Edversity.

CYBERSECURITY SPECIALIZATION PROGRAM WEEK 1 - DAY 1

Instructor: Muddassir Shafique

TA: Suleiman Taj

Agenda

Week 1: Introduction to Cyber Security and Kali Linux
Week 2: Networking and Security Fundamentals
Week 3: Cryptography
Week 4: OS Security
Week 5: Web Security
Week 6: Incident Response and Management
Week 7: Security Policies and Risk Management
Week 8: Emerging Technologies and Future trends
Week 9: CAPSTONE Project and Review
Week 10: CAPSTONE Project Presentations

What We'll Learn Today

What is cybersecurity?

What are common threats?

Who are the attackers?

What is Kali Linux?

Try some tools and commands!

What comes to mind when you hear “hacker”?

What is cybersecurity?

Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

- In essence, cybersecurity is about defense in the digital world. It involves a multi-layered approach to secure information and technology assets, including:
- Protecting Confidentiality: Ensuring that sensitive information is only accessible to authorized individuals.
- Maintaining Integrity: Guaranteeing that data remains accurate and unaltered during storage and transmission.
- Ensuring Availability: Making sure that systems and data are accessible to authorized users when needed.

What is cybersecurity?

- Cybersecurity is crucial in today's interconnected world, where individuals, businesses, and governments rely heavily on digital infrastructure. A robust cybersecurity strategy is essential to prevent data breaches, financial losses, reputational damage, and disruption of critical services.

What is cybersecurity?

🛡️ Cybersecurity: Protecting Your Digital World 🌐

Cybersecurity is all about safeguarding your valuable digital assets from harmful attacks. Think of it as building a strong fortress around your data and systems!

Your Digital Assets (What We Protect)

Devices

Laptops, Phones, Tablets

Data

Personal info, Files, Photos

Accounts

Banking, Social Media, Email

What is cybersecurity?

CIA Traid

- 🔐 C – Confidentiality
- 🛠️ I – Integrity
- 🔄 A – Availability

What is cybersecurity?

CIA Traid

- 🔐 C is for Confidentiality – Keeping Secrets Safe
- In your house:
- You keep your diary, money, and personal things in a locked drawer. You don’t let just anyone walk in and look around.
- In cybersecurity:
- Confidentiality means only the right people can access your data.
- 🔑 You use passwords, encryption, and access controls to keep things private—just like locking the drawer.

What is cybersecurity?

CIA Traid

- 🛠️I is for Integrity – Keeping Things Unchanged
- In your house:
- You write your school project and keep it safe. One day, you find someone scribbled all over it and added fake stuff. Uh-oh!😱
- That's a loss of integrity—your original work got messed up.
- In cybersecurity:
- Integrity means your data stays exactly how it was meant to be—untouched and trustworthy.

What is cybersecurity?

CIA Traid

- 🔍 You use checksums, digital signatures, and version control to make sure no one has changed your data without permission.

What is cybersecurity?

CIA Traid

- A is for Availability – Always Ready When You Need It
- In your house:
- You want to watch cartoons on TV, but—boom—the power's out, or someone cut the cable wire. Now you can't access it, even though you own it.
- In cybersecurity:
- Availability means your systems and data are ready and working whenever you need them.

What is cybersecurity?

CIA Traid

- 💡 You use backups, redundancy, and cyber defense against attacks (like DDoS) to make sure your services stay online and usable.

What is cybersecurity?

Putting It All Together:

- Imagine your house is your castle, and cybersecurity makes sure:
- No stranger sneaks in and reads your diary (Confidentiality)
- No one replaces your homework with garbage (Integrity)
- You can turn on your TV or computer whenever you want (Availability)

What are common threats??

What is a threat and What are common Threats

- Malware
- Phishing
- Ransomware
- Data breaches
- Surprizes

What are common threats??

Malware (Short for “Malicious Software”)

Malware is a broad umbrella term that includes all types of harmful software:

- Viruses, worms, ransomware, trojans, spyware, adware... you name it.
- Its purpose could be stealing data, spying, damaging devices, or just annoying users.

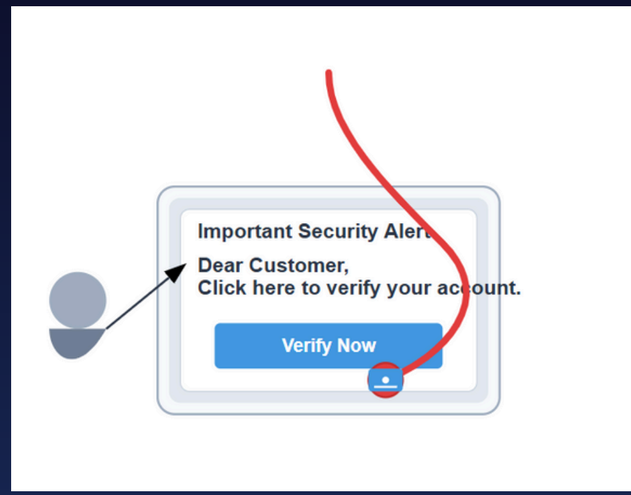
What are common threats??

