Security

CompTIA A+ certification, Core 1 (220-1201) and Core 2 (220-1202)

28% of the exam · 11 exam objectives · 220-1202

Domain 2 covers how a technician protects people, devices and data. It starts with physical and logical security measures and their purposes, the Windows security settings (accounts, permissions, Defender, firewall, BitLocker and EFS), and the wireless security protocols and authentication methods. It then covers malware types with the tools to detect, remove and prevent them, social engineering attacks, threats and vulnerabilities, and the procedure for removing malware from a SOHO computer. The second half applies this to practice: hardening workstations, securing mobile devices, choosing the right data destruction or disposal method, securing SOHO routers and wireless networks, and configuring browser security settings.

You should be able to: A laptop holding customer PII is stolen, and its solid-state drive will later be retired. Which control protects the data while the laptop is missing, and why is degaussing the wrong way to retire the drive?

Every exam objective: the key point and the trap

2.1 Summarize various security measures and their purposes.

Physical security keeps people and vehicles away from assets: bollards stop vehicles, fences and lighting deter and expose intruders, an access control vestibule holds one person between two interlocked doors, and guards, video surveillance, alarm systems, motion sensors and magnetometers detect and respond.

Trap: Counting a password and a PIN, or a password and a security question, as multifactor. They are both something you know, so they are one factor.

2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.

Microsoft Defender Antivirus is managed in Windows Security, Virus and threat protection: real-time protection can be turned on or off, and Protection updates downloads new definitions. A third-party antivirus normally turns Defender's real-time protection off.

Trap: Using EFS to protect a USB flash drive or a whole laptop. EFS protects individual files for one user; BitLocker To Go and BitLocker protect whole drives.

2.3 Compare and contrast wireless security protocols and authentication methods.

WPA2 encrypts wireless traffic with the Advanced Encryption Standard (AES). Its personal mode uses a pre-shared key, whose captured handshake can be attacked offline.

Trap: Confusing RADIUS and TACACS+. RADIUS is for network access and encrypts only the password; TACACS+ is for device administration and encrypts the whole packet.

2.4 Summarize types of malware and tools/methods for detection, removal, and prevention.

A Trojan hides inside software that looks useful; a virus attaches to files and spreads when they run; a boot sector virus infects disk startup code; a rootkit hides itself and other malware from the operating system.

Trap: Treating EDR, XDR and MDR as the same thing. EDR and XDR are tools; MDR is a service with people who use them.

2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities.

Phishing tricks people through messages: vishing by voice, smishing by text, QR code phishing through a scanned code, spear phishing at a chosen person and whaling at a senior executive.

Trap: Calling a weakness an attack or the other way round. An unpatched or EOL system is a vulnerability; phishing, tailgating and a DDoS are threats that exploit people or systems.

2.6 Given a scenario, implement procedures for basic small office/home office (SOHO) malware removal.

Step 1: investigate and verify the malware symptoms, so the technician knows the problem is malware.

Trap: Creating a restore point before cleaning, or leaving System Restore on during remediation. Either can preserve the malware and bring it back.

2.7 Given a scenario, apply workstation security options and hardening techniques.

Data-at-rest encryption, such as BitLocker full-disk encryption, keeps a drive's contents unreadable without the key, even when the drive is removed and read in another computer.

Trap: Choosing a sign-in control, such as a lockout or a firmware password, to protect a stolen drive. Only encryption protects data once the drive is read in another computer.

2.8 Given a scenario, apply common methods for securing mobile devices.

Hardening techniques: device encryption, screen locks and configuration profiles. A swipe offers no authentication; patterns and PIN codes are something the user knows; fingerprint and facial recognition are biometrics.

Trap: Picking a locator application when the question asks how to protect data on a phone that will not be recovered. Locating finds the device; a remote wipe protects the data.

2.9 Compare and contrast common data destruction and disposal methods.

Physical destruction of hard drives: drilling, shredding, degaussing and incineration. The drive cannot be used again afterward.

Trap: Treating a quick format as erasure, or choosing degaussing for a solid-state drive.

2.10 Given a scenario, apply security settings on SOHO wireless and wired networks.

Change the default administrator password first: every other setting can be undone by someone with the factory credentials.

Trap: Believing that disabling SSID broadcast secures the network. The name is still in the traffic, so encryption does the real work.

2.11 Given a scenario, configure relevant security settings in a browser.

Browser download and installation: use trusted sources, avoid untrusted ones, and compare a file's hash with the vendor's published value to confirm it was not altered.

Trap: Expecting private-browsing mode to hide activity from the network. It only stops the browser keeping history, cookies and form data on the device.

Key terms

MFA: Multifactor Authentication

TPM: Trusted Platform Module

UAC: User Account Control

EFS: Encrypting File System

WPA: Wi-Fi Protected Access

BYOD: Bring Your Own Device

MDM: Mobile Device Management

PII: Personally Identifiable Information

UPnP: Universal Plug and Play

SSID: Service Set Identifier

ExamDragon, examdragon.com/aplus. Independent exam preparation, written in our own words to the 220-1202 exam objectives. CompTIA and A+ are trademarks of CompTIA, Inc.