



# The Cybersecurity Mindset

Cybersecurity  
Cybersecurity 101 Day 1



# CompTIA Partnership

---

As part of the course, all students will receive:

➤ **Access to CompTIA CertMaster Practice for Security+**

- An adaptive knowledge assessment and certification training companion tool that will help you gain knowledge and prepare for the Security+ CompTIA exam.
- Features question-first design, real-time learning analytics, and content refreshers to help reinforce and test what you know and close knowledge gaps.
- You will receive access partway through the course.

➤ **CompTIA Security+ exam voucher**

- Exam vouchers are valid for 12 months.
- You will receive it at the end of course, in order to give the voucher the longest shelf-life possible and give you time to study.



# 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.



Explain how cybersecurity is an assessment of threats and mitigation of risks.



List different types of user, web, server, and database cybersecurity attacks.



Identify risk mitigation plan framework for user, web server, and database attacks.

# 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 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 become a focal point for organized crime, nation states, and private enterprises.

The screenshot shows a news article from CSO Online. The header features the CSO logo and navigation links for 'INSIDER' and 'Sign In | Register'. The article is categorized as a 'FEATURE' and has a large, bold title: 'Cybercrime: Much more organized'. Below the title, a paragraph discusses the shift in cybercrime from lone individuals to organized groups driven by profit.

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)<sup>2</sup>, 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?

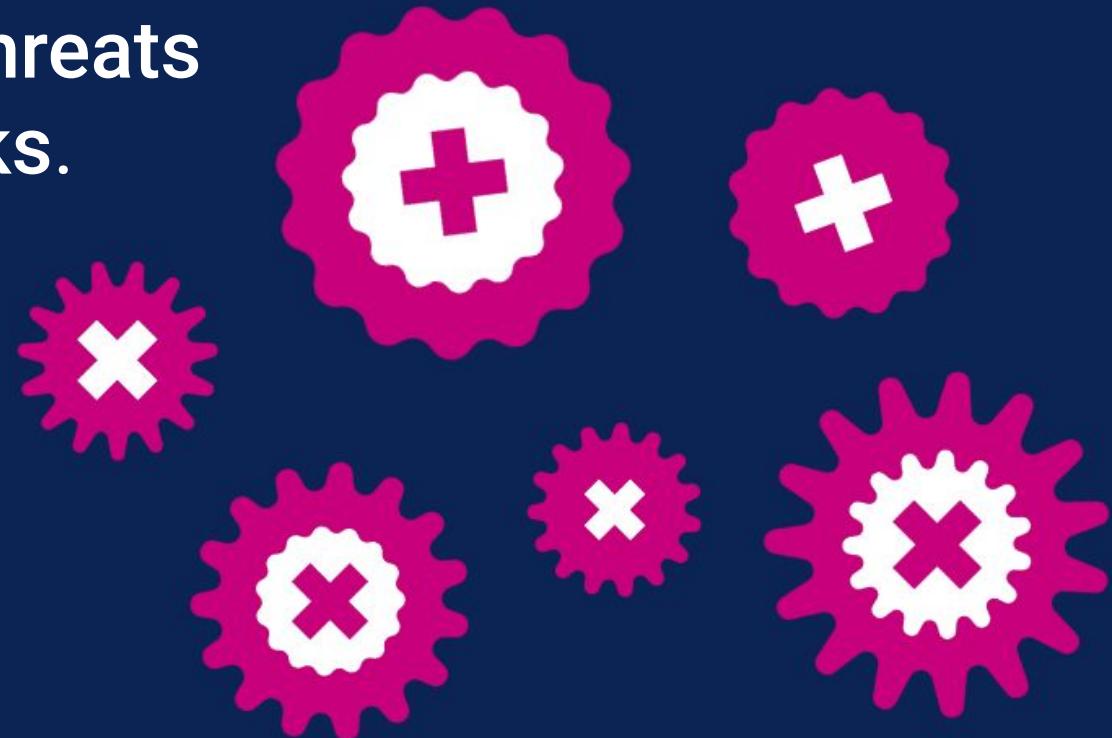
# Everyone's First Thoughts:

Hackers and complicated code...

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



**Cybersecurity** is really  
about **assessing threats**  
and **mitigating risks**.



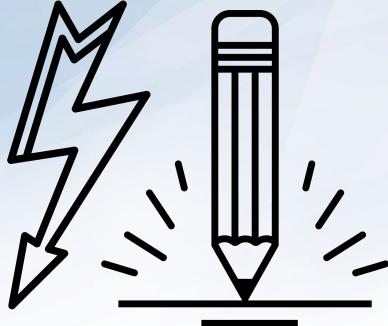
# Assessing Threats: A Wild USB Appears!

---

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!





## Quick Activity: A Wild USB Appears!

Turn to the person next to you and discuss what could happen.

1. How might it be that a USB drive is able to immediately execute running code?
2. Why can't our computer stop the drive from running?
3. How might we defend against malevolent USBs like this?

Suggested Time: 5 Minutes



# 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.



# 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

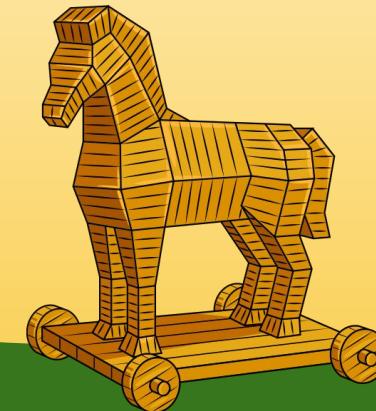


What can be done to stop connected car hacking?

# Mitigating Risks

---

Historically, organizations viewed cybersecurity from the lens of the **castle model**: managing risks meant building walls and keeping the bad actors **out**.



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

# Course Overview

# Our Future Tool Belt

Our Goals:

Threat Assessment

Risk Mitigation

Our Tools:

Network Security

Web Security

OS Security

Cryptography

Penetration Testing

Vulnerability Assessment

Security Policy

Risk Analysis

Compliance Strategy

Operational Security

UNIX Command Line

Wireshark

Kali Linux

Nmap

Nessus

Metasploit

Burp Suite

SIEMS and more...



# Daily Routine

---

In class, we'll run through the following:

-  Set Objectives
-  Brief Background Lecture
-  Instructor Demonstrations
-  Thought Exercises
-  In-Class Skill Builders
-  Project Work

# Curriculum at a Glance

## Module 1 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

## Module 2: 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.

## Module 3: Networks and Network Security, and Project 1

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

## Module 4: Offensive Security, and Project 2

Web applications, databases, and the vulnerabilities and hardening associated with them. Windows and Linux penetration testing, using tools such as Nessus, Metasploit, and Burpsuite.

## Module 5: Defensive Security

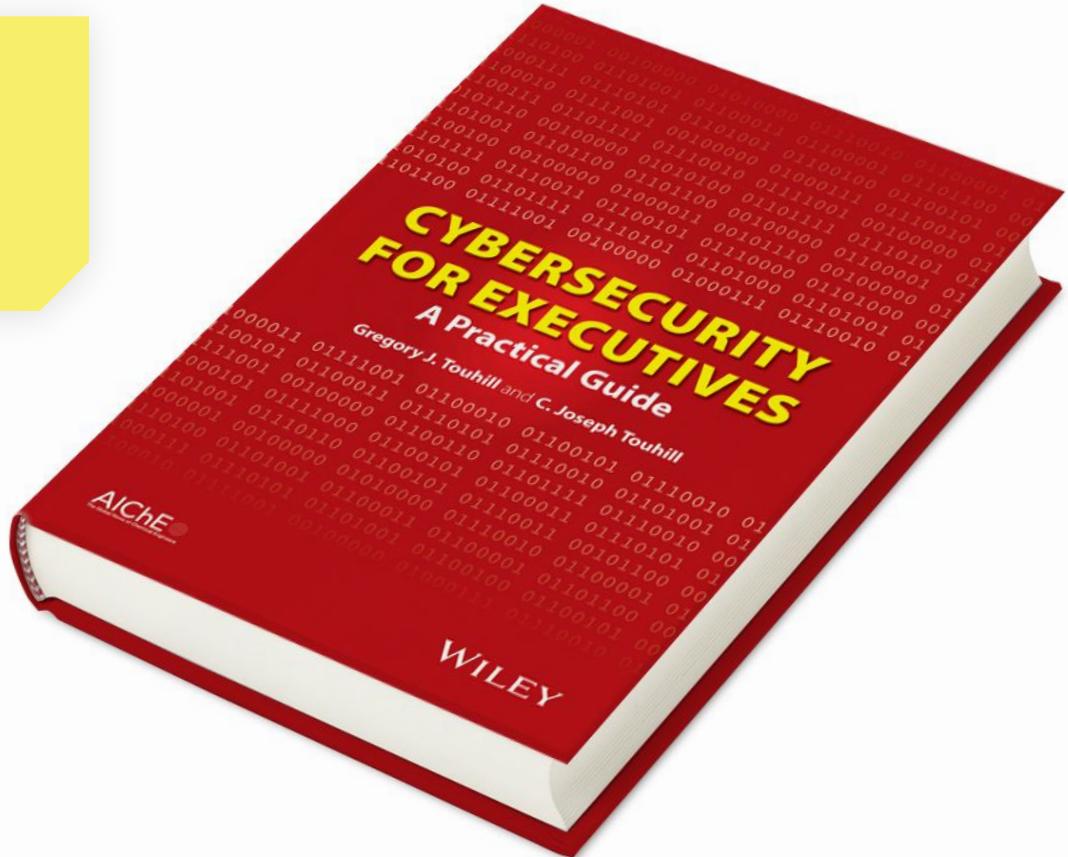
SIEMs with Splunk. Setting up security monitoring, alerts, dashboards, and custom reports. Understanding of the Incident Response framework, and responding to breaches and incidents. Using Forensic tools to recover deleted data.

## Module 6: Review and Final Projects

Certification prep and review. Interviewing and career prep practice. Final projects involving deployment of virtual networks to the cloud.

# Example Activity: Cybersecurity Policy and Strategy

We'll learn how to talk about cybersecurity risks, strategy, and policy in a broad organizational and business capacity.



