MICROSOFT 98-367

Microsoft Security Fundamentals Certification Questions & Answers

Exam Summary – Syllabus –Questions

98-367
Microsoft Technology Associate (MTA) - Security Fundamentals
40-60 Questions Exam – 700/1000 Cut Score – Duration of 45 minutes

Table of Contents:

Know Your 98-367 Certification Well:.....2

Microsoft 98-367 Security Fundamentals Certification Details: 2

98-367 Syllabus:.....3

Microsoft 98-367 Sample Questions: 5

Study Guide to Crack Microsoft Security Fundamentals 98-367 Exam: 8

Know Your 98-367 Certification Well:

The 98-367 is best suitable for candidates who want to gain knowledge in the Microsoft Windows Server. Before you start your 98-367 preparation you may struggle to get all the crucial Security Fundamentals materials like 98-367 syllabus, sample questions, study guide.

But don't worry the 98-367 PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the 98-367 syllabus?
- How many questions are there in the 98-367 exam?
- Which Practice test would help me to pass the 98-367 exam at the first attempt?

Passing the 98-367 exam makes you Microsoft Technology Associate (MTA) - Security Fundamentals. Having the Security Fundamentals certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Microsoft 98-367 Security Fundamentals Certification Details:

Exam Name	Microsoft Technology Associate (MTA) - Security Fundamentals
Exam Code	98-367
Exam Price	$127 (USD)
Duration	45 mins
Number of Questions	40-60
Passing Score	700 / 1000
Books / Training	**40032A: Networking and Security Fundamentals: Training two-pack for MTA Exams 98-366 and 98-367 (five days)** **40367A: Security Fundamentals: MTA Exam 98-367 (three days)**
Schedule Exam	**Pearson VUE**
Sample Questions	**Microsoft Security Fundamentals Sample Questions**
Practice Exam	**Microsoft 98-367 Certification Practice Exam**

98-367 Syllabus:

Topic	Details	Weights
Understand security layers	Understand core security principles - Confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering; attack surface analysis; threat modelling Understand physical security - Site security; computer security; removable devices and drives; access control; mobile device security; keyloggers Understand Internet security - Browser security settings; secure websites Understand wireless security - Advantages and disadvantages of specific security types; keys; service set identifiers (SSIDs); MAC filters	25-30%
Understand operating system security	Understand user authentication - Multifactor authentication; physical and virtual smart cards; Remote Authentication Dial-In User Service (RADIUS); biometrics; use Run As to perform administrative tasks Understand permissions - File system permissions; share permissions; registry; Active Directory; 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 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 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 Understand encryption - Encrypting file system (EFS); how EFS-encrypted	35-40%

Topic	Details	Weights
	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 Understand malware - Buffer overflow; viruses, polymorphic viruses; worms; Trojan horses; spyware; ransomware; adware; rootkits; backdoors; zero day attacks	
Understand network security	Understand dedicated firewalls - Types of hardware firewalls and their characteristics; when to use a hardware firewall instead of a software firewall; stateful versus stateless firewall inspection; Security Compliance Manager; security baselines Understand network isolation - Routing; honeypot; perimeter networks; network address translation (NAT); VPN; IPsec; server and domain isolation Understand protocol security - Protocol spoofing; IPsec; tunneling; DNSsec; network sniffing; denial-of-service (DoS) attacks; common attack methods	20-25%
Understand security software	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 Understand email protection - Antispam, antivirus, spoofing, phishing, and pharming; client versus server protection; Sender Policy Framework (SPF) records; PTR records Understand server protection - Separation of services; hardening; keep server updated; secure dynamic Domain Name System (DNS) updates; disable unsecure authentication protocols; Read-Only Domain Controllers (RODC)	15-20%

Microsoft 98-367 Sample Questions:

Question: 1

Creating MD5 hash for files is an example of ensuring what?

a) Confidentiality
b) Availability
c) Least privilege
d) Integrity

Answer: d

Question: 2

Which type of security service is concerned with preventing or detecting any tampering with data?

a) Authentication
b) Availability
c) Integrity
d) Confidentiality

Answer: c

Question: 3

How does the sender policy framework (SPF) aim to reduce spoofed email?

a) It provides a list of IP address ranges for particular domains so senders can be verified.
b) It includes an XML policy file with each email that confirms the validity of the message.
c) It lists servers that may legitimately forward mail for a particular domain.
d) It provides an encryption key so that authenticity of an email message can be validated

Answer: a

Question: 4

You have a training room with 10 computers. You need to be able to control what software can be run by specific users logging on to the computers. What should you use?

(Choose two.)

a) SmartScreen Filtering
b) Network Access Protection
c) Software restriction policies
d) AppLocker
e) A firewall filter

Answer: c, d

Question: 5

Which type of firewall allows for inspection of all characteristics of a packet?

a) NAT
b) Stateful
c) Stateless
d) Windows Defender

Answer: b

Question: 6

What does implementing Windows Server Update Services (WSUS) allow a company to manage?

a) Shared private encryption key updates
b) Updates to Group Policy Objects
c) Active Directory server replication
d) Windows updates for workstations and servers

Answer: d

Question: 7

You need to ensure that all security updates have been applied to one of your servers. What should you use?

a) Microsoft Baseline Security Analyzer
b) ScanState.exe
c) A RADIUS server
d) Windows Deployment Services

Answer: a

Question: 8

Windows Firewall is a:

a) stateless software firewall.
b) stateful software firewall.
c) means of physically protecting a Windows server.
d) hardware firewall.

Answer: b

Question: 9

A mail system administrator scans for viruses in incoming emails to increase the speed of mail processing. Select the correct answer if the underlined text does not make the statement correct. Select "No change is needed" if the underlined text makes the statement correct.

a) Decrease the chances of a virus getting to a client machine
b) Verify that the senders of the messages are legitimate
c) Ensure that all links in the messages are trustworthy
d) No change is needed.

Answer: a

Question: 10

To implement multifactor authentication you should use:

a) encryption.
b) a smart card and a PIN.
c) a username and password.
d) a biometric input device.

Answer: b

Study Guide to Crack Microsoft Security Fundamentals 98-367 Exam:

- Getting details of the 98-367 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 98-367 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Microsoft provided training for 98-367 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 98-367 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 98-367 practice tests is must. Continuous practice will make you an expert in all syllabus areas.