COMPTIA A+ CORE 2 (220-1002) EXAM CHAPTER 27: SECURING COMPUTERS

OBJECTIVE MAPPING*

EPISODE : THREATS

CORE 2 EXAM OBJECTIVES

DOMAIN 2: NETWORKING

2.5 Compare and contrast social engineering, threats, and vulnerabilities

- DDoS
- DoS
- Zero-day
- Man-in-the-middle
- Spoofing
- Zombie

DOMAIN 3: HARDWARE

3.2 Given a scenario, troubleshoot and resolve PC security issues

- Common symptoms
  - Disappearing files

EPISODE : PHYSICAL SECURITY

CORE 2 EXAM OBJECTIVES

DOMAIN 2: NETWORKING

2.1 Summarize the importance of physical security measures

- Mantrap
- Badge reader
- Smart card
- Security guard
- Door lock
- Hardware tokens
- Cable locks
- Server locks
- USB locks
- Privacy screen
- Key fobs

EPISODE : PASSWORDS AND AUTHENTICATION

CORE 2 EXAM OBJECTIVES

DOMAIN 2: NETWORKING

2.5 Compare and contrast social engineering, threats, and vulnerabilities

- Brute force

- Dictionary
- Rainbow table

2.7 Given a scenario, implement security best practices to secure a workstation

- Password best practices
  - Setting strong passwords
  - Password expiration
  - Screensaver required password
  - BIOS/UEFI passwords
  - Requiring passwords

EPISODE : MALWARE

CORE 2 EXAM OBJECTIVES

DOMAIN 2: NETWORKING

2.4 Given a scenario, detect, remove, and prevent malware using appropriate tools and methods

- Malware
  - Ransomware
  - Trojan
  - Keylogger
  - Rootkit
  - Botnet
  - Worm
  - Spyware

2.5 Compare and contrast social engineering, threats, and vulnerabilities

- Noncompliant systems

DOMAIN 3: HARDWARE

3.2 Given a scenario, troubleshoot and resolve PC security issues

- Common symptoms
  - Pop-ups
  - Browser redirection
  - Security alerts
  - Application crash
  - OS updates failures
  - Rogue antivirus
  - Spam
  - Hijacked email
  - Invalid certificate (trusted root CA)

EPISODE : ANTI-MALWARE

CORE 2 EXAM OBJECTIVES

DOMAIN 2: NETWORKING

2.4 Given a scenario, detect, remove, and prevent malware using appropriate tools and methods

- Tools and methods
  - Antivirus
  - Anti-malware
  - Recovery console
  - Backup/restore
  - End user education
  - Software firewalls

- SecureDNS

DOMAIN 3: HARDWARE

3.3 Given a scenario, use best practice procedures for malware removal

- Identify and research malware symptoms
- Quarantine the infected systems
- Disable System Restore (in Windows).
- Remediate the infected systems.
  - Update the anti-malware software
  - Scan and use removal techniques (safe mode, pre-installation environment).
- Schedule scans and run updates
- Enable System Restore and create a restore point (in Windows).
- Educate the end user.

EPISODE : SOCIAL ENGINEERING

CORE 2 EXAM OBJECTIVES

DOMAIN 2: NETWORKING

2.5 Compare and contrast social engineering, threats, and vulnerabilities

- Social engineering
  - Phishing
  - Spear phishing
  - Impersonation
  - Shoulder surfing
  - Tailgating
  - Dumpster diving

EPISODE : LICENSING

CORE 2 EXAM OBJECTIVES

DOMAIN 4: VIRTUALIZATION AND CLOUD COMPUTING

4.6 Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts

- Licensing/DRM/EULA
  - Open-source vs. commercial license
  - Personal license vs. enterprise licenses

EPISODE : INCIDENT RESPONSE

CORE 2 EXAM OBJECTIVES

DOMAIN 4: VIRTUALIZATION AND CLOUD COMPUTING

4.1 Compare and contrast best practices associated with types of documentation

- Incident documentation

4.6 Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts

- Incident response
  - First response
  - Identify
    - Report through proper channels
    - Dada/device preservation
    - Use of documentation/documentation changes
  - Chain of custody
    - Tracking of evidence/documenting process

EPISODE : ENVIRONMENTAL CONTROLS

CORE 2 EXAM OBJECTIVES

DOMAIN 4: VIRTUALIZATION AND CLOUD COMPUTING

4.5 Explain environmental impacts and appropriate controls

- MSDS documentation for handling and disposal
- Temperature, humidity level awareness, and proper ventilation
- Power surges, brownouts, and blackouts
    - Battery backup
    - Surge suppressor
- Protection from airborne particles
    - Enclosures
    - Air filters/mask
- Dust and debris
    - Compressed air
    - Vacuums

*This document can be used to determine what CompTIA A+ exam objectives are in each episode, as well as map where those objectives are in the official “CompTIA A+ 220-1001 Exam Objectives (2.0)” PDF resource that accompanies this course.

**Why am I seeing different Core exams than what I’m studying? In some cases, you may be watching a video series that focuses on the Core 1 exam, however some of the episodes contain Core 2 exam objectives, or vice versa. There are 2 reasons for this: 1) The other Core exam topic is covered to give you a better, fuller understanding of the surrounding topics, and 2) Some episodes contain information from both Core exams because the topics coincide with each other and are more easily taught in 1 episode than breaking them out into separate episodes.