Vendor: GIAC

Exam Code: GPEN

Exam Name: GIAC Penetration Tester

Version: DEMO

QUESTION 1
Which of the following are the scanning methods used in penetration testing?
Each correct answer represents a complete solution. Choose all that apply.

A. Vulnerability
B. Port
C. Network
D. Services

Answer: ABC

QUESTION 2
An executive in your company reports odd behavior on her PDA. After investigation you discover that a trusted device is actually copying data off the PDA. The executive tells you that the behavior started shortly after accepting an e-business card from an unknown person. What type of attack is this?

A. Session Hijacking
B. PDA Hijacking
C. Privilege Escalation
D. Bluesnarfing

Answer: D

QUESTION 3
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?

A. TCP FTP proxy scanning
B. Eavesdropping
C. Web ripping
D. Fingerprinting

Answer: C

QUESTION 4
Which of the following statements is true about the Digest Authentication scheme?

A. In this authentication scheme, the username and password are passed with every request, not just when the user first types them.
B. A valid response from the client contains a checksum of the username, the password, the given random value, the HTTP method, and the requested URL.
C. The password is sent over the network in clear text format.
D. It uses the base64 encoding encryption scheme.

Answer: B

QUESTION 5
Which of the following tools is used to verify the network structure packets and confirm that the packets are constructed according to specification?

A. EtherApe
B. Snort decoder
C. AirSnort
D. snort_inline

Answer: B

QUESTION 6
Which of the following is NOT an example of passive footprinting?

A. Scanning ports.
B. Analyzing job requirements.
C. Performing the whois query.
D. Querying the search engine.

Answer: A

QUESTION 7
You work as a Network Administrator for Infosec Inc. Nowadays, you are facing an unauthorized access in your Wi-Fi network. Therefore, you analyze a log that has been recorded by your favorite sniffer, Ethereal. You are able to discover the cause of the unauthorized access after noticing the following string in the log file:

(Wlan.fc.type_subtype eq 32 and llc.oui eq 0x00601d and llc.pid eq 0x0001)

When you find All your 802.11b are belong to us as the payload string, you are convinced about which tool is being used for the unauthorized access. Which of the following tools have you ascertained?

A. AirSnort
B. Kismet
C. AiroPeek
D. NetStumbler

Answer: D

QUESTION 8
Which of the following options holds the strongest password?

A. california
B. $#164aviD^%
C. Admin1234
D. Joe12is23good

Answer: B

QUESTION 9
Which of the following encryption modes are possible in WEP?
Each correct answer represents a complete solution. Choose all that apply.

A. No encryption
B. 256 bit encryption
C. 128 bit encryption
D. 40 bit encryption

Answer: ACD

QUESTION 10
Which of the following tools can be used to perform brute force attack on a remote database?
Each correct answer represents a complete solution. Choose all that apply.

A. FindSA
B. SQLDict
C. nmap
D. SQLBF

Answer: ABD

QUESTION 11
Which of the following statements are true about WPA?
Each correct answer represents a complete solution. Choose all that apply.

A. WPA-PSK converts the passphrase into a 256-bit key.
B. WPA provides better security than WEP.
C. WPA-PSK requires a user to enter an 8-character to 63-character passphrase into a wireles s client.
D. Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used.

Answer: ABCD

QUESTION 12
Which of the following are the limitations for the cross site request forgery (CSRF) attack?
Each correct answer represents a complete solution. Choose all that apply.

A. The target site should have limited lifetime authentication cookies.
B. The attacker must target a site that doesn't check the referrer header.
C. The target site should authenticate in GET and POST parameters, not only cookies.
D. The attacker must determine the right values for all the form inputs.

Answer: BD

QUESTION 13
You want to integrate the Nikto tool with nessus vulnerability scanner. Which of the following steps will you take to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. Restart nessusd service.
B. Place nikto.pl file in the /var/www directory.
C. Place nikto.pl file in the /etc/nessus directory.
D. Place the directory containing nikto.pl in root's PATH environment variable.

Answer: AD

QUESTION 14
Which of the following tools can be used to read NetStumbler's collected data files and present street maps showing the logged WAPs as icons, whose color and shape indicates WEP mode and signal strength?

A. NetStumbler
B. StumbVerter
C. WEPcrack
D. Kismet

Answer: B

QUESTION 15
Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

A. Encouraging others to harass the victim
B. False accusations
C. Attempts to gather information about the victim
D. False victimization

Answer: B

QUESTION 16
Which of the following statements are true about MS-CHAPv2?
Each correct answer represents a complete solution. Choose all that apply.

A. It is a connectionless protocol.
B. It can be replaced with EAP-TLS as the authentication mechanism for PPTP.
C. It provides an authenticator-controlled password change mechanism.
D. It is subject to offline dictionary attacks.

Answer: BCD

QUESTION 17
You work as a Network Administrator for Net World International. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. There are ten Sales Managers in the company. The company has recently provided laptops to all its Sales Managers. All the laptops run Windows XP Professional. These laptops will be connected to the company's network through wireless connections. The

company's management wants to implement Shared Key authentication for these laptops. When you try to configure the network interface card of one of the laptops for Shared Key authentication, you find no such option. What will you do to enable Shared Key authentication?

A. Install PEAP-MS-CHAP v2
B. Install Service Pack 1
C. Enable WEP
D. Install EAP-TLS

Answer: C

QUESTION 18
Which of the following ports will you scan to search for SNMP enabled devices in the network?

A. 163
B. 123
C. 151
D. 161

Answer: D

QUESTION 19
Which of the following attacks is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker?

A. DoS
B. Sniffing
C. Man-in-the-middle
D. Brute force

Answer: C

QUESTION 20
In which of the following scanning techniques does a scanner connect to an FTP server and request that server to start data transfer to the third system?

A. Bounce attack scanning
B. Xmas Tree scanning
C. TCP FIN scanning
D. TCP SYN scanning

Answer: A

Thank You for Trying Our Product

PassLeader Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **STNAR2014**