TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **GPEN**

Title : GIAC Certified Penetration Tester

Version : Demo

1.You execute the following netcat command:
c:\target\nc -1 -p 53 -d -e cmd.exe
What action do you want to perform by issuing the above command?
A. Capture data on port 53 and performing banner grabbing.
B. Listen the incoming traffic on port 53 and execute the remote shell.
C. Listen the incoming data and performing port scanning.
D. Capture data on port 53 and delete the remote shell.
Answer: B

2.TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning.?
A. Solaris
B. Red Hat
C. Windows
D. Knoppix
Answer: C

3.You work as a professional Ethical Hacker. You are assigned a project to perform blackhat testing on www.we-are-secure.com. You visit the office of we-are-secure.com as an air-condition mechanic. You claim that someone from the office called you saying that there is some fault in the air-conditioner of the server room. After some inquiries/arguments, the Security Administrator allows you to repair the air-conditioner of the server room.
When you get into the room, you found the server is Linux-based. You press the reboot button of the server after inserting knoppix Live CD in the CD drive of the server. Now, the server promptly boots backup into Knoppix. You mount the root partition of the server after replacing the root password in the /etc/shadow file with a known password hash and salt. Further, you copy the netcat tool on the server and install its startup files to create a reverse tunnel and move a shell to a remote server whenever the server is restarted. You simply restart the server, pull out the Knoppix Live CD from the server, and inform that the air-conditioner is working properly.
After completing this attack process, you create a security auditing report in which you mention various threats such as social engineering threat, boot from Live CD, etc. and suggest the countermeasures to stop booting from the external media and retrieving sensitive data. Which of the following steps have you suggested to stop booting from the external media and retrieving sensitive data with regard to the above scenario?
Each correct answer represents a complete solution. Choose two.
A. Encrypting disk partitions
B. Using password protected hard drives
C. Placing BIOS password
D. Setting only the root level access for sensitive data
Answer: A,B

4.Which of the following statements are true about KisMAC?
A. Data generated by KisMAC can also be saved in pcap format.
B. It cracks WEP and WPA keys by Rainbow attack or by dictionary attack.
C. It scans for networks passively on supported cards.
D. It is a wireless network discovery tool for Mac OS X.
Answer: A,C,D

5.A Web developer with your company wants to have wireless access for contractors that come in to work on various projects. The process of getting this approved takes time. So rather than wait, he has put his own wireless router attached to one of the network ports in his department. What security risk does this present?
A. An unauthorized WAP is one way for hackers to get into a network.
B. It is likely to increase network traffic and slow down network performance.
C. This circumvents network intrusion detection.
D. None, adding a wireless access point is a common task and not a security risk.
Answer: A

6.Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?
A. Man-in-the-middle
B. ARP spoofing
C. Port scanning
D. Session hijacking
Answer: B

7.Which of the following statements are true about SSIDs?
Each correct answer represents a complete solution. Choose all that apply.
A. SSIDs are case insensitive text strings and have a maximum length of 64 characters.
B. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.
C. SSID is used to identify a wireless network.
D. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.
Answer: B,C,D

8.Adam works on a Linux system. He is using Sendmail as the primary application to transmit emails. Linux uses Syslog to maintain logs of what has occurred on the system. Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?
A. /log/var/logd
B. /var/log/logmail
C. /log/var/mailog
D. /var/log/mailog
Answer: D

9.You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup
D.HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
Answer: D

10.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: A,B,C

11.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

12.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

13.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

14.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

15.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

16.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

17.Which of the following options holds the strongest password?
A. california
B. $#164aviD^%
C. Admin1234
D. Joe12is23good
Answer: B

18.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: A,C,D

19.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: A,B,D

20.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: A,B,C,D

21.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: B,D

22.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: A,D

23.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

24.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

25.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: B,C,D

26.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

27.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

28.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

29.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

30.Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?
A. Patent
B. Spam
C. Phishing
D. Artistic license
Answer: A