AP CYBERSECURITY • EXERCISE SHEET

4.1 Device Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 45 marks**

KEY WORDS malware 恶意软件 • patch 补丁 • iot 物联网 • ram 内存 • worm 蠕虫

Objective

Build the skills to answer exam questions on device types, **malware** 恶意软件, common **device vulnerabilities** 设备漏洞, and rating device risk.

You must be able to:

- identify the four types of computing device, including embedded and **IoT** 物联网 devices
- name malware by its behaviour, and say what makes fileless malware different
- explain how each common device vulnerability is exploited
- rate a device risk high, moderate or low, and justify the rating

1 Worked examples

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

The four device types

Type	What defines it
Server	provides one or more services to other computers (DNS, DHCP, FTP). Any computer can be a server
Personal computer	designed for one person's work or recreation
Handheld	smaller, battery powered - tablets, smartphones
Embedded	part of a machine, with a specific instruction set for that machine's components

Everyday devices with embedded computers are **IoT** devices - found in transport, buildings, medical equipment and homes. They matter to security because they are numerous, rarely patched, and often shipped with a default password.

Naming malware by its behaviour

The question always describes *what it did*, so match the behaviour, not the word.

Malware	The behaviour that names it
Virus	must be **activated by the user** opening or executing a file
Worm	spreads computer to computer **without human interaction**
Trojan	hidden inside software that seems harmless; a **RAT** gives remote access
Ransomware	**encrypts** files and demands payment for the key
Spyware	tracks the user's actions and reports back
Keylogger	logs **keystrokes**, from which usernames and passwords are extracted
Logic bomb	triggers only when a **condition** is met - a date, an OS version, a file change
Rootkit	reaches the **operating system**, controls nearly everything, and hides itself

Fileless malware is the exception to the whole table: it is not a file at all. It lives in **RAM** and drives **legitimate programs already installed** on the device, so scanning the disk for a malicious file finds nothing.

Example. Files are unreadable and a screen demands payment - **ransomware**. It spread to every machine overnight with nobody clicking anything - the delivery was a **worm**. Name both when the evidence supports both.

The device vulnerabilities and how each is exploited

- **Unpatched software** - an exploit already exists for a known flaw, so the attack needs no new work.
- **Weak authentication** - the password is guessed, or social engineering makes the user give it up.
- **No BIOS/UEFI password** - the machine can be booted into a special mode, bypassing the operating system entirely.
- **Autorun enabled** - malware on an inserted external drive runs by itself.
- **Open ports** - the adversary simply connects.
- **No firewall, or a misconfigured one** - malicious data cannot be filtered out.
- **No anti-malware software** - nothing stops the install.

Rating a device risk

Ask **what is compromised** and **how likely** the exploit is.

Rating	When
High	sensitive data or critical operations could be compromised
Moderate	weak authentication, or a vulnerability less likely to be exploited
Low	exploiting it would have little impact

A rating is only worth marks with the *because*. "High risk, because the device holds patient records and an unpatched flaw with a public exploit needs no skill" earns; "high risk" alone does not.

2 Practice

2.1 Name the type of computing device in each case.

(a) A machine running DHCP for the office network. [1]

(b) The control unit inside a washing machine. [1]

(c) A tablet used on a train. [1]

(d) A networked security camera in a home. [1]

2.2 Name the malware from its behaviour.

(a) It encrypts every document and displays a payment demand. [1]

(b) It copies itself across the network with no user action. [1]

(c) It records everything typed and sends it to an outside server. [1]

(d) It activates only on the first day of the next financial year. [1]

(e) It hides itself inside the operating system and controls the whole machine. [1]

2.3 Explain what makes **fileless malware** difficult to detect. [2]

2.4 State the difference between a **virus** and a **worm**. [2]

2.5 For each vulnerability, describe how an adversary exploits it.

(a) Autorun is enabled. [1]

(b) There is no BIOS/UEFI password. [1]

(c) Software has not been patched. [1]

(d) A port is left open. [1]

2.6 Explain why a missing or misconfigured firewall is a device vulnerability. [2]

2.7 Rate each risk high, moderate or low, and justify.

(a) A hospital server holding patient records runs an operating system with a publicly documented unpatched flaw. [2]

(b) A staff-room printer accepts a four-character password. [2]

(c) A disconnected demonstration laptop holding only sample data has autorun enabled. [2]

3 Exam-style questions

3.1 Which malware spreads without any user action? [1]

- **A** virus
- **B** worm
- **C** trojan
- **D** logic bomb

3.2 An IoT device is best described as [1]

- **A** any device connected to a company network
- **B** an everyday device containing an embedded computer
- **C** a handheld battery-powered computer
- **D** a server providing a service to other computers

