Cybersecurity Essentials

1.1 Cybersecurity Threats Vulnerabilities and Attacks

1.1.1 Threat Domains

With organizations facing an ever-growing number of cyber threats, it is critical that they have robust security solutions in place. But in order to protect themselves, organizations first need to know what vulnerabilities exist within their threat domains. A 'threat domain' is an area of control, authority or protection that attackers can exploit to gain access to a system.

There are many ways that attackers can uncover vulnerabilities and exploit systems within a domain. **Attackers can exploit systems within a domain through:**

1. Direct, physical access to systems and networks.
2. Wireless networking that extends beyond an organization's boundaries.
3. Bluetooth or near-field communication (NFC) devices.
4. Malicious email attachments.
5. Less secure elements within an organization's supply chain.
6. An organization's social media accounts.
7. Removable media such as flash drives.
8. Cloud-based applications.

Cybersecurity professionals can also use these domains to perform an analysis of an organization's current cybersecurity status. In this module, we will look at the different types of domains that exist within an organization. It is important to approach cybersecurity risks from a multi-scale, systems perspective, taking into account the interaction of cyber, physical and human systems.

1.1.2 Types of Cyber Threats

Cyber threats can be classified into different categories. This allows organizations to assess the likelihood of a threat occurring and understand the monetary impact of a threat so that they can prioritize their security efforts.

Select the headings for examples of cyber threats in each of these categories.

Software attacks

- A successful denial-of-service (DoS attack).
- A computer virus.

Software errors

- A software bug.
- An application going offline.
- A cross-site script or illegal file server share.

Sabotage

- A backdoor, or a worm that erases files.
- An authorized user successfully penetrating and compromising an organization's primary database.
- The defacement of an organization's website.

Human error

- Inadvertent data entry errors.
- An employee dropping a laptop

Theft

- Laptops or equipment being stolen from an unlocked room.

Hardware failures

- Hard drive crashes.
- A firewall misconfiguration.

Utility interruption

- Electrical power outages.
- Water damage resulting from sprinkler failure.

Natural disasters

- Severe storms such as hurricanes or tornados.
- Earthquakes.
- Floods.
- Fires.

1.1.3 Internal vs External Threats

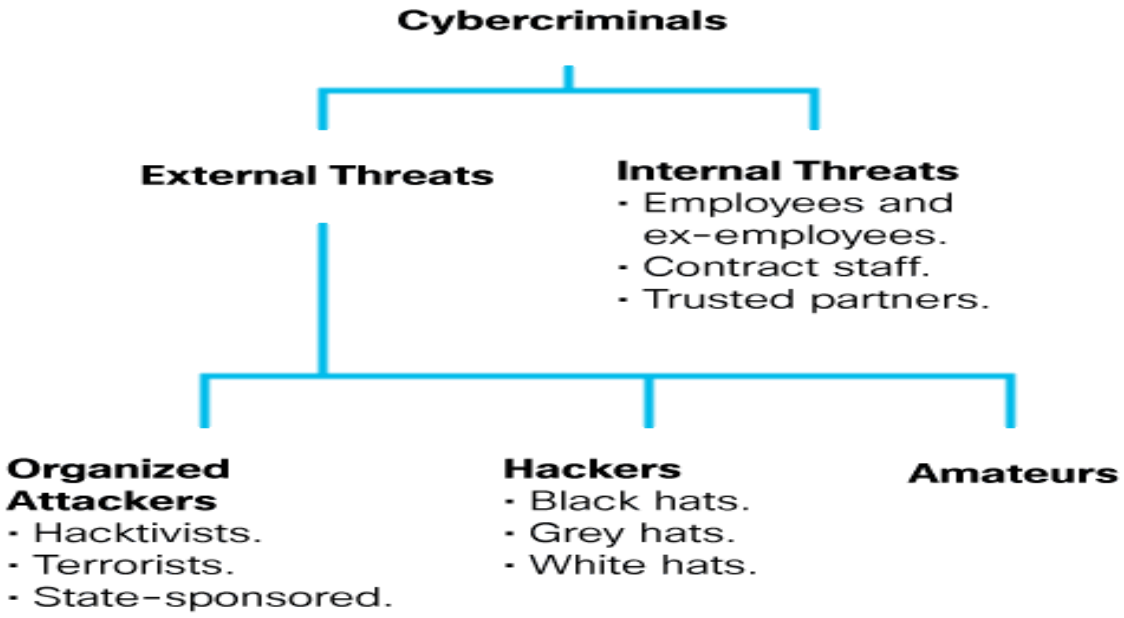
Threats can originate from both within and outside of an organization, with attackers seeking access to valuable sensitive information such as personnel records, intellectual property and financial data.