Type	Definition	Spreads Automatically?	Needs User Action?	Primary Goal	Example Behavior
Virus	Attaches to files or programs and spreads when activated	❌ No	✅ Yes	Corrupt or destroy data	Deletes or alters files once opened
Worm	Self-replicating malware that spreads through networks	✅ Yes	❌ No	Spread quickly, slow networks	Copies itself across networked computers
Malware	Umbrella term for all types of malicious software	🔄 Varies	🔄 Varies	Varies: damage, theft, spying	Includes viruses, worms, trojans, ransomware
Ransomware	Encrypts or locks data and demands payment for release	🔄 Varies	🔄 Varies	Extort money from victims	Locks files and displays ransom message

What are common threats??

Concept – What is Phishing?

- **Deceptive Digital Fraud:** Phishing is a cybercrime where attackers attempt to trick individuals into revealing sensitive information (e.g., usernames, passwords, credit card details) or downloading malicious software.
- **Impersonation is Key**: Attackers typically disguise themselves as a trustworthy entity, such as a legitimate company, government agency, or even a known individual.
- **Goal:** Data Theft or System Compromise: The ultimate aim is to gain unauthorized access to accounts, commit financial fraud, or infect systems with malware for further exploitation.
- **Common Vectors:** While often associated with email, phishing can occur through various digital channels, including text messages (smishing), phone calls (vishing), and social media.



What are common threats??

Method – How Phishing is Performed

- **Step 1: Lure Creation:** Attackers craft convincing-looking emails, messages, or websites that mimic legitimate sources. These often include urgency, threats, or enticing offers to prompt immediate action.
- **Step 2: Distribution:** The deceptive messages are sent to a large number of potential victims, often through bulk email campaigns or targeted approaches.
- **Step 3: Deception & Execution:** When a victim clicks on a malicious link or opens an attachment, they are directed to a fake website or unknowingly download malware. The fake website then prompts them to enter sensitive information, or the malware executes in the background.
- **Step 4: Data Harvesting/Exploitation:** Once the information is entered or the malware is installed, the attackers collect the data or gain control over the compromised system, allowing them to carry out their malicious objectives.

What are common threats??

Method - How Phishing is Performed

1

Lure Creation

Attackers craft convincing fake emails, messages, or websites.

2

Distribution

Deceptive messages are sent to a large number of victims.

3

Deception & Execution

Victim interacts with the lure (clicks link, opens attachment).

4

Data Harvesting

Attackers collect stolen data or gain control

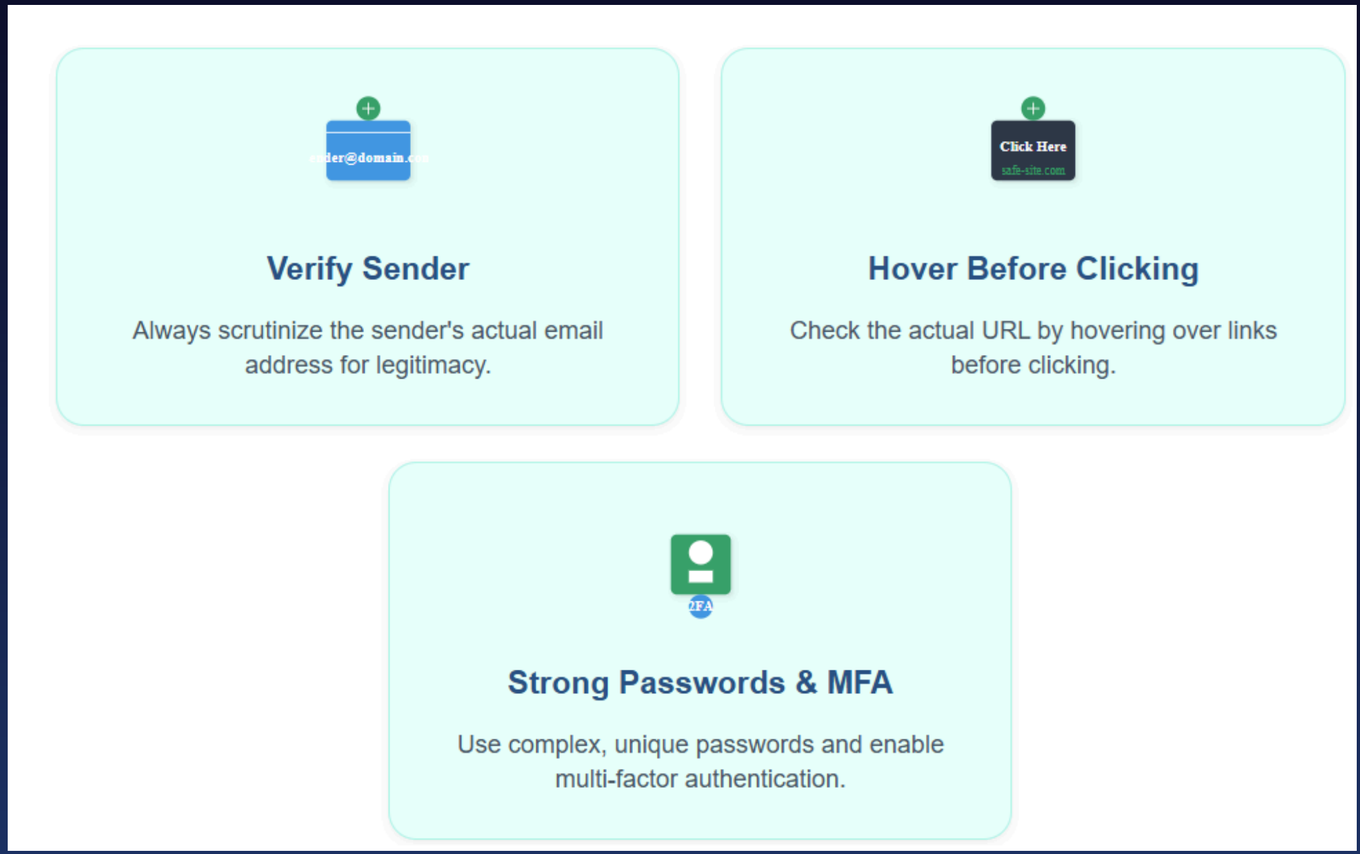
What are common threats??

