Exercise walk-through

Device Vulnerabilities and Attacks ▪ 4.1

eXercise

You must be able to

- identify types of device, including **IoT** 物联网 devices
- name malware by its behaviour (virus, worm, ransomware, RAT, rootkit)
- rate device risk high, moderate, or low

Method — Naming malware

A virus needs a user to run a file. A worm spreads by itself. Ransomware encrypts files for money. A remote access trojan (RAT) gives remote control. A rootkit hides deep in the OS.

Method — Rating device risk

High = an unpatched critical device (e.g. a hospital server). Low = a low-value device with an unused open port. The value and criticality of the device set the level.

Practice 2.1 ▪ 2 marks

State the key difference between a virus and a worm.

Solution 2.1

Method: Naming malware

Worked steps

a virus needs a user to open/run a file B1; a worm spreads by itself with no human action B1.

Practice 2.2 ▪ 1 mark

Name the malware that encrypts a victim's files and demands payment.

Solution 2.2

Method: Naming malware

Worked steps

ransomware B1.

Practice 2.3 ▪ 1 mark

An organisation has not applied a critical security update to its email server.
(a) State the risk level.
(b) Justify your answer.

Solution 2.3

Method: Rating device risk

Worked steps

(a) high B1. (b) an unpatched critical service can be exploited with serious impact B1.

Exam-style 3.1 ▪ 1 mark

Which malware spreads across a network WITHOUT any user action?

A virus

B worm

C trojan

D spyware

Solution 3.1

Method: Naming malware

A virus

B worm ✓

C trojan

D spyware

Worked steps

B. a worm self-spreads; a virus needs a user.

Exam-style 3.2 ▪ 1 mark

An internet-connected thermostat is an example of a(n)

A server

B IoT device

C mainframe

D firewall

Solution 3.2

A server

B IoT device ✓

C mainframe

D firewall

Worked steps

B. everyday embedded connected devices are IoT devices.

Exam-style 3.3 ▪ 1 mark

Malware on a device gives an adversary full remote control of it.
(a) Name the type of malware.
(b) State one action the adversary could then take.

Solution 3.3

Method: Naming malware

Worked steps

(a) a remote access trojan (RAT) B1. (b) e.g. steal files, watch the user, or use it as a foothold B1.