PW0-204

CWNP

Wireless LAN Security

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=PW0-204

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your PW0-204 exam in first attempt, but also you can get a high score to acquire CWNP certification.

If you use pass4sureofficial PW0-204 Certification questions and answers, you will experience actual PW0-204 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our CWNP exam prep covers over 95% of the questions and answers that may be appeared in your PW0-204 exam. Every point from pass4sure PW0-204 PDF, PW0-204 review will help you take CWNP PW0-204 exam much easier and become CWNP certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial CWNP PW0-204 course:

** Up-to-Date CWNP PW0-204 questions taken from the real exam.*
** 100% correct CWNP PW0-204 answers you simply can't find in other PW0-204 courses.*
** All of our tests are easy to download. Your file will be saved as a PW0-204 PDF.*
** CWNP PW0-204 brain dump free content featuring the real PW0-204 test questions.*

CWNP PW0-204 certification exam is of core importance both in your Professional life and CWNP certification path. With CWNP certification you can get a good job easily in the market and get on your path for success. Professionals who passed CWNP PW0-204 exam training are an absolute favorite in the industry. You will pass CWNP PW0-204 certification test and career opportunities will be open for you.

QUESTION: 1
Which of the following protocols is used to provide on-demand authentication within an ongoing data transmission?

A. LEAP
B. EAP
C. PPTP
D. CHAP

Answer: D

Explanation:
The Challenge Handshake Authentication Protocol (CHAP) is used to provide on-demand authentication within an ongoing data transmission. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that uses a secure form of encrypted authentication. Using CHAP, network dial-up connections are able to securely connect to almost all PPP servers.Answer option A is incorrect. LEAP (Lightweight Extensible Authentication Protocol) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication between a wireless client and a RADIUS server. LEAP allows clients to re-authenticate frequently. The clients get a new WEP key upon each successful authentication.Answer option C is incorrect. Point-to-Point Tunneling Protocol (PPTP) is a remote access protocol. It is an extension of the Point-to-Point Protocol (PPP). PPTP is used to securely connect to a private network by a remote client using a public data network, such as the Internet.
Virtual private networks (VPNs) use the tunneling protocol to enable remote users to access corporate networks securely across the Internet. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection. Answer option B is incorrect. Extensible Authentication Protocol (EAP) is an authentication protocol that provides support for a wide range of authentication methods, such as smart cards, certificates, one-time passwords, public keys, etc. It is an extension to Point-to-Point Protocol (PPP), which allows the application of arbitrary authentication mechanisms for the validation of a PPP connection.

QUESTION: 2
Which of the following is a common Windows authentication protocol used by the IEEE 802.1X security standard?

A. TACACS
B. LDAP
C. RADIUS
D. SSL/TLS

Answer: C

Explanation:
Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service. When a person or device connects to a network often authentication is required. RADIUS is commonly used by ISPs and corporations managing access to the Internet or internal networks employing a variety of networking technologies, including modems, DSL, wireless and VPNs. It is a common Windows authentication protocol used by the IEEE 802.1X security standard. Answer option A is incorrect. Terminal Access Controller Access-Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon. It uses UDP port 49 as the default port.Answer option B is incorrect. Lightweight Directory Access Protocol (LDAP) is a protocol used to query and modify information stored within directory services. Answer option D is incorrect. The Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) protocols are used to provide transport level security for Web services applications.

QUESTION: 3
Which of the following authentication processes are specified by the IEEE 802.11 standards? Each correct answer represents a complete solution. Choose all that apply.

A. Open System authentication
B. RADIUS
C. Shared Key authentication
D. EAP

Answer: AC

Explanation:
Open System authentication is the default authentication method used by 802.11 devices. But, in fact, it provides no authentication at all. It exchanges messages between the two wireless devices without using any password or keys. A device configured to use the Open System authentication cannot refuse to authenticate

