The Cybersecurity Mindset

Cybersecurity

Lesson 1.1

Class Objectives

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

Explain the course structure and general direction of the program.

Recognize the high-level security strategies and tools covered in class.

Define cybersecurity as the assessment of threats and the mitigation of risk.

Give a clear definition of the CIA triad and its elements.

The Rising Cyber Threat

Why is cybersecurity such a desired skill these days?

Reason 1:

Explosive Growth in Dependence of IT

Nearly every personal, social, and commercial aspect of our lives makes contact with **vulnerable IT infrastructure**.

Reason 2:

More Users (Targets) on Connected Devices

More people than ever before are logged into connected devices— often for the majority of their
waking (and sleeping) hours.

Reason 3:

Better Tools for Bigger Damage

Today's cyberattacks are becoming more sophisticated, aggressive, and disruptive than ever before.

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV WATCHLIST CRAMER PRO

TECH

Solarwinds hackers are targeting the global IT supply chain, Microsoft says

PUBLISHED MON, OCT 25 2021·7:46 AM EDT

Sam Shead
@SAM_L_SHEAD

SHARE

KEY POINTS

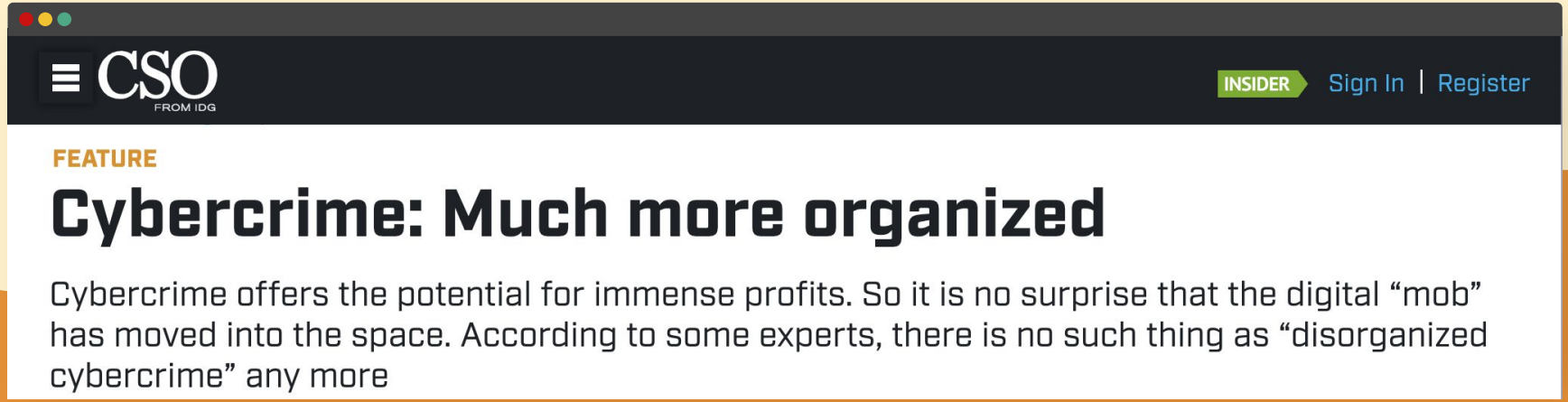
- Nobelium, as the hacking group is known, has "been attempting to replicate the approach it has used in past attacks by targeting organizations integral to the global IT supply chain" according to Tom Burt, corporate vice president of customer security and trust at Microsoft.
- The hackers have been using phishing emails and a technique known as password spray, which involves trying commonly used passwords such as Password1 or 1234 against multiple accounts before moving on to try a second password.
- Some 140 resellers and technology service providers have been targeted by Nobelium so far, according to Microsoft, which said it believes 14 have been compromised.

https://www.cnbc.com

Reason 4:

Significant Investment by Bad Actors

The field was once populated by individual “lone attackers.”
It has now become a focal point for organized crime,
nation states, and private enterprises.



Reason 5:

70% of cyber security professionals say that their organization has been impacted by the ongoing global cybersecurity skills shortage.

ESG Research Report,
The Life and Times of Cybersecurity Professionals

Defining Cybersecurity

What is the first thing the word “cybersecurity” brings to mind?

Everyone's First Thoughts:

Attackers and **complicated code**...

But cybersecurity ***isn't*** about attackers and complicated code...

Cybersecurity is really about assessing threats and mitigating risks.

Know the Threats

To the experienced cybersecurity professional, risks are everywhere.

A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business

Updated 8:46 AM ET, Tue July 30, 2019

New Hacking Technique Can Steal Info Through PC Speakers and Headphones

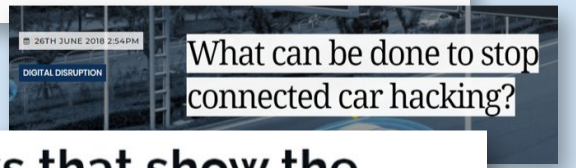
TECHNOLOGY

Email Is Dangerous

Electronic mail as we know it is drowning in spam, forged phishing mails, and other scams and hacks. It's going to get worse before it gets better.

