

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

3.2 An IoT device is best described as [1]

- | | | | | | |
|--|--|---|---|---|---|
| <table border="1"><tr><td>A</td><td>B</td></tr><tr><td>C</td><td>D</td></tr></table> | A | B | C | D | A any device connected to a company network |
| A | B | | | | |
| C | D | | | | |
| | 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 | B |
| C | D |
- 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 | B | A exploiting it would have almost no impact |
| C | D | 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.

- Name the malware and state the evidence that identifies it. [2]
- Identify **two** device vulnerabilities in the scenario and explain how each could have contributed to the attack. [4]
- Rate the risk from the IoT sensors and justify your rating against the criteria. [3]
- The IT manager argues the scanners are low risk because “they only scan barcodes”. Evaluate this argument. [3]
- Recommend **three** controls, each addressing a different vulnerability you named, and state which one you would implement first and why. [4]
