FUNDAMENTALS OF CYBERSECURITY CONCEPTS

Created by : Raushan

Linkedin : https://www.linkedin.com/in/raushan-patel-8823b3241/

COVERS TOPICS LIKE-

- Fundamentals of cybersecurity.
- Types of cybersecurity threats (eg.,phishing, malware).
- Common vulnerabilities (eg.,weak passwords, unpatched software).
- Risk management strategies.

Fundamentals of cybersecurity?

- Fundamentals of cybersecurity are the basics principles and practices that help protect information and systems from cyber attacks.
- Some of the important device protection, securing online connection, securing email communication, and performing timely backups of files and documents.
- One of the best models common models for cybersecurity is the CIA triad.
- Which stands for Confidentiality, integrity, and availability.

CONFIDENTIALITY !

- Confidentiality refers to the measures you take to ensure your data is kept secret or private.
- This includes personal information like:
  - Credit card information
  - Social Security numbers
  - Physical addresses
  - Medical records
  - Account login information
- Keep Data secrets and private.

INTEGRITY !

- Integrity in cybersecurity means ensuring your data remains trustworthy, accurate, and safeguarded against unauthorized modification or destruction.
- This can be done by:
  - Using end-to-end encryption to protect sensitive data while in transit and at rest
  - Setting access controls so only authorized personnel can access specific information
  - Ensuring no one user is given enough access to be able to misuse a system on their own
  - Backing up data
- Keeps Data trustworthy and Accurate.

AVAILABILITY !

- Availability ensures that systems, networks, and applications are functioning so authorized users can access data when they need to.
- Availability can be severely impacted in situations like:
  - Natural disasters
  - Power outages
  - Deliberate cyberattacks, like denial-of-service (DoS) attacks or ransomware

- Keeps Systems and networks accessible.

Types of cybersecurity Threats!

- Malware (Worm, Trojan, Viruses, Spyware)
- Phishing
- Ransomware
- Distributed denial-of-service (DDoS) attacks
- Advanced persistent threats