The SIM Hijackers

Has someone hacked your webcam? Here's how to stop cyber-snoopers



Critical Bluetooth Flaws Put Over 5 Billion Devices At Risk Of Hacking

Five nightmarish attacks that show the risks of IoT security

The Internet of Things is not going away -- and neither are the attacks that exploit device vulnerabilities. Here are five incidents that illustrate what users and device developers need to do to prevent breaches.

By Jack Wallen | June 1, 2017 -- 16:31 GMT (09:31 PDT) | Topic: Cybersecurity in an IoT and Mobile World

Mitigating Risks

Historically, organizations viewed cybersecurity from the lens of the **castle model**:

Managing risks meant building walls and keeping the bad actors out.

Mitigating Risks

Today, security professionals operate in a world where breaches are assumed, and risks associated with such events also need to be mitigated.

Daily Routine

In class, we'll run through the following:

- Objectives
- Brief background lecture
- Instructor demonstrations
- Thought exercises
- In-class skill builders
- Project work

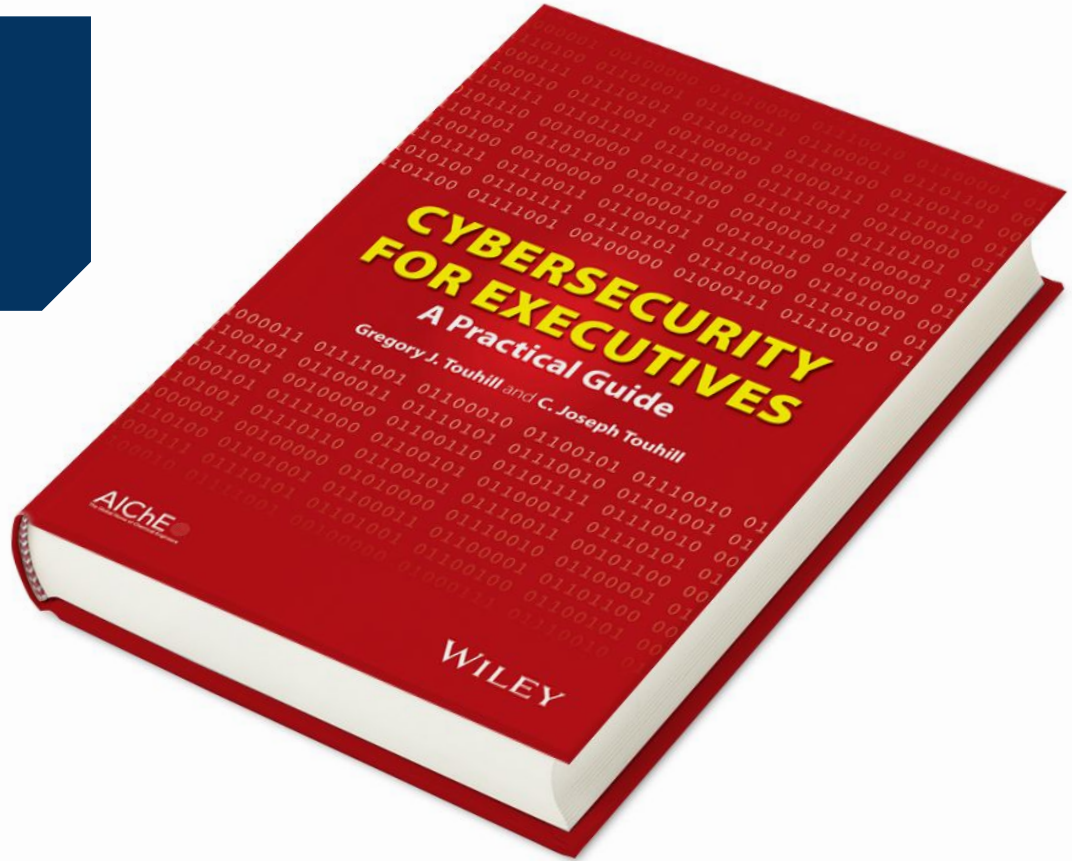
Course Overview

Curriculum at a Glance: Modules

01	Security Fundamentals	Learn to think like cybersecurity professionals by assessing threats and mitigating risks. Look at security from an organizational perspective via governance, risk, and compliance. Understand how security controls impact an organization and its employees.
02	System Administration	Linux and Windows systems administration. Practical experience working with the command line and commands that are prominent in IT roles. Configure and audit servers, and harden them from malicious attacks. Programming via Bash and PowerShell.
03	Networks and Network Security, and Project 1	Network configuration, design, protocols, and data communication. Network security, cryptography, and cloud virtualization and security. Project 1 involving the deployment of an ELK monitoring stack.
04	Offensive Security	Web applications, databases, and associated vulnerabilities and hardening. Windows and Linux penetration testing, using tools such as Nessus and Metasploit.
05	Defensive Security and Project 2	SIEM with Splunk. Setting up security monitoring, alerts, dashboards, and custom reports. Using forensic tools to recover deleted data. Project 2 involving attacking and monitoring vulnerable VMs.
06	Review and Final Projects	Certification prep and review. Interviewing and career prep practice. Final project involving deployment of a vulnerable web application, dashboard creation and live traffic analysis.

