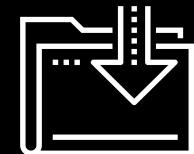




The Cybersecurity Mindset

Cybersecurity
Lesson 1.1



All students will receive
access to CompTIA
CertMaster Practice for
Security+.

The **CompTIA CertMaster Practice for Security+** is an adaptive knowledge assessment and certification training companion tool that helps you prepare for the Security+ CompTIA exam.

- It features question-first design, real-time learning analytics, and content refreshers to reinforce and test what you know and close knowledge gaps.
- You will receive access later in the course when it is covered.

All graduates in good standing will receive
CompTIA Exam Voucher Choice.

Upon graduating in good standing, you will receive a
CompTIA Exam Voucher for one of the following exams:

- Security+, Network+, Linux+, Server+, or Cloud+
- If you choose a voucher other than Security+, you will receive access to a second Certmaster practice tool that aligns with your choice.
- Your Career Director will be available to help you decide which voucher is best for you based on your skill set and professional goals.
- Vouchers will be sent via email and are valid for 12 months.

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 cyber attacks are becoming more sophisticated, aggressive, and disruptive than ever before.



The screenshot shows a news article from CNBC.com. The header features the NBC peacock logo and the word "CNBC". Below the logo is a dark blue navigation bar with categories: MARKETS, BUSINESS, INVESTING, TECH, POLITICS, CNBC TV, WATCHLIST, CRAMER, and PRO. The main title "TECH" is in a small font above the main headline. The headline reads "Solarwinds hackers are targeting the global IT supply chain, Microsoft says". Below the headline is the publication date "PUBLISHED MON, OCT 25 2021 7:46 AM EDT". The author is listed as "Sam Shread @SAM_L_SHREAD". To the right of the author's name are sharing icons for Facebook, Twitter, LinkedIn, and Email. A horizontal line separates the author information from the main content. On the left side of the content area, there is a "KEY POINTS" section. The main content consists of three bullet points. The first point discusses the hacking group Nobielum attempting to replicate their past attack methods. The second point details the use of phishing emails and password spray. The third point states that 140 resellers and technology service providers have been targeted so far, with 14 accounts believed to be compromised.

KEY POINTS

- Nobielum, 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 Nobielum so far, according to Microsoft, which said it believes 14 have been compromised.

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.

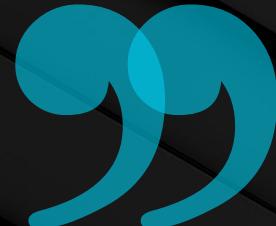
The screenshot shows a web browser window with a dark header bar. The header includes the CSO logo (three horizontal bars followed by the letters 'CSO' and 'FROM IDG'), a 'INSIDER' button, and links for 'Sign In' and 'Register'. Below the header, the word 'FEATURE' is written in orange. The main title of the article is 'Cybercrime: Much more organized' in large, bold, black letters. The article's content begins with the following paragraph:

Cybercrime offers the potential for immense profits. So it is no surprise that the digital “mob” has moved into the space. According to some experts, there is no such thing as “disorganized cybercrime” any more

Reason 5:

70% of cybersecurity 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?

Common 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.

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

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

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.

New Hacking Technique Can Steal Info Through PC Speakers and Headphones

The SIM Hijackers

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



What can be done to stop connected car hacking?

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: Units

01

Security Fundamentals

Learn to think like a cybersecurity professional 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

Network configuration, design, protocols, and data communication. Network security, cryptography, and cloud virtualization and security.

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

SIEM with Splunk. Setting up security monitoring, alerts, dashboards, and custom reports. Using forensic tools to recover deleted data.

