AP CYBERSECURITY • EXERCISE SHEET

3.1 Network Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 53 marks**

KEY WORDS arp 地址解析协议 • switch 交换机 • arp poisoning 地址解析投毒 • dns poisoning 域名投毒 • mac flooding 物理地址泛洪

Objective

Build the skills to answer exam questions on common **network attacks** 网络攻击, how network vulnerabilities are exploited, and rating network risk.

You must be able to:

- explain what **ARP** 地址解析协议 does and how ARP poisoning abuses it
- describe MAC flooding, DNS poisoning and the smurf attack, and say what each achieves
- explain how an adversary exploits open ports, unsecured wireless and unauthenticated networks
- explain what a **vulnerability scanner** 漏洞扫描器 produces and how skill affects likelihood
- rate a network risk high, moderate or low and justify it

1 Worked examples

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

■ ARP, and the attack that abuses it

The **address resolution protocol** is used by a default gateway to build a table pairing **IP addresses with MAC addresses**, so traffic for an IP can be delivered to the right physical device.

ARP has no authentication - a device is believed when it claims an address. **ARP poisoning** plants false pairings so traffic destined for a legitimate device is delivered to the adversary instead, who can then read, alter or drop it.

■ The four named network attacks

Attack	What the adversary does	What it achieves
ARP poisoning	plants false IP-to-MAC pairings	traffic is misdelivered to the adversary
MAC flooding	sends the switch many Ethernet frames, each with a **different** MAC address	overwhelms the switch's table, forcing it to **broadcast** - so the adversary sees traffic meant for others
DNS poisoning	pretends to be an authoritative name server and plants a **fake DNS record**	users are sent to the adversary's server while typing the correct address
Smurf	floods the network with **ICMP** requests	a **denial of service** - the network cannot serve legitimate users

Two of these steal traffic (ARP poisoning, MAC flooding), one redirects users (DNS poisoning), and one denies service (smurf). Naming which of the three effects a scenario shows is usually the first mark.

■ How networks are actually entered

- **Malicious traffic** can flood a network (DoS), **map** its internal structure, or **spoof** a legitimate device.
- **A compromised device** is used to reach other devices on the same **LAN** - lateral movement.
- **A physical data port** without **port security** enabled gives an adversary who plugs in direct LAN access.
- **Wireless signals broadcasting beyond the building** can be picked up from outside a physically secure space.
- **Networks that do not authenticate devices and users** are easy to join, and an adversary inside the network attacks from within.
- **An open network port** can have a wireless access point plugged into it, creating a **rogue access point**.
- **Weak wireless encryption** can be broken, allowing interception.

■ Assessing network risk

Network vulnerabilities let an adversary intercept and alter data in transit, launch a DoS, or move laterally to reach more of the network.

Automated vulnerability scanners check networks, devices and applications for **known** vulnerabilities and produce a report - usually with a severity rating for each finding.

The likelihood factor specific to networks: **exploiting a network vulnerability often requires advanced technical ability**, so a serious flaw that only a highly skilled adversary can use may still be less likely to be exploited than a trivial one.

Rating	When
High	an adversary can **easily** have significant impact - capturing traffic, spoofing a legitimate device
Moderate	could give an adversary **information** about systems or devices on the network
Low	difficult to exploit, and minimal negative impact

Notice the word **easily** in the high row: severity alone does not make a risk high - the ease of exploitation is part of the definition.

2 Practice

2.1 State what ARP does on a network. [2]

2.2 Explain how an ARP poisoning attack lets an adversary read traffic they were never sent. [2]

2.3 Explain how MAC flooding causes a switch to reveal traffic. [3]

2.4 Name the attack in each case.

(a) Users typing the correct web address arrive at the adversary's server. [1]

(b) The network is flooded with ICMP requests and stops responding. [1]

(c) The switch's address table is overwhelmed by frames with many different MAC addresses. [1]

2.5 State the category of harm - interception, redirection or denial of service - for each of ARP poisoning, DNS poisoning and a smurf attack. [3]

2.6 Explain how each of these gives an adversary access to a LAN.

(a) A data port in a public reception area with no port security. [2]

(b) A wireless access point whose signal reaches the car park. [2]

(c) An open network port in an unused office. [2]

2.7 State **three** things an adversary can do by sending malicious traffic into a network. [3]

2.8 Explain what an automated vulnerability scanner produces and one limitation of relying on it. [3]

2.9 Rate each risk and justify.

(a) Wireless encryption that a highly skilled adversary could break after sustained effort, on a network carrying payroll data. [2]

(b) A misconfiguration that reveals the model numbers of devices on the network. [2]

(c) An unsecured data port in a locked server room used only by two administrators. [2]

3 Exam-style questions

3.1 ARP pairs [1]

- **A** domain names with IP addresses
- **B** IP addresses with MAC addresses
- **C** MAC addresses with switch ports
- **D** usernames with devices

3.2 A smurf attack is a type of [1]

- **A** interception attack
- **B** denial of service attack
- **C** privilege escalation
- **D** social engineering

3.3 MAC flooding works by [1]

- **A** planting a fake DNS record
- **B** forcing the switch to broadcast by overwhelming its address table
- **C** breaking the wireless encryption key
- **D** plugging a rogue access point into an open port

3.4 A network vulnerability that would give an adversary information about devices on the network, but no direct access, is best rated [1]

- **A** high
- **B** moderate
- **C** low
- **D** it cannot be rated without a scan

3.5 A community sports centre has a single flat network. Its reception desk has a wall data port that visitors can reach; port security is not enabled. The Wi-Fi has no device authentication and its signal is strong in the adjacent car park. A vulnerability scan reports weak wireless encryption and an unused open port in a store room. The centre's network carries membership records including bank details, and the till system.