another device.Shared key authentication is an authentication method specified in the 802.11 standard. In this authentication, a static WEP key should be configured on the client. The shared key authentication has the following processes:
1. The client makes a request to the access point for shared key authentication by sending an authentication request.
2. The access point sends authentication response to the client. Authentication response contains challenge text in a clear text format.
3. The client uses its locally configured WEP key to encrypt the challenge text and replies with a subsequent authentication request.
4. If the access point can decrypt the authentication request and retrieve the original challenge text, then it responds with an authentication response that allows the client to access the network.
Answer option B is incorrect. The radius-server key command is used to set the authentication and encryption key for all RADIUS communications between the switch and the RADIUS server. This command runs in the global configuration mode of the switch. In order to disable the key, the no form of this command is used.
Syntax:
Switch(config)#radius-server key {string}
Where the word string is a key used to set authentication and encryption for all RADIUS communications between the switch and the RADIUS server. Answer option D is incorrect. Extensible Authentication Protocol (EAP) is an authentication protocol that provides support for a wide range of authentication methods, such as smart cards, certificates, one-time passwords, public keys, etc. It is an extension to Point-to-Point Protocol (PPP), which allows the application of arbitrary authentication mechanisms for the validation of a PPP connection.

QUESTION: 4
Which of the following methods are capable of operating in wireless networks? Each correct answer represents a complete solution. Choose all that apply.

A. EAP-TLS
B. LEAP
C. PEAP
D. EAP-TTLS

Answer: BAD

Explanation:
The methods that are capable of operating in wireless networks are as follows:
LEAP: The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary EAP method developed by Cisco Systems prior to the IEEE ratification of the 802.11i security standard. There is no native support for LEAP in any Windows operating system, but it is widely supported by third-party client software most commonly

included with WLAN (wireless LAN) devices. Due to the wide adoption of LEAP in the networking industry, many other WLAN vendors claim support for LEAP.EAP-TLS: EAP-Transport Layer Security (EAP-TLS) is an IETF open standard and is well-supported among wireless vendors. The security of the TLS protocol is strong, provided the user understands potential warnings about false credentials. It uses PKI to secure communication to a RADIUS authentication server or another type of authentication server. EAP-TTLS: 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. Answer option C is incorrect. PEAP is not a method operated in wireless networks.

QUESTION: 5
John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

A. Rainbow attack
B. DoS attack
C. Replay attack
D. ARP spoofing

Answer: B

Explanation:
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 a network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to the network. The effects of a DoS attack are as follows:
Saturates network resources
Disrupts connections between two computers, thereby preventing communications between services
Disrupts services to a specific computer
Causes failure to access a Web site
Results in an increase in the amount of spam

A Denial-of-Service attack is very common on the Internet because it is much easier to accomplish.
Most of the DoS attacks rely on the weaknesses in the TCP/IP protocol.Answer option C is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet.Answer option D is incorrect. Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The attack can only be used on networks that actually make use of ARP and not another method of address resolution. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. Generally, the aim is to associate the attacker's MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it. ARP spoofing attacks can be run from a compromised host, or from an attacker's machine that is connected directly to the target Ethernet segment. Answer option A is incorrect. The rainbow attack is the fastest method of password cracking. This method of password cracking is implemented by calculating all the possible hashes for a set of characters and then storing them in a table known as the Rainbow table. These password hashes are then employed to the tool that uses the Rainbow algorithm and searches the Rainbow table until the password is not fetched.

QUESTION: 6
Which of the following protocols uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers?

A. TFTP
B. HTTPS
C. SCP
D. SSL

Answer: D

Explanation:
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport

Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. URLs that require an SSL connection start with https: instead of http:.Answer option C is incorrect. The SCP protocol sends data in encrypted format. It is used to prevent potential packet sniffers from extracting usable information from data packets. The protocol itself does not provide authentication and security; it relies on the underlying protocol, SSH, to provide these features. SCP can interactively request any passwords or passphrases required to make a connection to a remote host, unlike rcp that fails in this situation.The SCP protocol implements file transfers only. It does so by connecting to the host using SSH and there executes an SCP server (scp). The SCP server program is typically the same program as the SCP client. Answer option A is incorrect. Trivial File Transfer Protocol (TFTP) is a file transfer protocol, with the functionality of a very basic form of File Transfer Protocol (FTP). TFTP can be implemented in a very small amount of memory. It is useful for booting computers such as routers which did not have any data storage devices. It is used to transfer small amounts of data between hosts on a network, such as IP phone firmware or operating system images when a remote X Window System terminal or any other thin client boots from a network host or server. The initial stages of some network based installation systems (such as Solaris Jumpstart, Red Hat Kickstart and Windows NT's Remote Installation Services) use TFTP to load a basic kernel that performs the actual installation. TFTP uses UDP port 69 for communication.Answer option B is incorrect. Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure (website security testing) identification of the server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.Difference from HTTP As opposed to HTTP URLs which begin with "http://" and use port 80 by default, HTTPS URLs begin with "https://" and use port 443 by default.HTTP is insecure and is subject to man-in-the-middle and eavesdropping attacks which can let attackers gain access to website accounts and sensitive information. HTTPS is designed to withstand such attacks and is considered secure.