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

```

GET /counter/
000001IMKqMAdoTw8bMbxFg2zHjraZnwghk2xY5rpqqa6RhRl06U7zbn07DD8M0P17pZrl1NTv383vBY7CIMAtzGZPifYdnKrvwm19MmBG_W0bGLe74J074zik2n
-N_qCHL09TFUXHSRMQ12 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@.....;
.....telibrary_DownloadFile.....PLAYBACK_LOCATION_wChapterNum.....CL_COLOR_CONTRAST..CL_COLOR_RED_COMPONENT..CL_COLO
R.....<0.....DR_IS_PROTECTED_CONTENT_BDROM_BKDR_SET_DUMMY_WI.....R.+
.....<0.....DR_IS_PROTECTED_CONTENT_BDROM_BKDR_SET_DUMMY_WI.....R.+
.....Back : Vol = %d....Callback Pm.....{.....o.t. ....B.D.J.
....content.....{.B.D.P.y.B.D.v.....(value)
failed....PyL.....a.CreateWindowExW....RegisterClassExW....wvprintf.....r.o.u.n.d(.).....[PyDVDEngine] m_pImmapi->Vid.....AG_Resume.UOP_FLAG_ShowMenu Chapter...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_BKDR_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.....$^.....^.....'.....Subtitle.CCLDVDEngine_IsSubtitleEnabled..CCLDVDEngin.....rocessPyBDUOPCmd..0:CCLDVDEngine.....
....DVAUD_UOP_2....DVAUD_UOP_1....DVAUD_UOP_0.....y.....y.....y.....y.....h. .....
....Global variables {
....ne_IsAnalyzed.CCLDVDEngine_GetEmptyList.....CONDARY_VIDEO_ATTR_dwAspectRat.....A.....%.
....DD_ACAP_STEREO..BDROMDEF_DDLOSSLESS_DD_ACAP_RESERV.....A.....%.
4 client pkts(s), 1,240 server pkts(s), 7 turns.
Entire conversation (1851 kB) Show data as ASCII Stream 4 Find Next
Help Hide this stream Print Save as... Close

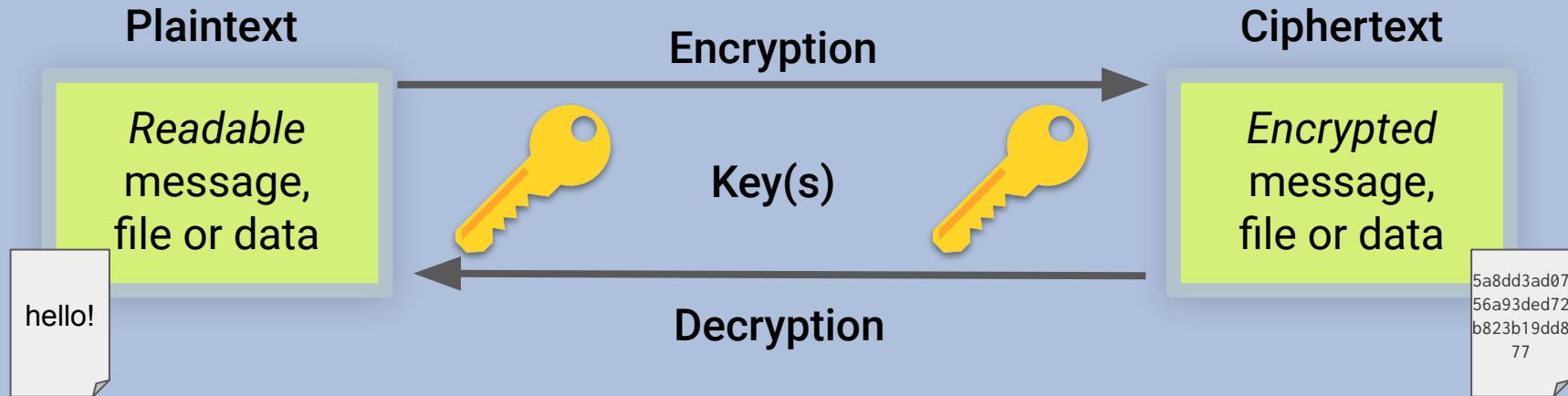
```

# Example Activity: Analyzing Web Traffic for Suspicious Activity

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

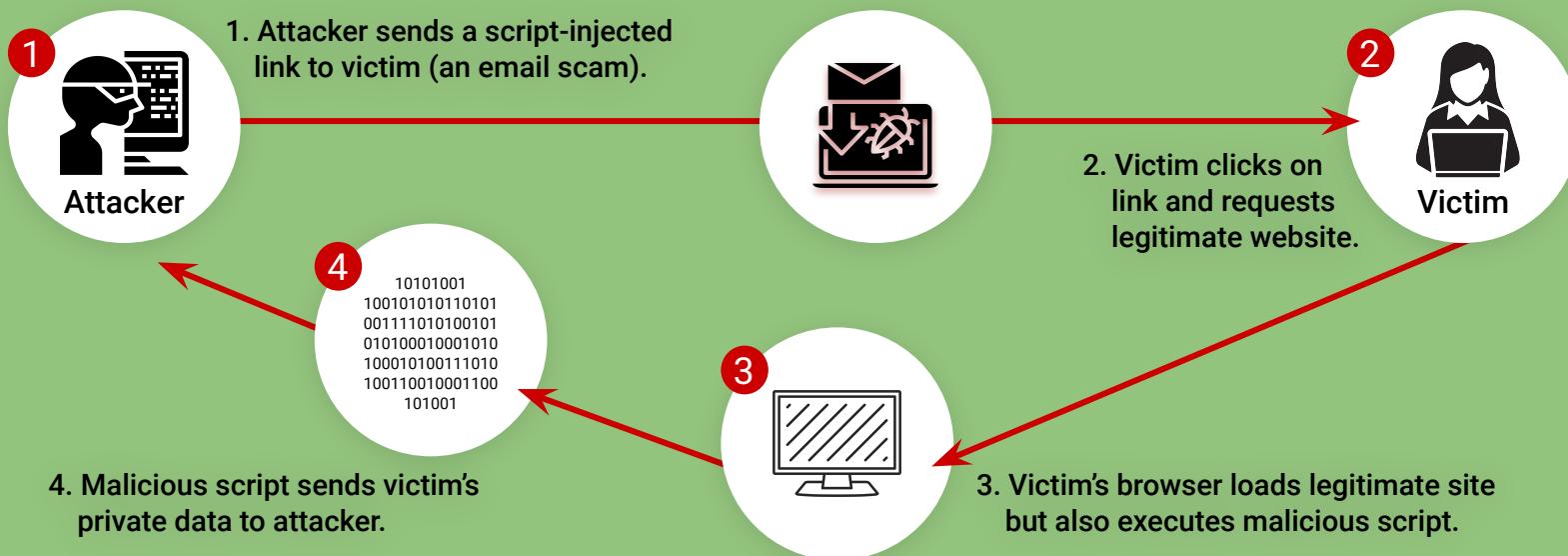
## Example Activity: **Encryption / Decryption Systems**

We'll learn how modern cryptography works and how historic methods of encryption could be broken through simple means.



# Example Activity: Web Application Hardening

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



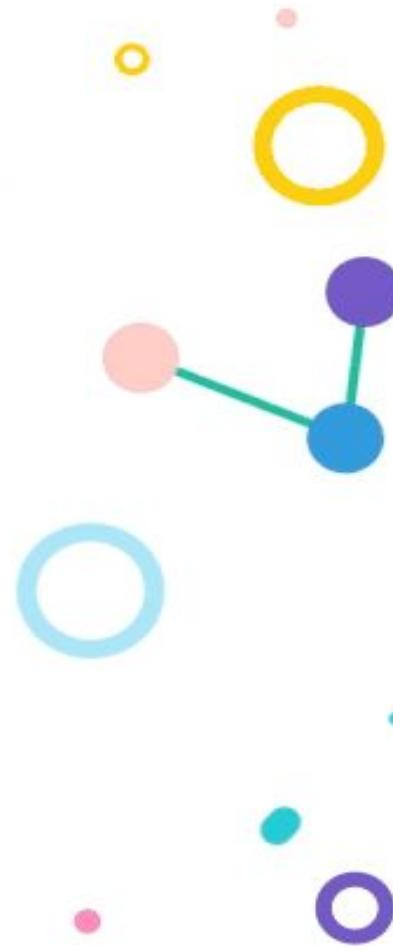
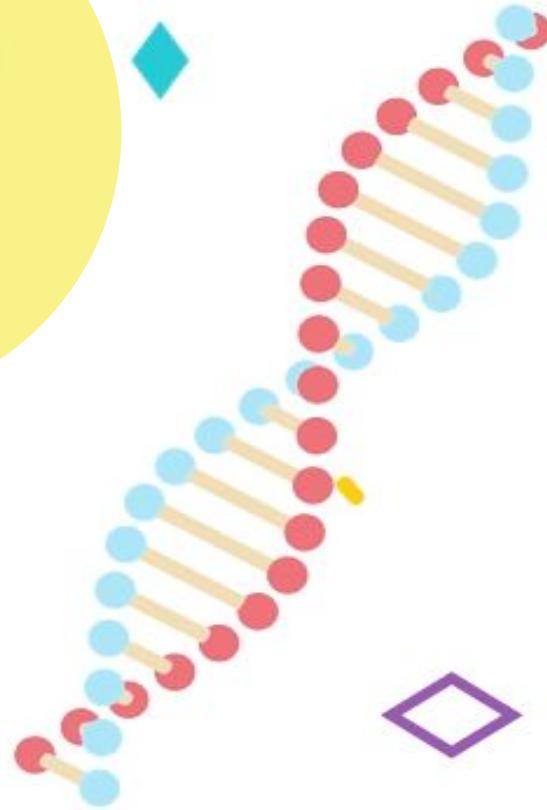
# Example Activity: Identify Vulnerabilities in Unpatched Systems

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

```
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
| afd_loginexec                   AppleFileServer_LoginExt_PathName_Overflow
| aim_gosaway                     AOL_Instant_Messenger_gosaway_Overflow
| altn_webadmin                   Alt-N_WebAdmin_USER_Buffer_Overflow
| apache_chunked_win32            Apache_Win32_Chunked_Encoding
| arkeia_agent_access             Arkeia_Backup_Client_Remote_Access
| arkeia_type77_nacos              Arkeia_Backup_Client_Type_77_Overflow_(Mac_OS_X)
| arkeia_type77_win32              Arkeia_Backup_Client_Type_77_Overflow_(Win32)
| avastats_configdir_remote_exec  AVStats_configdir_Remote_Command_Execution
| backupupexec_agent               Veritas_Backup_Exe_Windows_Remote_Agent_Overflow
| backupupexec_dump                Veritas_Backup_Exec_Windows_Remote_File_Access
| backupupexec_ns                  Veritas_Backup_Exec_Named_Service_Overflow
| backupupexec_registry            Veritas_Backup_Exec_Server_Registry_Access
| badblue_ext_overflow             BadBlue_2.5_EXT.dll_Buffer_Overflow
| backbone_netwatch_heap          Backbone_NetWatch_Remote_Snap_Overflow
| blackice_pcap_icq                 BlackICE_PCAP_ICQ_Farser_Buffer_Overflow
| cabrightstor_disco               CA_BrightStar_Discovery_Service_Overflow
| cabrightstor_disco_servicepcpc  CA_BrightStar_Discovery_Service_SERVICEPCP_Overflow
| cabrightstor_sagagent            CA_BrightStar_Agent_for_Microsoft_SQL_Overflow
| cabrightstor_unigagent           CA_BrightStar_Universal_Agent_Overflow
| cacti_graphimage_xsec            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 >
```

