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]

Solutions

2.1 acceptable use policy - the range of activities permissible, prohibited or required by users on the organisation's devices; **password policy** - the requirements for user passwords; **software installation policy** - what software, if any, users may install, and the process for requesting it.

2.2 any three of: a minimum or maximum password length; a minimum or maximum time a password may be kept; a prohibition of password reuse; construction rules such as no dictionary words or character-set requirements; a suggestion to use a secure password manager rather than writing passwords down.

2.3 users installing software freely can install malware disguised as a legitimate tool, or software with vulnerabilities the organisation has not assessed; the policy therefore provides a **process for requesting** software so it can be checked and installed by someone authorised.

2.4 it holds a database of malware **signatures** and periodically scans the files on the device, checking whether any file matches one of those signatures.

2.5 it **quarantines** the malware and **removes** it.

2.6 detection depends on a matching signature already being in the database; brand-new malware has no signature yet, so nothing matches and it is not recognised - and the same applies to fileless malware, which is not a file to scan at all.

2.7 publishing a fix also publishes the existence of the flaw, so adversaries know exactly what to exploit and exploit code often follows quickly - the vulnerability becomes easy to use and the likelihood of attack rises sharply while the device remains unpatched.

2.8 any two of: it protects a single device even on a **compromised network** such as public Wi-Fi; it can block **outbound** traffic, stopping a compromised device calling out to a command-and-control server; it can block ports and services not needed for that specific device's role, which a shared network rule set cannot do per device.

2.9 (a) **no** - it is allowed. Rule 1 matches all outbound traffic first, and the first matching rule executes, so rule 2 is never reached. (b) put the specific deny above the general allow:

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

.

3.1 B.

3.2 B. It can block outbound traffic, and it does use an ACL.

3.3 B.

3.4 B.

3.5 (a) any four, each with a compromise: **no software installation policy** - staff install malware disguised as a font or plug-in, giving an adversary control of the device; **a signature database fourteen months stale** - any malware released since then is unrecognised, so infection is undetected; **dismissed operating-system updates** - publicly documented vulnerabilities remain exploitable, allowing an adversary to take over the device with little skill; **no host-based firewall** - nothing filters traffic on an untrusted cafe network, and a compromised laptop can call out to a command-and-control server unimpeded.

(b) the office firewall protects traffic crossing the office boundary, and these laptops spend their working time on client and cafe networks, where that firewall is not in the path at all. A host-based firewall is exactly the extra layer for a host connected to a network that may already be compromised - and it also blocks outbound traffic, which the office firewall cannot do once the laptop is elsewhere.

(c) the malware was first seen two months ago, so its signature exists, but the studio's database is fourteen months old and therefore does not contain it - nothing matched during the scan. After an update the signature would be present, so a scan would then detect and quarantine it - though only after the infection, which is why patching and prevention matter more than detection alone.

(d) three sensible rules with a defensible order, for example:

```
1  ALLOW  outbound  any -> ports 80, 443   (web)
2  DENY   inbound   any -> any
3  DENY   outbound  any -> any
```

Justification: rules are checked in order and the first match executes, so the specific allows must come above the broad denies; putting the deny first would block the studio's own web traffic and the laptop would be unusable. Blocking all inbound and all other outbound follows the rule that ports and services not needed for the device's role should always be blocked.

(e) any two policies, each tied to a weakness: a **software installation policy** prohibiting staff installations and providing a request process, which closes the free-fonts-and-plug-ins route; an **acceptable use policy** stating what staff must do on studio devices - including not dismissing updates and not working on untrusted networks without the firewall enabled; a **password policy**, if the answer identified weak authentication among the weaknesses.