Surveying the Cyberspace

The difference between the impossible and the possible lies in a person's determination.

-Tommy Lasorda

Cybersecurity

Cybersecurity Day 2 *(1.2)*

Class Objectives

By the end of class today, students will be able to:

□ Articulate a clear definition of the CIA Triad and its elements.

□ Define and contextualize technical terms found in recent cybersecurity trends and reports.

□ Utilize cybersecurity trend reports to communicate risk patterns.

□ Conduct and present analysis on a vulnerability, exploit, or threat actor to a non-technical audience using independent research.

Let’s do a quick review!

Quick Review

Last class, we described cybersecurity as centering on **two concepts**.

What were they?

Quick Review

Last class, we described cybersecurity as centering on **two concepts**.

What were they?

Threat Assessment and
Risk Mitigation

Quick Review

How would you define these terms?

Threat Assessment

Risk Mitigation

Quick Review

How would you define these terms?

Threat Assessment

Structured process of identifying the risks posed to a group or system.

Risk Mitigation

Systematic reduction of the impact and/or the likely occurrence of a negative event.

Quick Review

In other words...

Threat Assessment

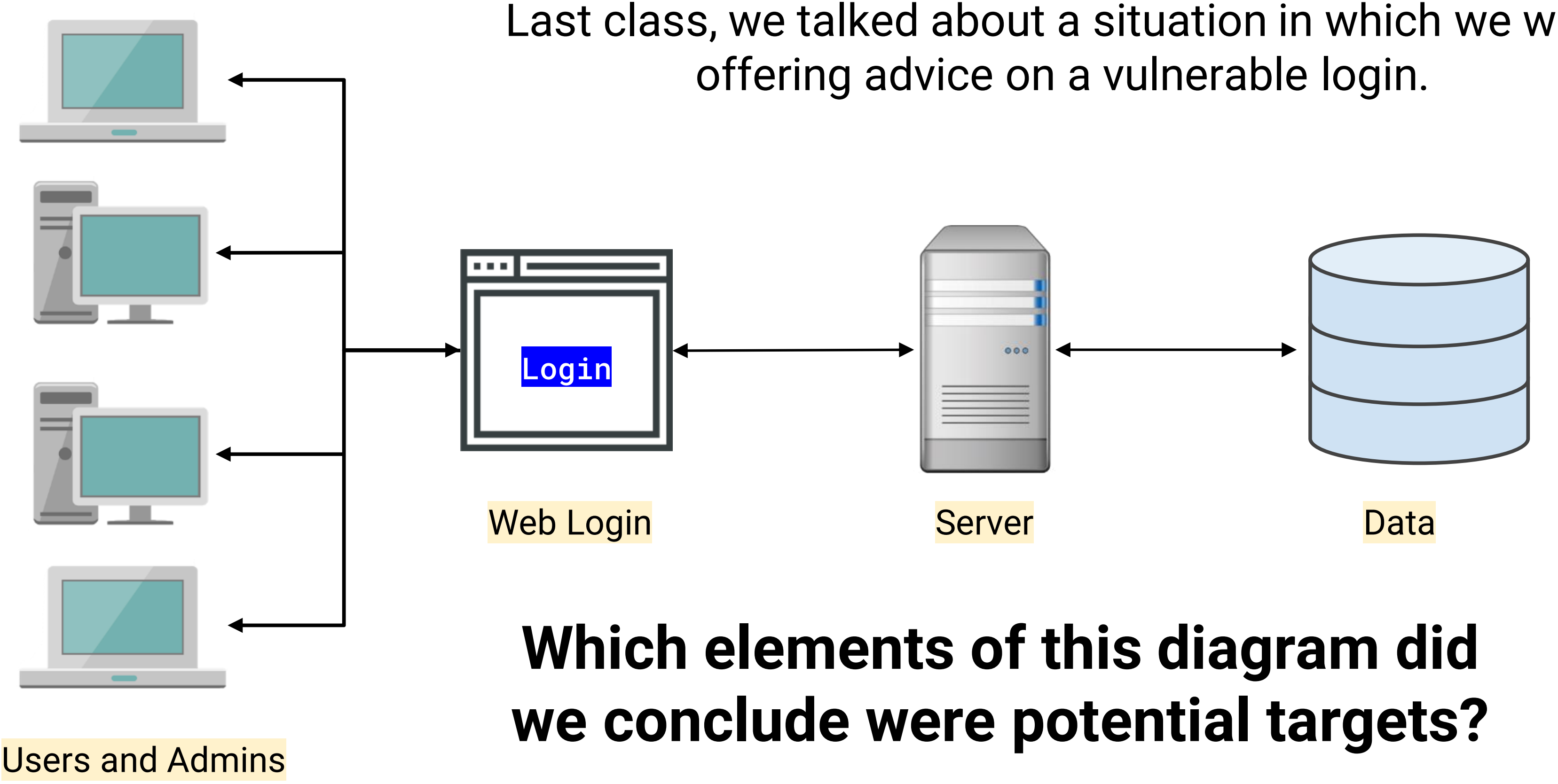
What Could Happen???

