Exercise walk-through

Detecting Attacks on Devices ▪ 4.4

eXercise

You must be able to

- define an IoC and name host-, file-, and behaviour-based IoCs
- read auth logs to tell guessing, spraying, and stuffing apart
- explain why offline password attacks cannot be detected

Method — Reading auth logs

One user with many wrong passwords = a guessing attack. Many users failing from one IP = password spraying. A burst of default credentials = credential stuffing.

Method — Offline attacks

Offline password attacks cannot be detected because the adversary already stole the hash database and is cracking it on their own computer, far from your logs.

Practice 2.1 ▪ 2 marks

Define an **indicator of compromise (IoC)**.

Solution 2.1

Worked steps

evidence in logs or files B1 that an adversary has compromised a device or network B1.

Practice 2.2 ▪ 2 marks

A log shows 50 failed logins for user ‘admin’ from one IP in 30 seconds. What does this indicate?

Solution 2.2

Worked steps

an online password-guessing attack on one account B1; many wrong passwords fast for one user is the signature B1.

Practice 2.3 ▪ 2 marks

Explain why offline password attacks cannot be detected.

Solution 2.3

Method: Offline attacks

Worked steps

the cracking happens on the adversary's own computer B1, away from the victim's systems and logs B1.

Exam-style 3.1 ▪ 1 mark

Many different users failing to log in from ONE IP address suggests

A credential stuffing

B password spraying

C salting

D patching

Solution 3.1

Method: Reading auth logs

A credential stuffing

B password spraying ✓

C salting

D patching

Worked steps

B. one IP, many users = password spraying.

Exam-style 3.2 ▪ 1 mark

A file whose hash matches known malware is an example of a

A host-based IoC

B file-based IoC

C behaviour-based IoC

D network segment

Solution 3.2

A host-based IoC

B file-based IoC ✓

C behaviour-based IoC

D network segment

Worked steps

B. matching a known-malware hash is a file-based IoC.

Exam-style 3.3 ▪ 1 mark

An analyst reviews authentication logs after an alert.
(a) State one pattern that would indicate credential stuffing.
(b) State one pattern that would indicate a single-account guessing attack.

Solution 3.3

Method: Reading auth logs

Worked steps

(a) a burst of default username:password pairs tried in quick succession B1. (b) many wrong passwords for one user account B1.