GSNA Q&As

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/gsna.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

The tool works under Windows 9x/2000. Which of the following tools can be used to automate the MITM attack?

A. Airjack

B. Kismet

C. Hotspotter

D. IKECrack

Correct Answer: A

Airjack is a collection of wireless card drivers and related programs. It uses a program called monkey_jack that is used to automate the MITM attack. Wlan_jack is a DoS tool in the set of airjack tools, which accepts a target source and BSSID to send continuous deauthenticate frames to a single client or an entire network. Another tool, essid_jack is used to send a disassociate frame to a target client in order to force the client to reassociate with the network and giving up the network SSID. Answer: C is incorrect. Hotspotter is a wireless hacking tool that is used to detect rogue access point. It fools users to connect, and authenticate with the hacker\\'s tool. It sends the deauthenticate frame to the victim\\'s computer that causes the victim\\'s wireless connection to be switched to a non-preferred connection. Answer: D is incorrect. IKECrack is an IKE/IPSec authentication crack tool, which uses brute force for searching password and key combinations of Pre-Shared-Key authentication networks. The IKECrack tool undermines the latest Wi-Fi security protocol with repetitive attempts at authentication with random passphrases or keys. Answer: B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card 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:

1.

To identify networks by passively collecting packets

2.

To detect standard named networks

3.

To detect masked networks

4.

To collect the presence of non-beaconing networks via data traffic

QUESTION 2

You work as a Web Deployer for UcTech Inc. You write the element for an application in which you write the sub-element as follows: * Who will have access to the application?

A. Only the administrator

B. No user

C. All users

D. It depends on the application.

Correct Answer: C

The element is a sub-element of the element. It defines the roles that are allowed to access the Web resources specified by the sub-elements. The element

is written in the deployment descriptor as follows:

---------- Administrator Writing Administrator within the

element will allow only the administrator to have access to the resource defined within the element.

QUESTION 3

Which of the following statements about the traceroute utility are true?

A. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.

B. It records the time taken for a round trip for each packet at each router.

C. It is an online tool that performs polymorphic shell code attacks.

D. It generates a buffer overflow exploit by transforming an attack shell code so that the new attack shell code cannot be recognized by any Intrusion Detection Systems.

Correct Answer: AB

Traceroute is a route-tracing utility that displays the path an IP packet takes to reach its destination. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host. This tool also records the time taken for a round trip for each packet at each router that can be used to find any faulty router along the path. Answer: C, D are incorrect. Traceroute does not perform polymorphic shell code attacks. Attacking tools such as AD Mutate are used to perform polymorphic shell code attacks.

QUESTION 4

Which of the following can be the countermeasures to prevent NetBIOS NULL session enumeration in Windows 2000 operating systems?

A. Denying all unauthorized inbound connections to TCP port 53

B. Disabling SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface

C. Editing the registry key HKLM\SYSTEM\CurrentControlSet\LSA and adding the value RestrictAnonymous

D. Disabling TCP port 139/445

Correct Answer: BCD

NetBIOS NULL session vulnerabilities are hard to prevent, especially if NetBIOS is needed as part of the infrastructure.

One or more of the following steps can be taken to limit NetBIOS NULL session vulnerabilities: 1.Null sessions require access to the TCP 139 or TCP 445 port, which can be disabled by a Network Administrator.

2.

A Network Administrator can also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface.

3.

A Network Administrator can also restrict the anonymous user by editing the registry values:

-a.Open regedit32, and go to HKLM\SYSTEM\CurrentControlSet\LSA.

-b.Choose edit > add value. Value name: RestrictAnonymous Data Type: REG_WORD Value: 2

Answer: A is incorrect. TCP port 53 is the default port for DNS zone transfer. Although disabling it can help restrict DNS zone transfer enumeration, it is not useful as a countermeasure against the NetBIOS NULL session enumeration.

QUESTION 5

Which of the following types of attack is described in the statement below?

"It is a technique employed to compromise the security of network switches. In this attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table."

A. Man-in-the-middle

B. Blind spoofing

C. Dictionary

D. MAC flooding

Correct Answer: D

MAC flooding is a technique employed to compromise the security of network switches. In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table. The result of this attack causes the switch to enter a state called fail open mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. A malicious user could then use a packet sniffer (such as Wireshark) running in promiscuous mode to capture sensitive data from other computers (such as unencrypted passwords, e- mail and instant messaging conversations), which would not be accessible were the switch operating normally. Answer: B is incorrect. Blind spoofing is a type of IP spoofing attack. This attack occurs when the attacker is on a different subnet as the destination host. Therefore, it is more difficult to obtain correct TCP sequence number and acknowledgement number of the data frames. In blind spoofing attack, an attacker sends several packets to the target computer so that he can easily obtain sequence number of each data frame. If the attacker is successful in compromising the sequence number of the data frames, the data is successfully sent to the target computer. Answer: C is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. Answer: A is incorrect. 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.

QUESTION 6

Which of the following is an enterprise-grade network/application/performance monitoring platform that tightly integrates with other smart building management systems, such as physical access control, HVAC, lighting, and time/attendance control?