Risk Mitigation

How Do we Handle It???

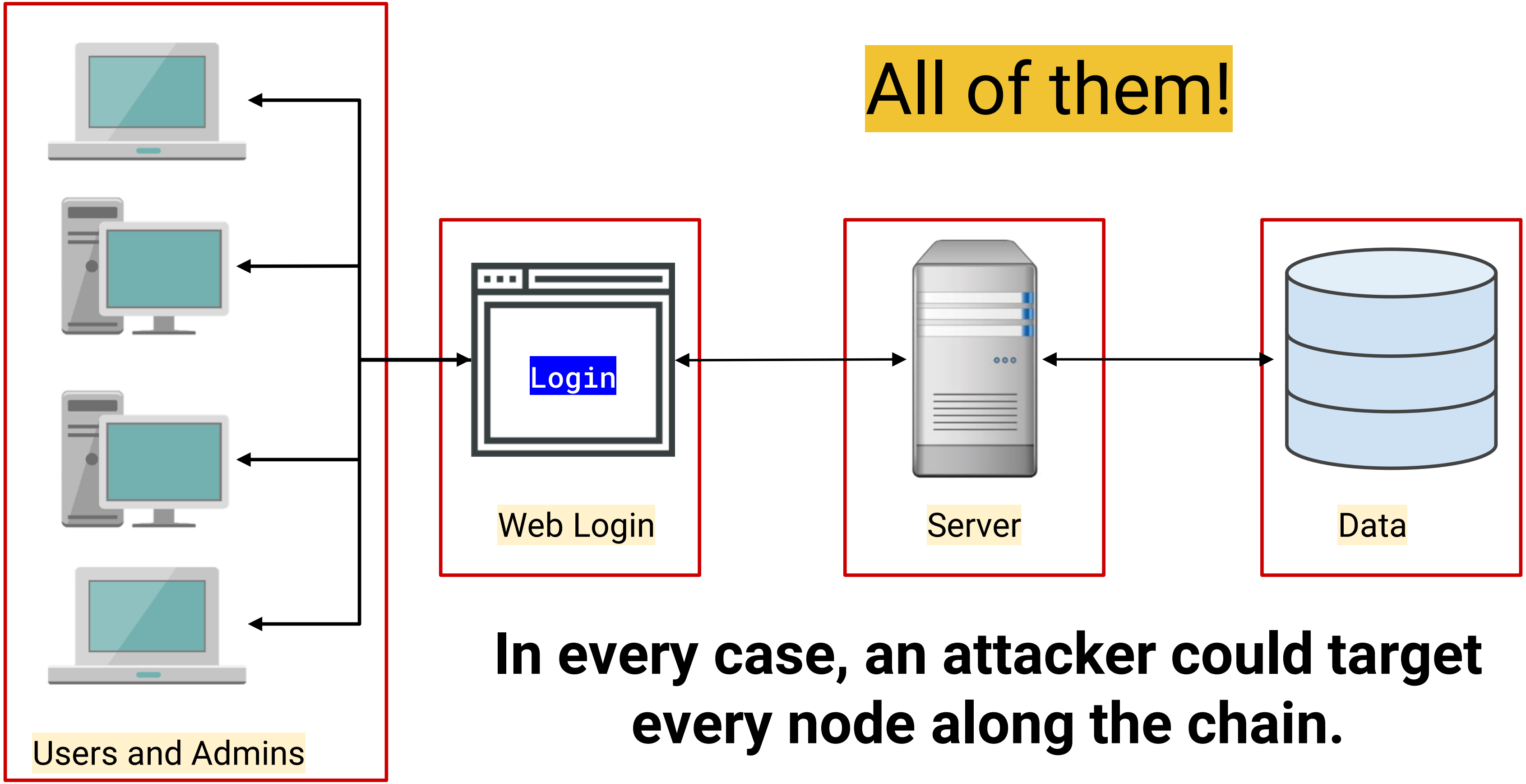
Quick Review

Last class, we talked about a situation in which we were offering advice on a vulnerable login.



Which elements of this diagram did we conclude were potential targets?

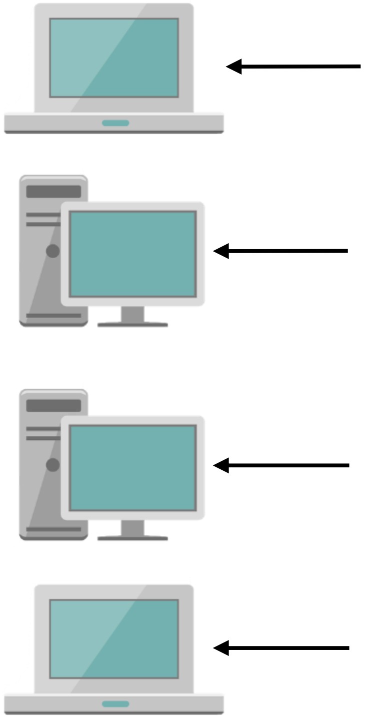
Quick Review



All of them!

In every case, an attacker could target every node along the chain.

