What is network sniffing?

A. Monitoring and capturing data packets

B. Encrypting network traffic

C. Blocking unauthorized access

D. Routing packets

Answer: A. Monitoring and capturing data packets

Password sniffing is problematic when passwords are transmitted in ____.

A. ciphertext

B. plaintext

C. hashes

D. signatures

Answer: B. plaintext

Which encryption prevents password sniffing?

A. SSL/TLS

B. HTTP

C. FTP

D. Telnet

Answer: A. SSL/TLS

What does a brute-force password attack do?

A. Tries common words

B. Tries all possible permutations

C. Uses precomputed hashes

D. Intercepts passwords

Answer: B. Tries all possible permutations

A dictionary attack uses ____.

A. random characters

B. rainbow tables

C. a precompiled wordlist

D. social engineering

Answer: C. a precompiled wordlist

A hybrid password attack combines ____ and ____.

A. brute-force and dictionary methods

B. hashing and encryption

C. poisoning and spoofing

D. phishing and vishing

Answer: A. brute-force and dictionary methods

What is a rainbow table attack?

A. Using social engineering

B. Using precomputed hashes

C. Capturing network packets

D. Exploiting software bugs

Answer: B. Using precomputed hashes

Which tool is primarily for network sniffing?

A. Wireshark

B. John the Ripper

C. Metasploit

D. Hydra

Answer: A. Wireshark

Which tool is a password cracker?

A. tcpdump

B. Kismet

C. John the Ripper

D. Ettercap

Answer: C. John the Ripper

Client-side attacks often rely on ____.

A. social engineering

B. SQL injection

C. ARP spoofing

D. DHCP spoofing

Answer: A. social engineering

Server-side attacks target ____.

A. user browsers

B. hosting servers

C. mobile devices

D. printers

Answer: B. hosting servers

Spoofing is an attack that ____.

A. encrypts data

B. assumes a false identity

C. deletes files
D. generates random passwords
Answer: B. assumes a false identity

Impersonation is a(n) ____ attack.
A. software-based
B. network-based
C. human-based
D. hardware-based
Answer: C. human-based

Session hijacking exploits ____.
A. inactive sessions
B. active sessions
C. password files
D. network logs
Answer: B. active sessions

ARP spoofing involves redirecting ____ to a wrong MAC address.
A. IP traffic
B. email messages
C. DNS queries
D. DHCP requests
Answer: A. IP traffic

A man-in-the-middle attack ____.
A. blocks communications
B. secretly relays and alters communications
C. encrypts data in transit
D. scans for open ports
Answer: B. secretly relays and alters communications

DNS spoofing modifies a DNS server's ____.
A. firmware
B. routing table
C. cache
D. ACL
Answer: C. cache

DHCP spoofing allows an attacker to ____.
A. steal passwords

B. assign IP addresses
C. encrypt traffic
D. block DHCP servers
Answer: B. assign IP addresses

Which tool can perform session hijacking?
A. Ettercap
B. CookieCatcher
C. Nmap
D. Wireshark
Answer: B. CookieCatcher

Which tool is used for spoofing attacks?
A. Metasploit
B. hping
C. Cain & Abel
D. All of the above
Answer: D. All of the above

A virus requires ____ to replicate.
A. user action
B. self-execution
C. network access
D. root privileges
Answer: A. user action

A worm is ____ replicating.
A. user-initiated
B. self-replicating
C. file-attached
D. scheduled
Answer: B. self-replicating

What type of malware displays unwanted advertisements?
A. Virus
B. Worm
C. Adware
D. Spyware
Answer: C. Adware

Malware that secretly collects data is called ____.

A. Spyware

B. Trojan

C. Rootkit

D. Worm

Answer: A. Spyware

A rootkit controls the system at ____.

A. application level

B. user level

C. lowest levels

D. network level

Answer: C. lowest levels

A logic bomb is triggered by ____.

A. a user click

B. a time or event

C. an update

D. network traffic

Answer: B. a time or event

Ransomware ____.

A. replicates like a worm

B. restricts access and demands ransom

C. displays ads

D. collects keystrokes

Answer: B. restricts access and demands ransom

Malvertisement delivers malicious code via ____.

A. email attachments

B. ads

C. USB drives

D. network shares

Answer: B. ads

Social engineering primarily exploits ____.

A. software vulnerabilities

B. hardware flaws

C. human trust

D. network protocols

Answer: C. human trust

Which technique involves looking over someone's shoulder to get information?

A. Tailgating

B. Piggybacking

C. Shoulder surfing

D. Dumpster diving

Answer: C. Shoulder surfing

Dumpster diving is a social engineering attack that targets ____.

A. live data

B. discarded information

C. network devices

D. Wi-Fi signals

Answer: B. discarded information

Pharming is related to ____.

A. DNS spoofing

B. password cracking

C. packet sniffing

D. malware

Answer: A. DNS spoofing

What is tailgating in security?

A. sniffing network traffic

B. following an authorized person into a restricted area

C. password cracking

D. phishing

Answer: B. following an authorized person into a restricted area

What is phishing?

A. social engineering via email

B. brute-force attack

C. man-in-the-middle

D. spoofing

Answer: A. social engineering via email

Which encryption uses the same key for encryption and decryption?

A. Asymmetric

B. Symmetric

C. Hashing
D. Digital signature
Answer: B. Symmetric

Asymmetric encryption uses ____ keys.
A. one
B. two (public and private)
C. three
D. none
Answer: B. two (public and private)

Hashing transforms data into a ____-length value.
A. variable
B. fixed
C. random
D. zero
Answer: B. fixed

Which technique provides non-repudiation?
A. Symmetric encryption
B. Hashing
C. Digital signature
D. DNS filtering
Answer: C. Digital signature

A digital certificate is used to prove ____.
A. data integrity
B. authenticity of an entity via PKI
C. physical security
D. network availability
Answer: B. authenticity of an entity via PKI

Which access control is enforced through policies and procedures?
A. Technical
B. Physical
C. Administrative
D. Multifactor
Answer: C. Administrative

Preventing unauthorized entry into facilities is an example of ____ access control.
A. Technical

B. Physical
C. Administrative
D. Logical
Answer: B. Physical

Technical access control includes ____.
A. encryption
B. security guards
C. policies
D. building locks
Answer: A. encryption

In "AAA," what does the first "A" stand for?
A. Authentication
B. Authorization
C. Accounting
D. Availability
Answer: A. Authentication

In "AAA," what does the second "A" stand for?
A. Authentication
B. Authorization
C. Access control
D. Accounting
Answer: B. Authorization

In "AAA," what does the third "A" stand for?
A. Availability
B. Access
C. Accounting
D. Administration
Answer: C. Accounting

Passwordless authentication means ____.
A. using multiple passwords
B. signing in without a password
C. using a PIN
D. hashing passwords
Answer: B. signing in without a password

Which encryption ensures confidentiality only?

A. Hashing

B. Symmetric encryption

C. Digital signature

D. DNS spoofing

Answer: B. Symmetric encryption

Which technique ensures data integrity?

A. Hashing

B. Asymmetric encryption

C. Administrative control

D. Physical access control

Answer: A. Hashing

Digital signatures are created using the sender's ____ key.

A. public

B. private

C. symmetric

D. hashing

Answer: B. private

Public Key Infrastructure (PKI) manages ____.

A. passwords

B. digital certificates and keys

C. network devices

D. user accounts

Answer: B. digital certificates and keys