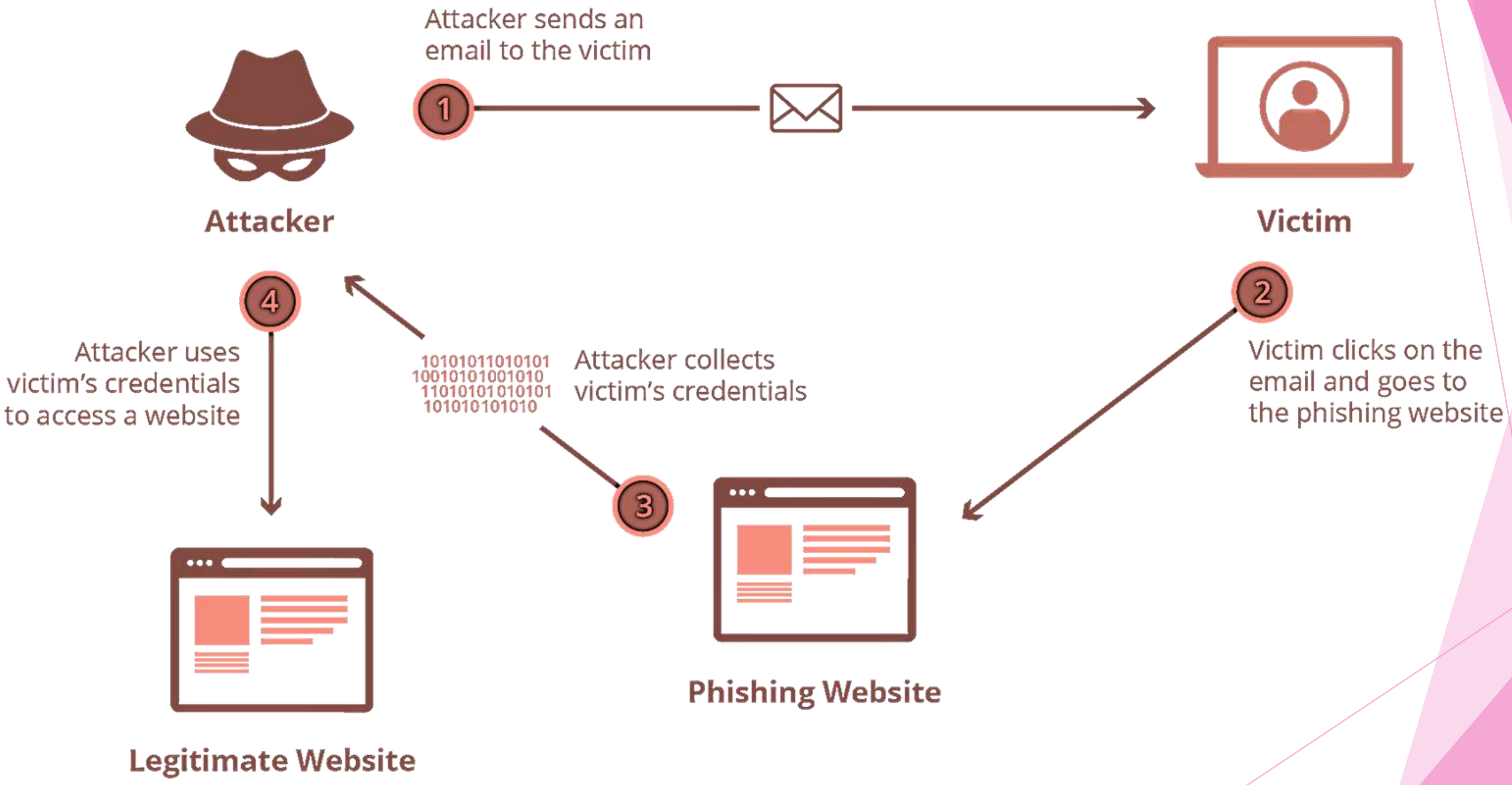
Malware threats !

- short for “malicious software”—is software specifically designed to gain unauthorized access to or damage a device or Networks.
- Common types of malware include:
- Trojan horses: malware disguised as a legitimate program that provides a hacker backdoor access to your computer
- Viruses: malware designed to change, corrupt, or destroy information that is then passed on to other systems, usually by otherwise benign means (like sending an email)
- Spyware: malware that is used by hackers to spy on your computer or mobile phone activities
- Worms: malware that can multiply and spread to other computers in the network

Phishing threats !

- Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.
- Phishing threat is type of social engineering attacks often steal information.
- It often likes through:
- Text message
- Email
- Phone calls
- Social media direct messages
- For example, in 2018 phishers targeted Netflix users through an email stating the popular streaming platform was “having some trouble” accessing the customer’s billing information.

How looks like !



Attacker sends an email to the victim

Victim clicks on the email and goes to the phishing website

Attacker collects victim's credentials

Attacker uses victim's credentials to access a website

Ransomware threats !

- Ransomware is malware that can lock, encrypt, and destroy personal files once it gains access to your computer.
- hackers typically use ransomware to extort money from their victims with promises of restoring the encrypted data.
- Ransomware is a type of malware that holds a victim’s data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker.
- According to the IBM Security X-Force Threat Intelligence Index 2023, ransomware attacks represented 17 percent of all cyberattacks in 2022.

Distributed denial-of-service (DDoS) attacks!

- Similar to ransomware, distributed denial-of-service (DDoS) attacks also compromise computer availability.
- DDoS attacks are used by cybercriminals attempting to flood or crash a website by triggering traffic from millions of botnets.
- Here’s how it works:
- The hacker forms a “zombie network” of remotely controlled hacked computers called botnets.
- The hacker uses the zombie network to flood a targeted website or internet server with traffic, rendering it inoperable.
- Once the website or server crashes, both website administrators and online visitors won’t be able to access it.