Example Activity: **Cybersecurity Policy and Strategy**

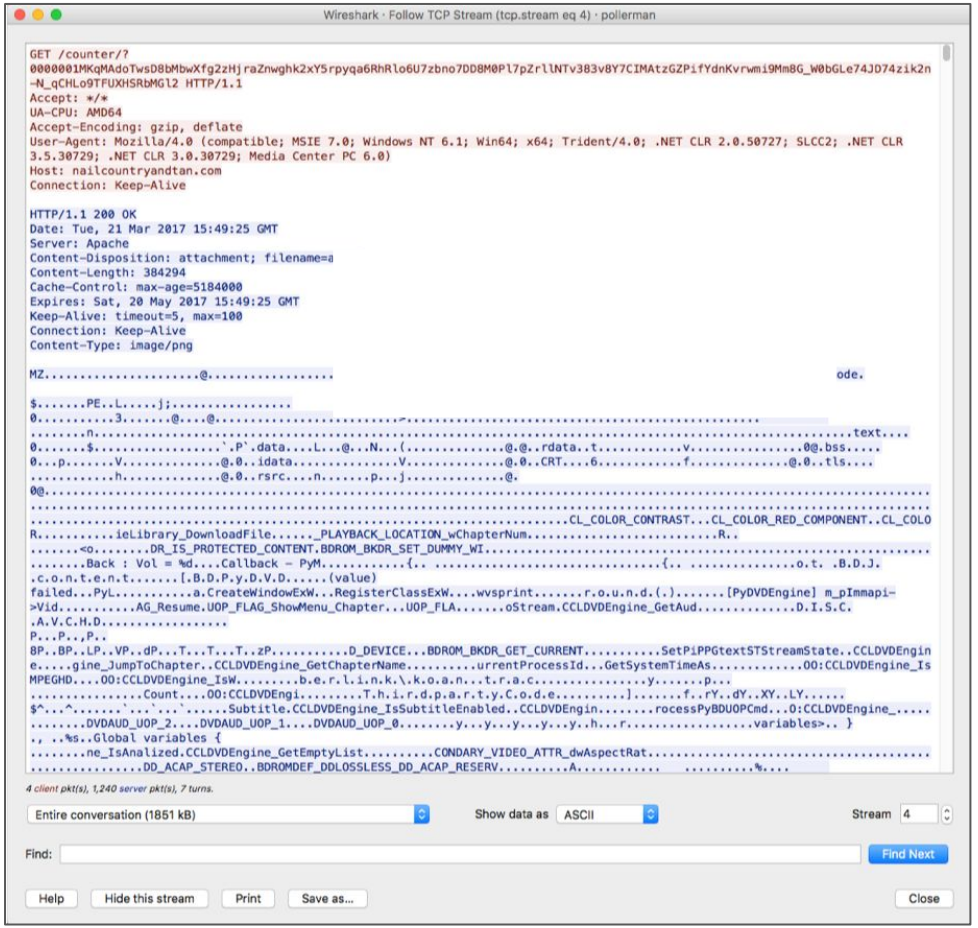
We'll look at security in the larger context of an organization and how security teams communicate risks and strategies to non-technical stakeholders.



Cybersecurity for Executives: A Practical Guide, by Gregory J. Touhill (Author), C. Joseph Touhill (Author), Wiley-AIChE, ©2014

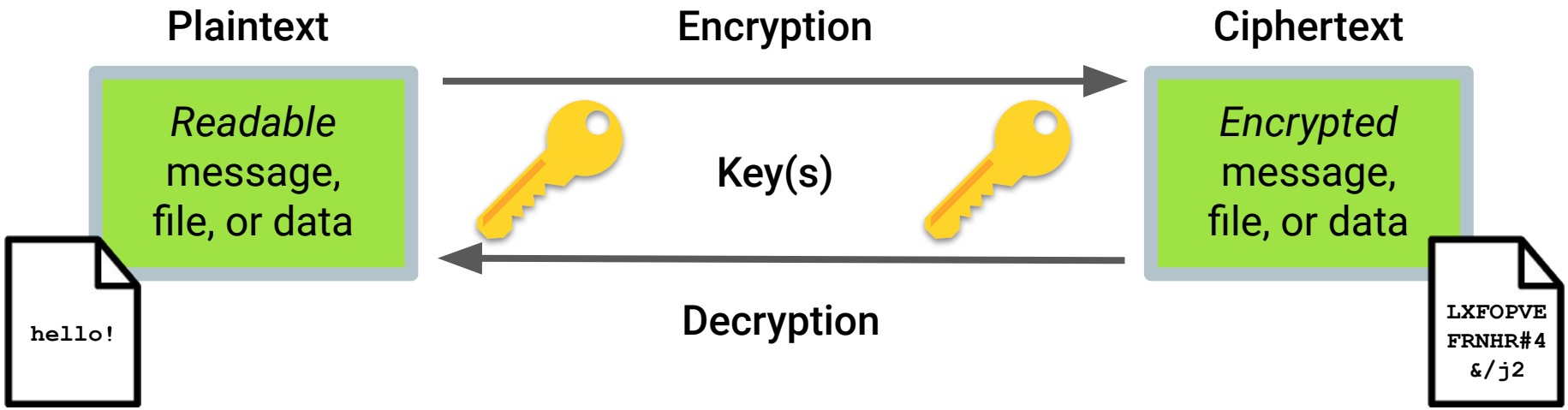
Example Activity:
Analyzing Web Traffic for Suspicious Activity