Protection – Safeguarding Users

- **Verify Sender:** Always scrutinize the sender's email address, not just the display name. Be wary of generic greetings.
- **Hover Before Clicking:** Hover over links to see the actual URL before clicking. Look for inconsistencies or suspicious domains.
- **Strong, Unique Passwords & MFA:** Use complex passwords for all accounts and enable multi-factor authentication (MFA) whenever possible.
- **Be Skeptical:** If an offer seems too good to be true or a request is unusual, it likely is. Contact the organization directly using official channels.
- **Report Suspicious Activity:** Report phishing attempts to your IT department or email provider.

What are common threats??

Protection – Safeguarding Users



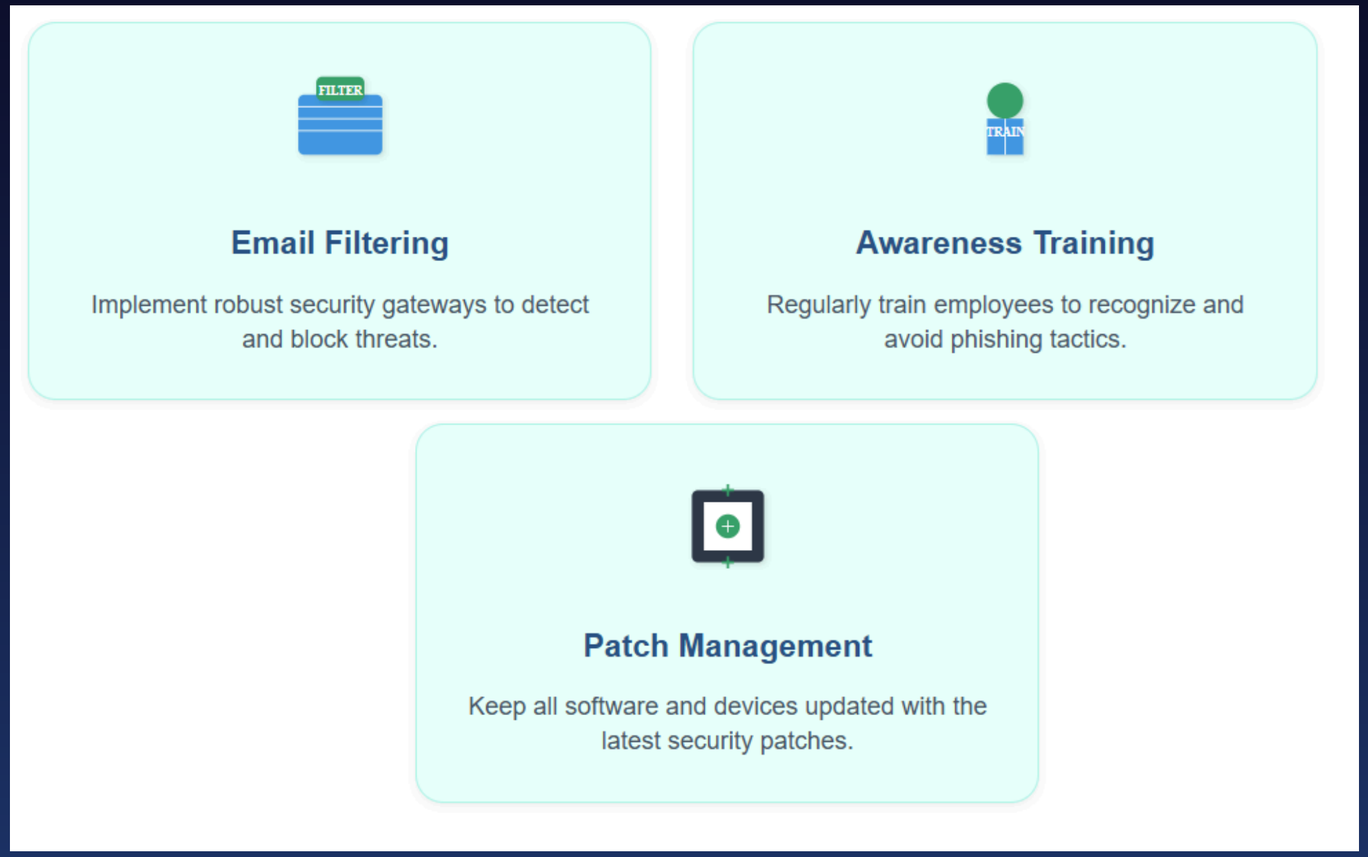
What are common threats??

