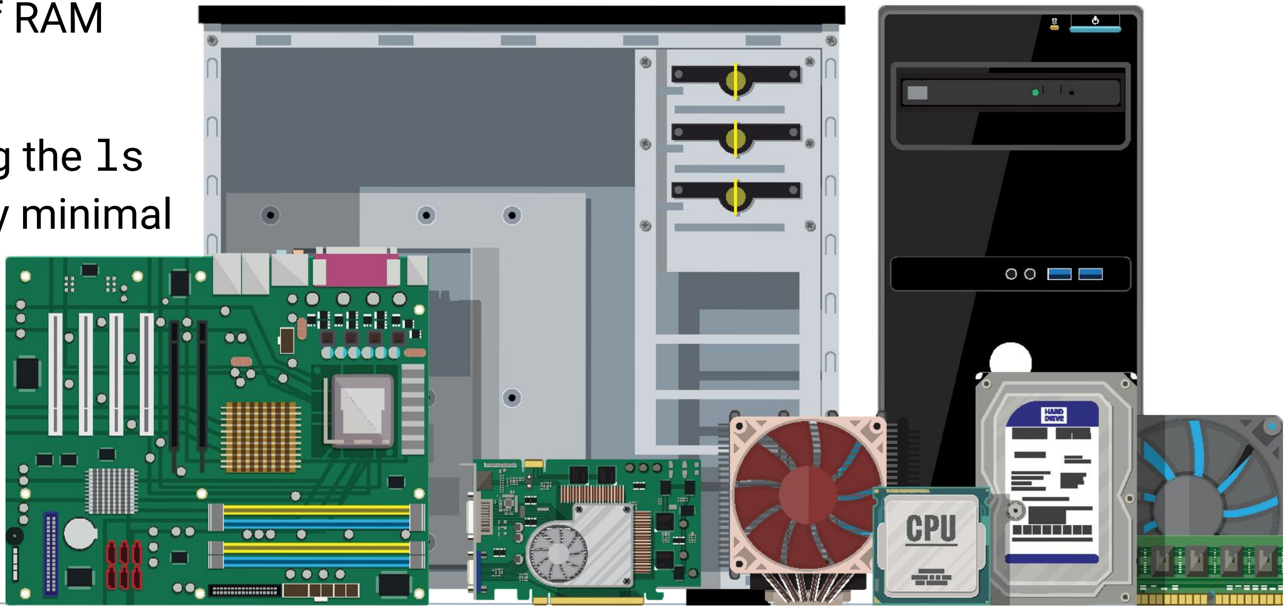
Files saved to a disk persist even after a process ends.

The Central Processing Unit (CPU)

The **Central Processing Unit (CPU)** acts as the brain of the system, determining how much work a process has to do, and how difficult that work is.

A difficult task, such as encrypting a large file, will use a lot of RAM and/or CPU.

Easier tasks, like executing the `ls` command, will require only minimal RAM and/or CPU.

