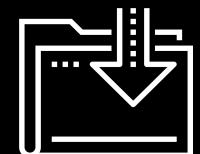




The Cybersecurity Mindset

Cybersecurity
Cybersecurity 101 Day 1



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

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



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.
- 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.



Articulate 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.

The Switch

Equifax's massive 2017 data breach keeps getting worse



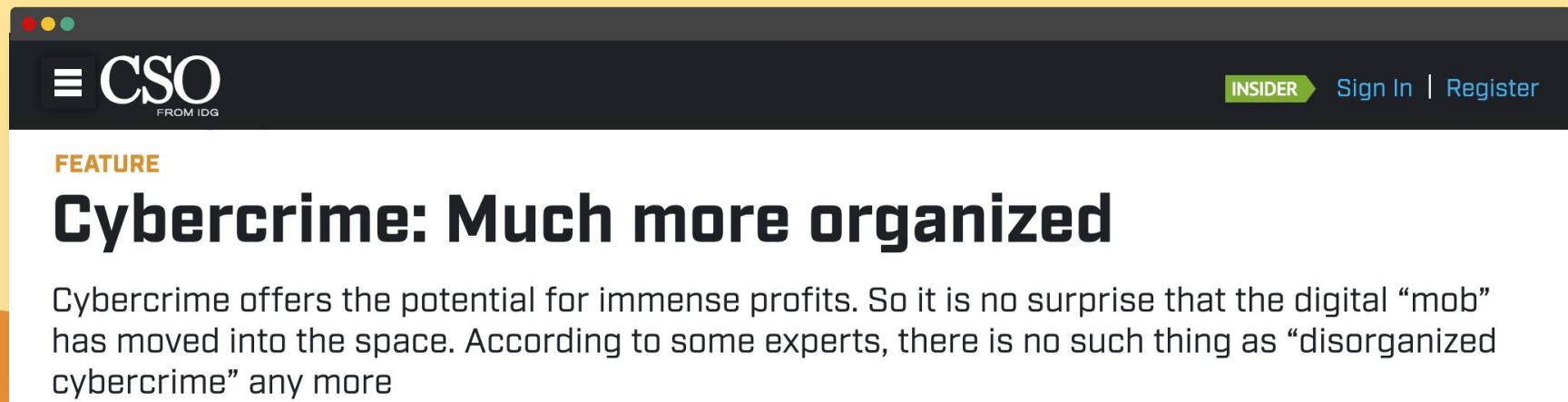
(Michael Nagle/Bloomberg News)

By Brian Fung
March 1, 2018

Equifax said Thursday that 2.4 million more consumers than previously reported were affected by the massive data breach the company suffered last year, adding to an already stunning toll.

Reason 4: Significant Investment by Bad Actors

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

A screenshot of a web page from CSO Online. The header features the CSO logo and navigation links for 'INSIDER' and 'Sign In | Register'. A 'FEATURE' tag is visible above the main article. The main title of the article is 'Cybercrime: Much more organized'. The article text discusses the shift from lone hackers to organized cybercrime due to its potential profits.

FEATURE

Cybercrime: Much more organized

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: Dire Shortage of Skilled Professionals

According to studies by (ISC)², there will be over 1.5 million unfilled cybersecurity positions by 2020.



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

Defining Cybersecurity



What is the first thing
you think of when you
hear “cybersecurity”?

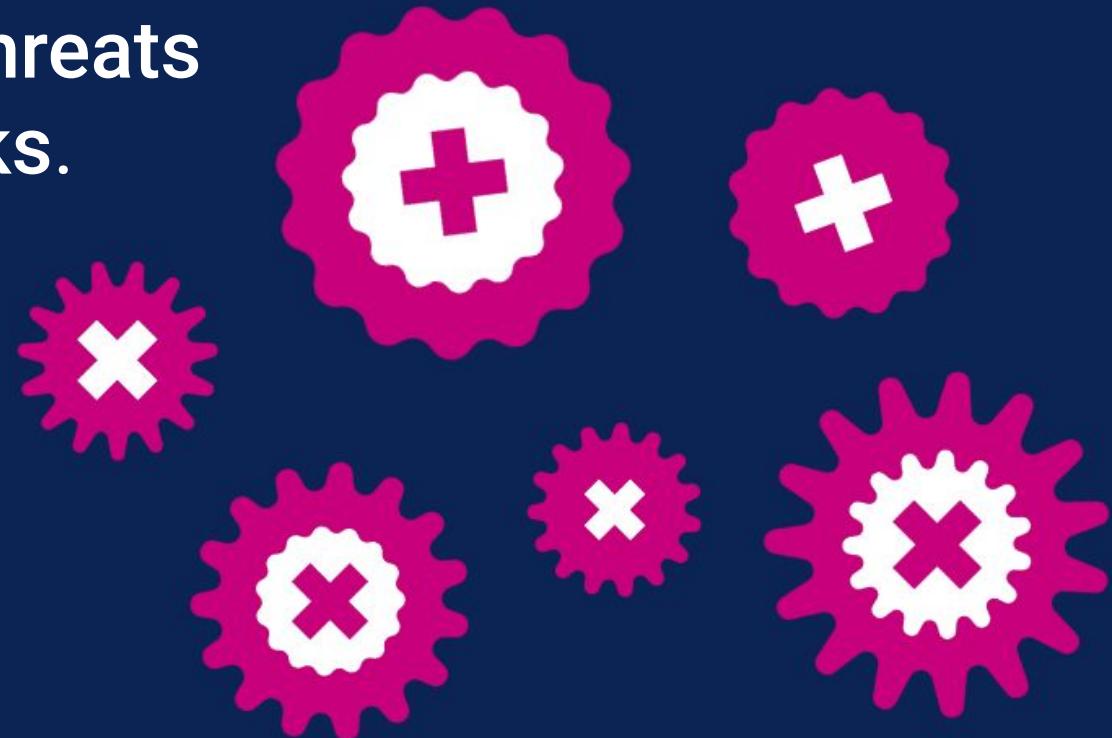
Everyone's First Thoughts:

Hackers and complicated code...

*But cybersecurity isn't about
hackers 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

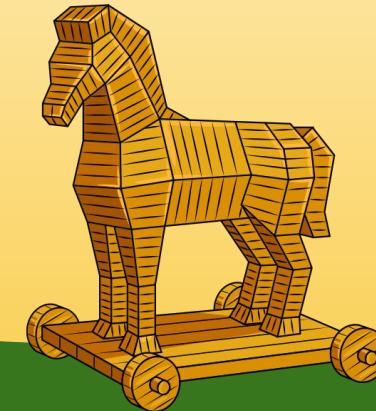
26TH JUNE 2018 2:54PM

DIGITAL DISRUPTION

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**.



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

Course Overview

Daily Routine

In class, we'll run through the following:



Objectives



Brief background lecture



Instructor demonstrations



Thought exercises



In-class skill builders



Project work

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. Hands-on 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.

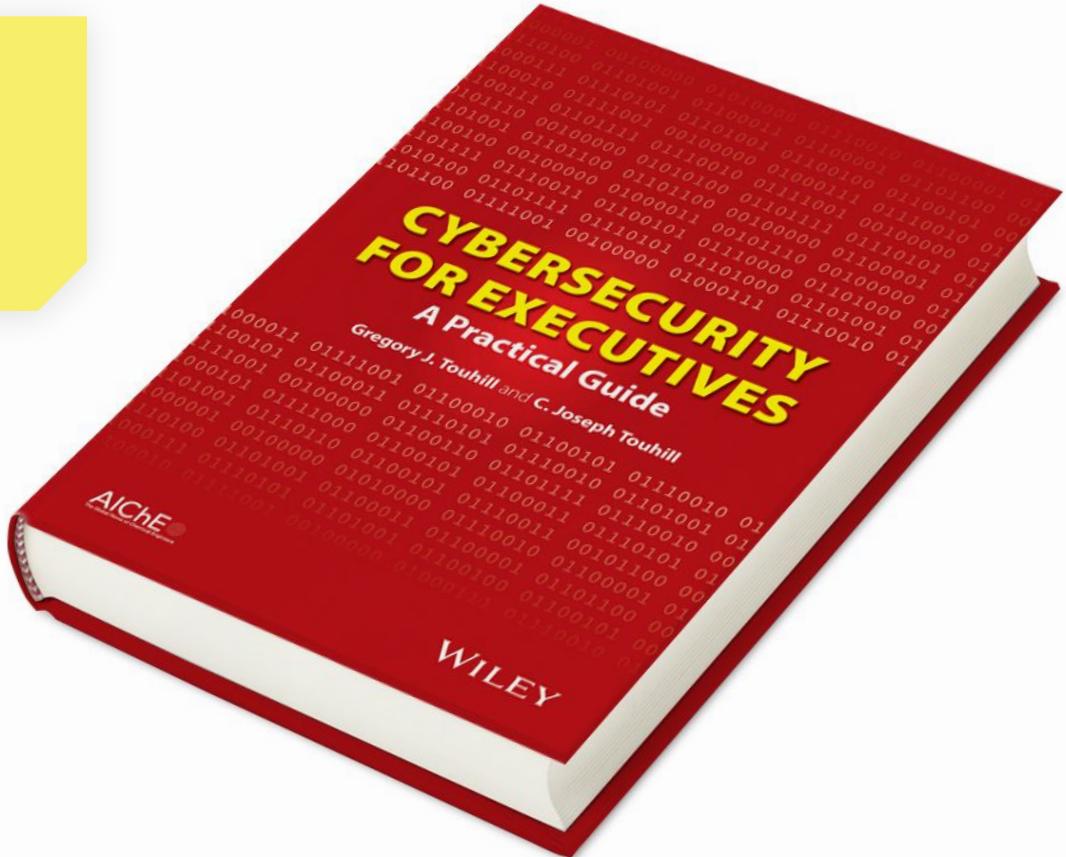
06

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.