Protection – Safeguarding Networks

- **Email Filtering & Anti-Phishing Solutions:** Implement robust email security gateways that detect and block known phishing attempts, malicious attachments, and suspicious links.
- **Security Awareness Training:** Regularly train employees to recognize phishing tactics and understand best practices for online security.
- **Patch Management:** Keep all software, operating systems, and network devices updated with the latest security patches to fix vulnerabilities.
- **Network Segmentation:** Divide the network into smaller segments to limit the lateral movement of attackers in case of a breach.
- **Incident Response Plan:** Have a clear plan in place for how to respond to and mitigate the impact of a successful phishing attack.

What are common threats??

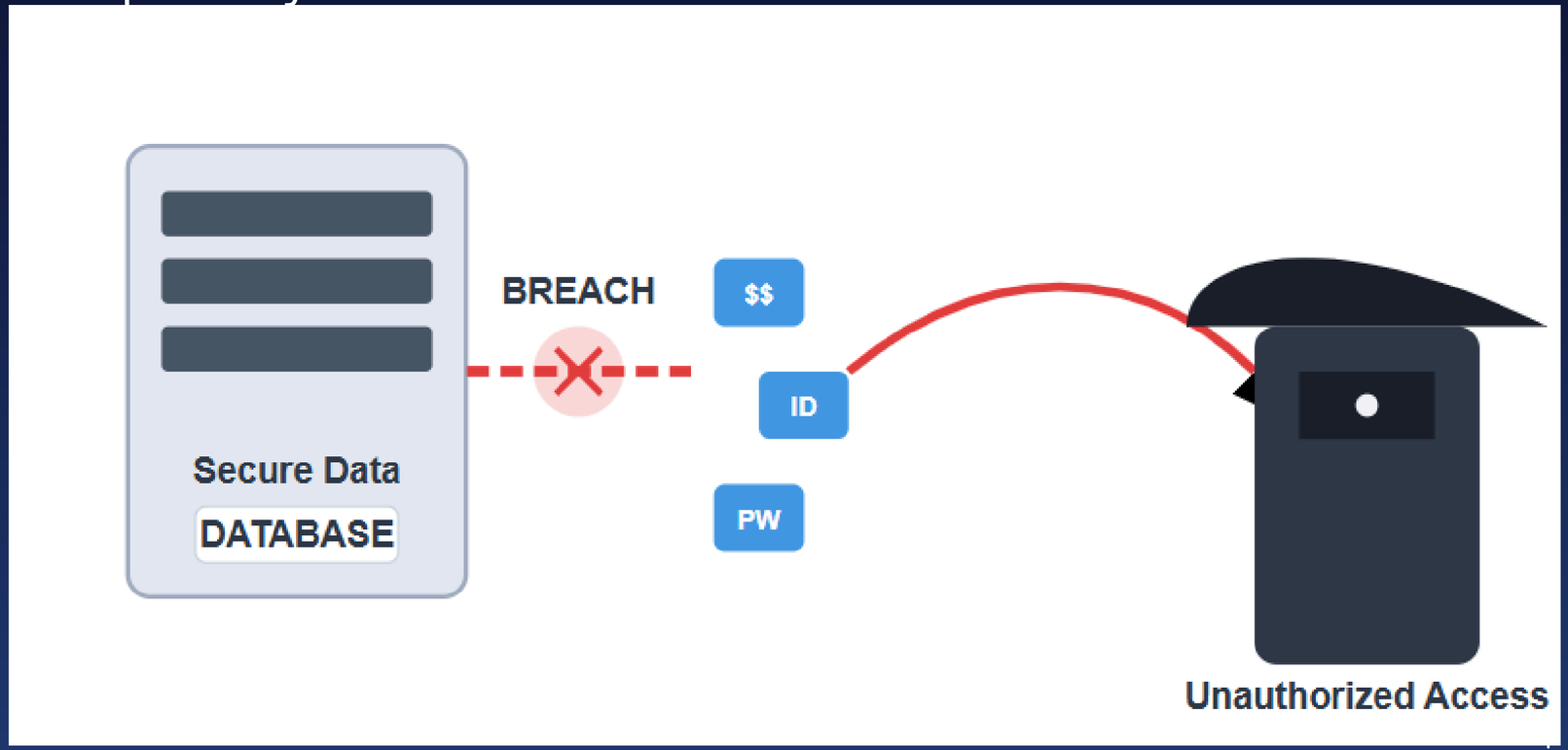
Protection – Safeguarding Networks



What are common threats??