Internal threats are usually carried out by current or former employees and other contract partners who accidentally or intentionally mishandle confidential data or threaten the operations of servers or network infrastructure devices by connecting infected media or by accessing malicious emails or websites.

The source of an **external threat** typically stems from amateur or or skilled attackers who can exploit vulnerabilities in networked devices or can use social engineering techniques, such as trickery, to gain access to an organization's internal resources.

Did you know that internal threats have the potential to cause greater damage than external threats?

This is because employees or partners working within an organization have direct access to its premises and infrastructure devices. They will also have insider knowledge of the organization's network, resources and confidential data, as well as the security countermeasures in place.



1.1.4 Know the Difference

Internal

1. A Former Employee was able to download customer information by remotely accessing network.
2. An employee clicked on a suspicious email link

External

1. An employee granted someone unauthorized physical access to @Apollo's HQ
2. An employee was tricked into giving out confidential information by someone pretending to be their manager

Cyber threats can spread in various ways such as through users themselves, via devices connected to the network or via services hosted on a public or private cloud. And don't forget the threat of a physical attack if the right security measures are not in place.

Let's look at these in more detail.

9.1 Final Course Exam

You will be assessed on the core concepts presented across each of the eight modules. There are fifty questions in total, and you need to score **at least 70%** to pass and achieve your **Grade.**

Q 1) What do you call an impersonation attack that takes advantage of a trusted relationship between two systems?

- **A. Spoofing**
- B. Sniffing
- C. Spamming
- D. Man-in-the-middle

Q 2) Joel, an Executive Manager at @Apollo, goes to an important meeting. His secretary receives a call from a person claiming that Joel is about to give an important presentation but the presentation files are corrupted. The caller sternly recommends that the secretary email the presentation right away, to a personal email address. The caller also states that Joel is holding the secretary responsible for the success of this presentation. ***What type of social engineering tactic does this scenario describe?***

- A. Urgency
- B. Familiarity
- C. Trusted partners
- **D. Intimidation**

Q 3) A few @Apollo employees report receiving an email stating that their account password will expire immediately and that they should reset their password within five minutes. ***How would you classify this email?***

- A. It is an impersonation attack
- **B. It is a hoax**
- C. It is a piggyback attack
- D. It is a DDoS attack

Q 4) Several @Apollo employees have reported that the network access is slow. After investigation, the network administrator has learned that one employee downloaded a third-party scanning program for the printer. ***What type of malware might have been introduced that is causing slow performance of the network?***

- A. Phishing
- B. Spam
- **C. Worm**
- D. Virus

Q 5) Several @Apollo employees have reported that they are unable to access the database on the main server. A database administrator verifies the issue and notices that the database file is encrypted. An hour later, the organization receives a threatening email demanding payment for the decryption of the database file. ***What type of attack has the organization experienced?***

- A. DoS attack

B. Ransomware
C. Trojan horse
D. Man-in-the-middle attack

Q 6) Passwords, passphrases and PINs are examples of which of the following security terms?

A. Access
B. Authorization
C. Identification
D. Authentication

Q 7) What term is used to describe the science of making and breaking secret codes?

A. Jamming
B. Impersonation
C. Spoofing
D. Factorization
E. Cryptography

Q 8) You are using a public key encryption to exchange a message with one of your colleagues. Which key should you use to encrypt your message?

A. Your colleague's private key
B. Your private key
C. Your colleague's public key
D. Your public key

Q 9) What type of cipher encrypts plaintext one byte or one bit at a time?

A. Elliptical
B. Stream
C. Hash
D. Enigma
E. Block

Q 10) What is the most difficult part of designing a cryptosystem?

A. Key management
B. The encryption algorithm
C. Key length
D. Reverse engineering

Q 11) Which of the following technologies could be used to prevent a hacker from launching a dictionary or brute-force attack of a hash?

A. HMAC
B. AES
C. Rainbow tables
D. MD5

Q 12) What name is given to the method that tries all possible password combinations until a match is found?

A. Birthday
B. Cloud
C. Cryptographic
D. Dictionary
E. Brute force
F. Rainbow tables

Q 13) Which of the following is a feature of a cryptographic hash function?

