GNSA Q&As

GIAC Systems and Network Auditor

Pass GIAC GNSA Exam with 100% Guarantee

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

https://www.passapply.com/gnsa.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 the Linux operating system. He wants to use a wireless sniffer to sniff the We-are-secure network.

Which of the following tools will he use to accomplish his task?

A. WEPCrack

B. Kismet

C. Snadboy\\'s Revelation

D. NetStumbler

Correct Answer: B

According to the scenario, John will use Kismet. 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, and802.11n 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: D is incorrect. NetStumbler is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. It detects wireless networks and marks their relative position with a GPS.

Answer: A is incorrect. WEPCrack is an open source tool that breaks IEEE 802.11 WEP secret keys.

Answer: C is incorrect. Snadboy\\'s Revelation is not a sniffer. It is used to see the actual password behind the asterisks.

QUESTION 2

You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem.

Which of the following utilities will you use to diagnose the problem?

A. PING

B. IPCONFIG

C. TRACERT

D. NSLOOKUP

Correct Answer: D

NSLOOKUP is a tool for diagnosing and troubleshooting Domain Name System (DNS) problems. It performs its function by sending queries to the DNS server and obtaining detailed responses at the command prompt. This information can be useful for diagnosing and resolving name resolution issues, verifying whether or not the resource records are added or updated correctly in a zone, and debugging other server-related problems. This tool is installed along with the TCP/IP protocol through the Control Panel. Answer: A is incorrect. The ping command-line utility is used to test connectivity with a host on a TCP/IP-based network. This is achieved by sending out a series of packets to a specified destination host. On receiving the packets, the destination host responds with a series of replies. These replies can be used to determine whether or not the network is working properly. Answer: B is incorrect. IPCONFIG is a command-line utility used to display current TCP/IP network configuration values and update or release the Dynamic Host Configuration Protocol (DHCP) allocated leases. It is also used to display, register, or flush Domain Name System (DNS) names. Answer: C is incorrect. TRACERT is a route-tracing Windows utility that displays the path an IP packet takes to reach the destination. It shows the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.

QUESTION 3

You work as a professional Ethical Hacker. You are assigned a project to perform blackbox testing of the security of www.we-are-secure.com. Now you want to perform banner grabbing to retrieve information about the Webserver being used by we-are-secure.

Which of the following tools can you use to accomplish the task?

A. Wget

B. WinSSLMiM

C. Whisker

D. httprint

Correct Answer: D

According to the scenario, you want to perform banner grabbing to retrieve information about the Webserver being used by we-are-secure. For this, you will use the httprint tool to accomplish the task. httprint is a fingerprinting tool that is

based on Web server characteristics to accurately identify Web servers. It works even when Web server may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask. It can also be

used to detect Web enabled devices that do not contain a server banner string, such as wireless access points, routers, switches, cable modems, etc. httprint uses text signature strings for identification, and an attacker can also add

signatures to the signature database.

Answer: A is incorrect. Wget is a Website copier that is used to analyze the vulnerabilities of a Website offline.

Answer: C is incorrect. Whisker is an HTTP/Web vulnerability scanner that is written in the PERL language. Whisker runs on both the Windows and UNIX environments. It provides functions for testing HTTP servers for many known security

holes, particularly the presence of dangerous CGIs.

Answer: B is incorrect. WinSSLMiM is an HTTPS Man in the Middle attacking tool. It includes FakeCert, a tool used to make fake certificates. It can be used to exploit the Certificate Chain vulnerability in Internet Explorer.

QUESTION 4

The employees of EWS Inc. require remote access to the company\\'s Web servers. In order to provide solid wireless security, the company uses EAP-TLS as the authentication protocol.

Which of the following statements are true about EAP-TLS?

A. It uses password hash for client authentication.

B. It uses a public key certificate for server authentication.

C. It is supported by all manufacturers of wireless LAN hardware and software.

D. It provides a moderate level of security.

Correct Answer: BC

EAP-TLS can use only a public key certificate as the authentication technique. It is supported by all manufacturers of wireless LAN hardware and software. The requirement for a client-side certificate, however unpopular it may be, is what

gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security trade-off.

Answer: D is incorrect. EAP-TLS provides the highest level of security.

Answer: A is incorrect. EAP-TLS uses a public key certificate for server authentication.

QUESTION 5

You are the Security Consultant and you frequently do vulnerability assessments on client computers. You want to have a standardized approach that would be applicable to all of your clients when doing a vulnerability assessment.

What is the best way to do this?

A. Utilize OVAL.

B. Create your own standard and use it with all clients.

C. Utilize each client\\'s security policies when doing a vulnerability assessment for that client.

D. Utilize the Microsoft security recommendations.

Correct Answer: A

Open Vulnerability Assessment Language (OVAL) is a common language for security professionals to use when checking for the presence of vulnerabilities on computer systems. OVAL provides a baseline method for performing vulnerability

assessments on local computer systems.

Answer: D is incorrect. While Microsoft security standards will be appropriate for many of your clients, they won\\'t help

clients using Linux, Macintosh, or Unix. They also won\\'t give you insight into checking your firewalls or routers.

Answer: C is incorrect. This would not fulfill the requirement of having a standardized approach applicable to all clients.

Answer: B is incorrect. This would not be the best way. You should use common industry standards, like OVAL.