

Exercise walk-through

1.2

Suspicious Website Logins

AP Cybersecurity

Password attacks – the warning signs

In an **online password attack** the adversary tries passwords against a **real** login page. The logs show it:

- many **failed** logins in a short time
- attempts at **unusual** hours
- attempts from **unknown** devices

Adversaries succeed because people choose **weak** passwords: a word + a two-digit year + a symbol (Summer24!), or a pet's name.

Those patterns are so common that a **dictionary** of likely passwords can be built from facts about you and tried automatically.

Suspicious Website Logins

A **password attack** is any attempt to log in using guessed or stolen passwords.

- many failed logins in a short time,
- login attempts at unusual hours,
- login attempts from unknown devices.
- Create passwords that are **long, random, and unique** - a **password manager** can generate and store them for you.

Unit 1 – key takeaways

1**Name the tactic**

urgency, consensus, intimidation –
not just “suspicious”

2**Authentication**

long, unique, from a manager –
plus MFA

3**Evil twin**

a copied SSID; HTTPS still
cannot be read

4**AI is dual-use**

the same tool attacks and defends
– which side is asked?

Exercises 2.1-2.3

2.1 State two signs, visible in a log, of an online password attack. [2]

2.2 Explain why a password like Summer2024! is weak. [2]

2.3 State two ways to make authentication stronger. [2]

Exercises 2.1-2.3

2.1 State two signs, visible in a log, of an online password attack. [2]

2.1

- any two of: many failed logins in a short time; logins at unusual hours; logins from unknown devices

2.2 Explain why a password like Summer2024! is weak. [2]

2.2

- it follows a common pattern - word + year + symbol - that an adversary's dictionary of guesses expects

2.3 State two ways to make authentication stronger. [2]

2.3

- any two of: use long/random/unique passwords; use a password manager; enable MFA

Exercises 3.1-3.2

3.1 Which log pattern most strongly suggests an online password attack?

[1]

☐

A one successful login

B many failed logins in a short time

C a file download

D a printer coming online

3.2 Which is the strongest password?

[1]

☐

A your dog's name

B P@ssword!

C a 16-character random string

D your birthday

Exercises 3.1-3.2

3.1 Which log pattern most strongly suggests an online password attack?

[1]

☐

A one successful login

B many failed logins in a short time

C a file download

D a printer coming online

3.1 B

- a burst of failed logins signals guessing

3.2 Which is the strongest password?

[1]

☐

A your dog's name

B P@ssword!

C a 16-character random string

D your birthday

3.2 C

- long + random + unique beats any pattern

Exercise 3.3 (a)

3.3 A company wants to reduce account takeovers.

(a) Name one authentication improvement they could require.

[1]

Exercise 3.3 (a)

3.3 A company wants to reduce account takeovers.

(a) Name one authentication improvement they could require.

[1]

(a)

- multifactor authentication / MFA

Exercise 3.3 (b)

3.3 A company wants to reduce account takeovers.

(b) Explain how it helps even if a password is stolen.

[2]

Exercise 3.3 (b)

3.3 A company wants to reduce account takeovers.

(b) Explain how it helps even if a password is stolen.

[2]

(b)

- MFA needs a second factor, so a stolen password alone cannot log in

Exercise 3.4

3.4 A fictional account has 15 failed logins and then one successful login from a new device. Give one suspicious feature, one legitimate alternative explanation, one additional evidence check and one authentication improvement. [4]

Exercise 3.4

3.4 A fictional account has 15 failed logins and then one successful login from a new device. Give one suspicious feature, one legitimate alternative explanation, one additional evidence check and one authentication improvement. [4]

3.4

Many failures or a new-device success is suspicious; a plausible alternative, such as genuine password mistakes followed by recovery, is stated; compare records or confirm with the owner through an established channel; use a long unique password and/or an independent second factor with an explanation of the risk reduced.