We'll learn to process complex network traffic logs to find evidence of malware being sent across networks.



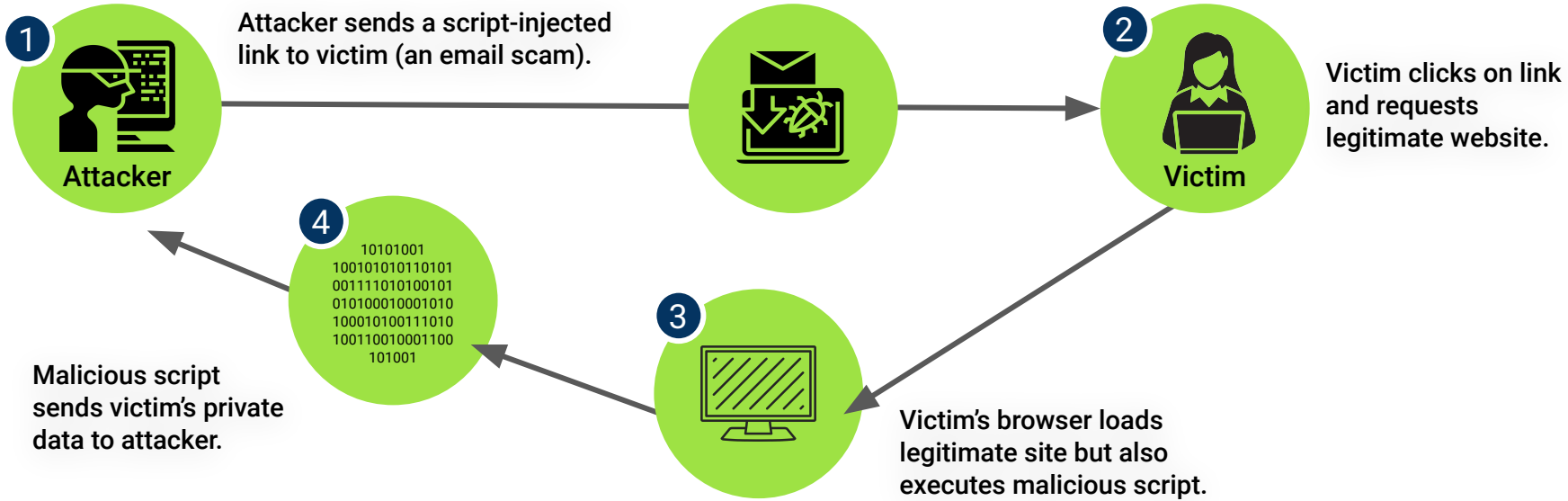
Example Activity: **Encryption / Decryption Systems**

We'll learn how modern cryptography works and how historic methods of encryption can be easily broken.



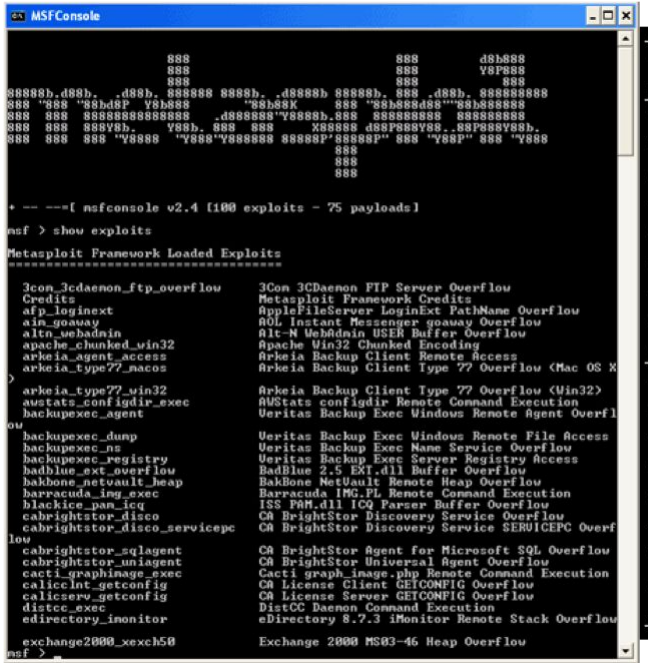
Example Activity: **Web Application Hardening**