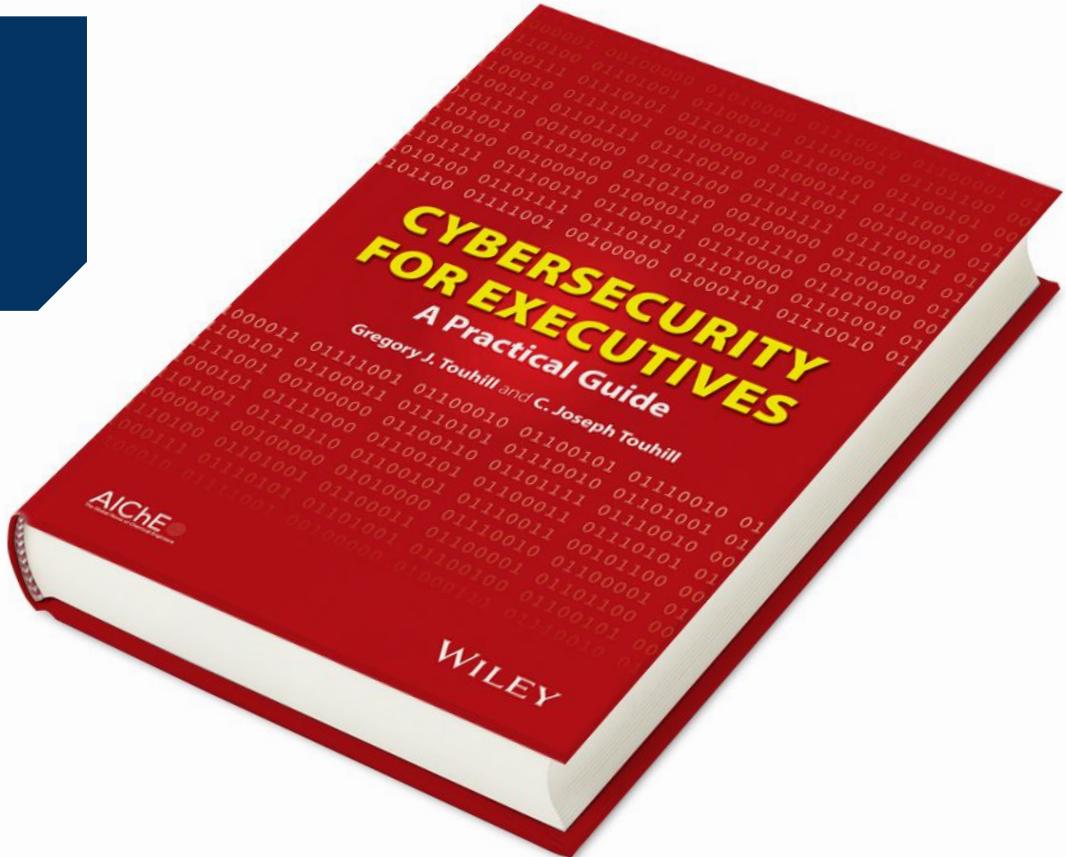
06

Review and Final Projects

Certification prep and review. Interviewing and career prep practice.

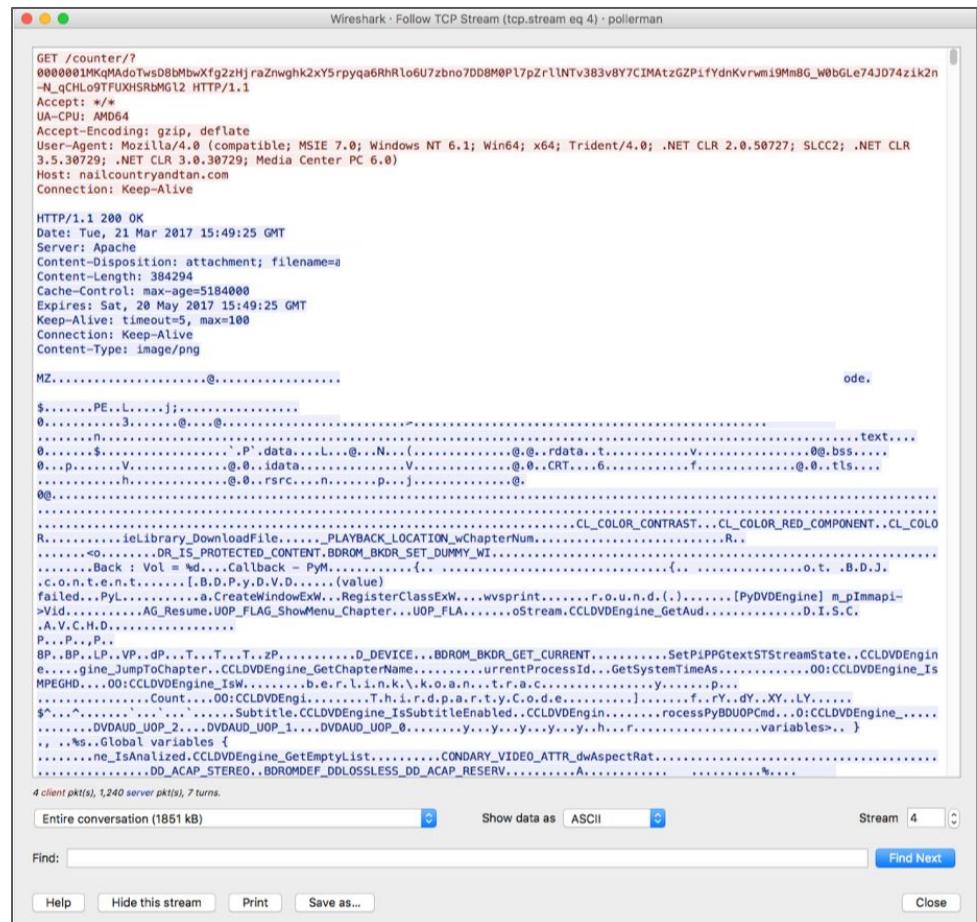
Example Activity: Cybersecurity Policy and Strategy