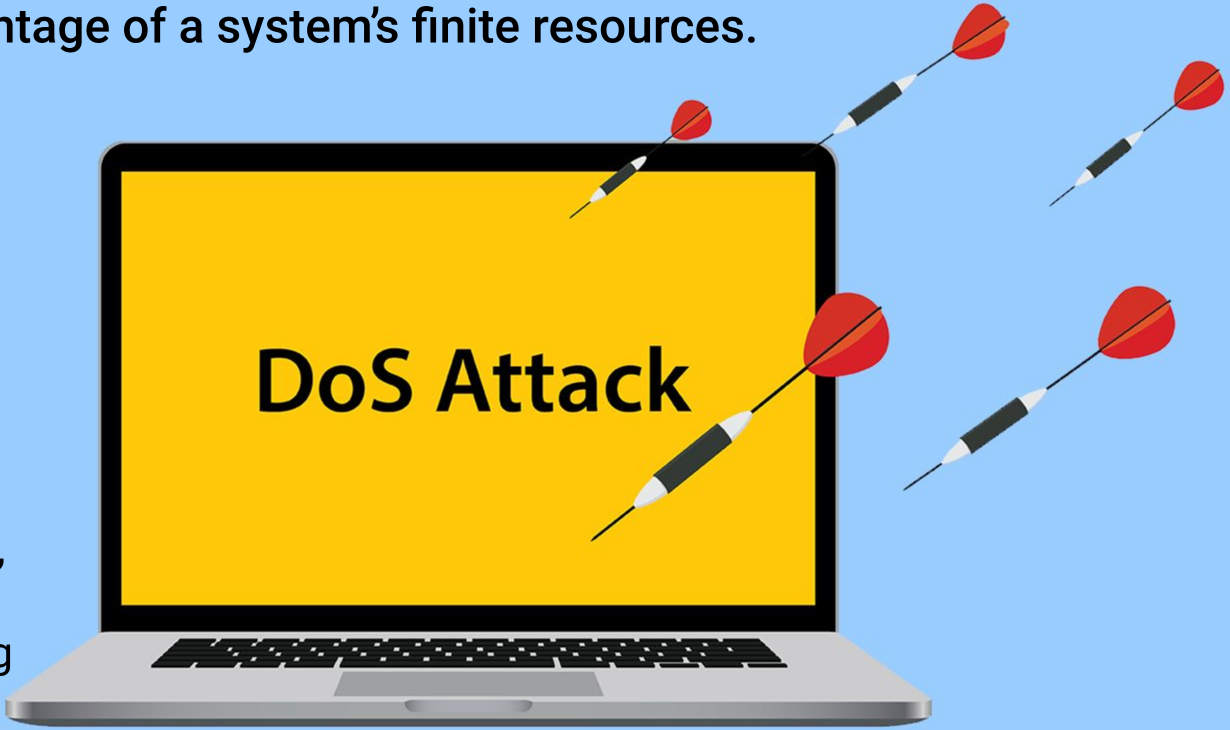


Targeting Resources

Hackers can take advantage of a system’s finite resources.