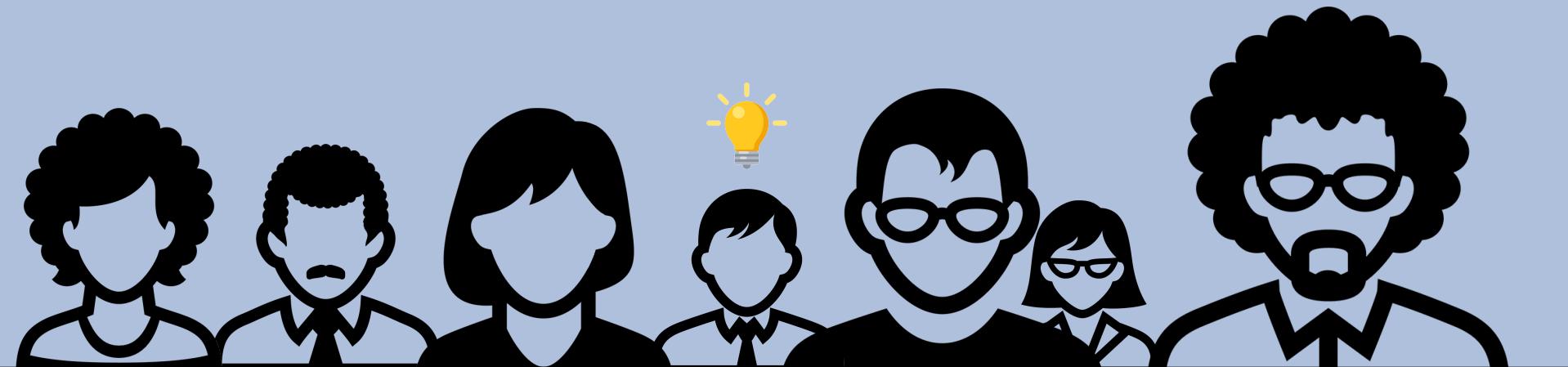
# Tips

**Tip:**  
Embrace  
Your  
Curiosity



## *Tip: Embrace being a beginner.*

Once you admit you “know nothing” (or *little*) about the many subject areas we cover in this course, you’ll be able to dig into these new topics and invest the time necessary to succeed.



# *Tip: Find your community now.*

You and your classmates are in this process together.  
Use each other for help!

**You all can bring value to the table.** Don't be afraid  
to speak up!



# *Tip: You need to put in the hours.*

There is no magic pill. This boot camp will require time and effort for you to learn and succeed.

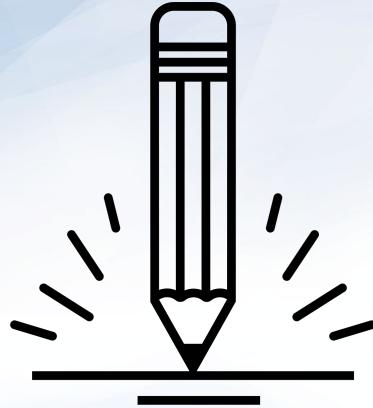
This class will challenge you. **Make sure to celebrate your progress along the way.**



**15:00**

*Break*





## **Activity:** Security Challenge #1: Attacking the Wall

In this security challenge, you and your group will play the role of security professionals tasked with handling a real-world situation.

Let's review the scenario first...

**Suggested Time:**  
**15 Minutes**



# SECURITY CHALLENGE #1



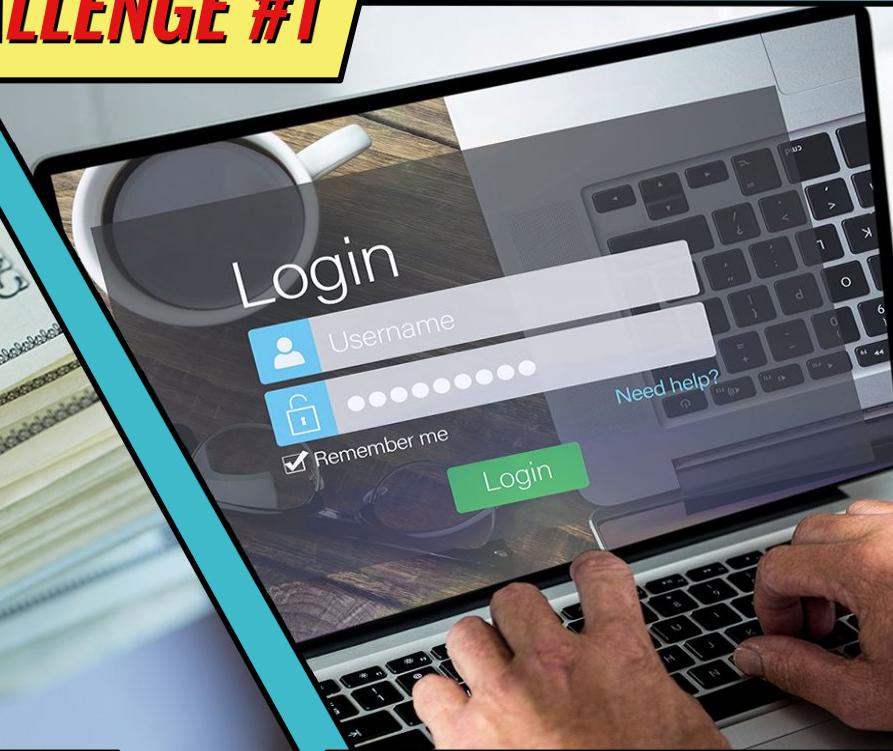
**Congratulations!** You and your team have just been hired by a very successful startup that runs a Bitcoin Dating Exchange.

While their founding team is brilliant, like many startups, **they don't know the first thing about security**.

# **SECURITY CHALLENGE #1**



They just handed you a bucket load of cash to solve their **single most pressing problem**.



Their log-in process is **totally insecure**. Hackers are **routinely logging in as users** (and administrators) and gaining access to company data and financial assets.



# **Activity Instructions:** Security Challenge #1: Attacking the Wall

---

## **Instructions:**

With your group, develop a list of 15 different ways that a malicious actor could penetrate the system and login as a user or administrator.

With each method, be prepared to describe the following:

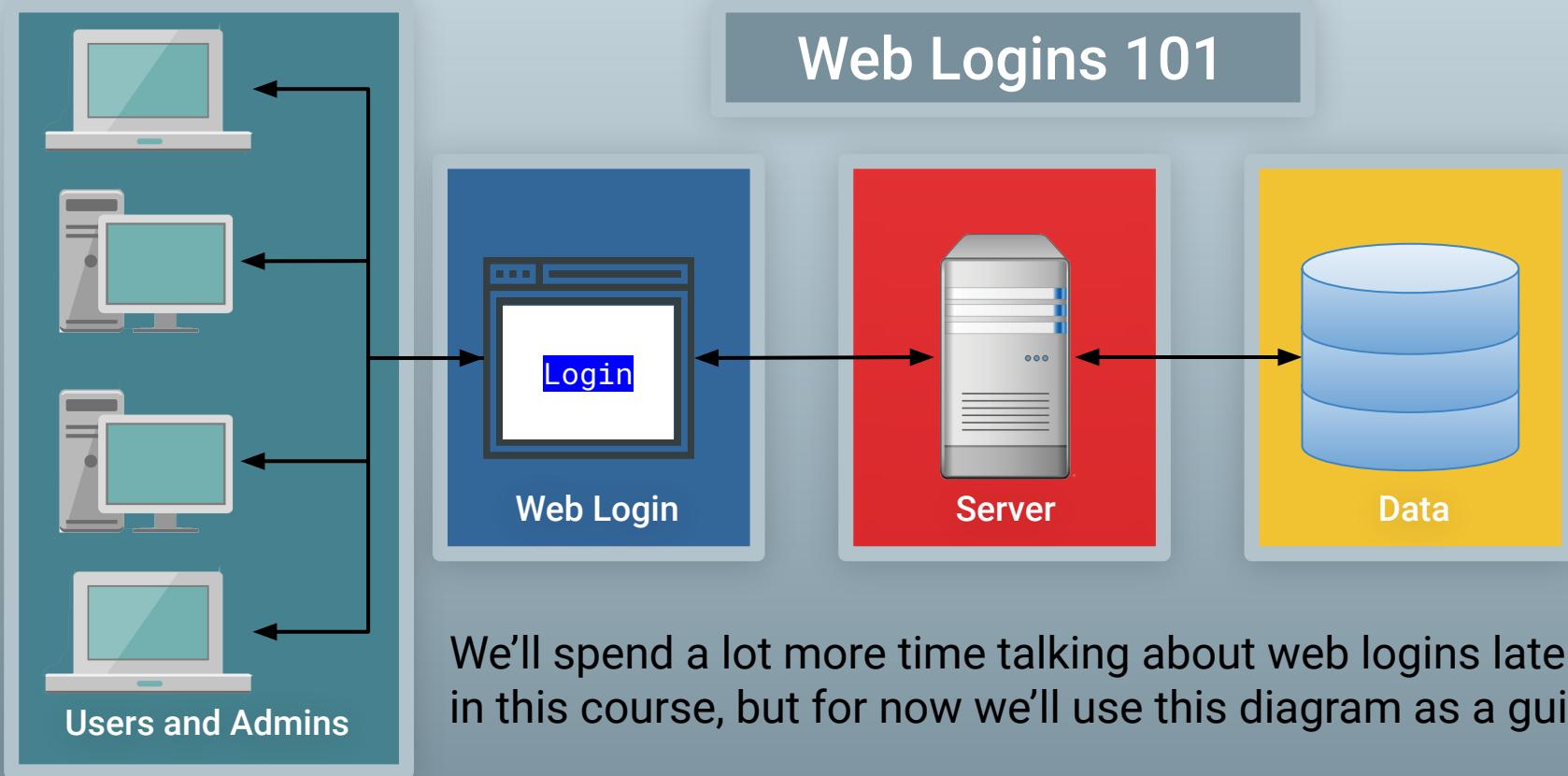
- Who (or what) is the initial target?
- How would the actor implement the attack?