A. The hash input can be calculated given the output value
B. **The hash function has a one-way mathematical function**
C. The output has a variable length
D. Hashing requires a public and private key

Q 14) What asymmetric algorithm provides an electronic key exchange method to share the secret key?

A. Hashing
B. Diffie-Hellman
C. WEP
D. DES
E. RSA

Q 15) Which of the following hashing technologies requires the exchange of keys?

A. Salting
B. HMAC
C. AES
D. MD5

Q 16) What type of access control do smart cards and biometrics provide?

A. Technological
B. Administrative
C. Physical
D. Logical

Q 17) Which 128-bit block cipher encryption algorithm does the U.S. government use to protect classified information?

A. Caesar
B. 3DES
C. Skipjack
D. Vigenere
E. AES

Q 18) Data in which state can be found in NAS and SAN services?

A. Data in storage
B. Encrypted data
C. Data in transit
D. Data in process

Q 19) Which of the following technologies can be used to ensure data confidentiality?

A. Identity management
B. Hashing
C. Encryption
D. RAID

Q 20) You have been asking to implement a data integrity program to protect data files that need to be electronically downloaded by @Apollo employees. You decide to use the strongest hashing algorithm available. Which hash algorithm would you choose?

A. MD5
B. SHA-1
C. AES
D. SHA-256

Q 21) What hashing algorithm is recommended for the protection of sensitive information?

A. SHA-256
B. AES-256
C. 3DES
D. MD5

Q 22) You have been asked to work with fellow @Apollo employees to improve data integrity during initial data entry and data modification operations. Several staff members ask you why the new data entry screens limit the types and size of data that can be entered into specific fields. You explain that this is a data integrity control. What does this mean?

A. Data entry controls which only allow entry staff to view current data
B. A validation rule which has been implemented to ensure completeness, accuracy and consistency of data
C. A limitation rule which has been implemented to prevent unauthorized staff from entering sensitive data
D. Data encryption operations that prevent any unauthorized users from accessing sensitive data

Q 23) What solution should be used to enforce the security policy that a computing device must be updated with the latest antimalware software before it can connect to an organization's network?

A. SAN
B. NAC
C. VPN
D. NAS

Q 24) Which of the following protocols pose threats to network switches? **Select two correct answers**

A. STP
B. IP
C. ICMP
D. RIP
E. WPA2
F. ARP

Q 25) Which of the following protocols would you use to provide security for employees that access an organization's systems remotely from home?

A. SCP
B. WPA
C. SSH
D. Telnet

Q 26) What are the most effective ways to defend against malware? **Select two correct answers**

A. Implement network firewalls
B. Install and update antivirus software
C. Implement a VPN
D. Implement RAID
E. Implement strong passwords
F. Update the operating system and other application software

Q 27) Which type of network poses increasing challenges to cybersecurity specialists due to the growth of BYOD policies?

A. Sneaker net
B. Virtual networks
C. **Wireless networks**
D. Wired networks

Q 28) Which wireless standard made AES and CCM mandatory?

A. WPA2
B. WPA
C. WEP
D. WEP2

Q 29) Which of the following protocols use the Advanced Encryption Standard (AES)? **Select two correct answers**

A. EAP
B. WPA2
C. TKIP
D. WPA
E. WEP

Q 30) The X.509 standard defines which of the following security technologies?

A. Biometrics
B. Strong passwords
C. Security tokens
D. **Digital certificates**

Q 31) @Apollo has just completed a security audit in which your department was cited for not conforming to X.509 requirements. What is the first security control that you need to examine?

A. Hashing operations
B. Data validation rules
C. VPN and encryption services
D. **Digital certificates**

Q 32) What technology should be implemented to verify the identity of an organization to authenticate its website and to provide an encrypted connection between a client and its website?

A. Digital signature
B. Salting
C. Asymmetric encryption
D. **Digital certificate**

Q 33) You have been asked to implement a system that controls what employees can and cannot do on @Apollo's network. ***Which of the following processes should be implemented to meet this requirement?***

A. User login auditing
B. A biometric fingerprint reader
C. Observations to be provided to all employees
D. A set of attributes that describe user access rights

Q 34) Being able to maintain availability during disruptive events describes which of the principles of high availability?

A. Single point of failure
B. Uninterruptible services
C. **System resiliency**
D. Fault tolerance

Q 35) When comparing biometric systems, what is the crossover error rate?