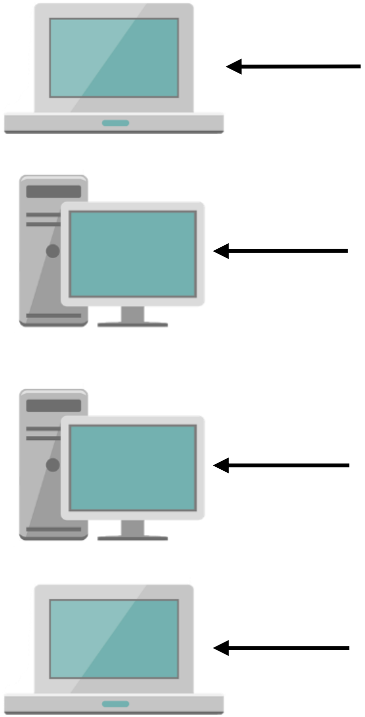
Quick Review



Users and Admins

Name Three User Attacks

Quick Review



Users and Admins

Name Three User Attacks

Malware Attacks

Man in the Middle

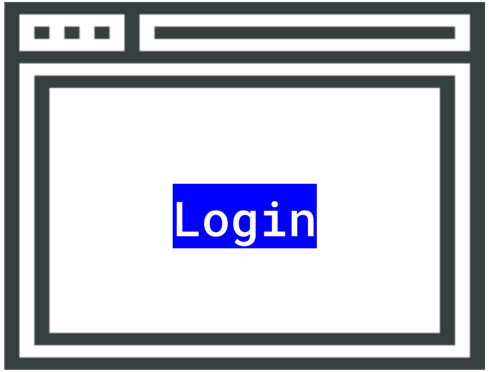
Social Engineering

Packet Sniffing

Credential Reuse

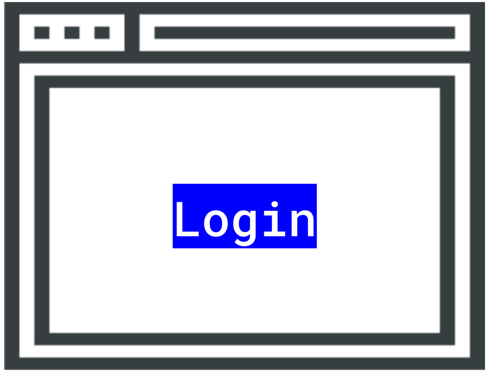
Computer Theft

Quick Review



Name One
Website Attack

Quick Review



Name One Website Attack

- Brute Force Injection
- Code Injection
- Session Stealing

Quick Review

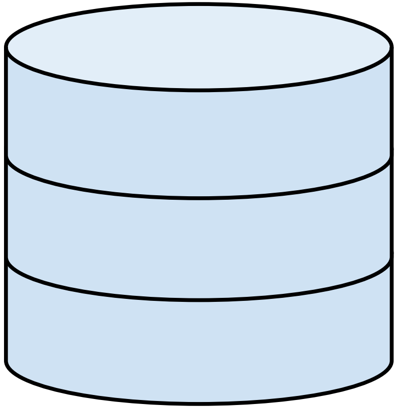
Name One
Server Attack

Quick Review

Name One Server Attack

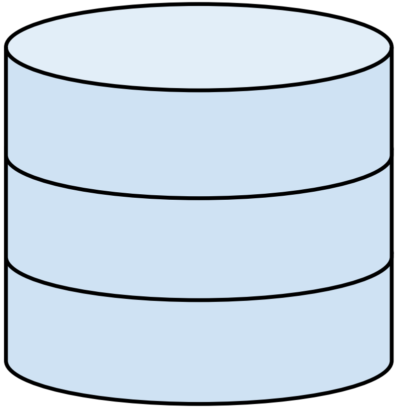
- OS Exploits
- Code Injection

Quick Review



Name One Database Attack

Quick Review



Name One Database Attack

- Default Credentials
- Unpatched Database
- Lack of Segregation

Quick Review

User Attacks

- Social Engineering
- Phishing Attacks
- Credential Reuse
- Malware Attacks
- Man in the Middle
- Packet Sniffing
- Computer Theft

Web Attacks

- Brute-Force Attacks
- Code Injection
- Faulty Sessions

Server Attacks

- OS Exploit
- Malicious Software

Database Attacks

- Default Credentials
- Unpatched Database
- Lack of Segregation

Name three Risk Mitigation Options

Quick Review

Sample Risk Mitigation Options

1. Educate all users on dangers of phishing and social engineering

2. Ensure passwords are truly unique to website (require characters atypical of other websites).

3. Ensure users are using multi-factor authentication (login + phone confirmation).

4. Ensure administrators can only access the network from a secure location (on premises).

5. Ensure passwords used are *strong* (alphanumeric + symbols).

6. Ensure login fields do *not* accept any code insertions.

7. Ensure users are immediately signed off upon closing a browser.

8. Ensure all servers are routinely patched against latest known vulnerabilities.

9. Ensure physical access to servers is protected by multiple forms of authentication

10. Ensure that all data stored in the database is encrypted and cannot be read without additional login information.

11. Ensure that all cloud security platforms follow best practices for security implementation.

Let’s Review: *Oh look, a Phone...*

Suppose *last class,* two students left their phones unattended at some point.

With the person sitting next to you, identify as many exploits possible in the event of a cell phone being stolen.

Hint: Be creative! Think like a hacker. What is the worst possible damage that could ensue. Try to do *real damage*. Think beyond the value of the phone itself.