(a) Identify **three** ways an adversary could join this network, and state which is easiest. [4]

(b) Explain what an adversary could do with the open port in the store room, naming the resulting attack. [3]

(c) Having joined the network, describe **two** attacks the adversary could run and the harm each causes. [4]

(d) The manager says the scan report "lists everything, so we are covered". Evaluate this, referring to what a scanner can and cannot find. [3]

(e) Rate the overall network risk, justifying against the criteria, and recommend the **two** changes you would make first. [4]

Solutions

2.1 ARP is used by the default gateway to build a table pairing IP addresses with MAC addresses, so traffic addressed to an IP reaches the correct physical device.

2.2 ARP has no authentication, so a false pairing of the adversary's MAC with a legitimate IP is accepted; traffic intended for that device is then delivered to the adversary, who can read, alter or drop it.

2.3 the adversary sends the switch many Ethernet frames, each carrying a different MAC address; this overwhelms the switch's address table, forcing it into broadcast mode so every frame goes to every port - including the adversary's.

2.4 (a) DNS poisoning. (b) smurf attack. (c) MAC flooding.

2.5 ARP poisoning - interception; DNS poisoning - redirection; smurf - denial of service.

2.6 (a) an adversary plugs directly into the port and, without port security, the switch accepts the device onto the LAN, giving them a position inside the network from which to launch further attacks. (b) the signal broadcasts beyond the physically secure space, so the adversary can pick up signals and beacon frames from outside the building and attempt to join or to break the encryption without ever entering. (c) an adversary can plug a wireless access point into it, creating a **rogue access point**, which gives them - and anyone else in range - wireless access to the internal network.

2.7 any three of: flood the network to create a denial of service; map the internal structure of the network; spoof a legitimate device.

2.8 it checks networks, devices and applications for **known** vulnerabilities and produces a report, usually with a severity rating for each finding. Limitation, any one: it finds only vulnerabilities already known and catalogued, so a novel flaw is missed; it reports the vulnerability but not whether an adversary is capable of exploiting it; and a report is not a fix.

2.9 (a) **moderate to high** - the impact is high because payroll data would be captured, but exploitation requires advanced technical ability and sustained effort, which reduces the likelihood; accept either rating if the answer weighs impact against difficulty. (b) **moderate** - it gives an adversary information about the systems or devices on the network without granting access. (c) **low** - it would be difficult to exploit given the physical control, and the likely negative impact is minimal.

3.1 B. Domain names to IP addresses is DNS; MAC to switch port is the switch's own table.

3.2 B. It floods the network with ICMP requests so it cannot serve legitimate users.

3.3 B.

3.4 B. That is the definition of the moderate rating.

3.5 (a) any three of: plug into the reception data port, which has no port security; join the Wi-Fi, which does not authenticate devices; break the weak wireless encryption from the car park; plug a rogue access point into the open store-room port. Easiest: **joining the Wi-Fi**, because it authenticates neither devices nor users and needs no physical entry at all. Maximum 4.

(b) an adversary can plug a wireless access point into the open port, creating a **rogue access point** that gives them continuing wireless access to the internal network from outside the building, without needing to return to the store room.

(c) any two, each named with its harm: **ARP poisoning** - false IP-to-MAC pairings so membership traffic including bank details is delivered to the adversary, who can read or alter it; **MAC flooding** - overwhelming the switch so it broadcasts, exposing till and membership traffic; **DNS poisoning** - redirecting staff to a fake login page; **smurf** - flooding with ICMP so the till system is unavailable and the centre cannot trade. Maximum 4.

(d) It is **wrong**. A scanner checks for **known** vulnerabilities only, so a novel technique or a flaw not yet catalogued does not appear, and no report is complete. A report is also only a list: it does not fix anything, and it says nothing about the network's design faults here - a single flat network with no segmentation is a serious weakness that no individual scan finding would name.

(e) **High**. An adversary can join with essentially no skill and no physical access, and once inside can capture traffic and spoof devices - the "easily, with significant impact" definition - against data that includes bank details. First two changes, any two justified: enable **device and user authentication** on the Wi-Fi and strengthen its encryption, which closes the easiest route; enable **port security** on the reception port and disable the unused store-room port, which closes the physical routes. Accept network **segmentation** separating the till and membership systems from guest traffic as one of the two, with justification.