AP CYBERSECURITY • EXERCISE SHEET

4.3 Protecting Devices

Name: _____ Class: _____ Date: _____ **Total: 51 marks**

KEY WORDS acl 访问控制列表 • acceptable use policy 可接受使用政策 • host-based firewall 主机防火墙 • anti-malware 反恶意软件 • patching 补丁更新

Objective

Build the skills to answer exam questions on **device managerial controls** 设备管理控制, **anti-malware** 反恶意软件, **patching** 补丁更新, and configuring a **host-based firewall** 主机防火墙.

You must be able to:

- describe the three device policies and say what each contains
- explain how anti-malware software detects and handles malware, and its limitation
- explain why updating the operating system and software makes a device more secure
- explain what a host-based firewall adds beyond a network firewall
- write and order firewall rules in an **ACL** 访问控制列表

1 Worked examples

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

■ The three device policies

Policy	What it describes
Acceptable use	the activities that are permissible, prohibited or **required** by users on the organisation's devices
Password	requirements for user passwords
Software installation	what software, if any, users may install - usually with a **process for requesting** software

A **password policy** may include: a minimum or maximum length; a minimum or maximum time a password may be kept; a **prohibition on reuse**; construction rules (no dictionary words, character-set requirements); and a suggestion to use a secure password manager rather than writing passwords down.

A **software installation policy** commonly **prohibits users installing software at all**, and provides a route to request it instead - which is what stops a user installing the "free video converter" that carries malware.

Anti-malware software

It **quarantines and removes** malware that can corrupt, spy on or destroy a system. It works from a **database of malware signatures**: it periodically scans the files on the device and checks whether any match a known signature.

Two consequences follow directly, and both are examinable:

- The signature database must be **kept current**, or newly released malware is not recognised.
- Malware with **no signature yet** passes - which is why fileless malware and novel attacks defeat it, and why anti-malware is one layer rather than the whole defence.

Why updating matters

When a vulnerability in an operating system or application is found, the vendor fixes it and **releases the fix as an update**. Keeping software at its most recent version prevents adversaries taking advantage of that vulnerability.

The exam's point is the **timing**: publishing a fix also publishes the existence of the flaw. An unpatched device is therefore vulnerable to an attack that is now publicly documented and needs little skill - which raises the *likelihood* half of the risk assessment, not just the severity.

The host-based firewall

A network firewall protects the boundary. A **host-based firewall** allows or denies traffic into or out of a **single device**, which matters because:

- it is an extra layer if the host is connected to a **compromised network** - a coffee-shop Wi-Fi, or an internal network an adversary has already reached;
- it can block **outbound** traffic, which is how a compromised device is stopped from calling out to a command-and-control server;
- it should always **block ports or services not needed** for that device's role.

It is software following a rule set - an **ACL** - exactly like a network firewall.

Writing and ordering ACL rules

A rule can allow or deny by **source or destination port, IP address, service, protocol, or application**.

Rules are checked in order, and the first rule that matches is the one that executes. Order therefore changes behaviour:

```
1  DENY   inbound   any         -> port 3389     (remote desktop)
2  ALLOW  inbound   10.0.5.0/24 -> port 3389
```

Rule 1 matches everything first, so rule 2 never runs and the administrators are locked out too. Reversed, the specific allow is evaluated first and the deny then catches everyone else - which is the standard shape: **specific rules above general ones, with a broad deny last.**

2 Practice

2.1 Name the three managerial policies for device security and state what each describes. [6]

2.2 State **three** requirements a password policy may include. [3]

2.3 Explain why a software installation policy usually prohibits users installing software, and what it provides instead. [2]

2.4 Explain how anti-malware software decides that a file is malware. [2]

2.5 State **two** things anti-malware software does with malware it finds. [2]

2.6 Explain why anti-malware software cannot detect a brand-new piece of malware. [2]

2.7 Explain why an unpatched device becomes **more** likely to be attacked once the vendor publishes the fix. [2]

2.8 State **two** things a host-based firewall can do that a network firewall alone cannot. [2]

2.9 A laptop's host-based firewall has these rules, checked in order:

```
1  ALLOW  outbound  any -> any
2  DENY   outbound  any -> port 4444
```

(a) State whether traffic to port 4444 is blocked, and explain why. [2]

(b) Rewrite the rules so the intended block works. [2]

3 Exam-style questions

3.1 Anti-malware software identifies malware by [1]

A watching for unusual login times
B comparing files against a database of malware signatures
C blocking traffic on unused ports
D checking the length of user input

3.2 A host-based firewall differs from a network firewall in that it [1]

A cannot block outbound traffic
B allows or denies traffic for a single device
C uses signatures rather than rules
D requires no access control list

3.3 In an ACL, when several rules could match the same traffic [1]

A the most restrictive rule is applied
B the first matching rule is executed
C all matching rules are applied in turn
D the last matching rule is executed

3.4 Which policy would forbid an employee installing a free file-compression tool downloaded from an unknown site? [1]

A password policy
B software installation policy
C cryptography policy
D wireless security policy

3.5 A design studio issues laptops that staff take to clients and to cafes. There is no software installation policy, and staff install fonts and plug-ins freely. Anti-malware is installed but its signature database was last updated fourteen months ago. The operating system prompts for updates, which staff dismiss. The laptops have no host-based firewall, on the grounds that "the office has a firewall already".

(a) Identify **four** weaknesses and state the compromise each could lead to. [8]

(b) Explain why "the office has a firewall already" is not a sufficient answer for these laptops. [3]

(c) A laptop is infected at a cafe with malware first seen two months ago. Explain why the installed anti-malware did not stop it, and whether it would stop it after an update. [3]

(d) Write **three** host-based firewall rules for these laptops, in a correct order, and justify the order. [4]

(e) Recommend the managerial controls the studio needs, and explain how each addresses a weakness you identified in (a). [4]