**Be prepared to share!**

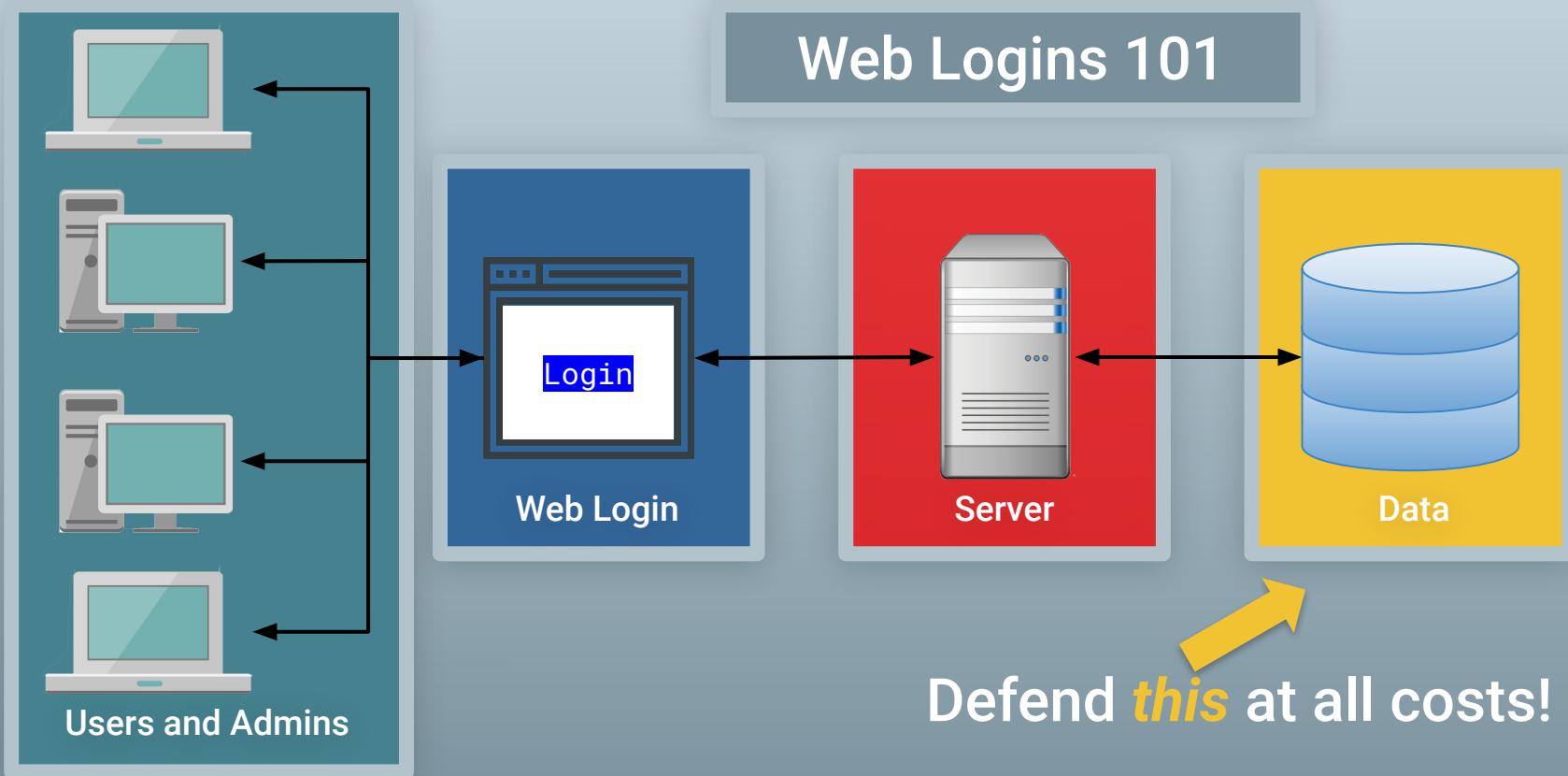
**Suggested Time:** 15 Minutes



# Activity: Security Challenge #1: Attacking the Wall

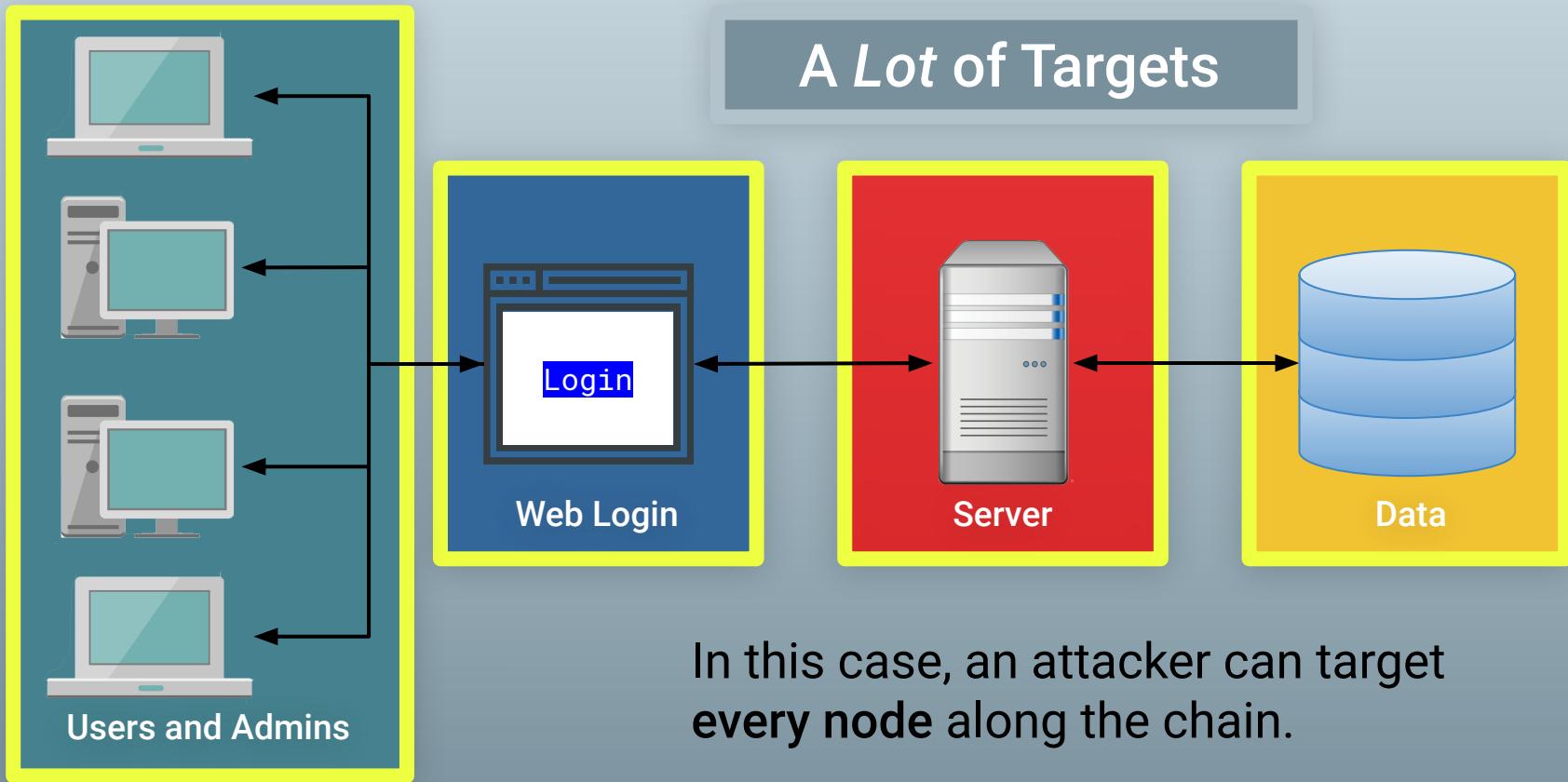


# Activity: Security Challenge #1: Attacking the Wall

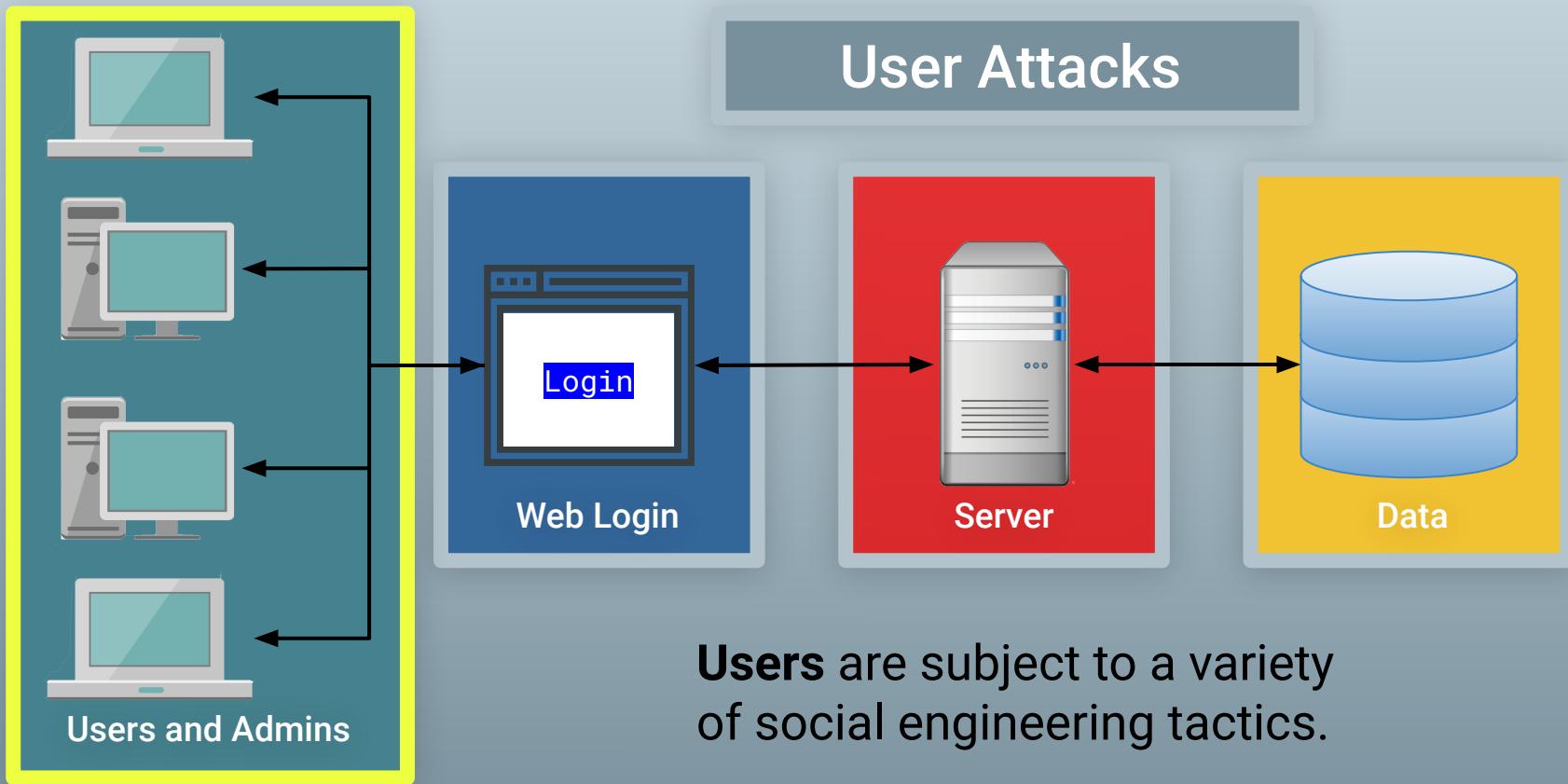