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



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.



The screenshot shows a Wireshark window titled "Follow TCP Stream (tcp.stream eq 4) · pollerman". The window displays a single TCP stream with the following details:

Request Headers:

```
GET /counter/?  
0000001MKMqAדוTwsD8bMbxFg2zHjraZnwghk2xY5rpvqa6RhRlo6Uzbno7DDBM0P17pZrlINTv3B3v8Y7CIMAtzGZP1fYdnKvrwm19MmBG_W0bGLe74JD74zik2n  
_N_qCHL09TfUXHSRbMG12 HTTP/1.1  
Accept: */*  
UA-CPU: AMD64  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)  
Host: nailcountryandtan.com  
Connection: Keep-Alive
```

Response Headers:

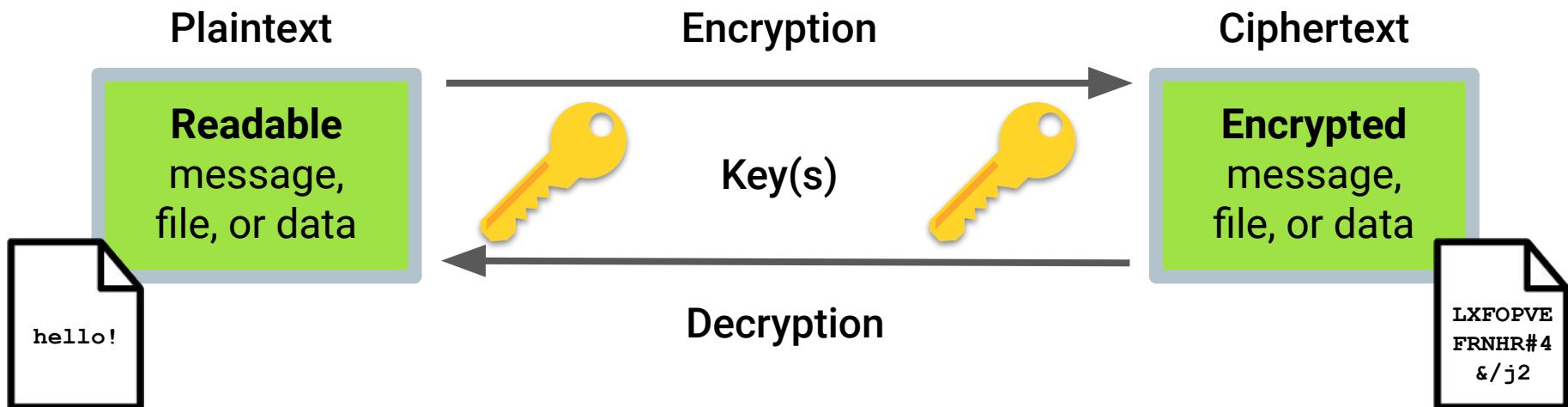
```
HTTP/1.1 200 OK  
Date: Tue, 21 Mar 2017 15:49:25 GMT  
Server: Apache  
Content-Disposition: attachment; filename=  
Content-Length: 384294  
Cache-Control: max-age=5184000  
Expires: Sat, 28 May 2017 15:49:25 GMT  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: image/png
```

Hex and ASCII Data:

The main pane shows the raw hex and ASCII data of the file. The ASCII pane contains numerous characters and symbols, including 'MZ', 'PE', 'L', 'J', '3', 'N', 'P', 'data', 'L', 'N', 'rdata', 't', 'v', 'bss', 'CRT', '6', 'f', 'tls', and various file headers like 'CL_COLOR CONTRAST', 'PLAYBACK_LOCATION', 'DR_IS_PROTECTED_CONTENT', 'BDROM_BKDR_SET_DUMMY_WI', 'Back : Vol = 4d...', 'Callback - Pym...', 'value', 'CreateWindowExW...', 'RegisterClassExW...', 'wvsprintf...', 'round(.)...', '[PyvDEngine] m_pImmapi...', 'AG_Resume.UOP_FLAG_ShowMenu Chapter...', 'UOP_FLA...', 'oStream.CCLDVDEngine_GetAud...', 'D.I.S.C.', 'AVCHD...', 'P...', 'BP...', 'LP...', 'VP...', 'DP...', 'T...', 'ZP...', 'D_DEVICE...', 'BDROM_BKDR_GET_CURRENT...', 'SetPIP.GetTextSTStreamState...', 'CCLDVDEngine...', 'gine_JumpToChapter...', 'CCLDVDEngine_GetChapterName...', 'urrentProcessId...', 'GetSystemTimeAs...', '00:CCLDVDEngine_IsMPEGHD...', '00:CCLDVDEngine_IsW...', 'be.r.l.in.k.\ko.an.tr.r.a.c...', 'y...', 'p...', 'Count...', '00:CCLDVDEngine...', 'T.h.i.r.d.p.a.r.t.y.C.o.d.e...', 'f...', 'r...', 'y...', 'X...', 'L...', '\$^...', '...', 'Subtitle.CCLDVDEngine_IsSubtitleEnabled...', 'CCLDVDEngine...', 'rocessPyBDUOPCmd...', '0:CCLDVDEngine...', 'DVDAUD_UOP_2...', 'DVDAUD_UOP_1...', 'DVDAUD_UOP_0...', 'y...', 'y...', 'y...', 'y...', 'h...', 'r...', 'variables...', '...Global variables {', '...ne_IsAnalyzed.CCLDVDEngine_GetEmptyList...', '...CONDARY_VIDEO_ATTR_dwAspectRat...', '...DD_ACAP_STEREO...', '...BDROMDEF_DDLOSSLESS_DD_ACAP_RESERV...', '...A...', '%...', '...Entire conversation (1851 kB)', 'Show data as ASCII', 'Stream 4', 'Find Next', 'Help', 'Hide this stream', 'Print', 'Save as...', 'Close']

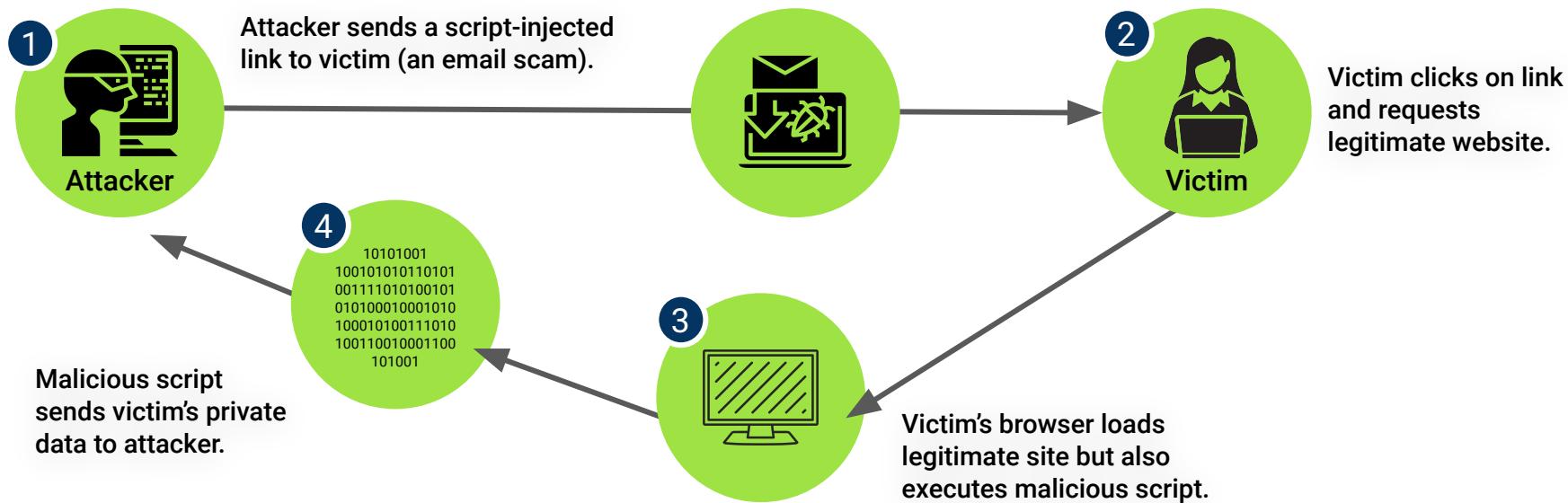
Example Activity: **Encryption / Decryption Systems**

We'll learn how modern cryptography works and how to break historic methods of encryption.