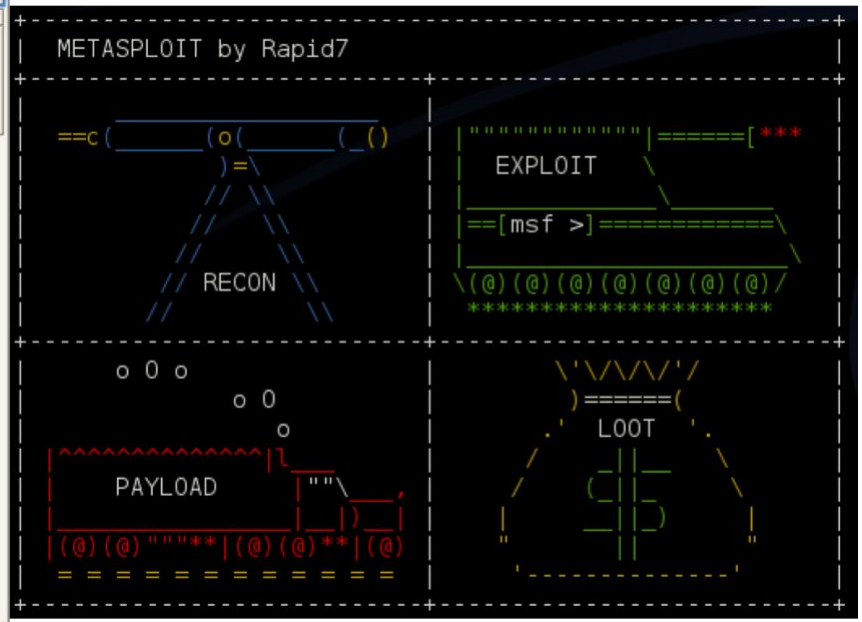
We'll learn how web applications can be defended against the most common attacks.



Example Activity: **Identify Vulnerabilities in Unpatched Systems**

We'll learn to use tools like Kali Linux, Nmap, and Metasploit to run penetration tests to identify known exploits.





Projects

These modules and assignments will culminate in three projects:

01

ELK Stack

The first project follows the Networking and Cloud Security units.

You will deploy an ELK monitoring stack within your virtual network.

02

Red Team vs. Blue Team

You will work as penetration testers and SOC analysts to attack and monitor vulnerable VMs.

03

Final Project

You will exploit a vulnerable web application, create dashboards to see alerts in real time, and analyze live traffic on a virtual network.

CTFs

Throughout the course, we'll also work through Capture the Flag and class-long activities:

Find flags on a Linux server.

Investigate data packets and find flags that tie to various networking concepts.

Create a custom Security Operations Center and use our monitoring tools to analyze and protect an organization from potential attacks.

Tools We'll Use

We will use **virtual machines** to operate the various operating systems and tools throughout the curriculum.

Virtual machines allow us to run different operating systems.

We can download and install virtual machines onto our computer.

In cases where we need to use more than one virtual machine, we will access a network of those machines on the cloud.

Tools We'll Use: Virtual Machines

There are three categories of lab solutions that you will use throughout the course.

Vagrant
local virtual
machine

Azure
Cloud Lab
Services

Personal
Azure Cloud
accounts

Tools We'll Use: Vagrant Local Machines

Starting in Week 3, we will use a Linux Ubuntu virtual machine to complete many systems administration, networking, monitoring, programming, and other tasks.

VirtualBox is a virtualization tool we will use to run various lab activities. It allows us to run different operating systems on our local machines.

Vagrant is a tool we'll use to build and set up our virtual environments. It allows us to run scripts to install these virtual machines, which will then be run using VirtualBox.

Terminal or **Git Bash:** We will be using the command line to download, install, and access our machines.

(ubuntu.com)

Tools We'll Use: Vagrant Local Machines

We will be using Vagrant with VirtualBox in the following units:

- Terminal
- Linux Systems Administration
- Linux Archiving and Logging Data
- Bash Scripting and Programming
- Networks I and II
- Cryptography
- Web Development
- SIEM I and II

Tools We'll Use: Azure Lab Services

Other units will require the use of **multiple** virtual machines.

Can anyone think of why we would need to run multiple virtual machines at the same time?

Tools We'll Use: Azure Lab Services

We would need to run multiple virtual machines at the same time in order to:

Practice offensive security

We need an attacking machine and a vulnerable target machine.

It would be unethical and most likely illegal to attack actual targets.

So we need to set up dummy machines to attack.

Set up and monitor alerts during our defensive security units

We need a machine that is equipped with monitoring and alerting capabilities.

We also need a machine to simulate an attack so we can test these monitors.