# Step #1: Assess the Target

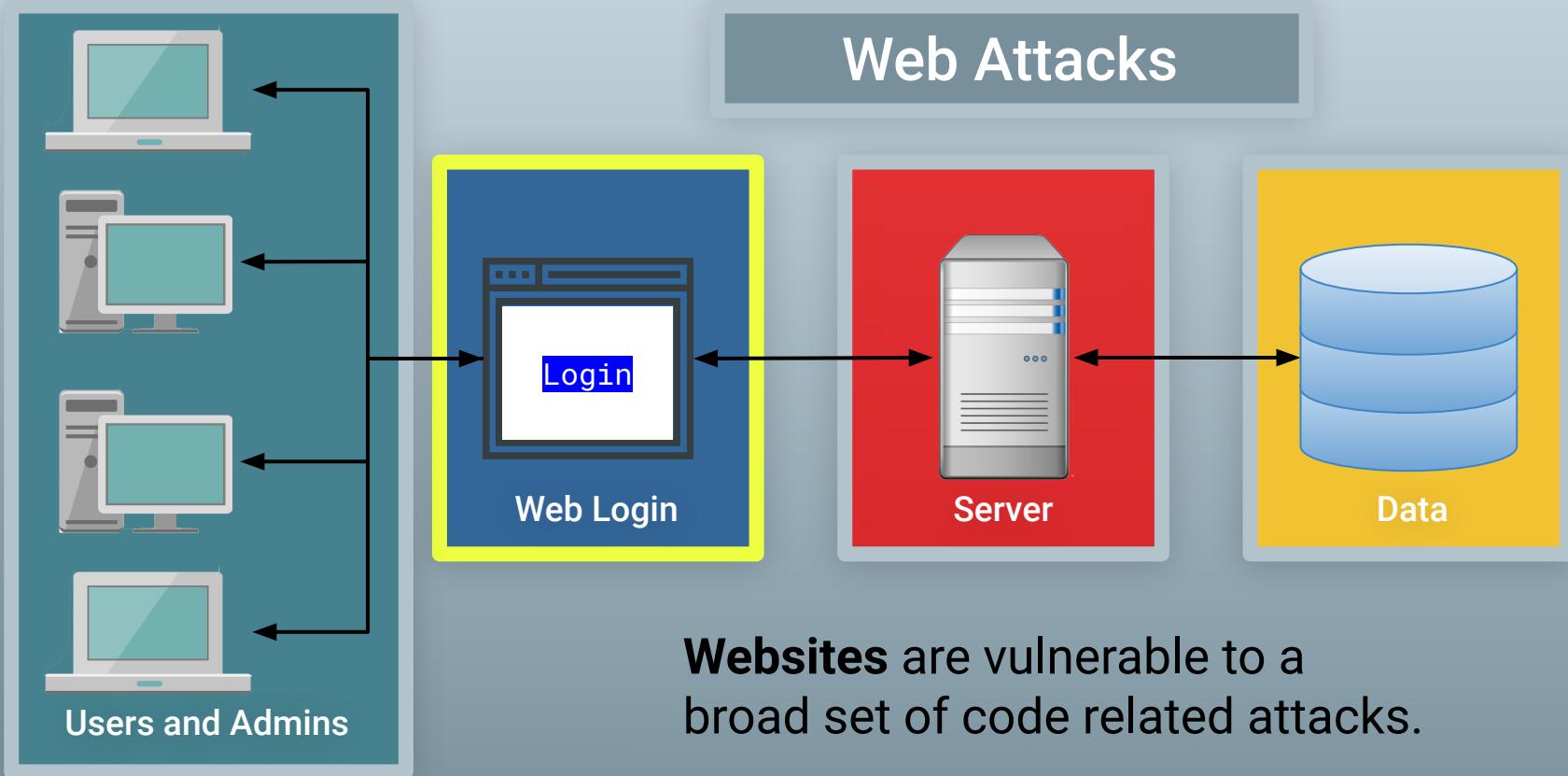
# Activity: Security Challenge #1: Attacking the Wall



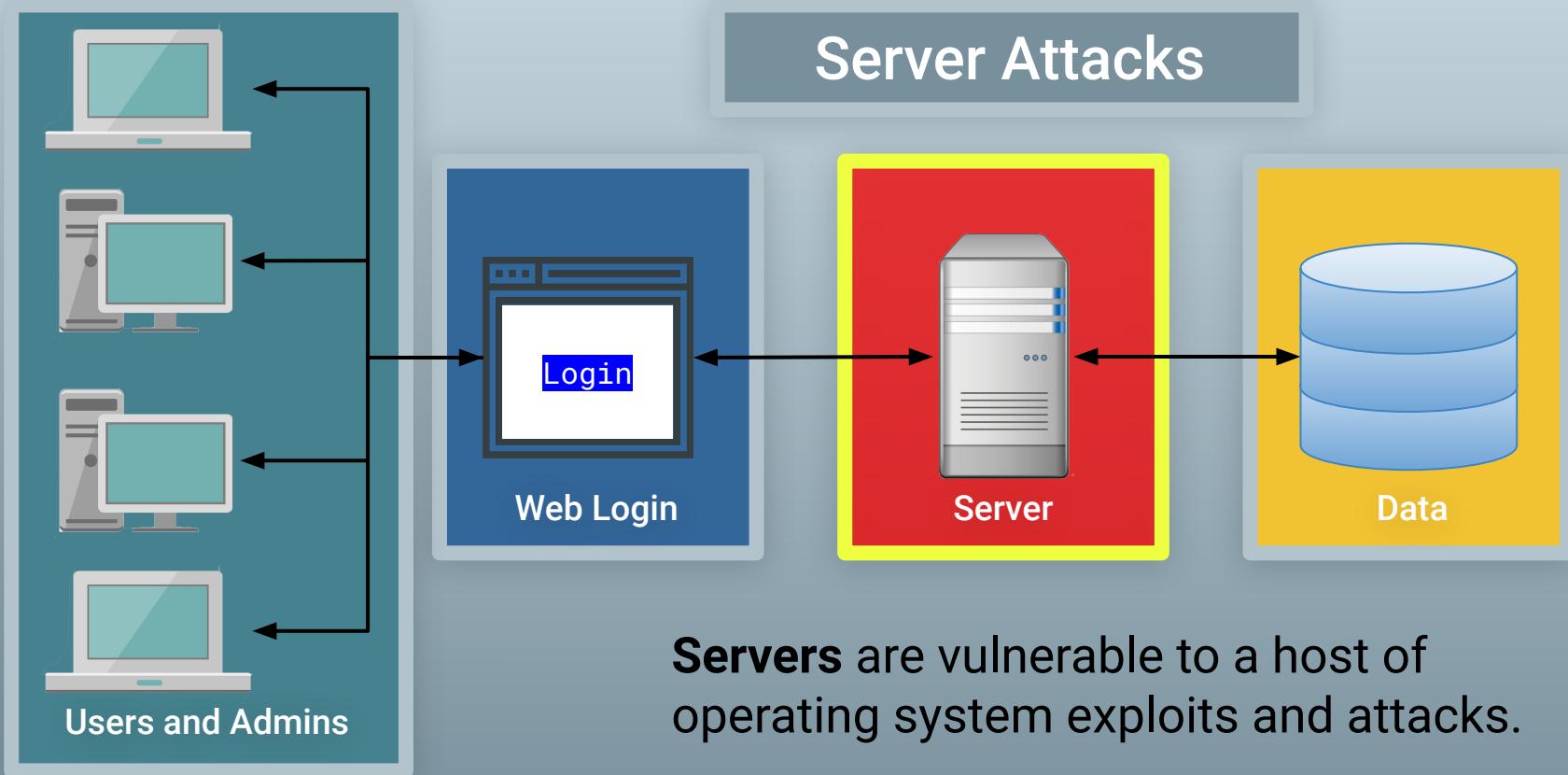
# Activity: Security Challenge #1: Attacking the Wall