Wireshark - Follow TCP Stream (tcp.stream eq 4) · polierman

```

GET /counter/
000001MKMqMAdoTwSD8bMbxFg2zHjraZnwghk2xY5rpqqa6RhRl06U7zbn07DD8M0P17pZrl1NTv383vBY7CIMAtzGZPifYdnKrvwm19MmBG_W0bGLe74J074zik2n
-N_qCHL9sTfUXHSRMQ12 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

HTTP/1.1 200 OK
Date: Tue, 21 Mar 2017 15:49:25 GMT
Server: Apache
Content-Disposition: attachment; filename=a
Content-Length: 384294
Cache-Control: max-age=5184000
Expires: Sat, 20 May 2017 15:49:25 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

MZ.....@.....ode.
$.....PE..L.....];
0.....3.....@.....;
0.....@.....;
0.....$.....'P'.data.....L.....@.....N.....(.....@.....rdata.t.....v.....@.bs...text...
0.....p.....V.....@.0.....idata.....V.....@.0.....CRT.....6.....f.....@.0.....tls...
0.....h.....@.0.....rsrc.....N.....p.....j.....@.
0@.....;
R....._elibrary_DownloadFile.....PLAYBACK_LOCATION_wChapterNum.....CL_COLOR_CONTRAST..CL_COLOR_RED_COMPONENT..CL_COLO
R.....<0.....DR_IS_PROTECTED_CONTENT_BDROM_BDOR_SET_DUMMY_WI.....R.+
.....<0.....Back : Vol = %d....Callback_PyM.....{.....}.....o.t. ....B.D.J.
.....content.....[B:D:P:y,D:V,...(value)
failed....PyL.....a.CreateWindowExW....RegisterClassExW....wvprintf.....r.o.u.n.d(.).....[PyDVDEngine] m_pImmapi->Vid.....AG_Resume.UOP_FLAG_ShowMenuChapter...UOP_FLA.....oStream.CCLDVDEngine_GetAud.....D.I.S.
.....A.V.C.H.D. .....
P.....P.+
BP.....LP.....VP.....dP.....T.....T.....zP.....D_DEVICE.....BDROM_BDOR_GET_CURRENT.....SetPIP.GetTextSTStreamState..CCLDVDEngine.....JumpToChapter..CCLDVDEngine_GetChapterName.....urrentProcessId.....GetSystemTimeAs.....00:CCLDVDEngine_IsMPEGHD...0:0:CCLDVDEngine_IsW.....ber.link.\ko.an..tr.a.c.....y.....p. .....
.....Count....0:0:CCLDVDEngi.....T.h.i.r.d.p.a.r.t.y.C.o.d.e.....].....f..ry..XY..LY.....
$^.....^.....Subtile.CCLDVDEngine_IsSubtitleEnabled..CCLDVDEngine.....rocessPyBDUOPCmd..0:CCLDVDEngine.....
.....DVAUD_UOP_2....DVAUD_UOP_1....DVAUD_UOP_0.....y.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.....%.

```

4 client pkts(s), 1,240 server pkt(s), 7 turns.

Entire conversation (1851 kB) Show data as ASCII Stream 4 Find Next

Find: Close

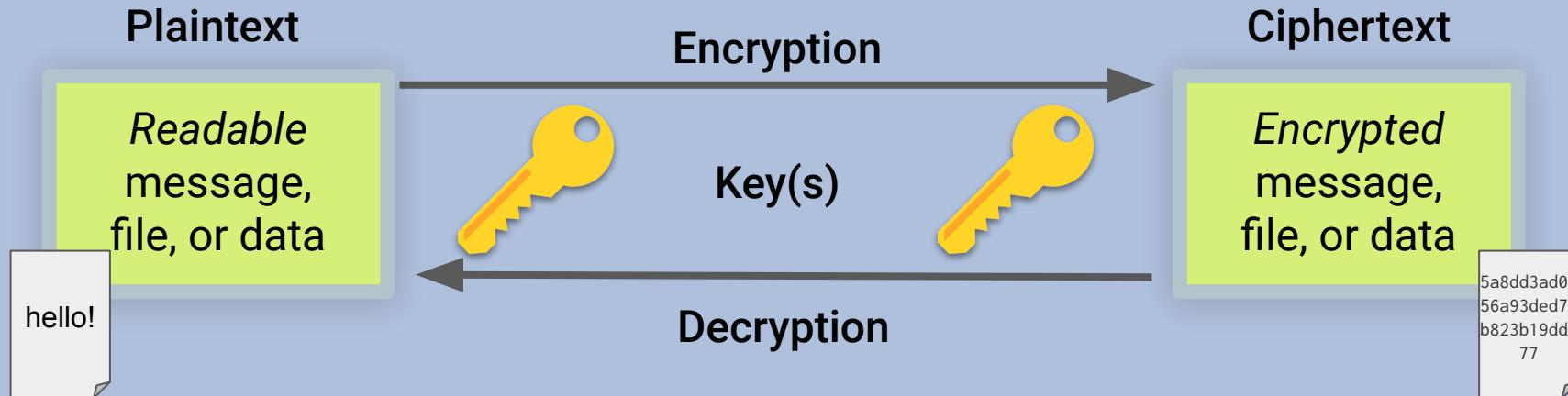
Help Hide this stream Print Save as...