Ensure data and resources remain available

If a main machine goes offline, we can create multiple machines to use as back ups.

Tools We'll Use: Azure Lab Services

Azure Lab Services will be used in the following units:

- Windows Administration and Hardening
- Windows Administration and Hardening
- Pentesting I and II
- Project 2: Red Team vs. Blue Team
- Forensics
- Final Project

Online Learning

In this section, we'll take some time to discuss best practices for conducting this course in an online environment.

Tips: Online Learning

01

Get to know your classmates and instructors

You'll get more out of the course if you feel like you're part of a shared community.

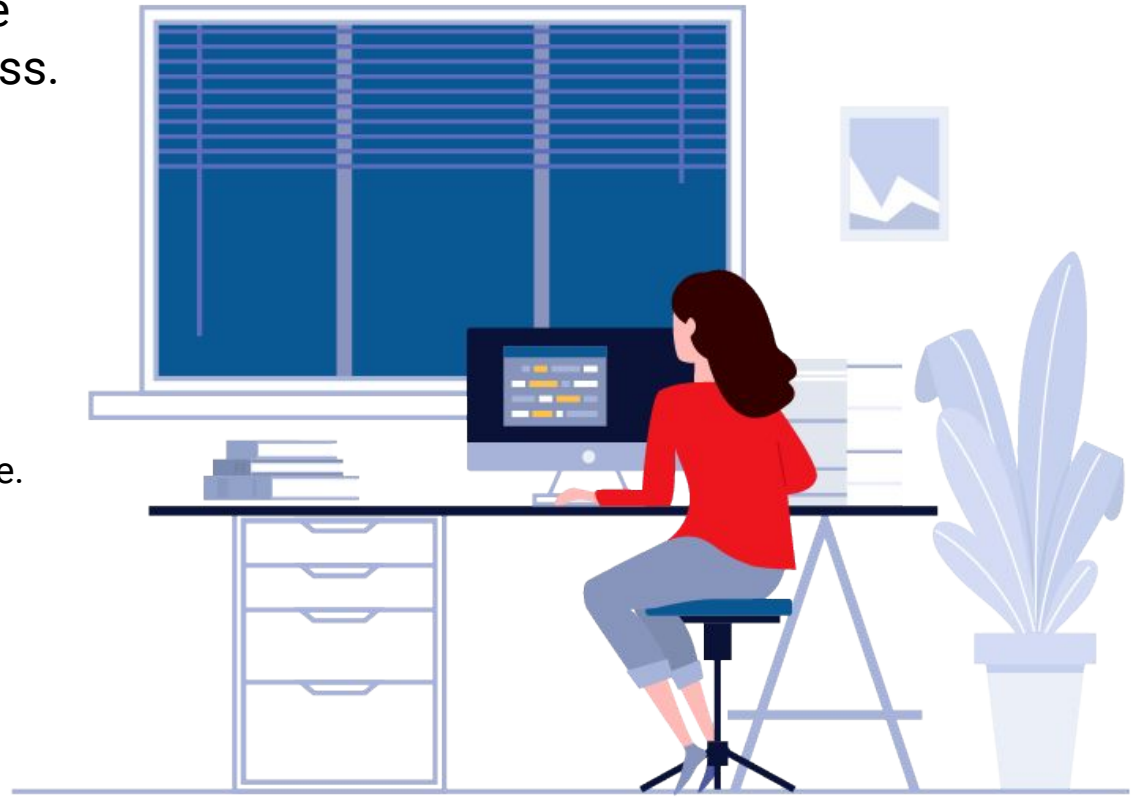
- Social connection can be difficult to develop through a computer screen, but there are ways to get to know your fellow classmates.
- Participate in class and in your cohort's Slack space.
- You don't have to get too personal, but you can share your specific security interest or career goals.

Tips: Online Learning

02

Treat class time like you would a live class.

- Try your best to make the area around you as distraction-free as possible.
- If you can, go to a quiet room, silence your phone, and ask others in your home to avoid distracting you while you're online.



Tips: Online Learning

03

Budget time for classwork, homework, and review.

In an online environment, it can be harder to keep track of due dates for assignments.

- Deliberately scheduling time throughout the week for your coursework will help.
- Set aside three hours, three to four times per week for studying and doing homework.
- Your work won't seem as overwhelming this way, and you won't be working on assignments last minute!

Best Practices

Help make online learning as productive and easy as possible with these guidelines:

01 **Always mute**. If you are not presenting, put yourself on mute.

02 **Include your first and last name for your screen name**.
Help everyone get to know you by including your full name.

03 **Keep your video on**. Be present during the online class.
This includes showing your face.

04 **Raise your hand in Zoom or use Slack for questions**. Don't interrupt a lecture. Use the hand raise feature in Zoom or ask the question via Slack.

05 **Use headphones with a microphone**. Background noise and feedback echoes can be an issue when using your computer mic and speakers.