Advanced persistent threats !

- Advanced persistent threats (APTs) are a type of attack on integrity used to infiltrate a network undetected for an extended period of time, all the while stealing valuable data without actually harming the network.
- Some of the consequences of an APT attack include:
- Theft of intellectual property
- Distribution of sensitive information
- Site takeovers
- Session hijacking
- Destruction of data
- APTs have the ability to destroy and manipulate files stored on computers and devices, targeting data like:
- Legal contracts
- Patent information

What is Vulnerability !

- A vulnerability in cybersecurity is a weakness in a host or system, such as a missed software update or system.
- Identifying cyber vulnerabilities is one of the most important steps organizations can take to improve and strengthen their overall cybersecurity posture.

Misconfigurations Vulnerability!

- Misconfigurations are the single largest threat to both cloud and app security. Because many application security tools require manual configuration, this process can be rife with errors and take considerable time to manage and update.
- As companies increase their use of cloud hosting for storage and computing, so increases the risk of attack on their cloud services. Proactive prevention is always preferred over required remediation.

Outdated or Unpatched Software !

- Software vendors periodically release application updates to either add new features and functionalities or patch known cybersecurity vulnerabilities.
- Unpatched or outdated software often make for an easy target for advanced cybercriminals.
- While software updates may contain valuable and important security measures, it is the responsibility of the organization to update their network and all endpoints.
- organizations should develop and implement a process for prioritizing software updates and patching.

Zero-day Vulnerabilities !

- The term “Zero-Day” is used when security teams are unaware of their software vulnerability, and they’ve had “0” days to work on a security patch or an update to fix the issue. “Zero-Day” is commonly associated with the terms Vulnerability, Exploit, and Threat. It is important to understand the difference:
- A Zero-Day Vulnerability is an unknown security vulnerability or software flaw that a threat actor can target with malicious code.
- A Zero-Day Exploit is the technique or tactic a malicious actor uses to leverage the vulnerability to attack a system.
- A Zero-Day Attack occurs when a hacker releases malware to exploit the software vulnerability before the software developer has patched the flaw.
- Zero-day attacks are extremely dangerous for cloud workloads because they’re unknown and can be very difficult to detect, making them a serious security risk. It’s like a thief sneaking in through a backdoor that was accidentally left unlocked.

Weak or Stolen User Credentials !

- Many users fail to create unique and strong passwords for each of their accounts.
- Reusing or recycling passwords and user IDs creates another potential avenue of exploitation for cybercriminals.
- Weak user credentials are most often exploited in brute force attacks when a threat actor tries to gain unauthorized access to sensitive data and systems by systematically trying as many combinations of usernames and guessed passwords as possible.
- Organizations should also consider implementing a multifactor authentication (MFA)
- identification, such as both a password and a fingerprint or a password and a one-time security token, to authenticate the user.

Risk management strategies !

- Risk management strategies are essential for identifying, assessing, and mitigating risks within an organization.
- Risk Acceptance: This involves acknowledging the risk and deciding to accept it without engaging in special efforts to control it.
- Risk Avoidance: This strategy aims to eliminate the risk by not engaging in the action that could trigger the risk.
- Risk Reduction: Implementing measures to reduce the likelihood or impact of the risk.

Risk management strategies !

- Risk Transference: This involves shifting the risk to a third party, such as through insurance or outsourcing.
- Risk Sharing: Sometimes, risks are shared between parties, which can be a viable option when the risk is too large for one party to handle alone.
- Loss Prevention and Reduction: This strategy focuses on preventing the occurrence of risks and reducing their impact if they do occur.

References !

- https://www.crowdstrike.com/
- Cybersecurity basics for beginners: 2024 guide – Norton
- https://www.knowledgehut.com/blog/security/cyber-security-fundamentals#common-types-of-cyber-attacks%C2%A0%C2%A0

Thank you

Github:- raushanpatel1 (Raushan patel) (github.com)