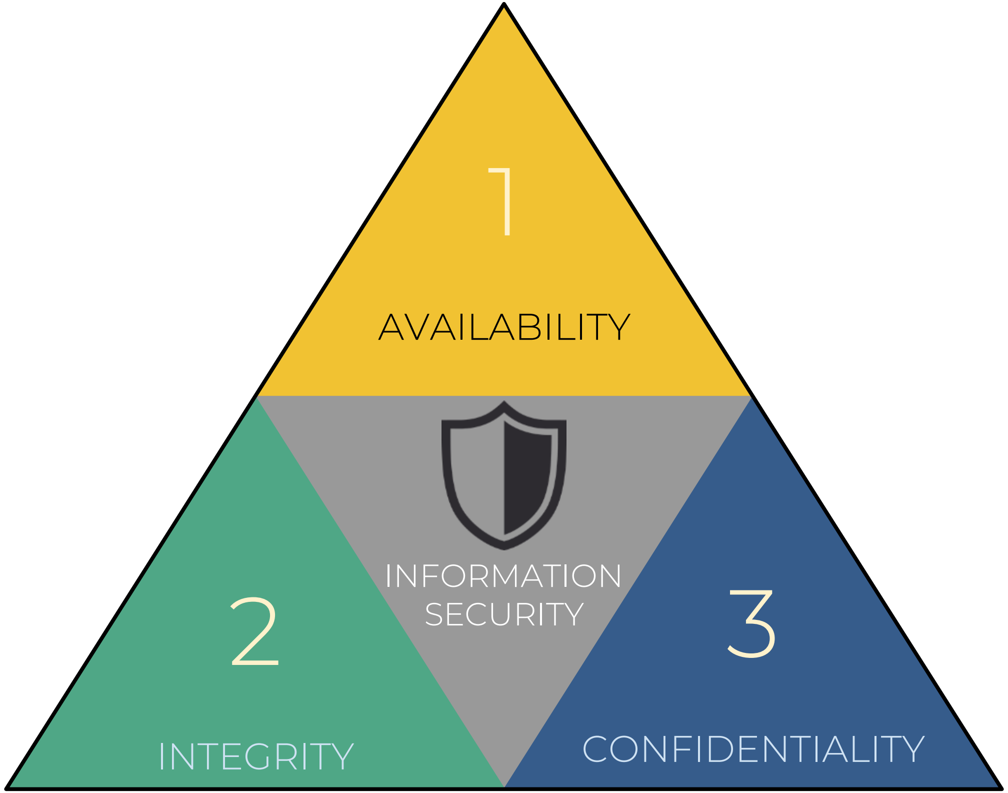
Let’s Review: *Oh look, a Phone...*

Potential Adverse Event

1. Cell phone can be wiped (cleared) and re-sold.
2. Cell phone memory can be harvested. Photos and sensitive material could be used for blackmail.
3. Credentials for email and social media accounts could be used to extract financial gain.
4. Installed applications could be used to make purchases.
5. Malware software could be directly installed to track future activity
6. Contacts on your phone could be socially engineered into providing monetary value.
7. Your phone could be used to conduct illegal activity.
8. Your identity could be stolen.

The CIA Triad

The InfoSec Bible: The CIA Triad



Activity: Define CIA Triad

In the next activity, we’ll dive deeper into the meaning of each component of the CIA Triad.

Suggested Time:

Your Turn: Define the CIA Triad

Instructions

Working with the person seated next to you:

1. Using a standard dictionary, take a few moments to define each element of the CIA Triad: Confidentiality, Integrity, and Availability.

2. Then, spend a few moments researching how these words translate in an information security context.

3. Then, think of 1-2 practical cases in which each element of the CIA triad could be impacted by an attack or breach.

CIA Triad Review

Confidentiality

Formal Definition:
The state of keeping or being kept secret or private.

IT Definition:
Ensuring sensitive information does not reach unauthorized people.

Example of Attack:
Private photos released on a forum.

Credit card numbers uncovered and exposed online.

CIA Triad Review

Integrity

Formal Definition:
The quality of being honest, whole, or undivided.

IT Definition:
Protected from modification by unauthorized parties.

Example of Attack:
Intercepted money transfer has the dollar amount insignificantly changed, allowing excess to be siphoned off.

Grades in university record system are modified to better grades.