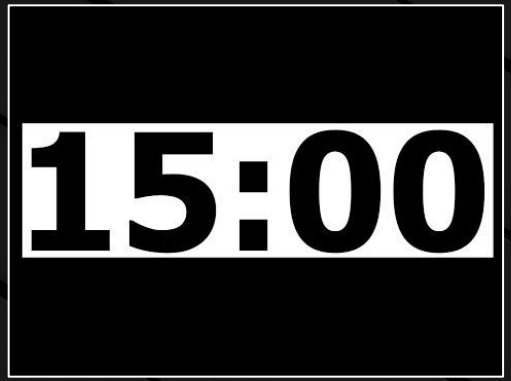
Slack is an online communication tool that is like a forum, instant messenger, and email all rolled into one. It's a tool used by countless organizations worldwide, and you'll be using it every single day for the next six months.

We will use Slack to send code snippets during class, share important announcements, and facilitate group exercises.

You should have received the link to your class-specific channel during orientation.

Though there is a Slack web application, for this course you should have the program installed on your machine.

After the break, we will divide into breakout groups and get started on our first activity!

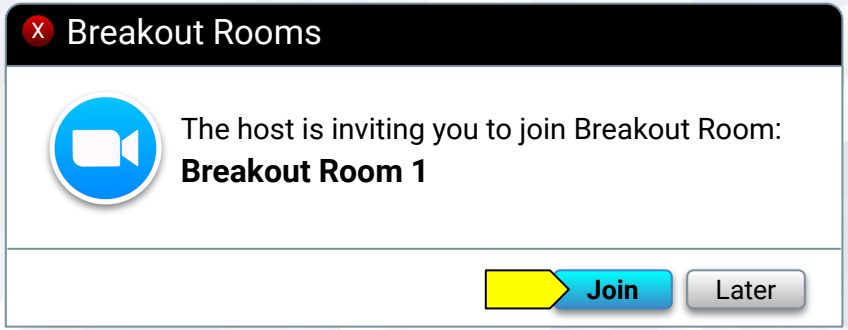

15:00

Assessing Threats: A Wild USB Appears!

Let’s say we found a USB drive laying on the ground. How much of a **threat** could that *really* be?

Let’s find out!

Activity:
A Wild USB Appears!



Suggested Time:

15 mins

Activity: A Wild USB Appears!

In your breakout groups, discuss the following scenario and questions:

When plugged into a computer, the USB drive immediately executes running code.

- How is a USB drive able to do this?
- Why can't our computer stop the drive from running?
- How might we defend against USBs like this?

Suggested Time:

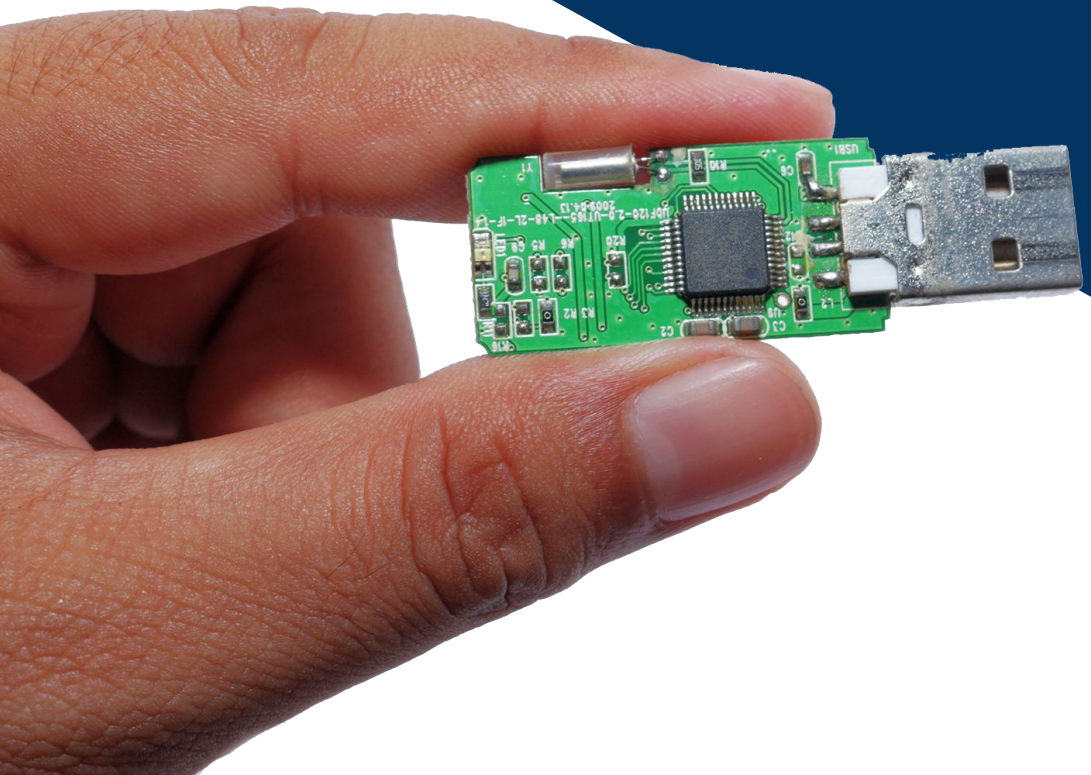
12 Minutes

Time's Up! Let's Review.

