**Name:** _______________ **Date:** _______________

# Answer Key: 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:

**Answer:** B) Spear phishing

Spear phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, using personalized details to increase legitimacy.

### 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.

**Answer:** A) True

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated.

### 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.

**Answer:** C) Virtual Private Network (VPN)

A VPN (Virtual Private Network) provides privacy and anonymity by creating a private network from a public internet connection, making your online actions virtually untraceable.

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

**Answer:** C) A malicious actor intercepts and alters communication between two parties who believe they are talking directly to each other.

MitM attacks involve an perpetrator positioning themselves in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties.

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

**Answer:** B) Penetration testing

Penetration testing (or pen testing) is a proactive security measure used to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

**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.**

**Answer:** B) False

While biometrics are strong, they are not infallible; high-resolution photos or 3D models can sometimes bypass facial recognition, and biometric data cannot be 'changed' if the database is leaked.

**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:**

**Answer:** C) Backdoor

A backdoor is a method of bypassing normal authentication in a cryptosystem or algorithm, often created for legitimate troubleshooting but dangerous if exploited.

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

**Answer:** D) Encryption

Encryption is the primary method used to protect data confidentiality, ensuring that even if data is intercepted, it cannot be read without the decryption key.

**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.**

**Answer:** A) True

Zero-day means the developers have had 'zero days' to fix the problem since it was discovered, making it a high-risk window for cyberattacks.

**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?**

**Answer:** B) Hardcoded default passwords that cannot be changed by the user.

**Name:** ________________ **Date:** ________________

Hardcoded default passwords are a massive risk because they are often publicly available online, allowing attackers to easily compromise thousands of devices at once.