Exercise walk-through

Detecting Network Attacks ▪ 3.5

eXercise

You must be able to

- distinguish a NIDS (alerts) from a NIPS (blocks) and a SIEM
- compare signature-based and anomaly-based detection
- state the trade-offs (speed, cost, false alarms, novel attacks)

Method — IDS vs IPS

An intrusion detection system (NIDS) only alerts - a human must act. An intrusion prevention system (NIPS) can also block the attack itself. A SIEM correlates data from many sources to spot patterns.

Method — Signature vs anomaly

Signature-based matches known attack signatures - fast, few false alarms, but blind to new attacks. Anomaly-based compares to a normal baseline - catches novel attacks but costs more and raises more false alarms.

Practice 2.1 ▪ 2 marks

State the difference between a NIDS and a NIPS.

Solution 2.1

Method: IDS vs IPS

Worked steps

a NIDS detects and alerts only B1; a NIPS can also block/stop the attack B1.

Practice 2.2 ▪ 2 marks

Give one advantage and one disadvantage of signature-based detection.

Solution 2.2

Method: Signature vs anomaly

Worked steps

advantage: fast, few false positives B1; disadvantage: cannot catch brand-new attacks B1.

Practice 2.3 ▪ 2 marks

Why does anomaly-based detection need a recorded baseline?

Solution 2.3

Method: Signature vs anomaly

Worked steps

it flags traffic that deviates from normal B1, so it must first know what normal looks like B1.

Exam-style 3.1 ▪ 1 mark

Which detection method is most likely to catch a brand-new attack?

A signature-based

B anomaly-based

C no detection

D a firewall log

Solution 3.1

Method: IDS vs IPS

A signature-based

B anomaly-based ✓

C no detection

D a firewall log

Worked steps

B. anomaly-based flags the unusual; signatures miss the new.

Exam-style 3.2 ▪ 1 mark

Which system detects an attack and alerts staff but does NOT block it?

A NIPS

B NIDS

C VPN

D UPS

Solution 3.2

Method: IDS vs IPS

A NIPS

B NIDS ✓

C VPN

D UPS

Worked steps

B. a NIDS alerts only; a NIPS can block.

Exam-style 3.3 ▪ 1 mark

A manufacturing plant deploys a signature-based network detection system.
(a) State one potential drawback compared with anomaly-based detection.
(b) Explain why this drawback occurs.

Solution 3.3

Method: Signature vs anomaly

Worked steps

(a) more false negatives / misses new attacks B1. (b) signature-based needs a known signature B1, so an attack with no signature yet slips through B1.