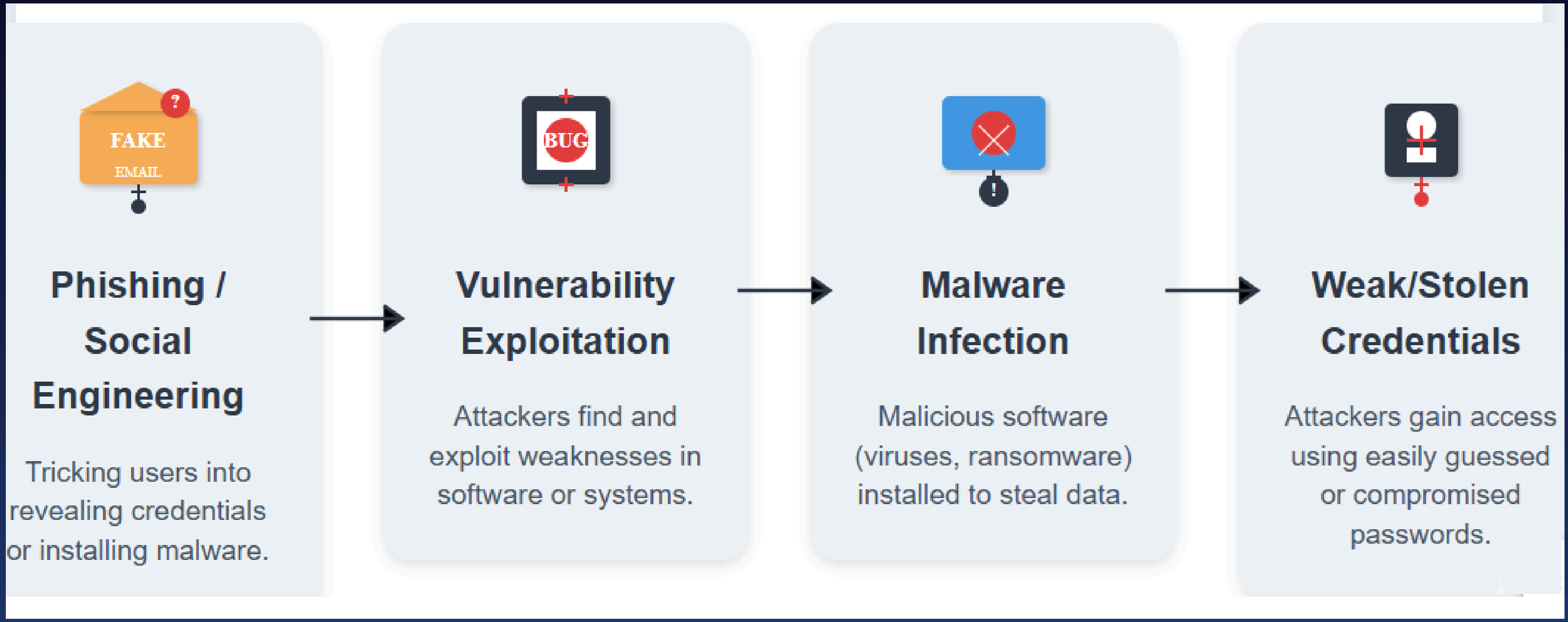
- **Data breach – Concept**

A data breach is a security incident where sensitive, protected, or confidential data is accessed, viewed, stolen, or used by an unauthorized individual. It represents a critical compromise of data security and privacy.



What are common threats??

- **Data breach – Method**



What are common threats??

- **Data breach – Protection**

User

Strong Passwords & MFA

Use complex, unique passwords and enable multi-factor authentication.

Vigilance & Awareness

Recognize phishing attempts and other social engineering tactics.

Data Minimization

Only share or store essential personal information.

Network

Encryption

Encrypt sensitive data at rest and in transit.

Firewalls & IDS/IPS

Implement network security to monitor and block malicious traffic.

Audits & Patching

Regularly scan for vulnerabilities and apply security updates.

What are common threats??

- Surprizes
- WannaCry (2017)
  - Ransomware attack affecting 200,000+ systems in 150 countries
  - Paralyzed NHS (UK health system), FedEx, railways, banks
  - Exploited a Windows vulnerability leaked by Shadow Brokers
- NotPetya (2017)
  - Posed as ransomware, but designed for total data destruction
  - Hit Ukraine, but spread globally — impacting Maersk, Merck, Rosneft
  - Estimated damages: >$10 billion
- Stuxnet (2010)
  - First known cyber weapon targeting industrial systems
  - Disrupted Iran's nuclear centrifuges
  - Highly advanced — believed to be developed by US & Israel

