

98-367: Security Fundamentals

This document shows where changes to Exam 98-367 have been made to include updates for Windows 10 as well as security and threat terms. These changes are effective as of June 23, 2016.

1. Understand security layers (25–30%)

- 1.1. Understand core security principles
Confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering; attack surface **analysis**; **threat modelling**
- 1.2. Understand physical security
Site security; computer security; removable devices and drives; access control; mobile device security; ~~disable Log On Locally~~; keyloggers
- 1.3. Understand Internet security
Browser **security** settings; ~~zones~~; secure websites
- 1.4. Understand wireless security
Advantages and disadvantages of specific security types; keys; service set identifiers (SSIDs); MAC filters

2. Understand operating system security (30–35%)

- 2.1. Understand user authentication
Multifactor **authentication**; **physical and virtual** smart cards; Remote Authentication Dial-In User Service (RADIUS); ~~Public Key Infrastructure (PKI)~~; ~~understand the certificate chain~~; biometrics; ~~Kerberos and time skew~~; use Run As to perform administrative tasks; ~~password reset procedures~~
- 2.2. Understand permissions
File **system permissions**; share **permissions**; registry; Active Directory; ~~NT file system (NTFS) versus file allocation table (FAT)~~; enable or disable inheritance; behavior when moving or copying files within the same disk or on another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; delegation; **inheritance**
- 2.3. Understand password policies
Password complexity; account lockout; password length; password history; time between password changes; enforce by using Group Policies; common attack methods; **password reset procedures**; **protect domain user account passwords**
- 2.4. Understand audit policies
Types of auditing; what can be audited; enable auditing; what to audit for specific purposes; where to save audit information; how to secure audit information
- 2.5. Understand encryption
Encrypting file system (EFS); how EFS-encrypted folders impact moving/copying files; BitLocker (To Go); TPM; software-based encryption; MAIL encryption and signing and other uses; virtual private network (VPN); public key/private key; encryption algorithms; certificate properties; certificate services; PKI/certificate services infrastructure; token devices; **lock down devices to run only trusted applications**
- 2.6. Understand malware
Buffer overflow; **viruses, polymorphic viruses**; worms; Trojan **horses**; spyware; **ransomware; adware; rootkits; backdoors; zero day attacks**

3. Understand network security (20–25%)

3.1. Understand dedicated firewalls

Types of hardware firewalls and their characteristics; when to use a hardware firewall instead of a software firewall; ~~SCMs and UTMs~~; stateful vs. stateless firewall inspection; Security Compliance Manager; security baselines

~~3.2. Understand Network Access Protection (NAP)~~

~~Purpose of NAP; requirements for NAP~~

3.3. Understand network isolation

~~Virtual local area networks (VLANs)~~; Routing; honeypot; perimeter networks; network address translation (NAT); VPN; IPsec; server and domain isolation

3.4. Understand protocol security

Protocol spoofing; IPsec; tunnelling; DNSsec; network sniffing; denial-of-service (DoS) attacks; common attack methods

4. Understand security software (15–20%)

4.1. Understand client protection

Antivirus; protect against unwanted software installations; User Account Control (UAC); keep client operating system and software updated; encrypt offline folders; software restriction policies; principle of least privilege

4.2. Understand email protection

Antispam, antivirus, spoofing, phishing, and pharming; client vs. server protection; Sender Policy Framework (SPF) records; PTR records

4.3. Understand server protection

Separation of services; hardening; keep servers updated; secure dynamic Domain Name System (DNS) updates; disable unsecure authentication protocols; Read-Only Domain Controllers (RODC); ~~separate management VLAN; Microsoft Baseline Security Analyzer (MBSA)~~