AP CYBERSECURITY • EXERCISE SHEET

3.1 Network Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

Objective

Build the skills to answer exam questions on network attacks like **ARP poisoning** 地址解析投毒, **MAC flooding** 物理地址泛洪, and **DoS** 拒绝服务.

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

1 Worked examples

Study these first. Each one shows the method for a task used later.

> ■ **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.
>
> ■ **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.

2 Practice

2.1 A log shows IP 192.168.1.13 mapped to two different MAC addresses. Name the likely attack. [2]

2.2 Explain what happens in an **on-path (man-in-the-middle)** attack. [2]

2.3 Many compromised machines flood a target website with traffic at once.

(a) Name this attack. [1]

(b) How does it differ from a plain DoS? [1]

3 Exam-style questions

3.1 A switch flooded with fake MAC addresses so it broadcasts all traffic is under a [1]

- **A** DNS poisoning attack
- **B** MAC flooding attack
- **C** smurf attack
- **D** buffer overflow

3.2 An unauthorised access point plugged into an open port is a [1]

- **A** screened subnet
- **B** rogue access point
- **C** honeypot
- **D** baseline

3.3 Users typing the correct bank URL are sent to a fake login page.

(a) Name the likely attack. [1]

(b) State what the attacker is trying to steal. [1]

4 Go further

- work through the **3.1 Network Vulnerabilities and Attacks** lesson on the **Learn** page;
- read the **Securing Networks** section of the AP Cybersecurity handout on the **Know** page.

Solutions

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

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

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

3.1 B. flooding the MAC table is MAC flooding.

3.2 B. a rogue access point bypasses the firewall.

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