➢ Vendor: Microsoft

➢ Exam Code: 98-367

➢ Exam Name: Security Fundamentals

➢ Question 91 -- Question 120

QUESTION 91
Which of the following is a attack type that is used to poison a network or computer to the point where the system is turned into unusable state?

A. Mail bombing
B. Pharming
C. Protocol spoofing
D. Denial of service (DOS)

Answer: D

QUESTION 92
Which of the following is a broadcast domain created by a switch?

A. VLAN
B. MAN
C. DMZ
D. VPN

Answer: A

QUESTION 93
Which of the following is an authentication protocol?

A. Kerberos
B. LDAP

C. TLS
D. PPTP

Answer: A

QUESTION 94
The company that you work for wants to set up a secure network, but they do not have any servers. Which three security methods require the use of a server? (Choose three.)

A. 802.1x
B. WPA2 Personal
C. WPA2 Enterprise
D. RADIUS
E. 802.11ac

Answer: ACD

QUESTION 95
Shredding documents helps prevent:

A. Man-in-the-middle attacks
B. Social engineering
C. File corruption
D. Remote code execution
E. Social networking

Answer: B
Explanation:
http://technet.microsoft.com/en-us/library/cc875841.aspx

QUESTION 96
Dumpster diving refers to a physical threat that a hacker might use to look for information about a computer network. 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. Phishing
B. Malware
C. Reverse Social engineering
D. No change is needed

Answer: D

QUESTION 97
An attorney hires you to increase the wireless network security for the law firm's office. The office has a very basic network, with just a modem and a router. Which of these security modes offers the highest security?

A. WPA-Personal
B. WEP
C. WPA2-Personal
D. WPA-Enterprise

Answer: C

QUESTION 98
Which type of firewall allows for inspection of all characteristics of a packet?

A. NAT
B. Stateful
C. Stateless
D. Windows Defender

Answer: B
Explanation:
http://en.wikipedia.org/wiki/Stateful_firewall

QUESTION 99
You are trying to establish communications between a client computer and a server. The server is not responding. You confirm that both the client and the server have network connectivity. Which should you check next?

A. Microsoft Update
B. Data Execution Prevention
C. Windows Firewall
D. Active Directory Domains and Trusts

Answer: D

QUESTION 100
You are an intern and are working remotely. You need a solution that meets the following requirements:
- Allows you to access data on the company network securely
- Gives you the same privileges and access as if you were in the office
What are two connection methods you could use? (Choose two.)

A. Forward Proxy
B. Virtual Private Network (VPN)
C. Remote Access Service (RAS)
D. Roaming Profiles

Answer: BD

QUESTION 101
Network Access Protection (NAP) enables administrators to control access to network resources based on a computer's:

A. Encryption level
B. Warranty
C. Physical location
D. Configuration

Answer: D
Explanation:
Network Access Protection (NAP) is a new set of operating system components included with the

Windows Server?2008 and Windows Vista?operating systems that provides a platform to help ensure that client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer's operating system and critical software. For example, computers might be required to have antivirus software with the latest signatures installed, current operating system updates installed, and a host-based firewall enabled. By enforcing compliance with health requirements, NAP can help network administrators mitigate some of the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software.

QUESTION 102
Which technology enables you to filter communications between a program and the Internet?

A. RADIUS server
B. Antivirus software
C. Software firewall
D. BitLocker To Go

Answer: C
Explanation:
There are two types of firewalls the Hardware Firewall and the Software Firewall. A Software Firewall is a software program and a Hardware Firewall is a piece of hardware. Both have the same objective of filtering communications over a system.

QUESTION 103
This question requires that you evaluate the underlined text to determine if it is correct. The first line of defense against attacks from the Internet is a software firewall. 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. hardware firewall
B. virus software
C. radius server
D. No change is needed

Answer: A

QUESTION 104
Which attack listens to network traffic of a computer resource?

A. Resource gathering
B. Denial of service
C. ARP poisoning
D. Eavesdropping
E. Logic bomb

Answer: D
Explanation:
Eavesdropping
In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping.
The ability of an eavesdropper to monitor the network is generally the biggest security problem that

administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

QUESTION 105
Which of the following describes a VLAN?

A. It connects multiple networks and routes data packets.
B. It is a logical broadcast domain across physical subnets.
C. It is a subnetwork that reveals a company's externally facing resources to the public network.
D. It allows different network protocols to communicate between different network segments.

