Network Security

CompTIA Network+ certification exam, N10-009

14% of the exam · 3 exam objectives · N10-009

Domain 4 covers why network security matters and how it is done: encryption for data in transit and at rest, certificates and PKI, identity and access management (MFA, SSO, RADIUS, TACACS+, LDAP, SAML), least privilege, physical security, deception, risk terms, compliance and segmentation (4.1); the attacks a network faces, from DoS and VLAN hopping to ARP and DNS poisoning, rogue devices, evil twins, on-path attacks, social engineering and malware (4.2); and the defences that apply in practice: device hardening, NAC with 802.1X, port security and MAC filtering, key management, ACLs, URL and content filtering, and trust zones with a screened subnet (4.3).

You should be able to: Users on one subnet find that the gateway's IP address in their ARP cache now maps to a coworker's laptop. Which attack is this, what position does it give the attacker, and which access control feature would stop an unknown laptop from joining the wired network in the first place?

Every exam objective: the key point and the trap

4.1 Explain the importance of basic network security concepts.

Encryption protects data in transit (moving across a network: TLS, IPsec, VPNs) and data at rest (stored on drives, databases and backups: full-disk and file encryption). Match the control to the state of the data.

Trap: Treating two secrets of the same kind (a password and a PIN) as MFA, or mixing up RADIUS and TACACS+: RADIUS is UDP and encrypts only the password; TACACS+ is TCP and encrypts the whole payload.

4.2 Summarize various types of attacks and their impact to the network.

Denial of service (DoS) floods or crashes a target from one source; distributed denial of service (DDoS) does it from many, often a botnet. Both attack availability.

Trap: Confusing MAC flooding (overloading the switch's address table) with ARP poisoning (lying about which MAC owns an IP), or a rogue DHCP server (wrong lease) with DNS poisoning (wrong name answer).

4.3 Given a scenario, apply network security features, defense techniques, and solutions.

Device hardening reduces a device's own attack surface: disable unused ports and services and change default passwords before a device goes into service.

Trap: Choosing MAC filtering when the question asks for the strongest way to control who joins: MAC addresses can be copied, so 802.1X is the better answer.

Key terms

CIA: Confidentiality, Integrity, and Availability

MFA: Multifactor Authentication

SSO: Single Sign-on

RADIUS: Remote Authentication Dial-in User Service

TACACS+: Terminal Access Controller Access Control System Plus

SAML: Security Assertion Markup Language

PKI: Public Key Infrastructure

ARP: Address Resolution Protocol

NAC: Network Access Control

ACL: Access Control List

ExamDragon, examdragon.com/netplus. Independent exam preparation, written in our own words to the N10-009 exam objectives. CompTIA and Network+ are trademarks of CompTIA, Inc.