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.

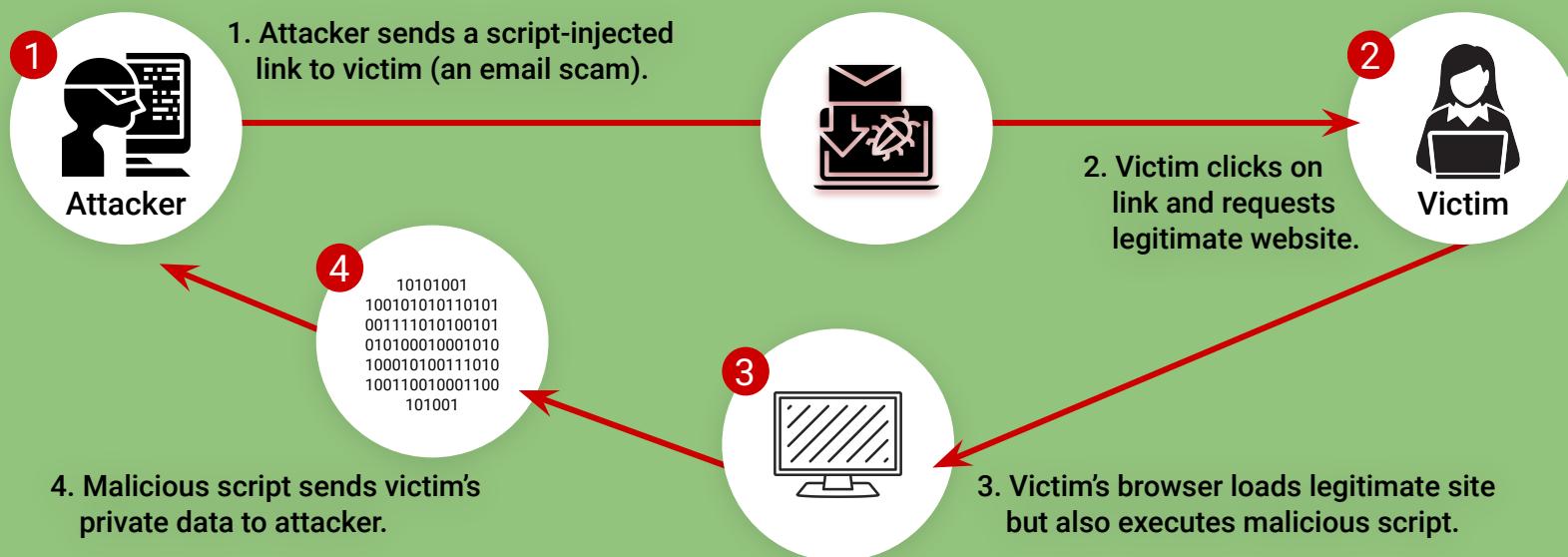
Example Activity: **Encryption / Decryption Systems**

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.

The image shows two windows of the Metasploit Framework. On the left is the MSFConsole window, displaying a list of available exploits and payloads. On the right is a graphical interface titled 'METASPOILIT by Rapid7' which maps the exploit selection process into four distinct phases: RECON, EXPLOIT, PAYLOAD, and LOOT.

