Question: 1

Which of the following does PEAP use to authenticate the user inside an encrypted tunnel?
Each correct answer represents a complete solution. Choose two.

A. AES
B. MS-CHAP v2
C. GTC
D. RC4

Answer: BC

Explanation:
PEAP uses only a server-side certificate. This certificate creates an encrypted tunnel in which the user is authenticated. PEAP (Protected EAP)
uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) or Generic Token Card (GTC) to authenticate the user inside an encrypted tunnel.
What is PEAP?
PEAP (Protected Extensible Authentication Protocol) is a method to securely transmit authentication information over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. PEAP is not an encryption protocol; as with other EAP protocols, it only authenticates a client into a network.
PEAP uses server-side public key certificates to authenticate the server. It creates an encrypted SSL/TLS (Secure sockets layer/Transport layer security) tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key. The resultant exchange of authentication information inside the tunnel to authenticate the client is then encrypted and the user credentials are thus safe and secure.
What is MS-CHAP v2?
Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is the new version of MS-CHAP. MS-CHAP v2 provides the highest level of security and encryption for dial-up connection in the environment consisting of both Windows NT and Windows 2000/XP dial-up clients. It provides mutual authentication, stronger initial data encryption keys,
and different encryption keys for sending and receiving data.
What is GTC?
GTC (Generic Token Card) is an alternative to PEAP-MSCHAPv2. GTC is used by the PEAP authentication protocol to tunnel password data that is used for token cards and plaintext authentication. It carries a text challenge from an authentication server and a reply that is generated by a security token. GTC does not generate session keys to secure network traffic.
Answer option D is incorrect. RC4 is a stream cipher designed by Ron Rivest. It is used in many applications, including Transport Layer Security (TLS), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), etc. RC4 is fast and simple. However, it has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded, nonrandom or related keys are used, or a single keystream is used twice. Some ways of using RC4 can lead to very insecure cryptosystems such as WEP.
Answer option A is incorrect. AES (Advanced Encryption Standard) is an encryption method used in WPA and WPA2.
What is AES?

The Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192, and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable. It became effective as a standard on May 26, 2002. As of 2009, AES is one of the most popular algorithms used in symmetric key cryptography. It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information.

Question: 2

Which of the following attacks are considered as authentication attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Man-in-the-middle attack
B. Denial-of-Service (DoS) attack
C. Jamming attack
D. Eavesdropper attack

Answer: AD

Explanation:
Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client.
Eavesdropping is the process of listening in private conversations. It also includes attackers listening in on the network traffic. For example, it can be done over telephone lines (wiretapping), e-mail, instant messaging, and any other method of communication considered private. Answer option C is incorrect. Jamming attacks can be a huge problem for wireless networks. Jamming is a technique that is used to simply shut down the wireless network. A jamming attack is performed whenever a hacker uses passive and active attacks to access valuable information from the network.
Answer option B is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers make Denial-of-Service attacks by sending a large number of protocol packets to a network. A DoS attack can cause the following to occur:
Saturate network resources. Disrupt connections between two computers, thereby preventing communications between services. Disrupt services to a specific computer.
A SYN attack is a common DoS technique in which an attacker sends multiple SYN packets to a target computer. For each SYN packet received, the target computer allocates resources and sends an acknowledgement (SYN-ACK) to the source IP address. Since the target computer does
not receive a response from the attacking computer, it attempts to resend the SYN-ACK. This leaves TCP ports in the half-open state. When an attacker sends TCP SYNs repeatedly before the half-open connections are timed out, the target computer eventually runs out of resources and is unable to handle any more connections, thereby denying service to legitimate users.

Question: 3

Which of the following keys is used to encrypt and decrypt all broadcast and multicast transmissions between the supplicant and an authenticator?

A. Master Key
B. Temporal Key
C. Group Temporal Key
D. Pairwise Transient Key

Answer: C

Explanation:
Group Temporal Key (GTK) is used to encrypt and decrypt all broadcast and multicast transmissions between the supplicant and an authenticator.
Answer option D is incorrect. Pairwise Transient Key (PTK) is used to encrypt and decrypt all unicast transmissions between the supplicant and an authenticator. Each PTK is used uniquely between each individual supplicant and an authenticator.
Answer option B is incorrect. Temporal Key is used in encrypting and decrypting the MSDU payload of IEEE 802.11 data frames between the supplicant and an authenticator.
Answer option A is incorrect. Master Key is not used in encrypting and decrypting IEEE 802.11 data frames.

Question: 4

You work as a System Administrator for Tech Perfect Inc. The company has a wireless LAN network. You want to implement a tool in the company's network, which monitors the radio spectrum used by the wireless LAN network, and immediately alerts you whenever a rogue access point is detected in the network. Which of the following tools will you use?

A. Firewall
B. WIPS
C. MFP
D. NAT

Answer: B

Explanation:
Wireless intrusion prevention system (WIPS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.
Rogue devices can spoof MAC address of an authorized network device as their own. WIPS uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.

