Name: _______________ Date: _______________

Operation Ghost Protocol: 8th Grade Cybersecurity Maneuvers

Deconstruct sophisticated digital threats and architect defensive strategies against advanced persistence and social engineering tactics.

---

1. An attacker uses a highly targeted email containing specific details about a school’s upcoming field trip to trick the principal into clicking a malicious link. This specialized attack is known as:

A. Adware injection
B. Spear phishing
C. DDoS saturation
D. Logic bomb

2. Using 'Zero Trust' architecture means that a system assumes every user or device attempting to access its resources is a potential threat, even if they were previously verified.

A. True
B. False

3. To secure communications across an untrusted public network, a _______ creates an encrypted tunnel that masks your IP address and protects your data from 'man-in-the-middle' attacks.

A. Virtual Desktop Interface (VDI)
B. Hypertext Transfer Protocol (HTTP)
C. Virtual Private Network (VPN)
D. Domain Name System (DNS)

4. Evaluate which of the following scenarios describes a 'Man-in-the-Middle' (MitM) attack.

A. An attacker floods a server with traffic until it crashes.
B. A hacker guesses a user's password using a list of common words.
C. A malicious actor intercepts and alters communication between two parties who believe they are talking directly to each other.
D. A user installs a program that records every keystroke they make.

5. Security professionals use _______, which involves authorized simulated attacks on a computer system to look for exploitable vulnerabilities before real hackers find them.

A. Crypto-mining
B. Penetration testing
C. Data scrubbing
D. Beta debugging

6. Biometric authentication, such as facial recognition or fingerprint scanning, is considered more secure than a password because physical traits can never be spoofed or bypassed.

A. True

B. False

7. A developer leaves a secret entry point in their software code to allow themselves easy access for maintenance, but it is later discovered by a cybercriminal. This is called a:

A. Trojan Horse
B. Sandbox
C. Backdoor
D. Firewall

8. The process of converting readable 'plaintext' into unreadable 'ciphertext' using a mathematical algorithm is known as _______.

A. Compression
B. Archiving
C. Formatting
D. Encryption

9. A 'Zero-Day Vulnerability' refers to a security hole in software that is unknown to the vendor and for which no patch or fix yet exists.

A. True
B. False

10. When analyzing the safety of an IoT (Internet of Things) device like a smart thermostat, which factor presents the highest security risk to a home network?

A. The device uses too much electricity.
B. Hardcoded default passwords that cannot be changed by the user.
C. The device connects via Bluetooth and Wi-Fi simultaneously.
D. The device requires a smartphone app for initial setup.