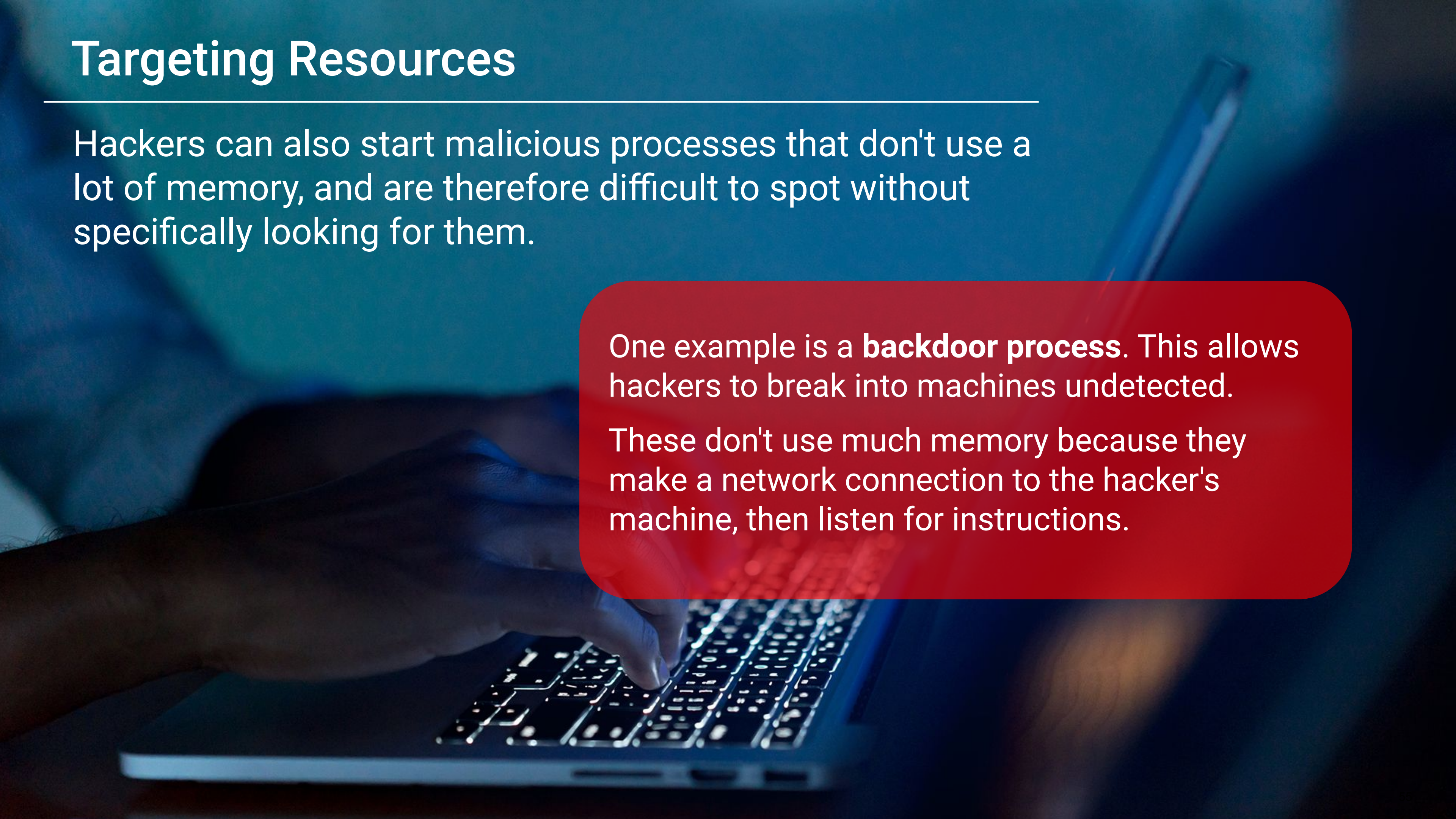
- Hackers can perform denial of service (DoS) attacks by launching processes that eat up memory on a target machine.

- This can slow down or crash the machine, making it unavailable to users, thus denying them service.



Targeting Resources

Hackers can also start malicious processes that don't use a lot of memory, and are therefore difficult to spot without specifically looking for them.



One example is a **backdoor process**. This allows hackers to break into machines undetected.

These don't use much memory because they make a network connection to the hacker's machine, then listen for instructions.