A. Airwave Management Platform

B. Andrisoft WANGuard Platform

C. akk@da

D. Aggregate Network Manager

Correct Answer: D

Aggregate Network Manager is an enterprise-grade network/application/performance monitoring platform that tightly integrates with other smart building management systems, such as physical access control, HVAC, lighting, and time/

attendance control.

Answer: A is incorrect. Airwave Management Platform (AMP) is wireless network management software. It offers centralized control for Wi-Fi networks. Some of its common features are access point configuration management, reporting,

user tracking, help desk views, and rogue AP discovery. Answer: C is incorrect. akk@da is a simple network monitoring system. It is designed for small and middle size computer networks. Its function is to quickly detect the system or network

faults and display the information about detected faults to the administrators. The information is collected by it in every single minute (a user can decrease this period to 1 second). Approximately all the services of the monitored hosts are

discovered automatically.

Answer: B is incorrect. Andrisoft WANGuard Platform offers solutions for various network issues such as WAN links monitoring, DDoS detection and mitigation, traffic accounting, and graphing.

QUESTION 7

Web applications are accessed by communicating over TCP ports via an IP address. Choose the two most common Web Application TCP ports and their respective protocol names. (Choose two) A. TCP Port 443 / S-HTTP or SSL

B. TCP Port 80 / HTTPS or SSL

C. TCP Port 443 / HTTPS or SSL

D. TCP Port 80 / HTTP

Correct Answer: CD

The two most common Web Application TCP ports are Port 443 and Port 80. HTTPS or SSL uses TCP port 443, whereas HTTP uses TCP Port 80.

Answer: B is incorrect. Port 80 is used for HTTP, not HTTPS. Answer: A is incorrect. S-HTTP is not the protocol name for Port 443. HTTPS or SSL is the name used for Port 443 traffic.

QUESTION 8

You work as a Network Administrator for XYZ CORP. The company has a TCP/IP-based network environment. The network contains Cisco switches and a Cisco router.

You run the following command for a router interface:

show interface serial0

You get the following output:

Serial0 is administratively down, line protocol is down

What will be your conclusion after viewing this output?

A. There is a physical problem either with the interface or the cable attached to it.

B. The router has no power.

C. There is a problem related to encapsulation.

D. The interface is shut down.

Correct Answer: D

According to the question, the output displays that the interface is administratively down. Administratively down means that the interface is shut down. In order to up the interface, you will have to open the interface with the no shutdown

command.

Answer: A is incorrect. Had there been a physical problem with the interface, the output would not have displayed "administratively down". Instead, the output would be as follows: serial0 is down, line protocol is down

Answer: B is incorrect. You cannot run this command on a router that is powered off. Answer: C is incorrect. Encapsulation has nothing to do with the output displayed in the question.

QUESTION 9

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows:

A. \whisker.pl -h target_IP_address -- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - = = Host: target_IP_address = Server: Apache/1.3.12 (Win32) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22 + 200 OK: HEAD /cgi-bin/printenv John recognizes /cgi-bin/printenv vulnerability (\\'Printenv\\' vulnerability) in the We_are_secure server. Which of the following statements about \\'Printenv\\' vulnerability are true?

B. With the help of \\'printenv\\' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

C. \\'Printenv\\' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

D. The countermeasure to \\'printenv\\' vulnerability is to remove the CGI script.

E. This vulnerability helps in a cross site scripting attack.

Correct Answer: ACD

\\'Printenv\\' vulnerability allows an attacker to input specially crafted links and/or other malicious scripts. For example, http://www/cgi-bin/printenv/alert (An attacker can misuse it!) Since \\'printenv\\' is just an example CGI script (It comes with various versions of the Apache Web server.) that has no real use and has its own problems, there is no problem in removing it. Answer: B is incorrect. \\'Printenv\\' does not maintain any log file of user activities.

QUESTION 10

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to make changes on a per-directory basis.

Which of the following Unix configuration files can you use to accomplish the task?

A. $HOME/.profile

B. $HOME/Xrootenv.0

C. $HOME/.htaccess

D. /var/log/btmp

Correct Answer: C

In Unix, the $HOME/.htaccess file provides a way to make configuration changes on a per directory basis. Answer: A is incorrect. In Unix, the $HOME/.profile file contains the user\\'s environment stuff and startup programs. Answer: B is incorrect. In Unix, the $HOME/Xrootenv.0 file contains networking and environment info. Answer: D is incorrect. In Unix, the /var/log/btmp file is used to store information about failed logins.

QUESTION 11

Mike works as a Network Engineer for XYZ CORP. The company has a multi-platform network. Recently, the company faced lots of blended threat issues that lead to several drastic attacks. Mike has been assigned a project to manage the resources and services of the company through both Intranet and Internet to protect the company from these attacks. Mike needs a system that provides auto-discovering and network topology building features to allow him to keep an intuitive view of the IT infrastructure.

What will Mike use to meet the requirement of the project?