CIA Triad Review

Availability

Formal Definition:
The quality of being able to be used or obtained.

IT Definition:
Operating systems, equipment and data are accessible and functioning correctly for those who need it.

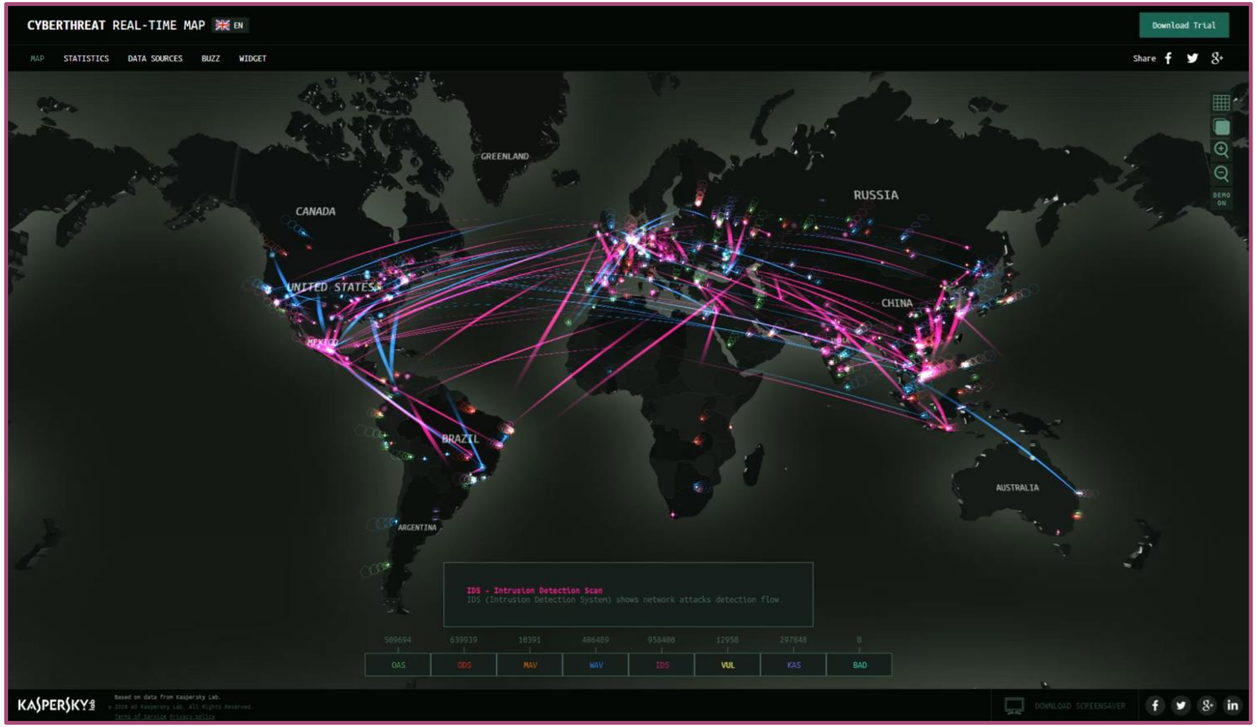
Example of Attack:
Hackers take down a web connected generator in a hospital.

Hackers use DoS attack to bring down financial service provider’s website.

Threat Landscape

Cyber Attack Maps (Kaspersky)

Threat maps visualize the current cybersecurity landscape, providing a great overview of “real-time” security threats.