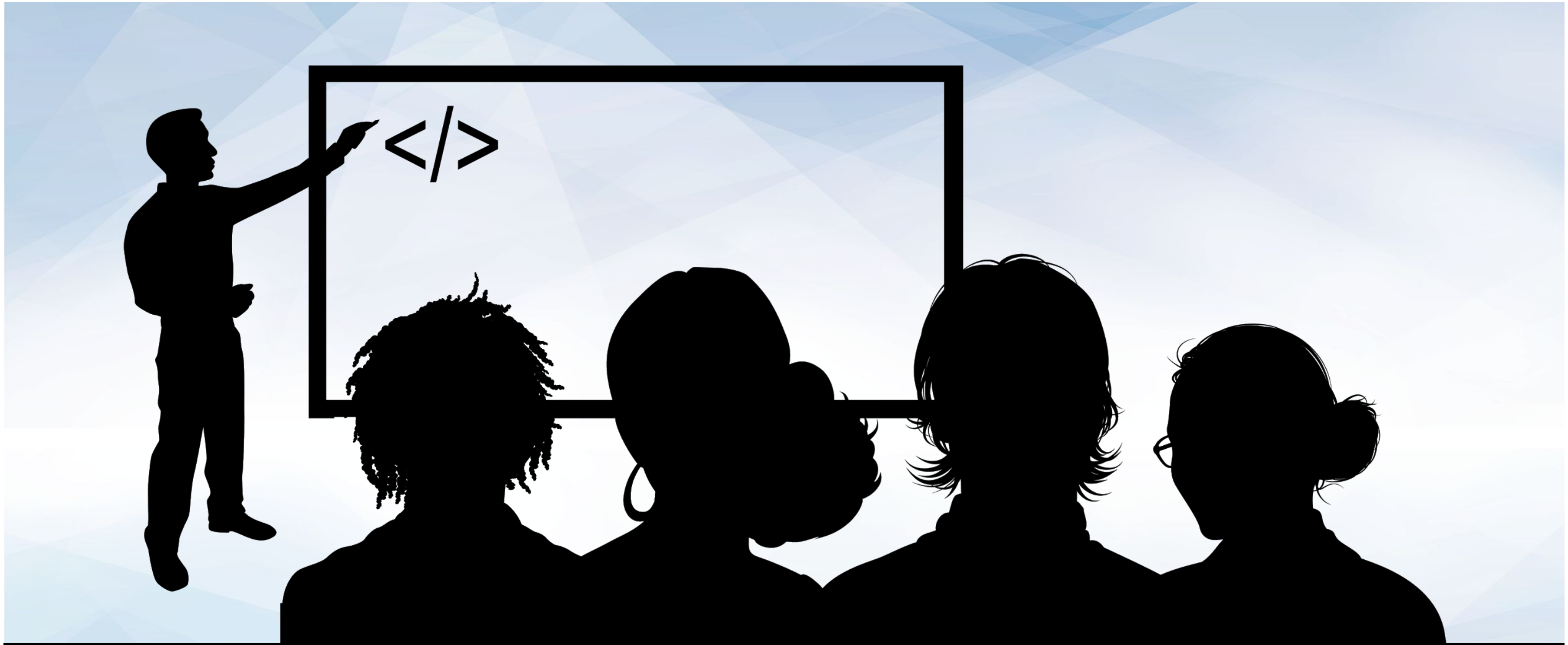
Managing Processes

Linux has several commands for managing processes:

`top`	Allows you to see all running processes in real time. It updates every three seconds to show what’s happening on the system.
`ps`	Allows you to take a snapshot of all the running processes on the system. Different arguments allow you to show different subsets of processes and use this output with other commands.
`kill`	Used to stop processes, usually ones causing problems. `kill` attempts to allow a process to finish before it shuts it down.

Dynamic analysis is the process of running a potentially malicious script and monitoring its effects.

Let’s run a potentially malicious script to determine how it affects system health.



Instructor Demonstration

Inspecting Malicious Files Demo

Activity: Processing Investigation

In this activity, you will monitor the system for processes that should not be running.

- Your senior admin asked that you record snapshots of processes as well as review processes in real time.
- If you notice anything amiss, `kill` the process and add your findings to the report.

Suggested Time:
25 Minutes

Times Up! Let’s Review.

Installing Packages

Packages

Administrators often install additional software to properly harden the machine.

- Linux offers downloadable tools called packages.
- New packages are installed with a tool called package manager.

We'll use the Ubuntu package manager, called **aptitude**. We will use aptitude with the command `apt`.

Packages

```
sudo apt install <package name>
```

Linux searches databases to find information about `<package name>`.
If found, it will be downloaded.

These databases are known as repositories.

Repositories specifically used to store and distribute packages are known as Personal Package Archives, or PPAs.

Packages

Today, we’ll install the following packages.

`lynis`	Checks that a Linux machine is properly secured.
`john`	Verifies that users are using strong passwords.
`chkrootkit`	Scans machines for the presence of a malware called rootkit.
`tripwire`	Monitors the file system for suspicious changes.

(Take Home) Activity: Installing packages.

In this activity, you will install and configure `tripwire`, `chkrootkit`, `john`, and `lynis`.

Suggested Time:
OYO

Times Up! Let’s Review.