A. eBox

B. dopplerVUe

C. David system

D. EM7

Correct Answer: C

David system is a network management system that allows a user to manage the resources and services through both Intranet and Internet. It provides auto-discovering and network topology building features to facilitate in keeping an

intuitive view of the IT infrastructure. The resources, real-time monitoring, and accessibility of historical data facilitate reaction to failures. Configured interfaces for monitored devices permit a user to focus on the most important aspects of their

work. Answer: B is incorrect. dopplerVUe is a network management tool that facilitates network discovery, mapping, alerts and alarm management, and bandwidth management system. It enables monitoring of Ping, SNMP, syslog, and WMI

performance metrics. It can also be used to monitor IPv6 devices, as well as services such as DNS, http, and email.

Answer: A is incorrect. eBox is an open source distribution and web development framework. This framework is used to manage server application configuration. It is based on Ubuntu Linux. It is projected to manage services in a computer

network. The modular design of eBox allows a user to pick and choose the services.

Answer: D is incorrect. EM7 is a network monitoring system that is used to measure IT infrastructure health and performance. It is an NMS integrated system. It is designed to help in optimizing the performance and availability of the networks,

systems, and applications. It facilitates trouble-ticketing, event management, reporting, IP management, DNS, and monitoring.

QUESTION 12

SIMULATION

Fill in the blank with the command to complete the statement below. Do not enter the full path of the command.

The _____ command supports system logging and kernel message trapping.

Correct Answer: sysklogd

The sysklogd command is used to support system logging and kernel message trapping. Sysklogd includes two system utilities: syslogd and klogd, which support system logging and kernel message trapping. Since, this utility supports both internet and UNIX domain sockets, it also supports both local and remote logging. Every logged message contains at least a time and a hostname field and sometimes a program name field as well.

QUESTION 13

Andrew works as a Network Administrator for Infonet Inc. The company has a Windows 2003 domain- based network. The network has five Windows 2003 member servers and 150 Windows XP Professional client computers. One of the member servers works as an IIS server. The IIS server is configured to use the IP address 142.100.10.6 for Internet users and the IP address 16.5.7.1 for the local network. Andrew wants the server to allow only Web communication over the Internet. He also wants to enable the local network users to access the shared folders and other resources.

How will Andrew configure the IIS server to accomplish this? (Choose three)

A. Enable the IP packet filter.

B. Permit all the ports on the network adapter that uses the IP address142.100.10.6.

C. Permit only port 25 on the network adapter that uses the IP address 142.100.10.6.

D. Permit all the ports on the network adapter that uses the IP address 16.5.7.1.

E. Permit only port 80 on the network adapter that uses the IP address 142.100.10.6.

Correct Answer: ADE

In order to configure the IIS server to allow only Web communication over the Internet, Andrew will have to use IP packet filtering to permit only port 80 on the network adapter that uses the IP address 142.100.10.6 for connecting to the Internet. This is because Web communication uses the Hyper Text Transfer Protocol (HTTP) that uses the TCP port 80. IP packet filtering restricts the IP traffic received by the network interface by controlling the TCP or UDP port for incoming data. Furthermore, Andrew wants to allow local users to access shared folders and all other resources. Therefore, Andrew will have to enable all the ports on the network adapter that uses the IP address 16.5.7.1 for the local network.

QUESTION 14

Which of the following commands is most useful for viewing large files?

A. cat

B. less

C. touch

D. cp

Correct Answer: B

The less command is most useful for viewing large files. The less command displays the output of a file one page at a time. Viewing large files through cat may take more time to scroll pages, so it is better to use the less command to see the

content of large files.

Answer: A is incorrect. The cat command is also used to view the content of a file, but it is most useful for viewing short files.

Answer: D is incorrect. The cp command is used to copy files and directories from one location to another. Answer: C is incorrect. The touch command is not used to view the content of a file. It is used to create empty files or to update file

timestamps.

QUESTION 15

Zorp is a proxy firewall suite developed by Balabit IT Security. Which of the following statements are true about Zorp?

A. It allows the administrators to fine-tune proxy decisions.

B. Zorp aims for compliance with the Common Criteria/Application Level Firewall Protection Profile for Medium Robustness.

C. It allows full analysis of embedded protocols.

D. The GPL versionof Zorp lacks much of the usability and functions from the other versions.

Correct Answer: ABC

Zorp is a proxy firewall suite developed by Balabit IT Security. Its core framework allows the administrator to fine-tune proxy decisions (with its built-in script language), and fully analyze embedded protocols (such as SSL with an embedded POP3 or HTTP protocol). The FTP, HTTP, FINGER, WHOIS, TELNET, and SSL protocols are fully supported with an application-level gateway. Zorp aims for compliance with the Common Criteria/Application Level Firewall Protection Profile for Medium Robustness. Zorp is released under GNU/GPL and commercial license too. The GPL version is completely usable and functional; however, it lacks some of the more advanced functions available in the commercially available version only. Some of the Zorp supported protocols are Finger, Ftp, Http, Pop3, NNTP, IMAP4, RDP, RPC, SIP, SSL, SSH, Telnet, Whois, LDAP, RADIUS, TFtp, SQLNet NET8, Rsh, etc. Answer: D is incorrect. The GPL version of Zorp is completely usable and functional; however, it lacks some of the more advanced functions available in the commercially available version only.