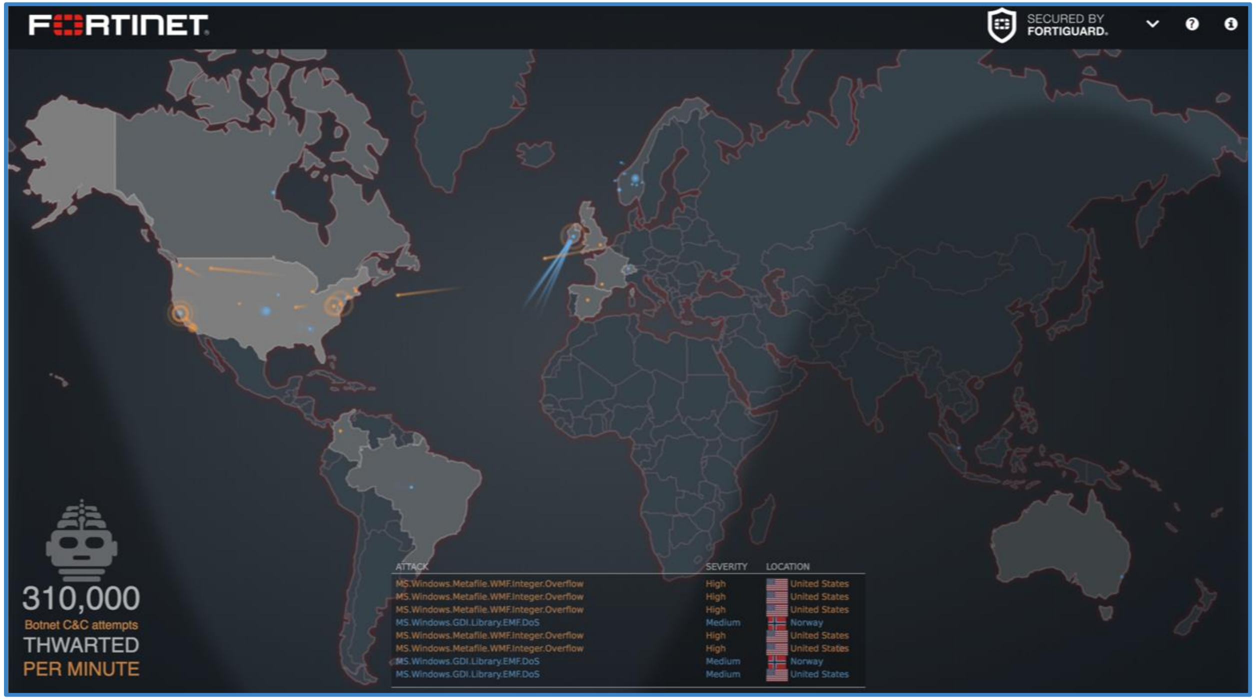
IDS - Intrusion Detection Scan
IDS (Intrusion Detection System) shows network attacks detection flow.

509694	639939	10391	486489	958488	12958	297848	8
OAS	ODS	MAV	WAV	IDS	VUL	KAS	BAD

Based on data from Kaspersky Lab.
© 2018 AO Kaspersky Lab. All Rights Reserved.
Terms of Service Privacy policy

Cyber Attack Maps (Fortinet)

Threat maps visualize the current cybersecurity landscape, providing a great overview of “real-time” security threats.



310,000
Botnet C&C attempts
THWARTED
PER MINUTE

ATTACK	SEVERITY	LOCATION
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.Windows.GDI.Library.EMF.DoS	Medium	Norway
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.Windows.Metafile.WMF.Integer.Overflow	High	United States
MS.Windows.GDI.Library.EMF.DoS	Medium	Norway
MS.Windows.GDI.Library.EMF.DoS	Medium	United States

Activity: Kaspersky + Fortinet Map Exploration

In this activity, you will navigate through Kaspersky and Fortinet maps and uncover what is displayed, what terminology arises, and any visible trends.

Instructions sent via Slack.

Suggested Time:
7 minutes

Your Turn: Kaspersky + Fortinet Map Exploration

Instructions:

Spend a few minutes playing around with the Kaspersky and Fortinet Threat Maps and, while on these websites, answer the following questions:

Link: https://threatmap.fortiguard.com/

https://cybermap.kaspersky.com/

1. What exactly are these websites showing?
2. Are there any terms used on these websites that you are unfamiliar with? Find and define at least three.
3. Are there any trends that stick out to you? Look for at least two.

7 Minutes

Reports, Blogs, and Research

Threat maps are fun visuals, but cyber professionals rely on prominent reports, blogs, and papers to stay up to date on the specific landscape.