Answer option D is incorrect. Network address translation (NAT) is a technique that allows multiple computers to share one or more IP addresses. NAT is configured at the server between a private network and the Internet. It allows the computers in a private network to share a global, ISP assigned address. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from public to private. Answer option A is incorrect. A firewall is a combination of software and hardware that prevents data packets from coming in or going out of a specified network or computer. It is used to separate an internal network from the Internet. It analyzes all the traffic between a network and the Internet, and provides centralized access control on how users should use the network. A firewall can also perform the following functions:
Block unwanted traffic.
Direct the incoming traffic to more trustworthy internal computers.
Hide vulnerable computers that are exposed to the Internet.
Log traffic to and from the private network.
Hide information, such as computer names, network topology, network device types, and internal user IDs from external users.
Answer option C is incorrect. MFP (Management Frame Protection) is a method used to detect spoofed management frames. A user can avoid the vulnerabilities by enabling MFP in the Cisco wireless LAN. MFP works with the controller-based thin-AP architecture and the Cisco IOS software-based autonomous APs when they are used in combination with the Cisco Wireless LAN Solutions Engine.
Cisco WLAN systems place a digital signature into the management frame. This signature is a field with an encrypted hash to check the message integrity. Only an authorized AP can create it and an authorized receiver can validate the signature. Packets that arrive without digital signatures are ignored.

Question: 5

Which of the following monitors program activities and modifies malicious activities on a system?

A. NIDS
B. Back door
C. RADIUS
D. HIDS

Answer: D

Explanation:
Host-based IDS (HIDS) is an Intrusion Detection System that runs on the system to be monitored. HIDS monitors only the data that is directed to or originating from that particular system on which HIDS is installed. Besides network traffic for detecting attacks, it can also monitor other parameters of the system such as running processes, file system access and integrity, and user logins for identifying malicious activities.
BlackIce Defender and Tripwire are good examples of HIDS. Tripwire is an HIDS tool that automatically calculates the cryptographic hashes of all system files as well as any other files that a network administrator wants to monitor for modifications. It then periodically scans all monitored files and recalculates information to see whether or not the files have been modified. It raises an alarm if changes are detected.
Answer option C is incorrect. RADIUS is an industry standard protocol to authenticate, authorize, and account for access server connections.

Answer option B is incorrect. Back door is a program or account that allows access to a system by skipping the security checks. Many vendors and developers implement back doors to save time and effort by skipping the security checks while troubleshooting. Back door is considered to be a security threat and should be kept with the highest security. If a back door becomes known to attackers and malicious users, they can use it to exploit the system.
Answer option A is incorrect. A Network-based Detection System (NIDS) analyzes data packets flowing through a network. It can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. It is responsible for detecting anomalous or inappropriate data that may be considered 'unauthorized' on a network. An NIDS captures and inspects all data traffic, regardless of whether or not it is permitted for checking.

Question: 6

Which of the following EAP protocols is primarily developed for second generation (2G) mobile networks?

A. EAP-AKA
B. EAP-FAST
C. EAP-SIM
D. EAP-TTLS

Answer: C

Explanation:
EAP-Subscriber Identity Module (EAP-SIM) is primarily developed for second generation (2G) mobile networks. Extensible Authentication Protocol Method for GSM Subscriber Identity Module, or EAP-SIM, is an Extensible Authentication Protocol (EAP) mechanism for authentication and session key distribution using the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM).
GSM cellular networks use a subscriber identity module (SIM) card to carry out user authentication. EAP-SIM uses a SIM authentication algorithm between the client and an Authentication, Authorization, and Accounting (AAA) server providing mutual authentication between the client and the network.
Answer option A is incorrect. EAP-Authentication and Key Agreement (EAP-AKA) is primarily developed for third generation (3G) mobile networks. Answer option B is incorrect. EAP-FAST (Flexible Authentication via Secure Tunneling) is a protocol proposal by Cisco Systems as a replacement
for LEAP. The protocol was designed to address the weaknesses of LEAP while preserving the "lightweight" implementation. Use of server certificates is optional in EAP-FAST. EAP-FAST uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are
verified.
Answer option D is incorrect. EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. It is widely supported across platforms; although there is no native OS support for this EAP protocol in Microsoft Windows, it requires the installation of small extra programs such as SecureW2. EAP-TTLS offers very good security. The client can but does not have to be authenticated via a CA-signed PKI certificate to the server. This greatly simplifies the setup procedure, as a certificate does not need to be installed on every client. After the server is securely authenticated to the client via its CA certificate and optionally the client to the server, the server can then use the established secure connection ("tunnel") to authenticate the client.

Question: 7

Which of the following keys are used by the symmetric key algorithm?
Each correct answer represents a complete solution. Choose all that apply.