MSFConsole Output:

```
+ -- ---[ msfconsole v2.4 (100 exploits - 75 payloads)
msf > show exploits
Metasploit Framework Loaded Exploits
=====
3Com_3cdaemon_ftp_overflow      3Com_3cdaemon_TFTP_Server_Overflow
Credits                           Metasploit Framework Credits
afp_loginexec                    AppleFileServer_LoginExt_PathName_Overflow
ain_gowaway                      AOL_Instant_Messenger_gowaway_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_type77_win32              Arkiea_Backup_Client_Type_77_Overflow_(Win32)
avstats_configdir_Remote_Command_Execution
backupexec_agent                 Veritas_Backup_Exe_Windows_Remote_Agent_Overflow
>
backupexec_dump                  Veritas_Backup_Exec_Windows_Remote_File_Access
backupexec_ns                     Veritas_Backup_Exec_Namespace_Overflow
backupexec_registry               Veritas_Backup_Exec_Server_Registry_Access
hadblue_ext_overflow              BadBlue_2.5_EXT.dll_Buffer_Overflow
backbone_netwatch_heap            Backbone_NetWatch_Remote_Scan_Overflow
backbone_p2p                       Backbone_P2P_Command_Conversation
blackice_p2p_icq                  ISS_FRM.dll_ICQ_Farser_Buffer_Overflow
cabrightstor_disc                CA_BrightStar_Discovery_Service_Overflow
cabrightstor_disc_servicepc      CA_BrightStar_Discovery_Service_SERVICEPC_Overflow
>
cabrightstor_saglient             CA_BrightStar_Agent_for_Microsoft_SQL_Overflow
cabrightstor_unagent              CA_BrightStar_Universal_Agent_Overflow
cacti_graphimage_exec              Cacti_graph_image.php_Remote_Command_Execution
caliclient_getconfig               CA_License_Client_GETCONFIG_Overflow
calicserv_getconfig                CA_License_Server_GETCONFIG_Overflow
distcc_exec                       DistCC_Daemon_Command_Execution
edirectory_imonitor               eDirectory_8.7.3_iMonitor_Remote_Stack_Overflow
exchange2000_xexch50              Exchange_2000_MS03-46_Heap_Overflow
msf >
```

METASPOILIT by Rapid7 Diagram:

```
graph TD
    RECON --> EXPLOIT
    EXPLOIT --> PAYLOAD
    PAYLOAD --> LOOT
    RECON --- EXPLOIT
    EXPLOIT --- PAYLOAD
    PAYLOAD --- LOOT
```

The diagram illustrates the workflow of a penetration test:

- RECON:** Reconnaissance phase, represented by a blue triangle.
- EXPLOIT:** Exploitation phase, represented by a green rectangle.
- PAYOUT:** Payload delivery phase, represented by a red rectangle.
- LOOT:** Data collection phase, represented by a yellow rectangle.

The interface uses various colors (blue, green, red, yellow) and symbols (triangles, rectangles) to visually map the complex process of selecting and executing an exploit.

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.



Projects

These modules and assignments will culminate in three projects:

ELK Stack

The first project follows the Networking and Cloud Security units.

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

Red Team vs. Blue Team

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

Final Project

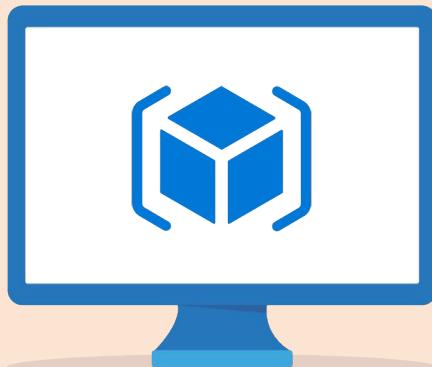
You will exploit a vulnerable web application, create dashboards to see alerts in real time, and analyze live traffic on a virtual network.

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.

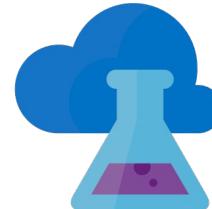


Vagrant
local virtual
machine



VAGRANT

Azure
Cloud Lab
Services



Personal
Azure Cloud
accounts



Azure

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.



ubuntu

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.