Schneier on Security

KrebsonSecurity

GRAHAM CLULEY

Security Weekly

CSO

TAOSECURITY

In the next few activities, you will use three prominent security reports to better understand the contemporary security landscape.

Activity: Vocabulary Research

In this activity, you will pair up, navigate through a report and complete a vocabulary worksheet as you progress.

Instructions sent via Slack.

Suggested Time:
15 Minutes

Your Turn: Vocabulary Research

Instructions:

Working in pairs of two and using the reports provided, complete the sections of the worksheet pertaining to the "Symantec Internet Security Threat" report.

Notes:

- Be extra mindful of defining words in a way that a lay person would understand. Don’t rely on one technical term to define another. Break it down to a form you truly understand.
- Use outside research when necessary to define the terms, but use the reports provided when explaining their significance. It’s important that you get comfortable reading technical documentation to draw out context.
- Copy the assignment into a new Google Doc before getting started. You will be submitting this assignment later in the week as your first “homework” assignment, but aim to complete at least the Symantec section by the end of class today.

15 Minutes

Time’s Up! Let’s Review.

Vocabulary Research

Take a Break!

Activity: Report Analysis

Now you will continue navigate through the provided articles and complete the Symantec Internet Security Threat report analysis worksheet

Instructions sent via Slack.

Suggested Time:
15 Minutes

Your Turn: Report Analysis

Instructions:

Working in groups of 3 and using the reports provided, complete the section of the worksheet pertaining to the Symantec Internet Security Threat report.

Notes:

- For each questions, use a combination of the reports provided and your independent judgement.
- Again, remember to answer questions in a way that would make sense to a lay person when possible. Don’t feel content just writing down technical jargon.
- Copy the assignment into a new Google Doc before getting started. You will be submitting this assignment later in the week as your first “homework” assignment, but aim to complete at least the Symantec section by the end of class today.

15 Minutes

Time’s Up! Let’s Review.

Report Analysis

Activity: Threat Research

In this activity, you will group up in 3, and research an assigned vulnerability, exploit, or threat actor.

Instructions sent via Slack

Suggested Time:
40 Minutes

Your Turn: Threat Research

Instructions:

Working in groups of three, you will be assigned a vulnerability, exploit, or threat actor.

Your task is to: Prepare a 5 minute presentation that provides an overview of the topic. Focus on answering the following question:

- What is or was the exploit, vulnerability, or threat actor?
- What damage has it done?
- What steps have or can be taken to mitigate the damage?

Notes:

- While you may be new to the field challenge yourself to “become the expert.” A huge part of being a security professional is getting up to speed quickly on technical situations using research.
- For those uncomfortable about the idea of presenting, challenge yourself to treat this as a safe place. Becoming a confident speaker is an important part of being a cybersecurity consultant that people can trust.

40 Minutes

Your Turn: Threat Research

Vulnerabilities, Exploits, Threat Actors

- * Conficker
- * Mirai botnet-Smurf Society
- * Code Red-Blue Thunder Team
- * BadRabbit-Blues Clues
- * APT-28-Blue Paws Team
- * APT-29-Jet Blue
- * Stuxnet-Blue Team
- * NotPetya
- * Gh0st RAT-Blues Threes
- * Morris Worm-Blue Sky Team
- * Necurs
- * BlankSlate
- * Other Vulnerability, Exploit, or Threat Actor

Wikipedia is not an acceptable source

Time’s Up! Let’s Review.

Threat Research

Homework Assignment:

You will present your research next class.

Additionally, you should complete the worksheets started in class. Check Bootcamp Spot for due dates.

Due Date:

Class Objectives Wrap Up

Today we discussed:

□ Articulate a clear definition of the CIA Triad and its elements.

□ Define and contextualize technical terms found in recent cybersecurity trends and reports.

□ Utilize cybersecurity trend reports to communicate risk patterns.

□ Conduct and present analysis on a vulnerability, exploit, or threat actor to a non-technical audience using independent research.