Example Activity: Web Application Hardening

We'll learn how to defend web applications 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.

The image displays two windows side-by-side. The left window is titled 'MSFConsole' and shows a terminal session with the following text:

```
+ ---[ msfconsole v2.4 (100 exploits - 75 payloads)
msf > show exploits
Metasploit Framework Loaded Exploits
=====
3Com_3cdaemon_ftp_overflow      3Com_3cdaemon_FTP_Server_Overflow
Credits                           Metasploit Framework Credits
afp_loginexec                    AppleFileServer_LoginExt_PathName_Overflow
ain_gosaway                       AOL_Instant_Messenger_gosaway_Overflow
altn_webadmin                     Alt-N_WebAdmin_USER_Buffer_Overflow
apache_chunked_win32              Apache_Win32_Chunked_Encoding
arkiea_agent_access               Arkiea_Backup_Client_Remote_Access
arkiea_type77_nacos               Arkiea_Backup_Client_Type_77_Overflow_(Mac_OS_X)
>                               Arkiea_Backup_Client_Type_77_Overflow_(Win32)
arvastas_configdir_remote_exec    AVSTATS_configdir_Remote_Command_Exection
bacupuxexec_agent                Veritas_Backup_Exe_Windows_Remote_Agent_Overflow
bacupuxexec_dump                 Veritas_Backup_Exec_Windows_Remote_File_Access
bacupuxexec_ns                   Veritas_Backup_Exec_Namespace_Overflow
bacupuxexec_registry              Veritas_Backup_Exec_Server_Registry_Access
badblue_ext_overflow              BadBlue_2.5_EXT.dll_Buffer_Overflow
badblue_netwaut_heap              Backbone_NetWare_Remote_Sleep_Overflow
backbone_pcap_digilog             Backbone_PCAP_Digilog_Connection
blackice_panic_icq                ISS_FGM.dll_ICQ_Farser_Buffer_Overflow
cabrightstor_disco               CA_BrightStar_Discovery_Service_Overflow
cabrightstor_disco_servicepcpc  CA_BrightStar_Discovery_Service_SERVICPC_Overflow
cabrightstor_sagagent             CA_BrightStar_Agent_for_Microsoft_SQL_Overflow
cabrightstor_unisagent            CA_BrightStar_Universal_Agent_Overflow
cacti_graphimage_xsec              Cacti_graph_image.php_Remote_Command_Exection
caliclient_getconfig              CA_License_Client_GETCONFIG_Overflow
calicserv_getconfig               CA_License_Server_GETCONFIG_Overflow
distcc_exec                       DistCC_Daemon_Command_Exection
edirectory_imonitor              eDirectory_8.7.3_iMonitor_Remote_Stack_Overflow
exchange2000_xexch50              Exchange_2000_MS03-46_Heap_Overflow
msf > 
```

The right window is a diagram titled 'METASPOILIT by Rapid7' with the following text:

```
+
+-----+ METASPOILIT by Rapid7 +-----+
|==c ( o( _ )_)=\\
|   / \ / \ / \ / \
|   \ \ \ \ \ \ \ \ \
|     RECON
|-----+-----+
|   " " " " " | =====[ ***
|   EXPLOIT \ \
|   ==[ msf > ]===== \
|   \(@) (@) (@) (@) (@) (@) (@) / \\
|   ***** * * * * * * * * * * * * *
|-----+-----+
|   \ \ \ \ \ \ / \
|   )=====(
|     LOOT
|-----+-----+
|   ^ ^ ^ ^ ^ | l
|   PAYLOAD
|   = = = = = = = =
|   (@) (@) " " " * | (@) (@) * * | (@)
|-----+-----+
```

Capture the Flag

Throughout the course, we'll also work through Capture the Flag (CTF) 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.

Four Projects

Project 1

Securing Cloud Apps:

In the first project week, you will build, secure, and protect a cloud application.

Project 2

Offensive Security CTF:

A three-day CTF in which you will use the skills that you have learned in the Offensive Security module to attack a fictional organization and determine their vulnerabilities.

Project 3

Building a Monitoring Solution:

You will design a custom monitoring solution for a fictional organization, monitoring the environment during a series of simulated attacks.

