Exercise walk-through

Best Practices for Public Networks ▪ 1.3

eXercise

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

Method — 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.

Method — 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.

Practice 2.1 ▪ 2 marks

Describe an **evil twin** attack in one or two sentences.

Solution 2.1

Worked steps

the adversary sets up a fake access point B1 with an SSID copied from the real network, so victims connect to it and their traffic can be read B1.

Practice 2.2 ▪ 2 marks

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

Solution 2.2

Method: Encryption still protects you

Worked steps

any two of: verify the exact network name B1; prefer HTTPS sites; use a VPN B1.

Practice 2.3 ▪ 1 mark

An attacker floods an area with a strong radio signal so no one can connect.
(a) Name this attack.
(b) State the broader category of attack it belongs to.

Solution 2.3

Method: Wireless attacks

Worked steps

(a) jamming B1. (b) denial of service / DoS B1.

Exam-style 3.1 ▪ 1 mark

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

A a highly skilled attacker

B a low-skilled attacker

C a security analyst

D a system administrator

Solution 3.1

A a highly skilled attacker

B a low-skilled attacker ✓

C a security analyst

D a system administrator

Worked steps

B. reusing others' tools indicates low skill.

Exam-style 3.2 ▪ 1 mark

On an evil-twin network, which of your activities stays protected?

A visiting an HTTP site

B visiting an HTTPS site

C sending an unencrypted email

D browsing over plain DNS

Solution 3.2

Method: Wireless attacks

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

Worked steps

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

Exam-style 3.3 ▪ 2 marks

A café's Wi-Fi signal reaches the car park outside.
(a) Explain why this is a security concern.
(b) State one control that reduces this exposure.

Solution 3.3

Worked steps

(a) an attacker outside can detect and probe the network B1 without entering the building B1. (b) control the signal strength so it stops at the walls B1.