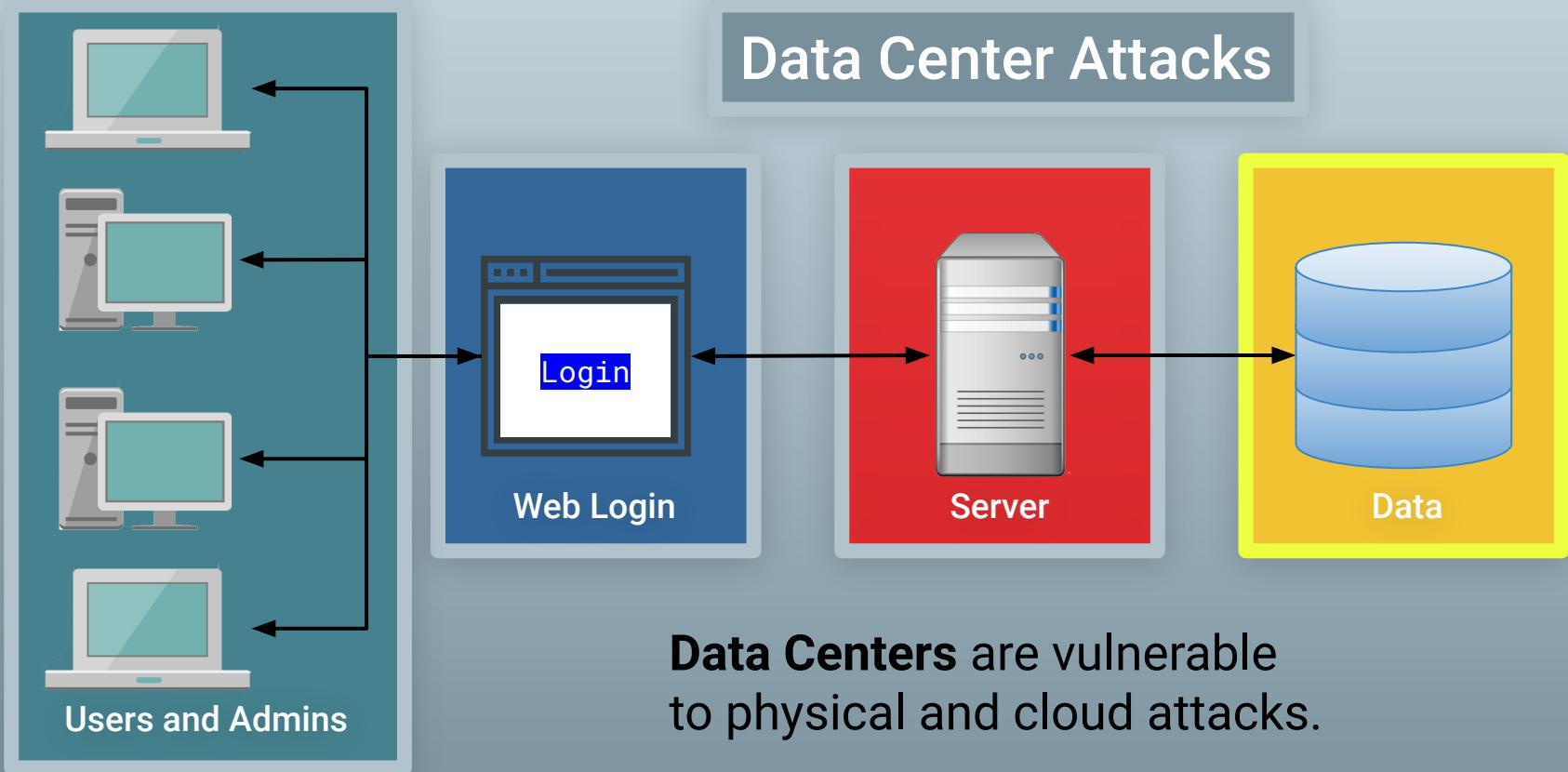
# Activity: Security Challenge #1: Attacking the Wall



# Activity: Security Challenge #1: Attacking the Wall



# Activity: Security Challenge #1: Attacking the Wall



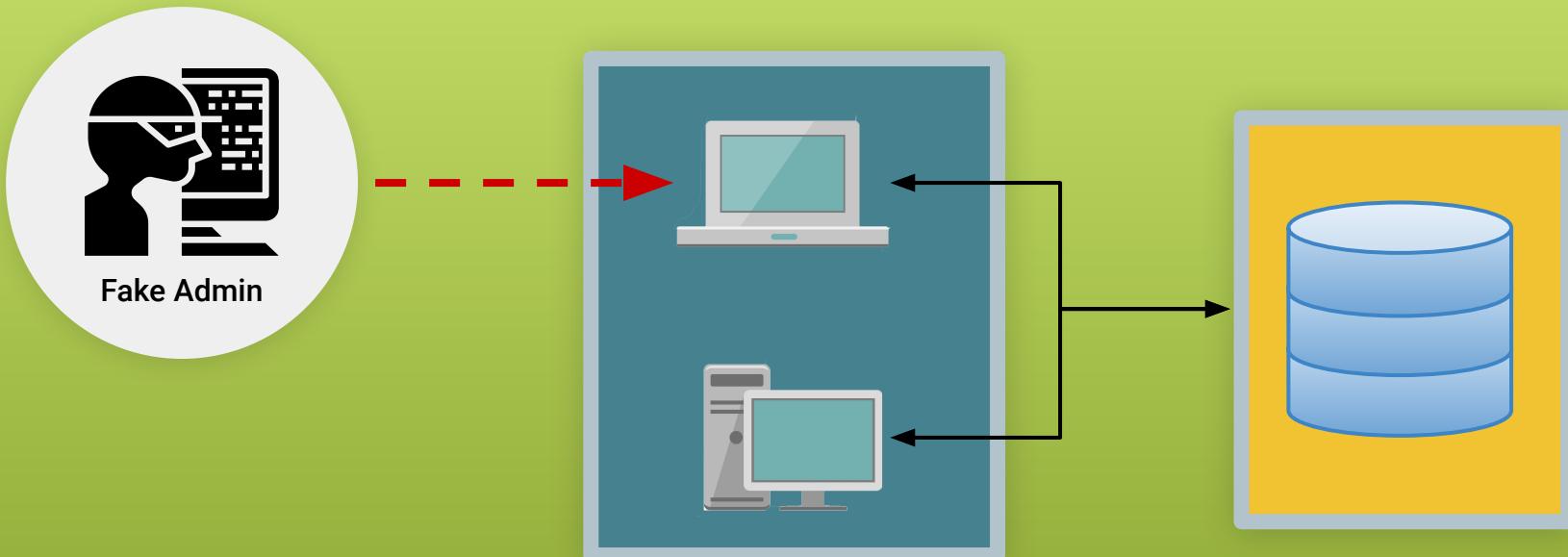
# Step #2: Define Attack Strategy

## Step 2: Defining Attack Strategies

---

### Attack Option #1: Social Engineering

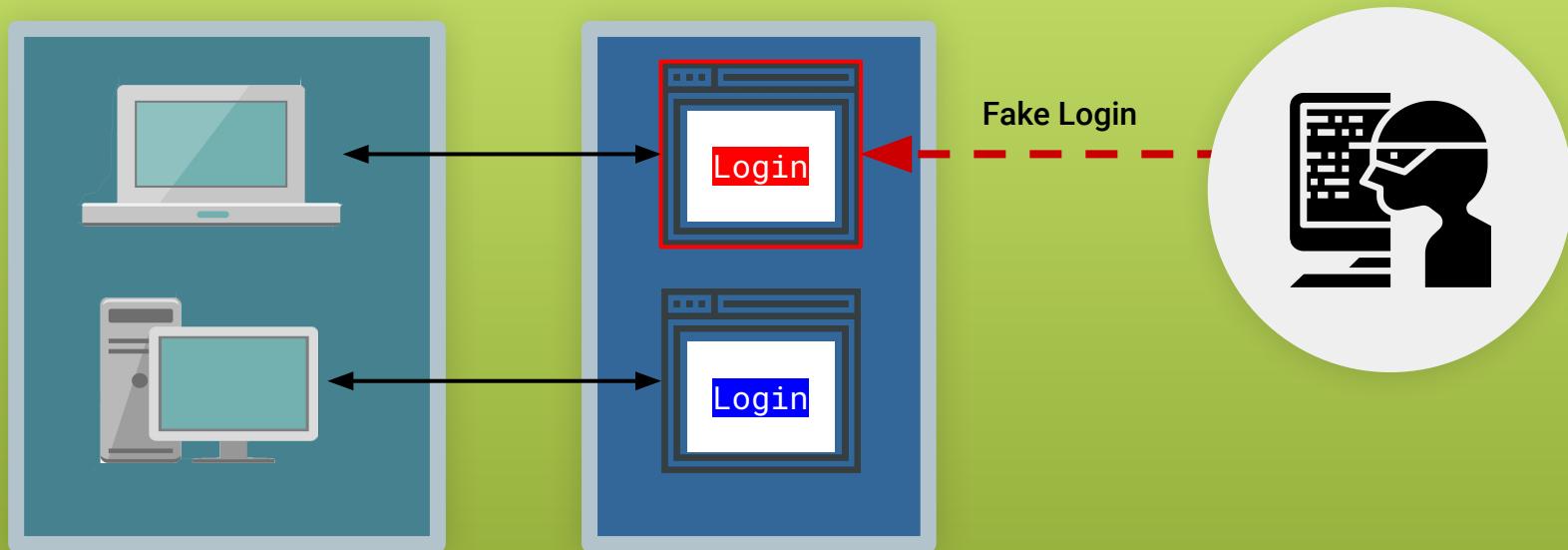
A hacker can ask users for their credentials by pretending to be an administrator.



## Step 2: Defining Attack Strategies

### Attack Option #2: Phishing

A hacker can attempt a phishing attack where users are redirected to fake login pages to capture user credentials.

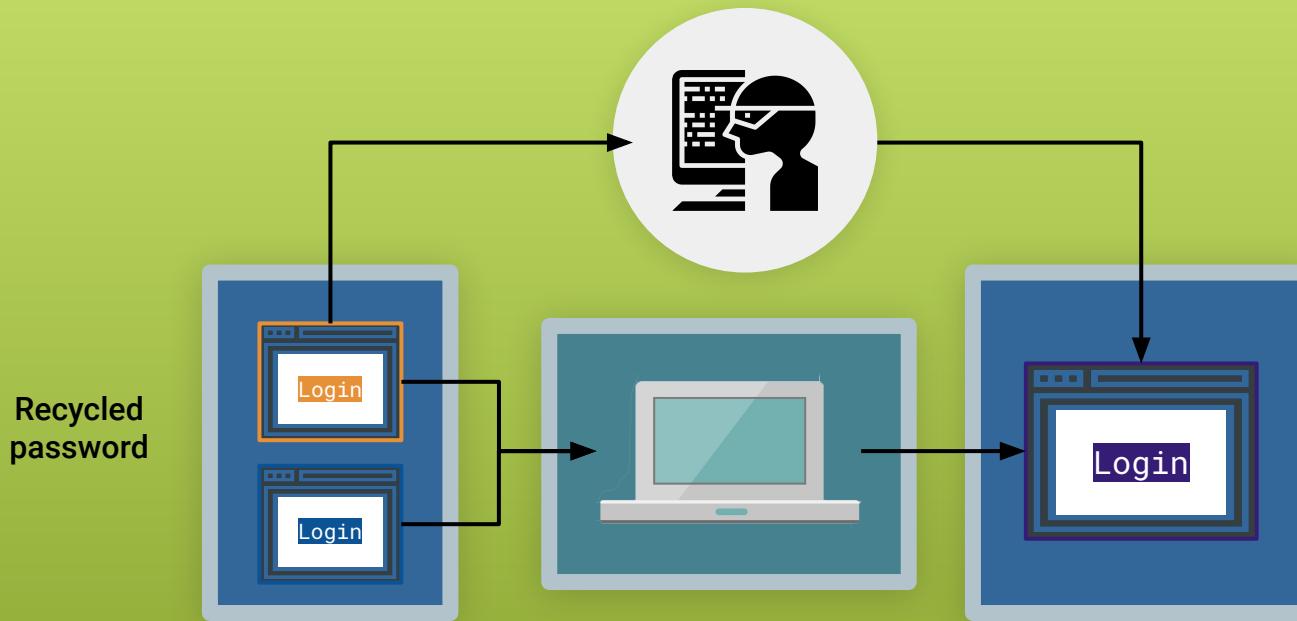


## Step 2: Defining Attack Strategies

---

### Attack Option #3: Credential Reuse

A hacker can find users' login and password information from other websites.