A. Group Temporal Key
B. Pairwise Transient Key
C. Private Key
D. Public Key

Answer: C

Explanation:
Private keys are used by the symmetric key algorithm.
What is private key?
In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages.
Answer option D is incorrect. A Public Key is known commonly to everybody. It is used to encrypt data. Only specific users can decrypt it. Data encryption is used to encrypt data so that it can only be decrypted with the corresponding private key owned by the public key owner. The public key is also used to verify digital signatures. This signature is created by the associated private key.
Answer option B is incorrect. Pairwise Transient Key (PTK) is a 64-byte key that comprises the following:
16 bytes of EAPOL-Key Confirmation Key (KCK): This key is used to compute MIC on WPA EAPOL Key message. 16 bytes of EAPOL-Key Encryption Key (KEK): AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client. 16 bytes of Temporal Key (TK): This key is used to encrypt/decrypt unicast data packets.
8 bytes of Michael MIC Authenticator Tx Key: This key is used to compute MIC on unicast data packets transmitted by the AP. 8 bytes of Michael MIC Authenticator Rx Key: This key is used to compute MIC on unicast data packets transmitted by the station.Pairwise Transient Key is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Authenticator
nonce (A Nonce), and Supplicant nonce (S Nonce) using pseudo-random function (PRF).
Answer option A is incorrect. Group Temporal Key (GTK) is a random value that is assigned by the broadcast/multicast source. It is used to protect broadcast/multicast medium access control (MAC) protocol data units. It is derived from a group master key (GMK).

Question: 8

Which of the following keys are types of pairwise transient key (PTK)?
Each correct answer represents a complete solution. Choose all that apply.

A. Temporal Key (TK)
B. Key Encryption Key (KEK)
C. Key Confirmation Key (KCK)
D. STSL Transient Key (STK)

Answer: ABC

Explanation:
Following are the types of pairwise transient key (PTK):

Key Confirmation Key (KCK): Key Confirmation Key (KCK) provides data integrity during the 4-way handshake and group key handshake processes. It binds the pairwise master key (PMK) to the AP.
Key Encryption Key (KEK): Key Encryption Key (KEK) provides data privacy during the 4-way handshake and group key handshake processes.
Temporal Key (TK): Temporal key (TK) encrypts and decrypts the MSDU payload of the IEEE 802.11 data frames between the client and the AP.Answer option D is incorrect. The STSL Transient Key (STK) is used in the peerkey handshake process.
What is Pairwise Transient Key?
Pairwise Transient Key (PTK) is a 64-byte key that comprises the following:
16 bytes of EAPOL-Key Confirmation Key (KCK): This key is used to compute MIC on WPA EAPOL Key message. 16 bytes of EAPOL-Key Encryption Key (KEK): AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client. 16 bytes of Temporal Key (TK): This key is used to encrypt/decrypt unicast data packets. 8 bytes of Michael MIC Authenticator Tx Key: This key is used to compute MIC on unicast data packets transmitted by the AP. 8 bytes of Michael MIC Authenticator Rx Key: This key is used to compute MIC on unicast data packets transmitted by the station.Pairwise Transient Key is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address
(SPA), Authenticator nonce (A Nonce), and Supplicant nonce (S Nonce) using pseudo-random function (PRF).

Question: 9

Fill in the blank with the appropriate term.
_____ is a hacking technique of changing an assigned Media Access Control (MAC) address of a networked device to a different one.

A. MAC spoofing

Answer: A

Explanation: MAC spoofing (or Identity theft) attack occurs when a cracker is able to listen on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only the authorized computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network "sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires and can easily get around that hurdle. MAC Spoofing is a technique of changing an assigned Media Access Control (MAC) address of a networked device to a different one. The changing of the assigned MAC address may allow the bypassing of access control lists on the servers or routers, either hiding a computer on a network or allowing it, to impersonate another computer.

Question: 10

Which of the following is a type of security management for computers and networks in order to identify security breaches?

A. EAP
B. IPS
C. IDS
D. ASA

Answer: C

Explanation:
Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network. Intrusion detection functions include the following:
Monitoring and analyzing both user and system activities
Analyzing system configurations and vulnerabilities
Assessing system and file integrity
Ability to recognize patterns typical of attacks
Analysis of abnormal activity patterns
Tracking user policy violations
Answer option B is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, the IPS can drop the offending packets while still allowing all other traffic to pass. Answer option D is incorrect. Adaptive Security Appliance (ASA) is a new generation of network security hardware of Cisco. ASA hardware acts
as a firewall, in other security roles, and in a combination of roles. The Cisco ASA includes the following components: Anti-x: Anti-x includes whole class of security tools such as Anti-virus, Anti-spyware, Anti-spam, etc. Intrusion Detection and Prevention: Intrusion Detection and Prevention includes tools such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for sophisticated kinds of attacks. Note: Earlier Cisco sold firewalls with the proprietary name PIX firewall. ASA is the new edition of security solutions by Cisco. Answer option A is incorrect. Extensible Authentication Protocol, or EAP, is a universal authentication framework frequently used in wireless networks and Point-to-Point connections. It is defined in RFC 3748, which has been updated by RFC 5247. Although the EAP protocol is not limited to wireless LANs and can be used for wired LAN authentication, it is most often used in wireless LANs. The WPA and WPA2 standard has officially adopted five EAP types as its official authentication mechanism. EAP is an authentication framework, not a specific authentication
mechanism. The EAP provides some common functions and a negotiation of the desired authentication mechanism.