Tools We'll Use: Vagrant Local Machines



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



Terminal



Networks I and II



Linux Systems Administration



Cryptography



Linux Archiving and Logging Data



Web Development



Bash Scripting and Programming



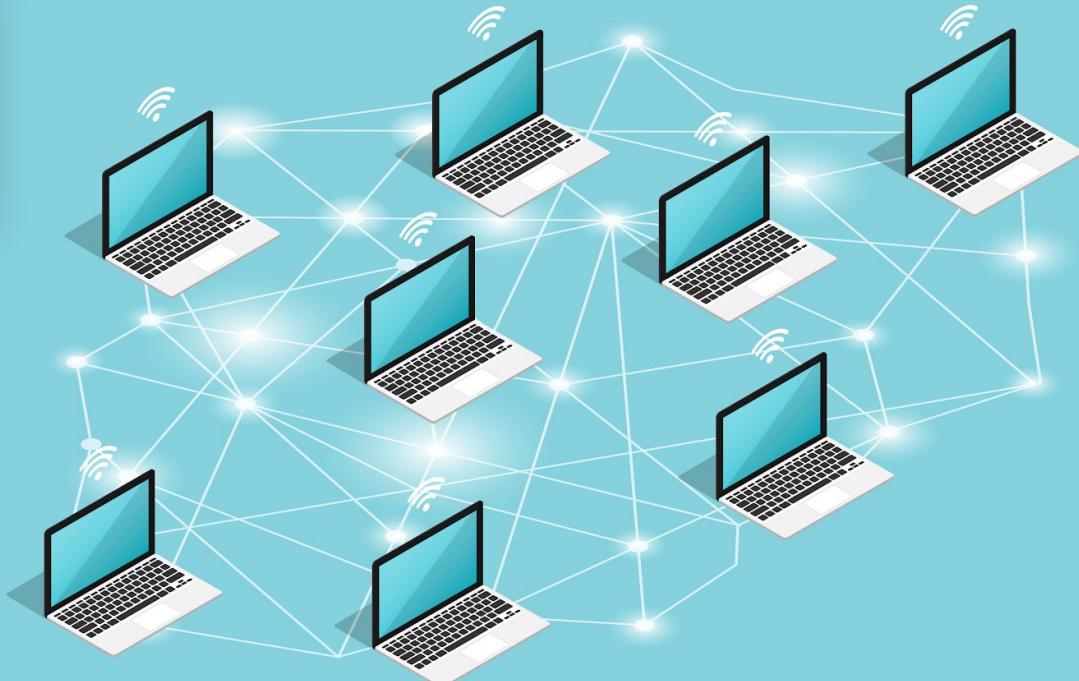
SIEM I and II

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:

01

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.

02

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.

02

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
-  Network Security
-  Web Vulnerabilities
-  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.

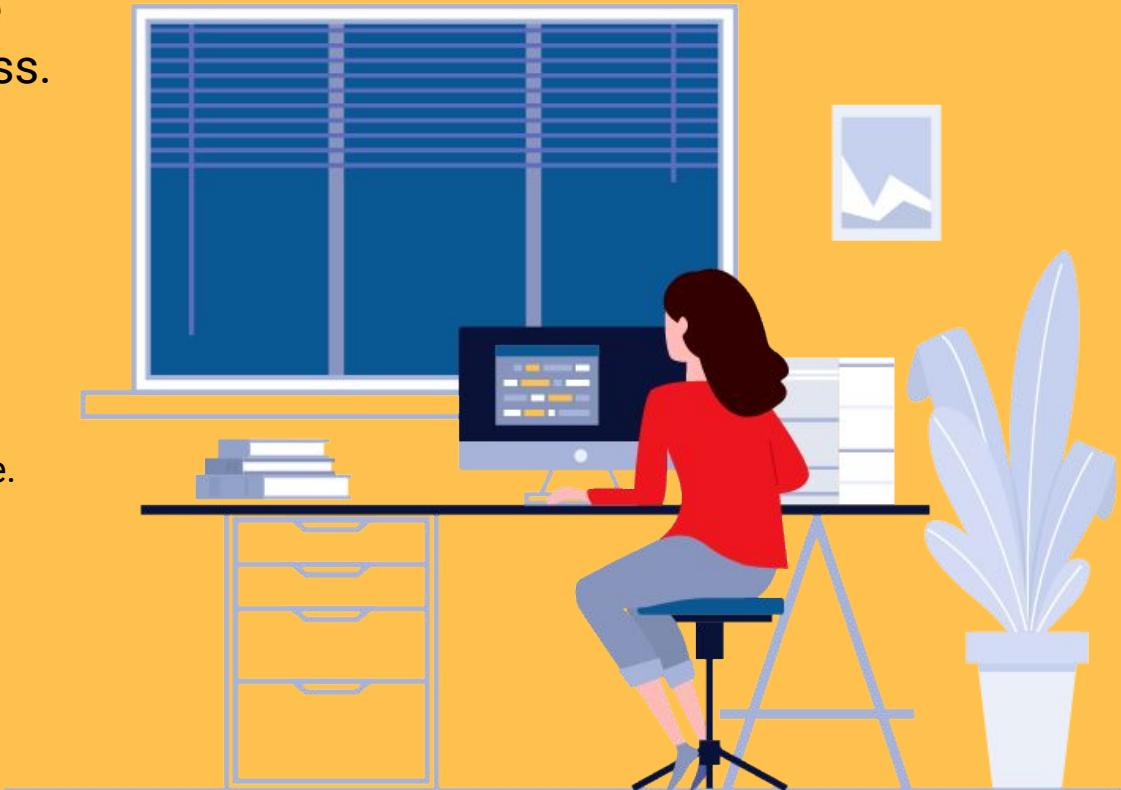


Tips: Online Learning

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 feel 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 speaking, 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

Break



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!





Breakout Rooms

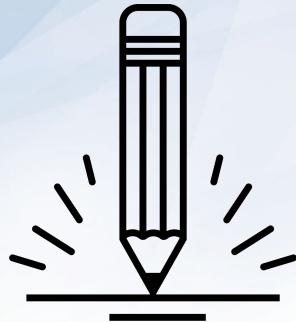


The host is inviting you to join Breakout Room:
Breakout Room 1

 **Join**

Later

Zoom Breakout Room Activity
A Wild USB Appears!