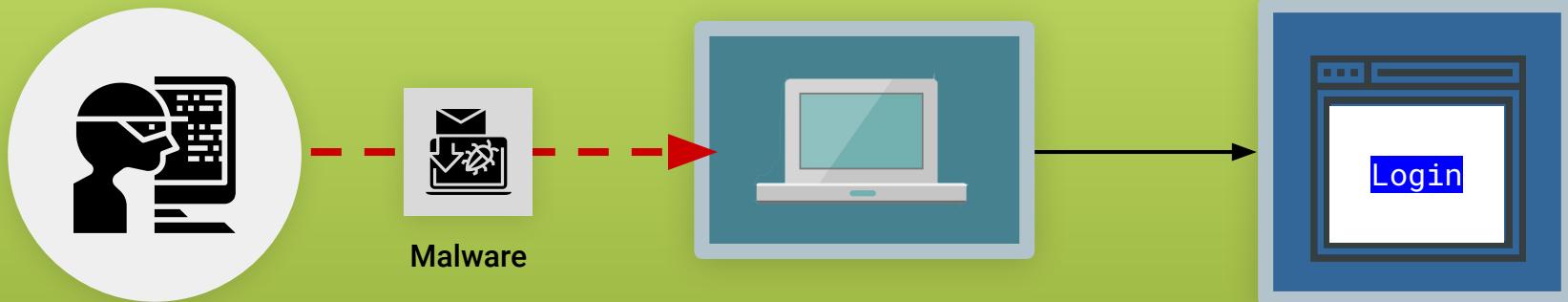


## Step 2: Defining Attack Strategies

---

### Attack Option #4: Malware

A hacker can deploy malware such as spyware or keyloggers to capture daily user activity.



## Step 2: Defining Attack Strategies

---

### Attack Option #5: Man in the Middle Attack

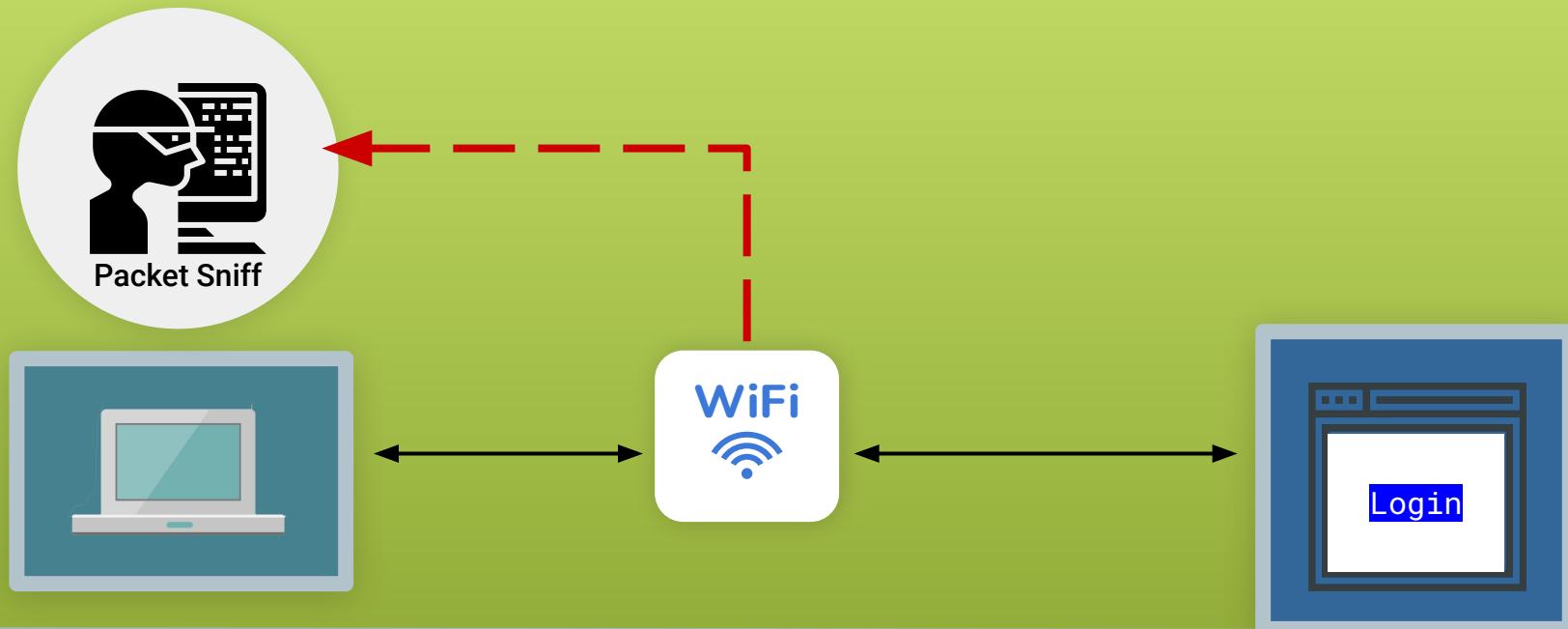
A hacker can create a man in the middle attack by providing a free WiFi hotspot to capture user credentials.



## Step 2: Defining Attack Strategies

### Attack Option #6: Sniff Packet

A hacker can sniff packet traffic across insecure wireless networks such as a cafe or restaurant.

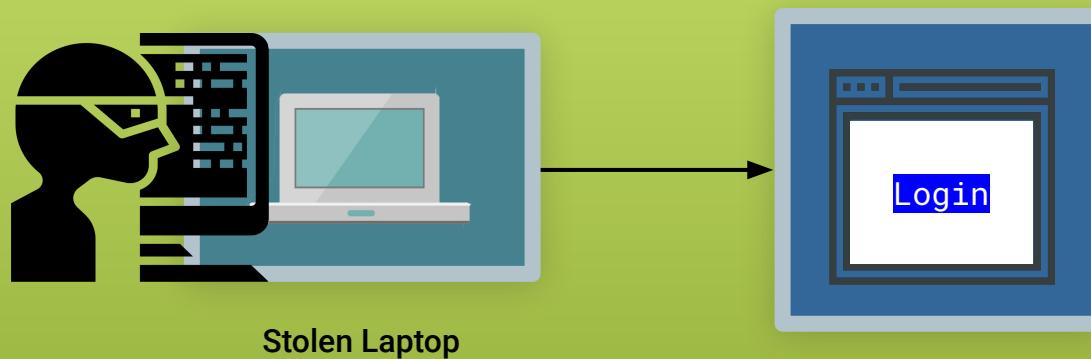


## Step 2: Defining Attack Strategies

---

### Attack Option #7: Stolen Hardware

A hacker can simply **steal a computer** and use the saved credentials to login.





Next: **website** attacks.

## Step 2: Defining Attack Strategies

---

### Attack Option #8: Brute Force Attack

A hacker can use a **brute force attack** to continuously attempt username and password combinations.



## Step 2: Defining Attack Strategies

### Attack Option #9: Code-Injection

A hacker can use a **code-injection attack** in which malicious code is directly injected into the username or password fields.