Project 4

bootCon:

In the final project, you will present independently researched projects that demonstrate one of the following:

1. Exploiting a vulnerability of an IOT device.
2. Developing code or a program that can complete a cybersecurity task.
3. Demonstration of how a cybersecurity tool that was not covered in class can accomplish a specific goal.



Tools We'll Use

We will use **virtual machines** to operate 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

You'll use three categories of lab solutions 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'll 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 run using VirtualBox.



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



Tools We'll Use: Vagrant Local Machines

We will use Vagrant with VirtualBox in the following modules:



Terminal



Linux Systems Administration



Linux Archiving and Logging Data



Bash Scripting and Programming



Networks I and II



Cryptography



Web Development

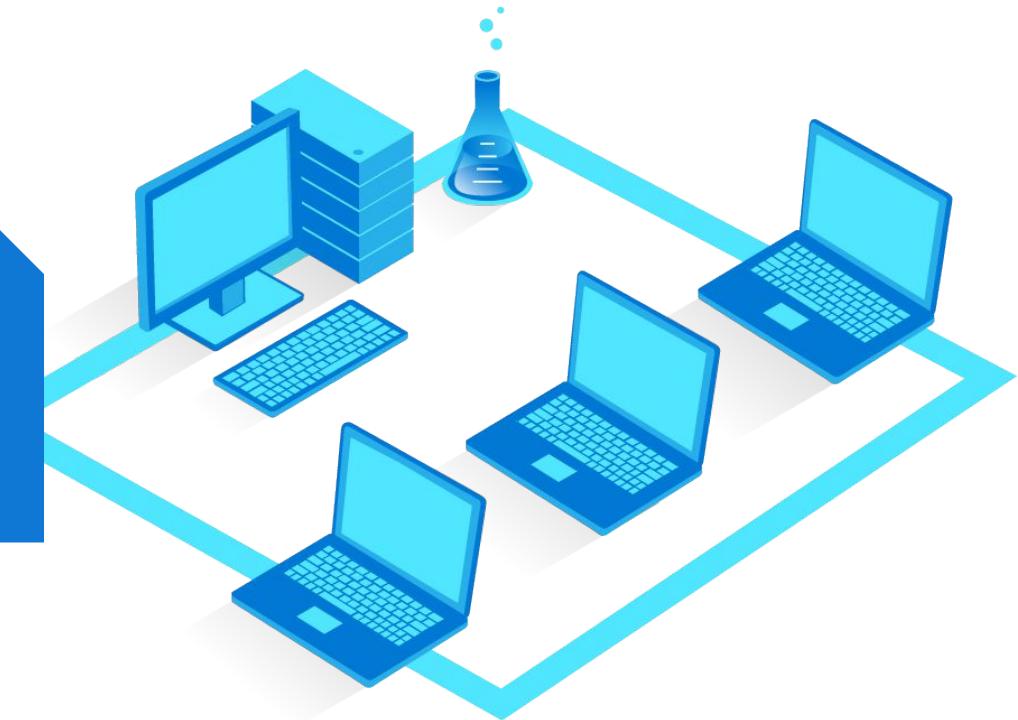


SIEM I and II

Tools We'll Use: Azure Lab Services

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

Why might we need to run multiple virtual machines at the same time?



Tools We'll Use: Azure Lab Services

We 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 the defensive security modules.

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 backups.

Tools We'll Use: Azure Lab Services

We'll use Azure Lab Services in the following modules:



Windows Administration and Hardening



Pentesting I



Pentesting II



Project 2



Forensics

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 become 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.