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.

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
- Integrity
- Availability

Confidentiality

The state of being kept secret or private.

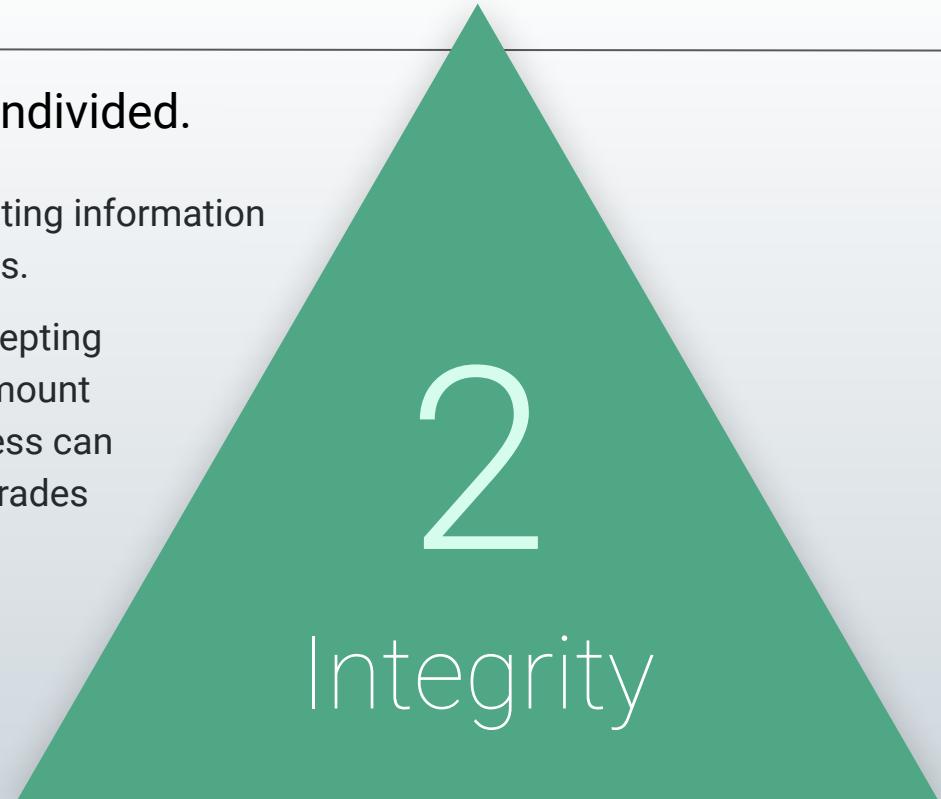
- This corner of the CIA triad is all about ensuring sensitive information does not reach unauthorized people.
- Examples of confidentiality attacks include uploading private photos and communications onto a forum and exposing credit card numbers online.
- Confidentiality comes down to the principle 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.