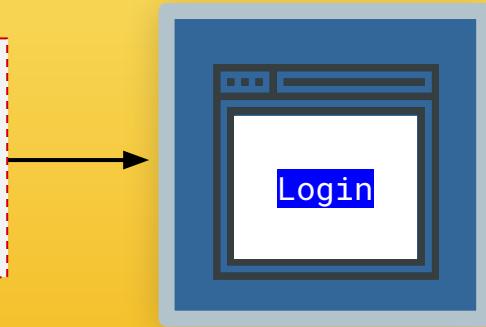


**Username:**

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ="' +
+ uName + '" AND Pass =''' + uPass + '''
```

Password Dictionary

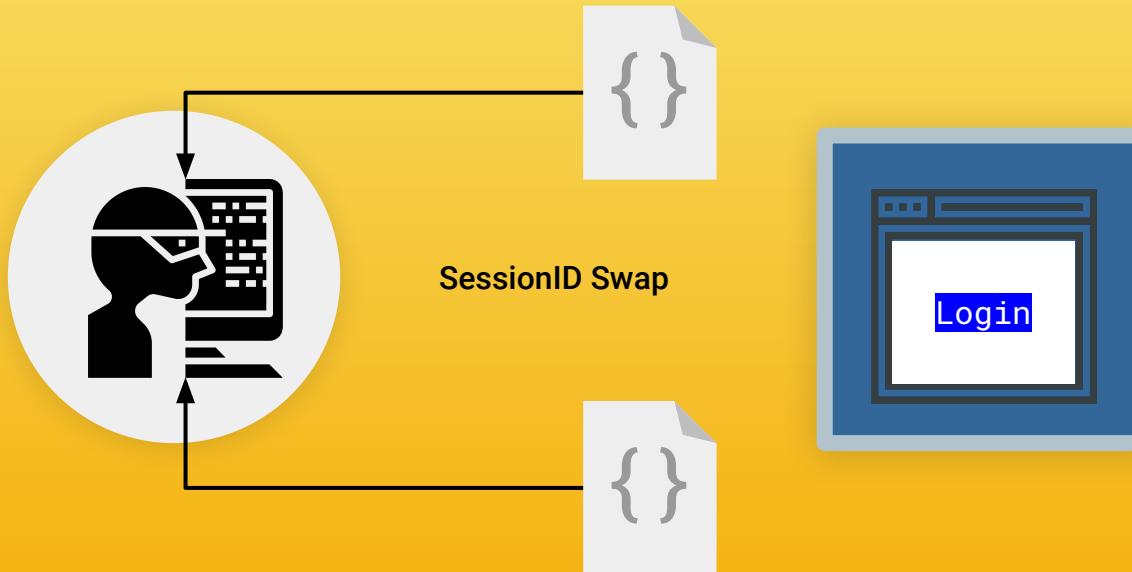


## Step 2: Defining Attack Strategies

---

### Attack Option #10: Faulty Session Management

A hacker can exploit faulty session management, when developers incorrectly implement code used to maintain login and logouts.





Next: **server** attacks.

## Step 2: Defining Attack Strategies

---

### Attack Option #11: OS Exploits

Servers, which run on operating systems like Windows and Linux, are subject to OS exploits when incorrectly patched.



## Step 2: Defining Attack Strategies

---

### Attack Option #12: Malicious Software

Malicious software can be directly loaded onto the server by USB or other means.





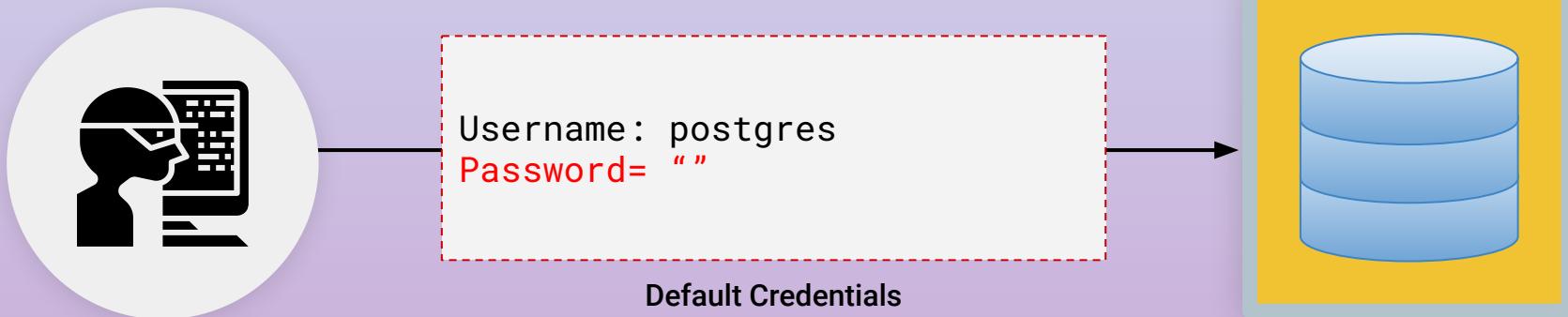
Finally: **database** attacks.

## Step 2: Defining Attack Strategies

---

### Attack Option #13: Default Credentials

Database management systems often come with **default credentials**, which might be left unchanged.

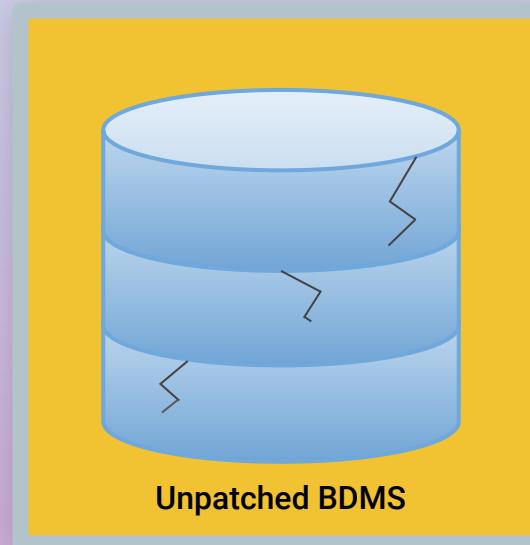


## Step 2: Defining Attack Strategies

---

### Attack Option #14: Unpatched Database

Database management systems might be unpatched against publicly known vulnerabilities.

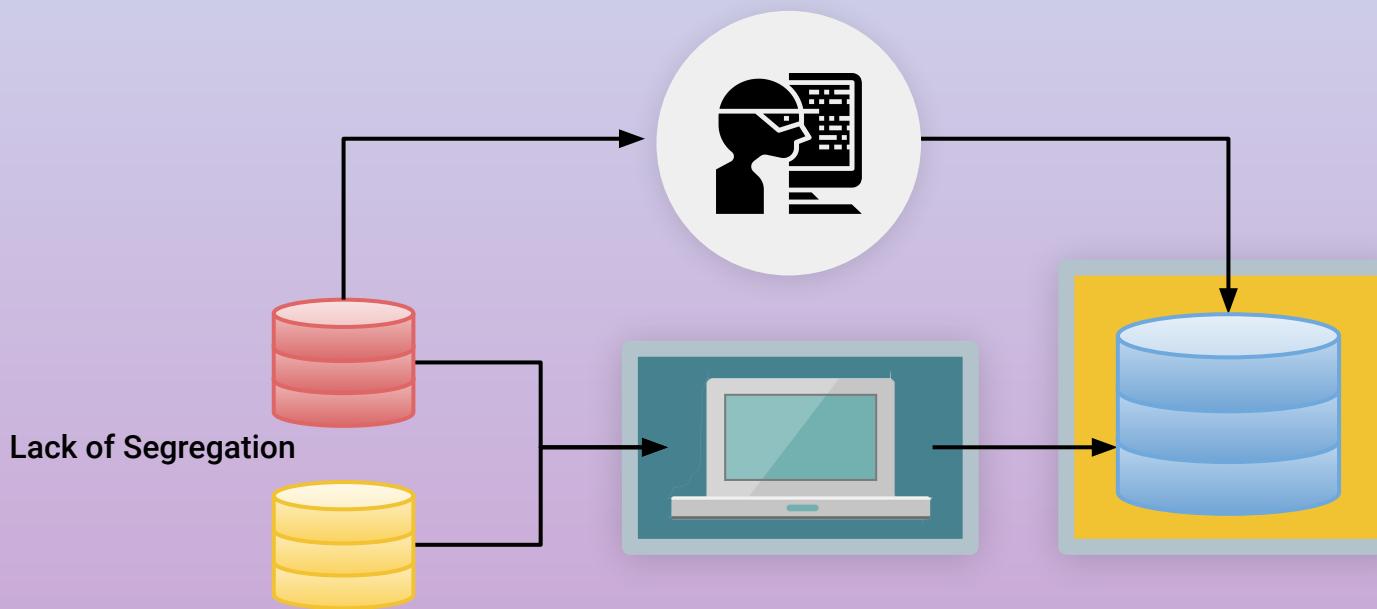


## Step 2: Defining Attack Strategies

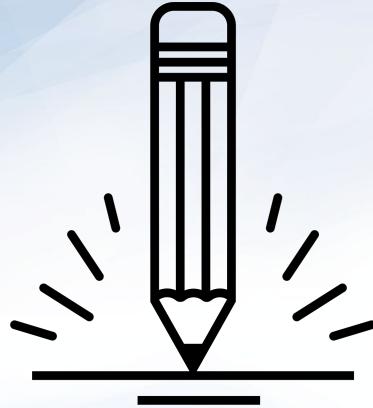
---

### Attack Option #15: Lack of Segregation

The database might be set up to **let a client look at another client's data**.



# Security Challenge #2



## Activity: Security Challenge #2: Defending the Wall

Now that we've assembled a list of potential attacks, your next task is to develop a list of at least 10 strategies to **mitigate** the website's risk of unauthorized access. *Be prepared to share!*

Suggested Time:  
15 Minutes



# Activity: Security Challenge #2: Defending the Wall

## 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

## Database Attacks

Default Credentials

Unpatched Database

Lack of Segregation

## Server Attacks

OS Exploit

Malicious Software

To help you get started,  
review this list of  
identified attack types.

# Step Three: Risk Mitigation Plan

# Step 3: Risk Mitigation Plan

## 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

## Database Attacks

Default Credentials

Unpatched Database

Lack of Segregation

## Server Attacks

OS Exploit

Malicious Software

**Risk Mitigation**  
begins by assessing  
all risks and looking  
for parallels.

# Step 3: Risk Mitigation Plan

## User Attacks

Social Engineering

Phishing Attacks

Credential Reuse

Malware Attacks

Man in the Middle

Packet Sniffing

Computer Theft

## User Risk Mitigation

1. Educate all users on the danger of phishing and social engineering.
2. Use randomly generated passwords.
3. Ensure users are employing multifactor authentication (password + phone confirmation).
4. Use HTTPS and only access sensitive content over secure channels.

# Step 3: Risk Mitigation Plan

Web Attacks

Brute-Force Attacks

Code Injection

Faulty Sessions

Server Attacks

OS Exploit

Malicious Software

## Web and Server Risk Mitigation

1. Ensure *strong* passwords are used (i.e., alphanumeric + symbol + special characters).
2. Sanitize any input in the web application form fields and filter out.
3. Ensure users are immediately logged out when closing a browser. (No preservation of login after 30 seconds of inactivity.)
4. Ensure all servers are routinely patched against latest known vulnerabilities.
5. Incorporate antivirus and user education.

# Step 3: Risk Mitigation Plan

---

## Suggested Plan

1. Educate all users on the dangers of phishing and social engineering.
2. Require randomly generated passwords.
3. Ensure users have multi-factor authentication (password + phone confirmation).
4. Use HTTPS and only access sensitive content over secure channels.
5. Ensure *strong* passwords are used (alphanumeric + symbols).
6. Sanitize any input in the web application form fields and filter the output.
7. Ensure users are immediately logged off when closing a browser. (No preservation of login after 30 seconds of inactivity.)
8. Ensure all servers are routinely patched against latest known vulnerabilities.
9. Ensure physical access to servers is protected by multiple forms of authentication (login + biometric).
10. Ensure that all data stored in the database is encrypted and cannot be read without additional login information.
11. Provide database access on need-to-know basis.
12. Log and monitor all database access.
13. Ensure that all cloud security platforms follow best practices for security implementation.

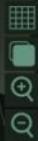
# Cybersecurity Framework

# Our Cybersecurity Framework

---

Even in our simple exercise, we can begin to see an emerging framework for addressing cybersecurity threats.



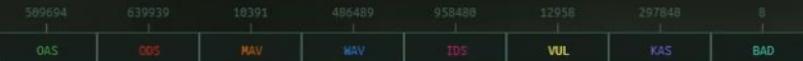


## Next Class...

---

We'll dive deeper into today's threat landscape and discuss modern cybersecurity tasks.

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



# Any Questions?