Exercise walk-through

Network Vulnerabilities and Attacks ▪ 3.1

eXercise

You must be able to

- identify a network attack from its evidence in a log
- explain an **on-path (man-in-the-middle) 中间人** attack
- distinguish a DoS from a DDoS

Method — Reading the trace

ARP poisoning shows one IP with two MAC addresses. MAC flooding shows a switch overwhelmed with new MACs. DNS poisoning redirects the real URL to a fake site. A smurf attack floods the broadcast address with ICMP.

Method — On-path attacks

In an on-path (man-in-the-middle) attack, both parties think they talk directly to each other but actually each talks to the adversary, who silently reads or alters every message.

Practice 2.1 ▪ 2 marks

A log shows IP 192.168.1.13 mapped to two different MAC addresses. Name the likely attack.

Solution 2.1

Method: Reading the trace

Worked steps

ARP poisoning B1; a duplicate MAC for one IP is its signature B1.

Practice 2.2 ▪ 2 marks

Explain what happens in an **on-path (man-in-the-middle)** attack.

Solution 2.2

Method: On-path attacks

Worked steps

the adversary secretly sits between two parties B1 and reads or alters their traffic while both think they communicate directly B1.

Practice 2.3 ▪ 1 mark

Many compromised machines flood a target website with traffic at once.
(a) Name this attack.
(b) How does it differ from a plain DoS?

Solution 2.3

Worked steps

(a) DDoS / distributed denial of service B1. (b) a DDoS uses many machines at once, not one B1.

Exam-style 3.1 ▪ 1 mark

A switch flooded with fake MAC addresses so it broadcasts all traffic is under a

A DNS poisoning attack

B MAC flooding attack

C smurf attack

D buffer overflow

Solution 3.1

Method: Reading the trace

A DNS poisoning attack

B MAC flooding attack ✓

C smurf attack

D buffer overflow

Worked steps

B. flooding the MAC table is MAC flooding.

Exam-style 3.2 ▪ 1 mark

An unauthorised access point plugged into an open port is a

A screened subnet

B rogue access point

C honeypot

D baseline

Solution 3.2

A screened subnet

B rogue access point ✓

C honeypot

D baseline

Worked steps

B. a rogue access point bypasses the firewall.

Exam-style 3.3 ▪ 1 mark

Users typing the correct bank URL are sent to a fake login page.
(a) Name the likely attack.
(b) State what the attacker is trying to steal.

Solution 3.3

Method: Reading the trace

Worked steps

(a) DNS poisoning B1. (b) login credentials (credential harvesting) B1.