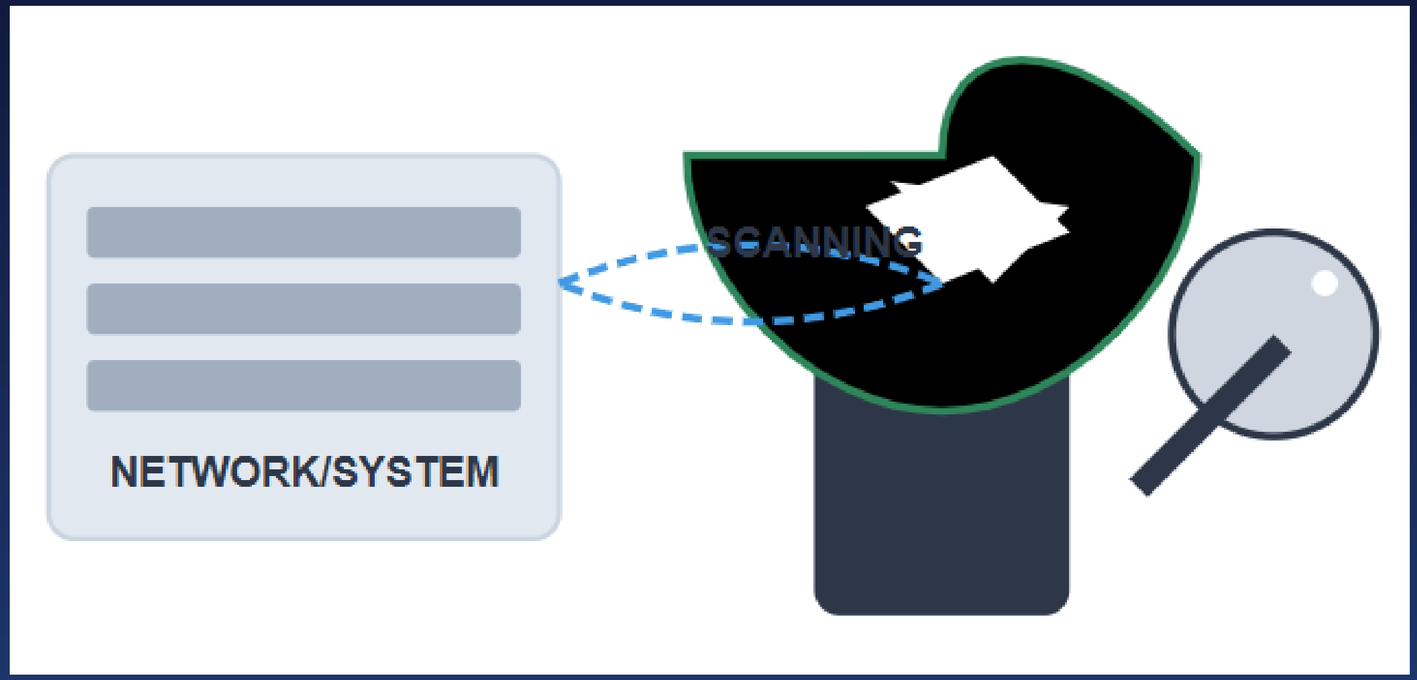
What are common threats??

- SolarWinds Supply Chain Attack (2020)
  - Nation-state level breach
  - Infiltrated major US government agencies and corporations
  - Attackers inserted malware into a routine software update
- Equifax Breach (2017)
  - 147 million Americans affected
  - Exposed SSNs, birth dates, and financial data
  - Caused massive legal and reputational fallout
-

Who are the attackers?

White hats (ethical hackers)

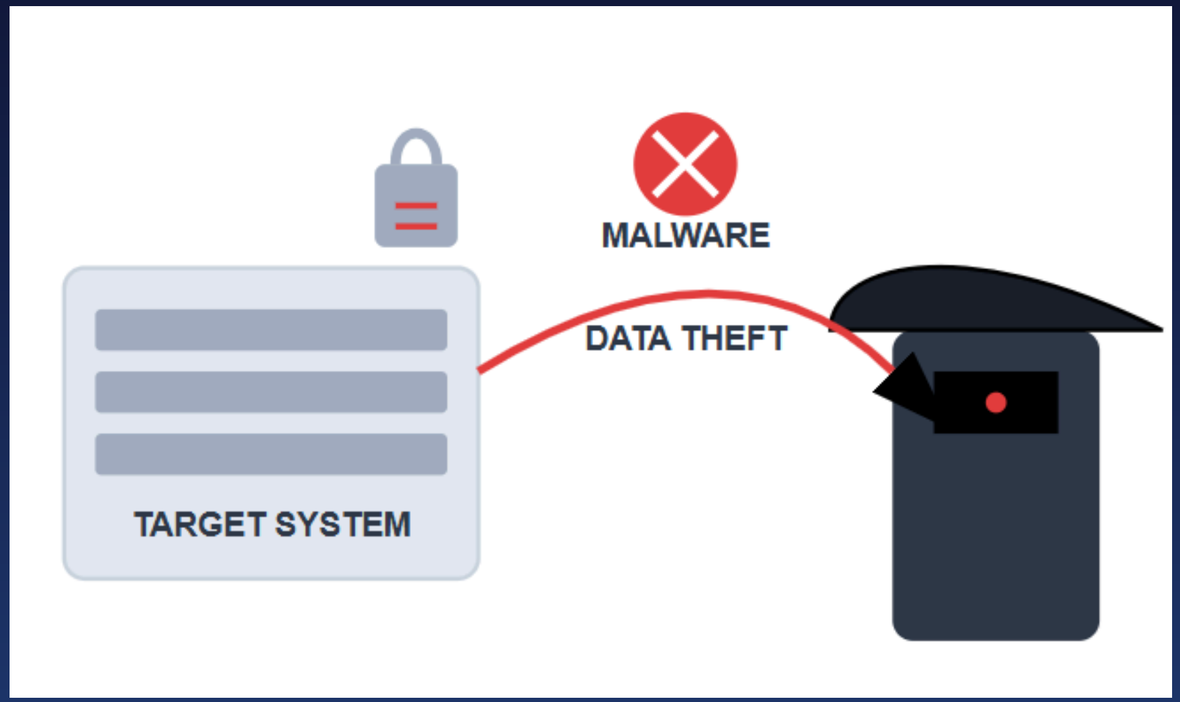
White Hats, also known as ethical hackers, are cybersecurity professionals who use their hacking skills for defensive purposes. They are authorized to test systems for vulnerabilities, identify weaknesses, and report them to organizations to improve security, preventing malicious attacks.