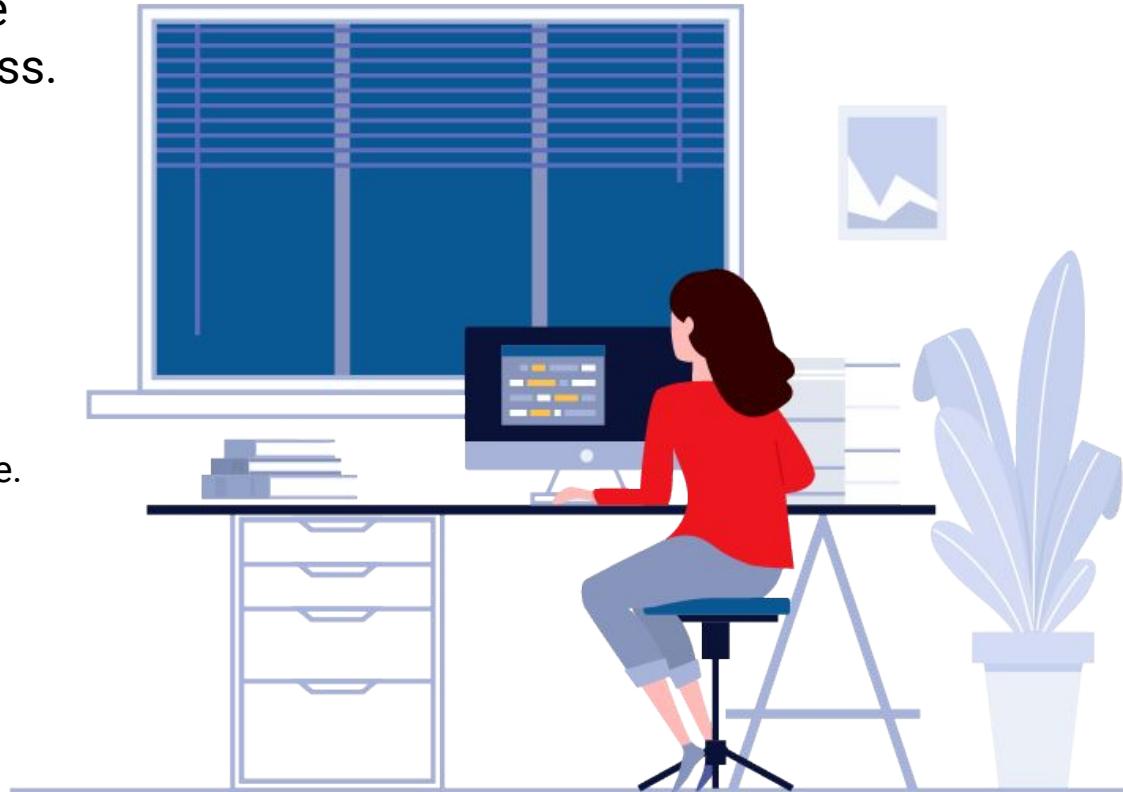


Tips: Online Learning

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,
Challenge assignments,
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 completing Challenge assignments.
- 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. Countless organizations worldwide use this tool, and you'll use 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

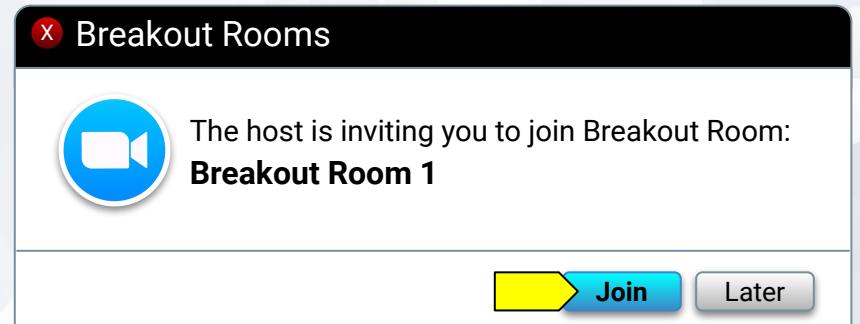
Assessing Threats: A Wild USB Appears!

Let's say we find a USB drive lying 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?