3.3 Malicious code runs entirely in RAM using PowerShell, already installed on the machine. This is [1]

- **A** a rootkit
- **B** fileless malware
- **C** a logic bomb
- **D** spyware

3.4 A device vulnerability is rated **moderate** rather than high when [1]

- **A** exploiting it would have almost no impact
- **B** it involves weak authentication, or is less likely to be exploited
- **C** the device is not connected to the internet
- **D** sensitive data or critical operations could be compromised

3.5 A regional logistics firm runs: a file server holding customer addresses and payment records; twenty warehouse handheld scanners that have never been updated since purchase; and forty IoT temperature sensors in refrigerated trailers, all still using the manufacturer's default password. The file server has no anti-malware software. One morning, staff find every file on the file server encrypted and a payment demand on screen. The scanners are unaffected.

(a) Name the malware and state the evidence that identifies it. [2]

(b) Identify **two** device vulnerabilities in the scenario and explain how each could have contributed to the attack. [4]

(c) Rate the risk from the IoT sensors and justify your rating against the criteria. [3]

(d) The IT manager argues the scanners are low risk because "they only scan barcodes". Evaluate this argument. [3]

(e) Recommend **three** controls, each addressing a different vulnerability you named, and state which one you would implement first and why. [4]

Solutions

2.1 (a) server. (b) embedded computer; accept IoT only if the machine is described as networked. (c) handheld / mobile computer. (d) IoT device.

2.2 (a) ransomware. (b) worm. (c) keylogger; accept spyware with justification. (d) logic bomb. (e) rootkit.

2.3 it is not a file - it lives in RAM, and it works through legitimate programs already installed on the device, so scanning the disk finds no malicious file and the activity looks like normal software running.

2.4 a virus must be activated by the user opening or executing a file; a worm spreads from computer to computer with no human interaction.

2.5 (a) malware placed on an external drive runs automatically when the drive is inserted. (b) the machine can be booted into a special mode, bypassing the operating system and its access controls. (c) an exploit already exists for the known flaw, so the adversary needs no new work and little skill. (d) the adversary connects to the device directly through that port.

2.6 a firewall filters the data arriving at the device; without one, or with it misconfigured, malicious data reaches the device and can disrupt it or be used to take control.

2.7 (a) **high** - patient records are sensitive data governed by law, and a publicly documented unpatched flaw makes exploitation highly likely. (b) **moderate** - it is weak authentication, but a printer holds little sensitive data, so the impact of compromise is limited. Accept low with a justification that impact is minimal. (c) **low** - the vulnerability is real, but the device is disconnected and holds only sample data, so exploiting it would have little impact.

3.1 B. A virus needs the user to open or execute a file; a trojan needs the user to install it; a logic bomb waits for a condition.

3.2 B. IoT is the everyday-device case of an embedded computer, not a general term for anything networked.

3.3 B. Living in RAM and abusing an already-installed legitimate program is exactly fileless malware. A rootkit is still a file and sits in the OS.

3.4 B. A is low, D is high, and C is not one of the criteria.

3.5 (a) **ransomware** - the files are encrypted and a payment demand is displayed, which is its defining behaviour.

(b) any two, each named and explained: **no anti-malware software** on the file server, so nothing stopped the malware installing; **default passwords** on the IoT sensors, which is weak authentication and gives an adversary an entry point onto the network; **unpatched scanners**, since software never updated since purchase carries known flaws with existing exploits.

(c) **High**. The sensors are numerous and all share a known default password, so the likelihood of compromise is very high and needs no skill; and although a temperature sensor holds no sensitive data itself, it sits on the same network as the payment records, and compromising refrigeration is a **critical operation** for a firm carrying chilled freight.

(d) The argument is **wrong**. Risk is not only about the data the device holds - an unpatched device on the network is a route to the devices that do hold sensitive data, which is exactly the lateral-movement path an adversary needs. Twenty devices never updated since purchase carry every flaw published since then, so likelihood is high even if the direct impact is low; and losing scanning would halt warehouse operations, so the impact is not negligible either.

(e) Three controls each matched to a different vulnerability - install and maintain anti-malware on the file server; change every default password and enforce a password policy on the sensors; establish a patching schedule for the scanners. First: **change the default passwords**, because it costs almost nothing, removes the highest-likelihood route in, and closes forty devices at once. Accept "restore from backup and patch the server first" if justified by the live incident.