Questions?

A Harmless USB?

What if the USB was a **mini keyboard emulator**? When connected, our computer registers it as a keyboard allowing it to kick off without restriction. Like most threats, their appearances are deceptive and seemingly safe.



The CIA Triad

Now, we will move on to our first concept: the three cornerstones of information security, known as **the CIA triad.**

What do each of these words mean to you?

Confidentiality

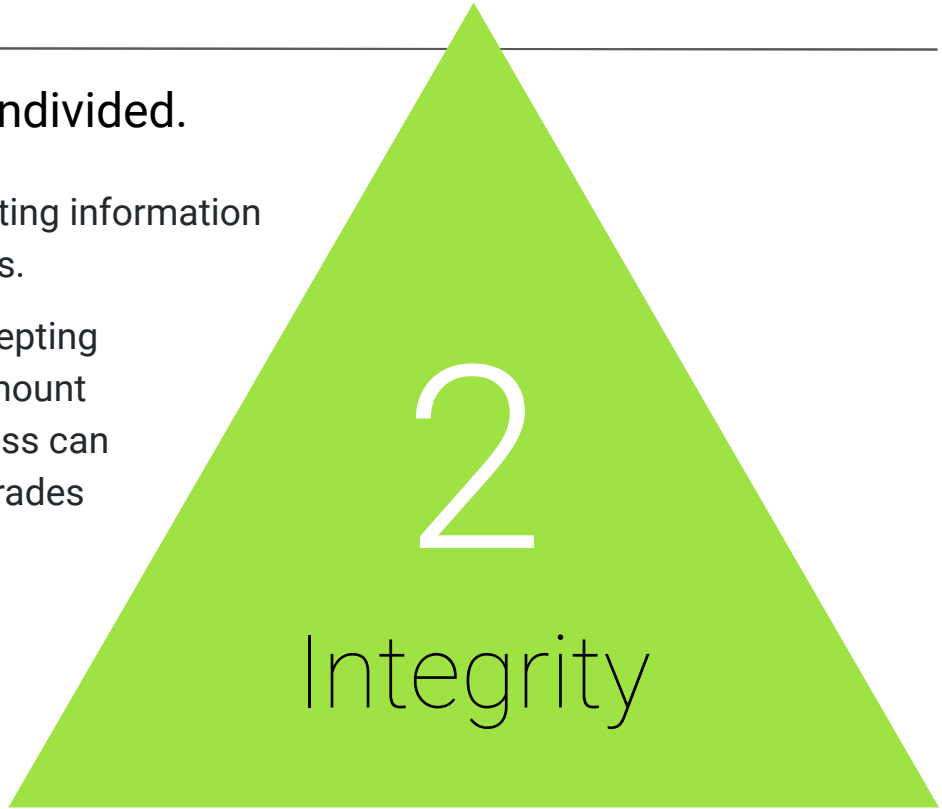
The state of being kept secret or private.

- This corner of the CIA triad is all about ensuring sensitive information does not reach unauthorized people.
- Examples of confidentiality attacks include uploading private photos and communications onto a forum and exposing credit card numbers online.
- Confidentiality comes down to the principle of “need to know.” Data or information should only be made available to those who need access to it.
- Confidentiality is enforced through measures like encryption and authentication.

Integrity

The quality of being honest, whole, or undivided.

- The integrity of information refers to protecting information from being modified by unauthorized parties.
- Examples of integrity attacks include intercepting money transfers and changing the dollar amount in seemingly insignificant ways, so the excess can be sent elsewhere, and altering university grades to be better or worse.
- Integrity attacks can be avoided by using a secure hashing algorithm and process when transferring data to ensure it isn't tampered with in transit.



Availability

The quality of being able to be used or obtained.

- Availability concerns occur when operating systems, equipment, and data are not functioning correctly, limiting accessibility to those who need it.
- Examples of availability attacks include bad actors taking down a web-connected generator and disabling a critical power supply, and using a denial of service attack to bring down a financial service provider's website, making it impossible for clients to make transactions.
- Creating regular backups of data is one way to maintain availability.

We will revisit these terms regularly throughout the course, and explain how various topics, skills, and practices are concerned with protecting each.

Activity: CIA Triad Security Scenario

In this activity, you will analyze a variety of brief security scenarios and identify which element of the CIA triad (confidentiality, integrity, availability) each situation is concerned with.

Suggested Time:

12 Minutes

Time's Up! Let's Review.

Questions?

Next Class

We will dive deeper into assessing risk and mitigating threats by evaluating specific attacks and vulnerabilities of users, web applications, servers and databases.


The End