Who are the attackers?

Black hats (criminal hackers)

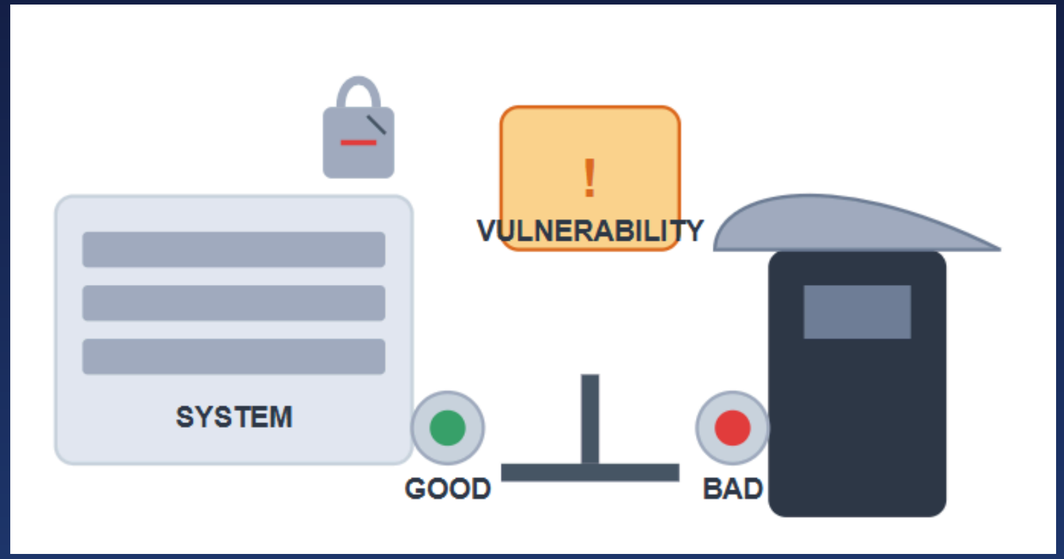
Black Hats, or criminal hackers, are individuals who gain unauthorized access to computer systems or networks with malicious intent. Their activities include stealing data, disrupting services, financial fraud, and deploying malware, often for personal gain or to cause damage.



Who are the attackers?

Gray hats (in between)

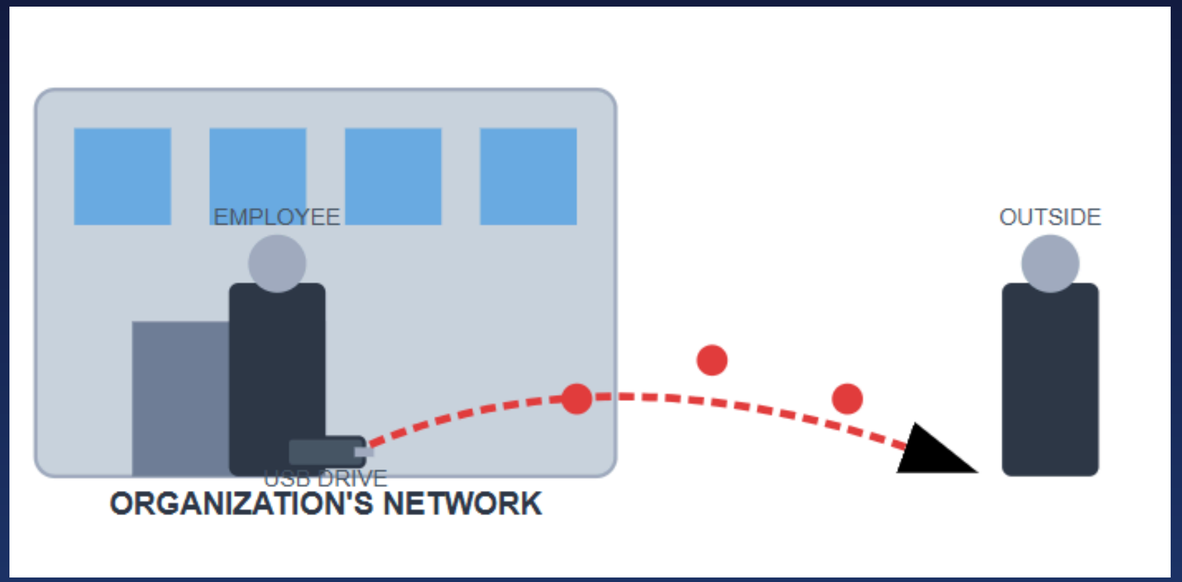
Gray Hats operate in a legal and ethical grey area. They often access systems without authorization to find vulnerabilities, similar to Black Hats, but their intent is not purely malicious. They might disclose vulnerabilities publicly or to the organization, sometimes seeking a reward, without prior permission.