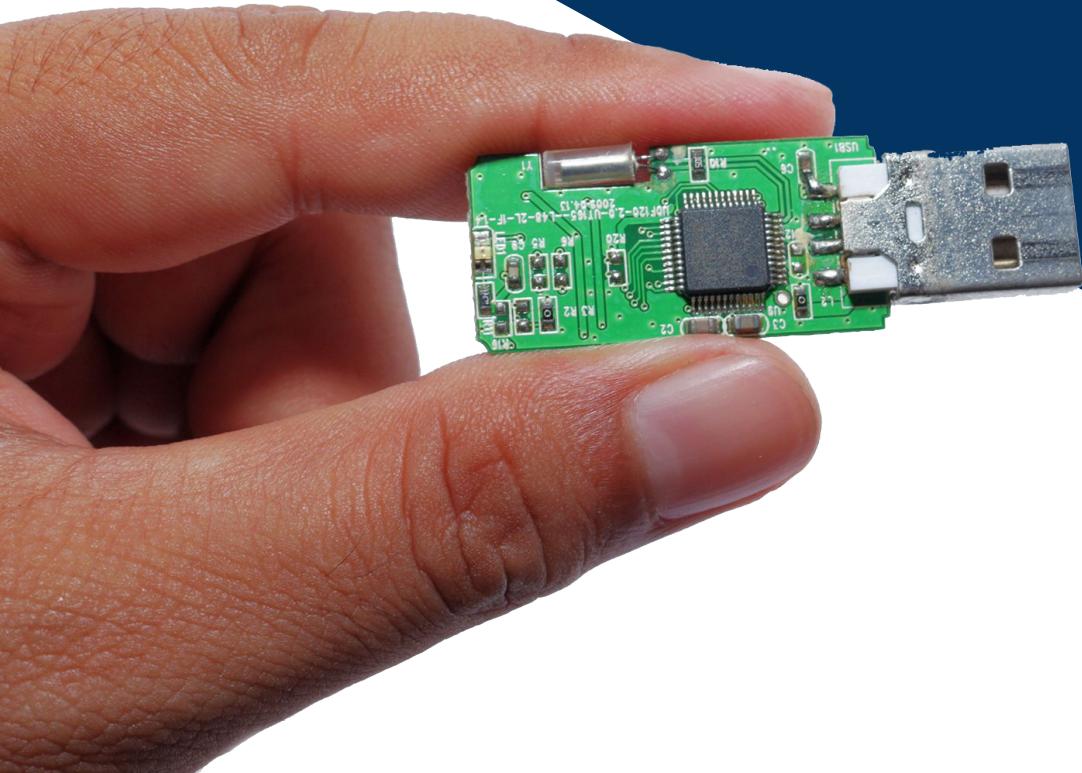


A Harmless USB?

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, its appearance is deceptive and seemingly safe.



The CIA Triad

The three cornerstones of information security are known as the **CIA triad**.



What do each of these words mean to you?



Confidentiality

The state of being kept secret or private.

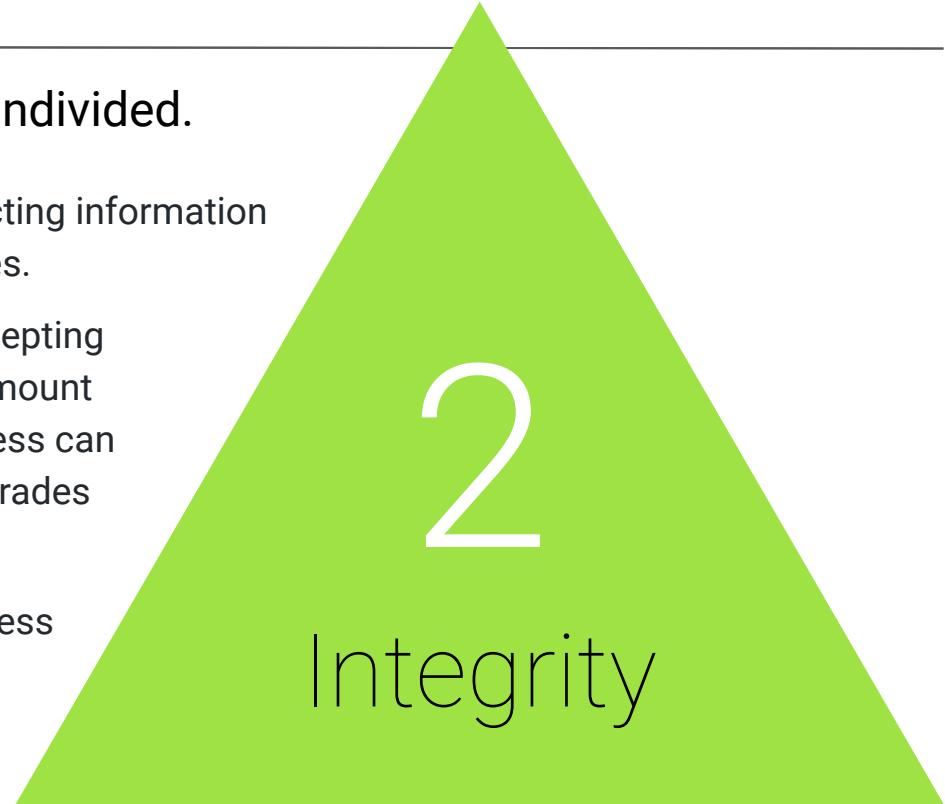
- This corner of the CIA triad is all about ensuring that sensitive information does not reach unauthorized people.
- Examples of confidentiality attacks include uploading private photos and communications onto a forum and exposing credit card numbers online.
- Confidentiality comes down to the principle 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.
- Using a secure hashing algorithm and process when transferring data to ensure it isn't tampered with in transit can help prevent integrity attacks.



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 access to those who need it.
- ▶ Examples of availability attacks include bad actors taking down a web-connected generator and disabling a critical power supply, or 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 concerns.

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*