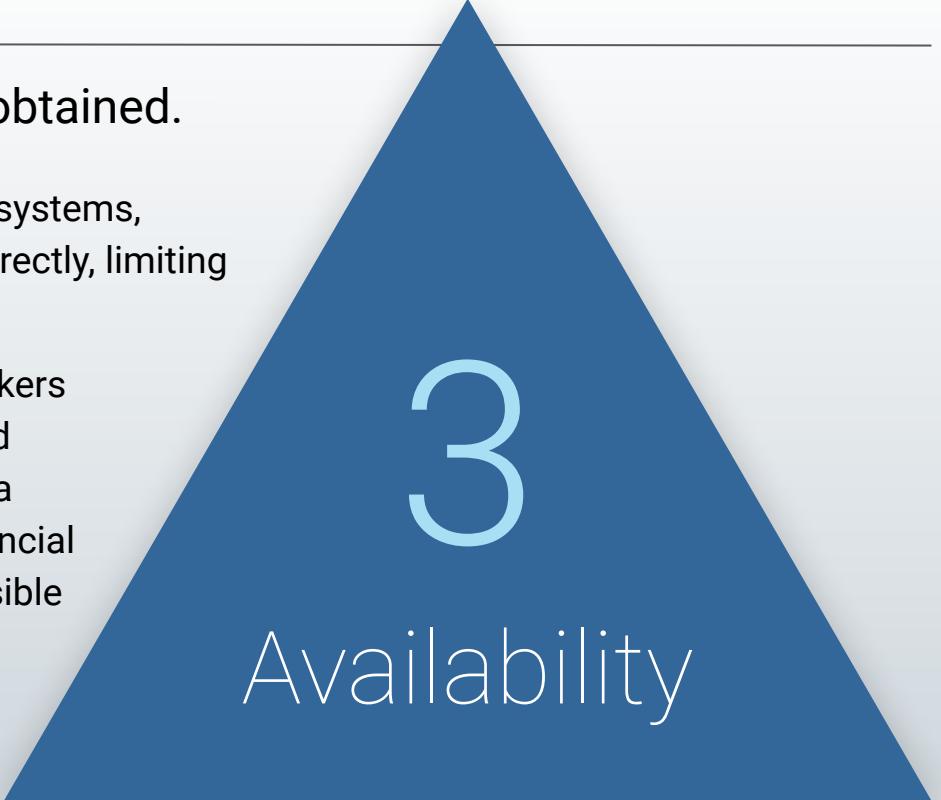
2

Integrity

Availability

The quality of being able to be used or obtained.

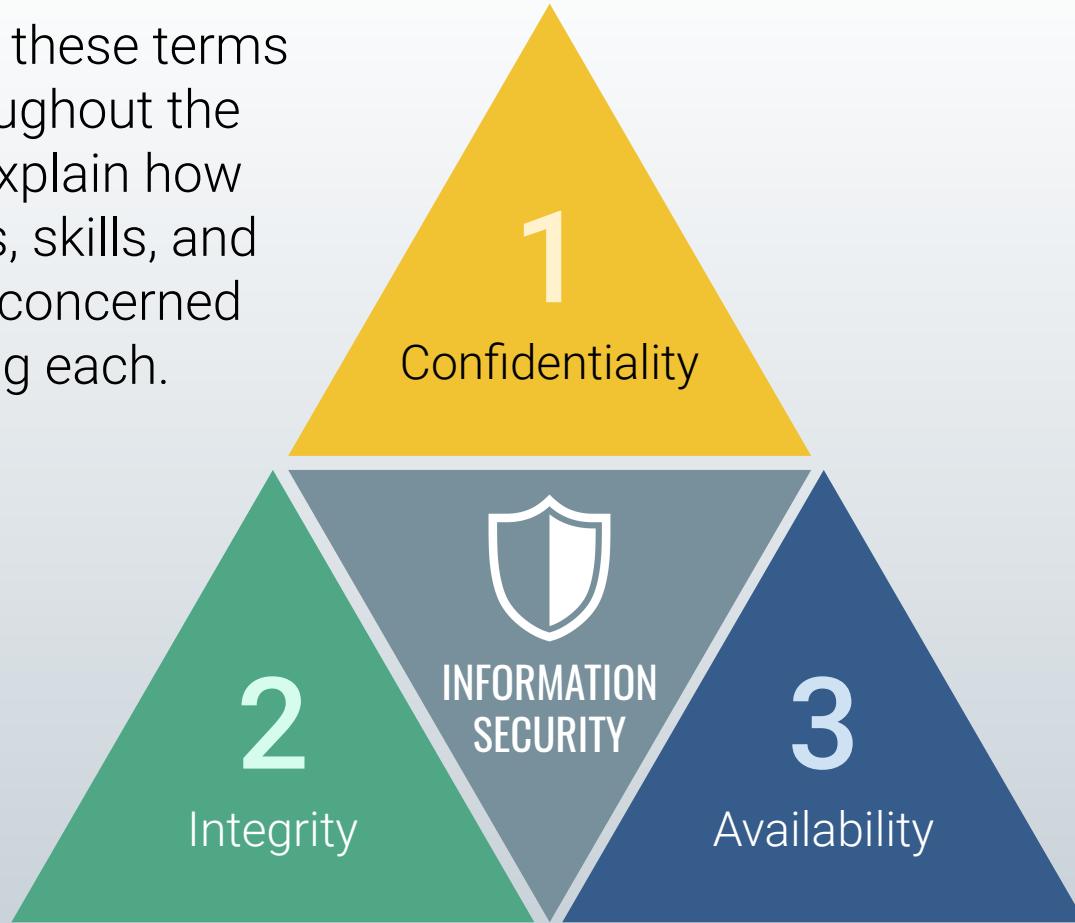
- ▶ Availability concerns occur when operating systems, equipment, and data are not functioning correctly, limiting accessibility to those who need it.
- ▶ Examples of availability attacks include hackers taking down a web-connected generator and disabling a critical power supply, and using a denial 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.

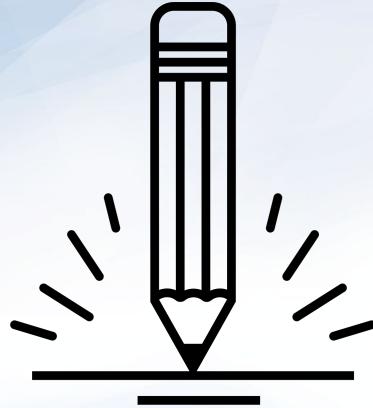


3

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.

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.



Any Questions?

*The
End*