QUESTION: 7
You have been hired to perform a penetration test on a client's network. You want to see if remote connections are susceptible to eavesdropping or perhaps session hijacking. Which network tool would be most helpful to you?

A. Vulnerability analyzer
B. Port scanner
C. Performance analyzer.
D. Protocol analyzer

Answer: D

Explanation:
A protocol analyzer allows you to view a network conversation and to see the text in English. If the conversation is not encrypted a protocol analyzer will quickly discover this vulnerability.Answer option B is incorrect. A port scanner can be used to find vulnerable ports and services, but not weaknesses in remote connections.

QUESTION: 8
Which of the following wireless network security solutions refers to an authentication process in which a user can connect wireless access points to a centralized server to ensure that all hosts are properly authenticated?

A. Remote Authentication Dial-In User Service (RADIUS)
B. IEEE 802.1x
C. Wired Equivalent Privacy (WEP)
D. Wi-Fi Protected Access 2 (WPA2)

Answer: B

Explanation:
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails.IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802 which is known as "EAP over LANs" or EAPOL. EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ISO 9314-2) in 802.1X-2004. The EAPOL protocol was also modified for use with IEEE 802.1AE (MACSec) and IEEE 802.1AR (Secure Device Identity / DevID) in 802.1X-2010. Answer option C is incorrect. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security, which is equivalent to wired networks, for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream.Answer option A is incorrect. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems,

DSL, access points, VPNs, network ports, Web servers, etc.RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server, are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine. RADIUS serves three functions: To authenticate users or devices before granting them access to a network.To authorize those users or devices for certain network services. To account for usage of those services. Answer option D is incorrect. WPA2 is an updated version of WPA. This standard is also known as IEEE 802.11i. WPA2 offers enhanced protection to wireless networks than WPA and WEP standards. It is also available as WPA2-PSK and WPA2-EAP for home and enterprise environment respectively.You work as a Network Administrator for uCertify Inc. You need to secure web services of your company in order to have secure transactions.

QUESTION: 9
Which of the following will you recommend for providing security?

A. HTTP
B. VPN
C. SSL
D. S/MIME

Answer: C

Explanation:
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. URLs that require an SSL connection start with https: instead of http:. Answer options D is incorrect. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy, and data security (using encryption).Answer options A is incorrect. Hypertext Transfer Protocol (HTTP) is a client/server TCP/IP protocol used on the World Wide Web (WWW) to display Hypertext Markup Language (HTML) pages. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example,

when a client application or browser sends a request to the server using HTTP commands, the server responds with a message containing the protocol version, success or failure code, server information, and body content, depending on the request. HTTP uses TCP port 80 as the default port.Answer option B is incorrect. A Virtual Private Network (VPN) is a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet.John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows: It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

QUESTION: 10
Which of the following tools is John using to crack the wireless encryption keys?

A. Kismet
B. AirSnort
C. Cain
D. PsPasswd

Answer: B

Explanation:
AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option A is incorrect. Kismet is an IEEE 802.11 wireless network sniffer and intrusion detection system.John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

QUESTION: 11
Which of the following tools is John using to crack the wireless encryption keys?

A. Kismet
B. AirSnort
C. Cain
D. PsPasswd

Answer: B

Explanation:
AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option A is incorrect. Kismet is an IEEE 802.11 wireless network sniffer and intrusion detection system. Fact what is Kismet? Hide Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless car that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a,802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets
To detect standard named networks
To detect masked networks
To collect the presence of non-beaconing networks via data traffic
Answer option C is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking,Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:
Dictionary attack Brute force attack Rainbow attack Hybrid attack
Answer option D is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows:

QUESTION: 12
Which of the following are the important components of the IEEE 802.1X architecture? Each correct answer represents a complete solution. Choose all that apply.

A. Authenticator server
B. Extensible Authentication Protocol (EAP)
C. Supplicant
D. Authenticator

Answer: CAD

Explanation:
The 802.1X standard is designed to enhance the security of wireless local area networks (WLANs) that follow the IEEE 802.11 standards.IEEE 802.1X provides an

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	SNIA