

Exercise walk-through

1.3

Best Practices for Public Networks

AP Cybersecurity

Know your adversary

Adversaries differ by *skill*:

Low-skilled – buy ready-made tools, reuse known **exploits**

High-skilled – write their own tools, find brand-new **zero days**

Their **motivation** varies too: greed, revenge, politics, or belief.

When ranking risks: high risk = high impact AND easy to exploit. A parking-lot Wi-Fi leak matters less than an open internal port.

Identify the wireless mechanism

A school investigates three separate incidents. Choose the attack and cite the fact that supports your answer.

- A An unauthorised access point copies the school's network name. Students connect to it, and an adversary captures their traffic.
- B An adversary's transmitter emits a strong signal on the wireless network's frequency. Legitimate devices cannot communicate with the access point.
- C An adversary drives around the building recording network beacons and the locations where the signal reaches outside. No connection is made.

Which case imitates an identity, which denies access, and which gathers information?

Explain what the adversary is doing

A: Evil twin . The fake **access point** copies the real **SSID** to attract connections. Capturing traffic is the aim; copying a name does not make the device trustworthy.

B: Jamming . Radio interference prevents legitimate wireless communication: a **denial of service** . The evidence is the interfering transmitter, not an outage alone.

C: War driving . The adversary maps wireless beacons and signal reach. Joining the network is not required. An authorised wireless survey can use similar observations; purpose and permission matter.

Does the right network name prove safety?

Two access points display the same school SSID. One is school-owned; the other belongs to an adversary. A student says:

“The name matches, so I know this is the school’s network. If I use HTTPS, nothing can go wrong.”

Identify the two overclaims. Explain what encrypted HTTPS protects, and name a separate step for checking which network to join.

Separate identity, content and access

A matching name is a check, not proof. An evil twin can copy it. Use the school's trusted connection instructions and confirm uncertainties with staff through a separate trusted channel.

Valid encrypted HTTPS protects content in transit. Capturing that traffic does not reveal its plaintext. It does not establish ownership of the hotspot or guarantee that every destination is trustworthy.

A fake network can still interfere with access or direct users toward a phishing site. Read the scenario: identify what is protected and what risk remains.

Exercises 2.1-2.2

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]

Exercises 2.1-2.2

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

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

2.2

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

Exercise 2.3 (a)

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

(a) Name this attack.

[1]

Exercise 2.3 (a)

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

(a) Name this attack.

[1]

(a)

- jamming

Exercise 2.3 (b)

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

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

[1]

Exercise 2.3 (b)

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

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

(b)

- denial of service / DoS

Exercises 3.1-3.2

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

Exercises 3.1-3.2

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

3.1 B

- reusing others' tools indicates low skill

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

3.2 B

- HTTPS encryption protects data even if traffic is intercepted

Exercise 3.3 (a)

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

(a) Explain why this is a security concern.

[2]

Exercise 3.3 (a)

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

(a) Explain why this is a security concern.

[2]

(a)

- an attacker outside can detect and probe the network without entering the building

Exercise 3.3 (b)

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

(b) State one control that reduces this exposure.

[1]

Exercise 3.3 (b)

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

(b) State one control that reduces this exposure.

[1]

(b)

- control the signal strength so it stops at the walls