A. The point at which the rate of false negatives and the rate of false positives are the same
B. Where the rate of rejection and the rate of false negatives meet
C. The point at which the rate of acceptability and the rate of false negatives converge
D. The point at which the rate of false positives and the acceptability rate are the same

Q 36) An employee in your organization has installed an unauthorized device on the network to view network traffic. What type of attack is this?

A. Spamming
B. Spoofing
C. Sniffing

D. Phishing

Q 37) Your organization has recently adopted a five nines program for two critical database servers. What type of controls will this involve?

A. Stronger encryption systems
B. Remote access to thousands of external users
C. Limiting access to the data on the systems
D. Improving reliability and uptime of the servers

Q 38) What is an example of a business continuity plan?

A. Identifying critical business processes, resources and relationships between systems by focusing on the consequences of an interruption to critical business functions
B. Getting critical systems to another location while the repair of the original facility is underway
C. Ensuring critical systems are online during a disaster
D. Identifying and analyzing potential events that may negatively impact an organization's assets

Q 39) Which of the following is the simplest exercise to use for training employees and testing an organization's disaster recovery plan?

A. Functional test
B. A simulation
C. Tabletop exercise
D. A full operational exercise

Q 40) Which of the following is considered a natural disaster?

A. Water damage resulting from sprinkler failure
B. A power failure
C. A labor strike
D. **An earthquake**

Q 41) Forensic procedures must be followed exactly to ensure the integrity of data obtained in an investigation. When making copies of data from a machine that is being examined, which of the following should be done to ensure it is an exact duplicate?

A. Open files on the original media and compare them to the copied data
B. Change the attributes of data to make it read-only
C. Perform a cyclic redundancy check using a checksum or hashing algorithm
D. Do nothing — imaging software always makes an accurate image

Q 42) @Apollo wants to adopt a labeling system based on the value, sensitivity and criticality of the information it handles. What element of risk management would you recommend?

A. Asset availability
B. Asset classification
C. Asset identification
D. Asset standardization

Q 43) An organization has installed antimalware. What type of security control is this?

- **A. Recovery control**
- B. Deterrent control
- C. Compensative control
- D. Detective control

Q 44) In which of the following situations would a detective control be warranted?

- A. When an organization cannot use a guard dog and must ∴ consider alternative control options
- **B. When an organization needs to identify prohibited activity**
- C. To restore an organization's system to a normal state after experiencing a breach
- D. When an organization needs to repair damage

Q 45) An organization only installs applications that meet its guidelines, and administrators increase security by eliminating all other applications. What is this called?

- A. Asset identification
- B. Asset availability
- C. **Asset standardization**
- D. Asset classification

Q 46) @Apollo plans to implement security training to educate employees about security policies. What type of security control is the organization trying to implement?

- A. Technological
- B. Physical
- C. Logical
- **D. Administrative**

Q 47) An organization purchases a server for $10,000. There is an exposure factor of 60% and the server experiences a failure every four months. How much should the organization spend per year on a countermeasure to protect the server?

- A. $2,000
- B. $3,000
- C. $4,000
- **D. $6,000**

Q 48) What law was enacted to prevent corporate accounting-related crimes in the U.S.?

- A. Gramm-Leach-Bliley Act
- **B. Sarbanes-Oxley Act**
- C. Import/Export Encryption Act
- D. The Federal Information Security Management Act

Q 49) Which of the following threats are mitigated through user awareness training and through tying security awareness to performance reviews?

- **A. User-related threats**

B. Physical threats
C. Cloud-related threats
D. Device-related threats

Q 50) What national resource was developed as a result of a U.S. Executive Order following a ten-month collaborative study involving over 3,000 security professionals?

A. The National Vulnerability Database
B. NIST Framework
C. ISO OSI model
D. ISO/IEC 27000

** *HTML file → correct answers : "is-correct" or "Correct, not selected"*

9.1.1 Quiz & Answers References

1. Cybersecurity Essentials 1.1 Final Quiz Answers Form B 100% 2018 - ITexam24
2. Cisco – Introduction to CyberSecurity Final Exam Answer 2021 Updated (priyadogra.com)
3. Cybersecurity Essentials 1.1 Final Quiz Answers Form B - ICT Community (examans.com)
4. Cybersecurity Essentials 1.12 Final Exam Answers - InfraExam 2022
5. Cybersecurity Essentials 1.1 Final Quiz Answers 100% 2018 - Premium IT Exam Answers (premiumexam.net)