Worksheet 4: Cybersecurity - Solutions

Section A: Multiple Choice (10 Marks)

Question 1:

What is the main goal of cyber security?

✅ **Answer: b) Protecting systems from digital attacks**

🔹 **Explanation:** Cyber security focuses on safeguarding computers, networks, and data from unauthorized access, cyberattacks (e.g., hacking, malware), and data breaches.

Question 2:

Which attack involves trying every possible password combination?

✅ **Answer: b) Brute-force**

🔹 **Explanation:** A brute-force attack systematically tries all possible password combinations until the correct one is found. Hackers use automated tools to speed up the process.

Question 3:

A Trojan horse malware:

✅ **Answer: b) Requires user execution to activate**

🔹 **Explanation:** Unlike viruses or worms, a Trojan disguises itself as legitimate software (e.g., a game or app) and only activates when the user runs it.

Question 4:

What does "https://" indicate in a URL?

✅ **Answer: b) Data is encrypted (SSL/TLS)**

🔹 **Explanation:** HTTPS (HyperText Transfer Protocol Secure) ensures data transmitted between the user and website is encrypted, preventing interception.

Question 5:

Which tool prevents unauthorized network access?

✅ **Answer: b) Firewall**

🔹 **Explanation:** A firewall monitors incoming/outgoing traffic and blocks unauthorized access based on predefined security rules.

Question 6:

Two-factor authentication (2FA) combines:

✅ **Answer: b) Password + biometrics/OTP**

🔹 **Explanation:** 2FA requires two verification methods (e.g., a password + fingerprint or a one-time SMS code).

Question 7:

DNS cache poisoning is used in:

✅ **Answer: a) Pharming**

🔹 **Explanation:** Pharming redirects users to fake websites by corrupting DNS records (e.g., typing "bank.com" leads to a hacker's site).

Question 8:

Ransomware typically:

✅ **Answer: b) Encrypts files for ransom**

🔹 **Explanation:** Ransomware locks files until a ransom is paid (e.g., WannaCry attack).

Question 9:

A proxy server enhances security by:

✅ **Answer: a) Hiding the user's IP address**

🔹 **Explanation:** Proxy servers act as intermediaries, masking the user's real IP and filtering malicious traffic.

Question 10:

Which is a biometric authentication method?

✅ **Answer: b) Fingerprint scanning**

🔹 **Explanation:** Biometrics use unique physical traits (e.g., fingerprints, facial recognition) for identity verification.

Section B: Short Answer (15 Marks)

Question 11:

Define *phishing* and give one example.

✅ **Answer:**

- **Phishing:** A cyberattack where hackers impersonate trusted entities (e.g., banks) via fake emails/websites to steal sensitive data.

- **Example:** An email pretending to be from "Netflix" asking you to "update payment details" via a malicious link.

Question 12:

Explain how a DDoS attack overwhelms a server.

✅ **Answer:**

A DDoS (Distributed Denial of Service) attack floods a target server with excessive traffic from multiple compromised devices (e.g., botnets). The server becomes overloaded, slowing down or crashing, making it unavailable to legitimate users.

Question 13:

List two differences between viruses and worms.

✅ **Answer:**

Virus	Worm
Requires a host program to execute.	Self-replicates without user action.
Spreads via infected files (e.g., email attachments).	Spreads through network vulnerabilities.

Question 14:

Why are automatic software updates important for security?

✅ **Answer:**

- **Patches vulnerabilities:** Updates fix security flaws hackers exploit (e.g., zero-day bugs).
- **Improves stability:** Fixes bugs that could cause crashes or data loss.
- **Adds security features:** New protections against emerging threats.

Question 15:

Describe one way to detect a fake website.

✅ **Answer:**

1. **Check the URL:**
   - Legitimate: https://www.amazon.com
   - Fake: https://www.amaz0n-login.com (misspelled).
2. **Look for HTTPS & padlock icon** (no lock = unsafe).

3. **Verify domain ownership** (e.g., click the padlock to see SSL certificate details).

Section C: Long Answer (15 Marks)

Question 16:

Case Study: A bank's customers received emails asking for password resets.

✅ **Part (a): Identify the attack type and two prevention methods.**

- **Attack Type: Phishing** (social engineering attack).
- **Prevention:**
    1. **Customer Education:** Teach users to spot phishing emails (e.g., check sender address, avoid clicking links).
    2. **Email Filters:** Use spam filters to block suspicious emails.

✅ **Part (b): Explain how SSL/TLS protects the bank's website.**

- **Encryption:** SSL/TLS scrambles data (e.g., login details) so hackers can't read it.
- **Authentication:** Verifies the website's identity (prevents fake sites).
- **Integrity:** Ensures data isn't altered during transmission.

Question 17:

Compare role-based access control (RBAC) and biometric authentication.

✅ **Answer:**

RBAC	Biometric Authentication
Grants permissions based on job roles (e.g., admin, intern).	Uses unique biological traits (e.g., fingerprints).
Pros: Easy to manage for large organizations.	**Pros:** Hard to fake; no passwords needed.
Cons: Risk of role misuse (e.g., insider threats).	**Cons:** Privacy concerns; hardware costs.