Who are the attackers?

Insider threats

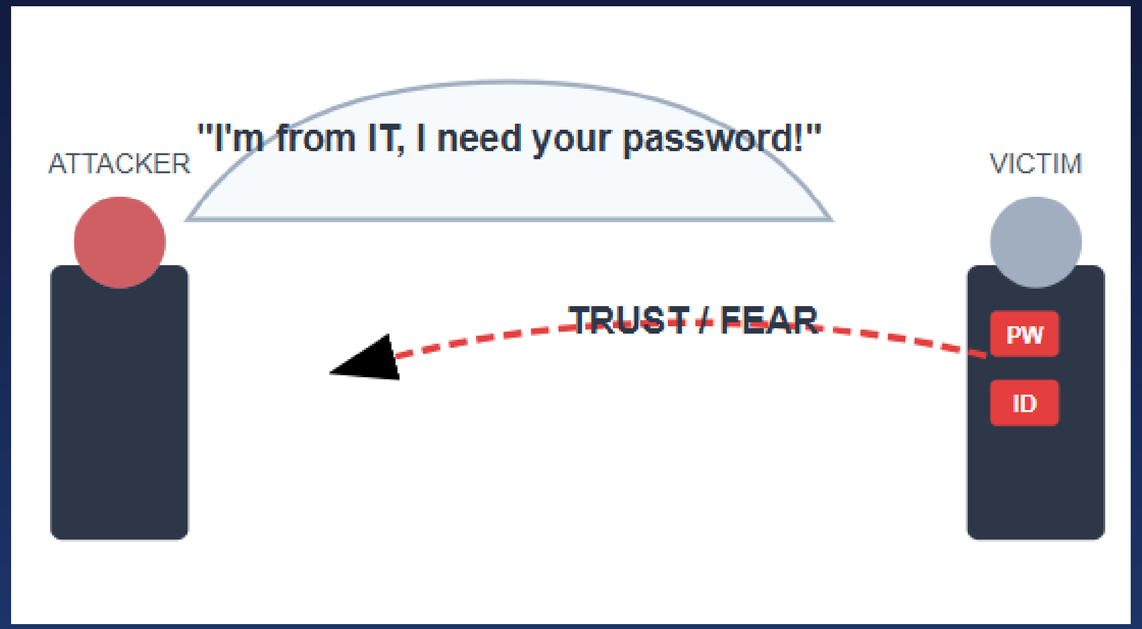
Insider Threats originate from within an organization, involving current or former employees, contractors, or business associates who have authorized access to systems or data. These threats can be malicious (e.g., data theft, sabotage) or accidental (e.g., negligence, human error), making them particularly difficult to detect.



Who are the attackers?

Social engineering

Social Engineering is a non-technical cyberattack method that relies on psychological manipulation to trick individuals into performing actions or divulging confidential information. Attackers exploit human trust, curiosity, fear, or urgency, often impersonating legitimate entities, to bypass security measures.



What is Kali Linux?

- A special version of Linux
- Made for cybersecurity tools
- Legal use only: testing & learning
- Used by pros and students

Comparsion of security OS

Base	Debian	Debian	Arch Linux
Pre-installed Tools	600+ ready-to-use tools	Many tools + privacy & dev tools	Minimal pre-installed, 2700+ tools available
User-Friendliness	Beginner-friendly, GUI-based	Lightweight, privacy-focused	Advanced users, command-line oriented
Community & Support	Large, official documentation	Growing community	Smaller, community-driven
Hardware Compatibility	Excellent, including ARM	Good, lightweight for older hardware	Focused on x86_64 only
Use Case	Penetration testing, professional	Pen-testing + privacy + development	Pen-testing, advanced customization

Lets install Kali

Bare Metal Install – Install Kali as the primary OS.

Virtual Machine (VM) – Use VirtualBox, VMware, or Hyper-V.

Live USB Boot – Run Kali from a USB without installing.

Persistent Live USB – Run Kali from USB with data saving.

Dual-Boot – Install alongside another OS (e.g., Windows).

ARM Installation – Install on devices like Raspberry Pi.

Windows Subsystem for Linux (WSL) – Run Kali inside Windows.

Link for Vm and kali linux download

https://www.kali.org/get-kali/#kali-platforms

https://www.oracle.com/pk/virtualization/technologies/vm/downloads/virtualbox-downloads.html

Let’s Meet the Terminal

- Text-based interface
- Powerful, fast
- First commands to try:
- pwd
- ls
- cd
- mkdir
- touch
- cat

What We Learned Today

- What is cybersecurity?
- What is Kali Linux?
- What is one command or tool you used?