Answer: B
Explanation:
VLAN (Virtual Local Network) is a logically separate IP subnetwork which allow multiple IP networks and subnets to exist on the same-switched network. VLAN is a logical broadcast domain that can span multiple physical LAN segments. It is a modern way administrators configure switches into virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones.

QUESTION 106
A network sniffer is software or hardware that:

A. Records user activity and transmits it to the server
B. Captures and analyzes network communication
C. Protects workstations from intrusions
D. Catalogs network data to create a secure index

Answer: B
Explanation:
A network sniffer is a computer tool that captures network data in the form of low-level packets. Network sniffers can be used for technical troubleshooting and analyzing the communication.

QUESTION 107
What is a service set identifier (SSID)?

A. A wireless encryption standard
B. The wireless LAN transmission type
C. The broadcast name of an access point
D. A wireless security protocol

Answer: C
Explanation:
SSID (service set identifier) is a function performed by an Access Point that transmits its name so that wireless stations searching for a network connection can 'discover' it. It's what allows your wireless adapter's client manager program or Windows built-in wireless software to give you a list of the Access Points in range.

QUESTION 108
To implement WPA2 Enterprise, you would need a/an:

A. RADIUS server
B. SSL server

C. WEP server
D. VPN server

Answer: A

QUESTION 109
You would implement a wireless intrusion prevention system to:

A. Prevent wireless interference
B. Detect wireless packet theft
C. Prevent rogue wireless access points
D. Enforce SSID broadcasting

Answer: C
Explanation:
http://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

QUESTION 110
The manager of a coffee shop hires you to securely set up WiFi in the shop.
To keep computer users from seeing each other, what should you use with an access point?

A. Client bridge mode
B. Client isolation mode
C. MAC address filtering
D. Client mode

Answer: B
Explanation:
Wireless Client Isolation is a unique security feature for wireless networks. When Client Isolation is enabled any and all devices connected to the wireless LAN will be unable to talk to each other.

QUESTION 111
E-mail bombing attacks a specific entity by:

A. Redirecting all e-mail to another entity
B. Sending high volumes of e-mail
C. Tracing e-mail to the destination address
D. Triggering high levels of security alerts

Answer: B
Explanation:
In Internet usage, an email bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

QUESTION 112
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 113
Which enables access to all of the logged-in user's capabilities on a computer?

A. Java applets
B. ActiveX controls
C. Active Server Pages (ASP)
D. Microsoft Silverlight

Answer: B

QUESTION 114
You need to install a domain controller in a branch office. You also need to secure the information on the domain controller. You will be unable to physically secure the server. Which should you implement?

A. Read-Only Domain Controller
B. Point-to-Point Tunneling Protocol (PPTP)
C. Layer 2 Tunneling Protocol (L2TP)
D. Server Core Domain Controller

Answer: A
Explanation:
A read-only domain controller (RODC) is a new type of domain controller in the Windows Server?2008 operating system. With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed.
An RODC hosts read-only partitions of the Active Directory Domain Services (AD DS) database.
http://technet.microsoft.com/en-us/library/cc732801 (v=ws.10).aspx

QUESTION 115
Which of the following ports is used by the Remote Desktop Protocol?

A. 80
B. 23
C. 3389
D. 110

Answer: C

QUESTION 116
Which of the following MMC snap-in consoles is used to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest?

A. Active Directory Domains and Trusts
B. Active Directory Administrative Center
C. Group Policy Management Console
D. Active Directory Sites and Services

Answer: D

QUESTION 117
Which of the following is used to create a secured connection over an unsecured network?

A. TCP/IP protocol
B. Virtual Private Network (VPN)
C. Single Sign-on (SSO)
D. Kerberos

Answer: B

QUESTION 118
Which of the following is the most common method for an attacker to spoof email?

A. Back door
B. Replay attack
C. Man-in-the-middle attack
D. Open relay

Answer: D

QUESTION 119
Which of the following security methods can be used to detect the DoS attack in order to enhance the security of the network?

A. Protocol analyzer
B. WIPS
C. WLAN controller
D. Spectrum analyzer

Answer: B

QUESTION 120
On which of the following is the level of security set for an Internet zone applied?

A. To the sites that you have specifically indicated as the ones that you trust.
B. To all the Websites by default.
C. To the sites that might potentially damage your computer, or your information.
D. To the Websites and content that are stored on a corporate or business network.

Answer: B