AP CYBERSECURITY • EXERCISE SHEET

1.3 Best Practices for Public Networks

Name: _____ Class: _____ Date: _____ **Total: 11 marks**

Objective

Build the skills to answer exam questions on adversary types and **wireless attacks** 无线攻击 on public networks.

You must be able to:

- classify adversaries by skill and **motivation** 动机
- describe wireless attacks: **evil twin** 双胞胎恶意热点, jamming, war driving
- recommend protections: verify the SSID, prefer HTTPS, use a **VPN** 虚拟专用网络

1 Worked examples

Study these first. Each one shows the method for a task used later.

> ■ **Wireless attacks**
>
> An evil twin copies the real network name (SSID) so victims connect to the attacker's access point. Jamming floods the air with a signal to block access (a denial of service). War driving detects networks and where their signal leaks.
>
> ■ **Encryption still protects you**
>
> On an evil twin, the adversary can read unencrypted traffic - but HTTPS sites stay encrypted, so your login is safe even on a fake access point.

2 Practice

2.1 Describe an **evil twin** attack in one or two sentences. [2]

2.2 State two things a user can do to stay safe on public Wi-Fi. [2]

2.3 An attacker floods an area with a strong radio signal so no one can connect.

(a) Name this attack. [1]

(b) State the broader category of attack it belongs to. [1]

3 Exam-style questions

3.1 An adversary who buys ready-made tools online and reuses known exploits is best described as [1]

- **A** a highly skilled attacker
- **B** a low-skilled attacker
- **C** a security analyst
- **D** a system administrator

3.2 On an evil-twin network, which of your activities stays protected? [1]

- **A** visiting an HTTP site
- **B** visiting an HTTPS site
- **C** sending an unencrypted email
- **D** browsing over plain DNS

3.3 A café's Wi-Fi signal reaches the car park outside.

(a) Explain why this is a security concern. [2]

(b) State one control that reduces this exposure. [1]

4 Go further

- work through the **1.3 Best Practices for Public Networks** lesson on the **Learn** page;
- read the **Introduction to Security** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 the adversary sets up a fake access point with an SSID copied from the real network, so victims connect to it and their traffic can be read.

2.2 any two of: verify the exact network name; prefer HTTPS sites; use a VPN.

2.3 (a) jamming. (b) denial of service / DoS.

3.1 B. reusing others' tools indicates low skill.

3.2 B. HTTPS encryption protects data even if traffic is intercepted.

3.3 (a) an attacker outside can detect and probe the network without entering the building. (b) control the signal strength so it stops at the walls.