DUMPSARENA

GCIA – GIAC Certified Intrusion Analyst Practice Test

GIAC GCIA

Version Demo

Total Demo Questions: 20

Total Premium Questions: 507

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	145
Topic 2, Volume B	146
Topic 3, Volume C	150
Topic 4, Volume D	66
Total	507

QUESTION NO: 1

Which of the following tools allows an attacker to intentionally craft the packets to gain unauthorized access?

Each correct answer represents a complete solution. Choose two.

A. Tcpdump

B. Ettercap

C. Mendax

D. Fragroute

ANSWER: C D

QUESTION NO: 2

Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

A. Netresident

B. Snort

C. Wireshark

D. NetWitness

ANSWER: C

QUESTION NO: 3

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. Active Directory integrated zone has been configured on the network. You want to create a text file that lists the resource records of a specified zone for your record. Which of the following commands will you use to accomplish the task?

A. DNSCMD /createdirectorypartition

B. DNSCMD /copydns

C. DNSCMD /zoneexport

D. DNSCMD /config

ANSWER: C

QUESTION NO: 4 - (SIMULATION)

SIMULATION Fill in the blank with the appropriate facts regarding IP version 6 (IPv6).

IP addressing version 6 uses_____ -bit address. Its____ IP address assigned to a single host allows the host to send and receive data.

ANSWER: 128 unicast -or- 128,unicast -or- 128, unicast

Explanation:

IP addressing version 6 uses 128 -bit address. Its unicast IP address assigned to a single host allows the host to send and receive data.

QUESTION NO: 5

Which of the following tools is used to collect volatile data over a network?

A. Liveview

B. Netcat

C. Pdd

D. FTimes

ANSWER: B

QUESTION NO: 6

Which of the following command line tools are available in Helix Live acquisition tool on Windows? Each correct answer represents a complete solution. Choose all that apply.

A. netstat

B. ipconfig

C. .cab extractors

D. whois

ANSWER: A B C

QUESTION NO: 7

Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses 'Faulkner' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone. Which of the following methods has the attacker used to crack Andrew's password?

Each correct answer represents a complete solution. Choose all that apply.

A. Zero-day attack

B. Dictionary-based attack

C. Rainbow attack

D. Denial-of-service (DoS) attack

E. Brute force attack

F. Buffer-overflow attack

G. Password guessing

H. Social engineering

ANSWER: B C E G H

QUESTION NO: 8

John works as a Network Security Administrator for NetPerfect Inc. The manager of the company has told John that the company's phone bill has increased drastically. John suspects that the company's phone system has been cracked by a malicious hacker. Which attack is used by malicious hackers to crack the phone system?

A. Sequence++ attack

B. Phreaking

C. Man-in-the-middle attack

D. War dialing

ANSWER: B

QUESTION NO: 9

Which of the following TCP/UDP port is used by the toolkit program netstat?

A. Port 23

B. Port 15

C. Port 7

D. Port 69

ANSWER: B

QUESTION NO: 10

Which of the following log files are used to collect evidences before taking the bit-stream image of the BlackBerry?

Each correct answer represents a complete solution. Choose all that apply.

A. user history

B. Transmit/Receive

C. Radio status

D. Roam and Radio

ANSWER: B C D

QUESTION NO: 11

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple smallsized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?

Each correct answer represents a complete solution. Choose all that apply.

A. Nessus

B. Whisker

C. Y.A.T.

D. Fragroute

ANSWER: A B

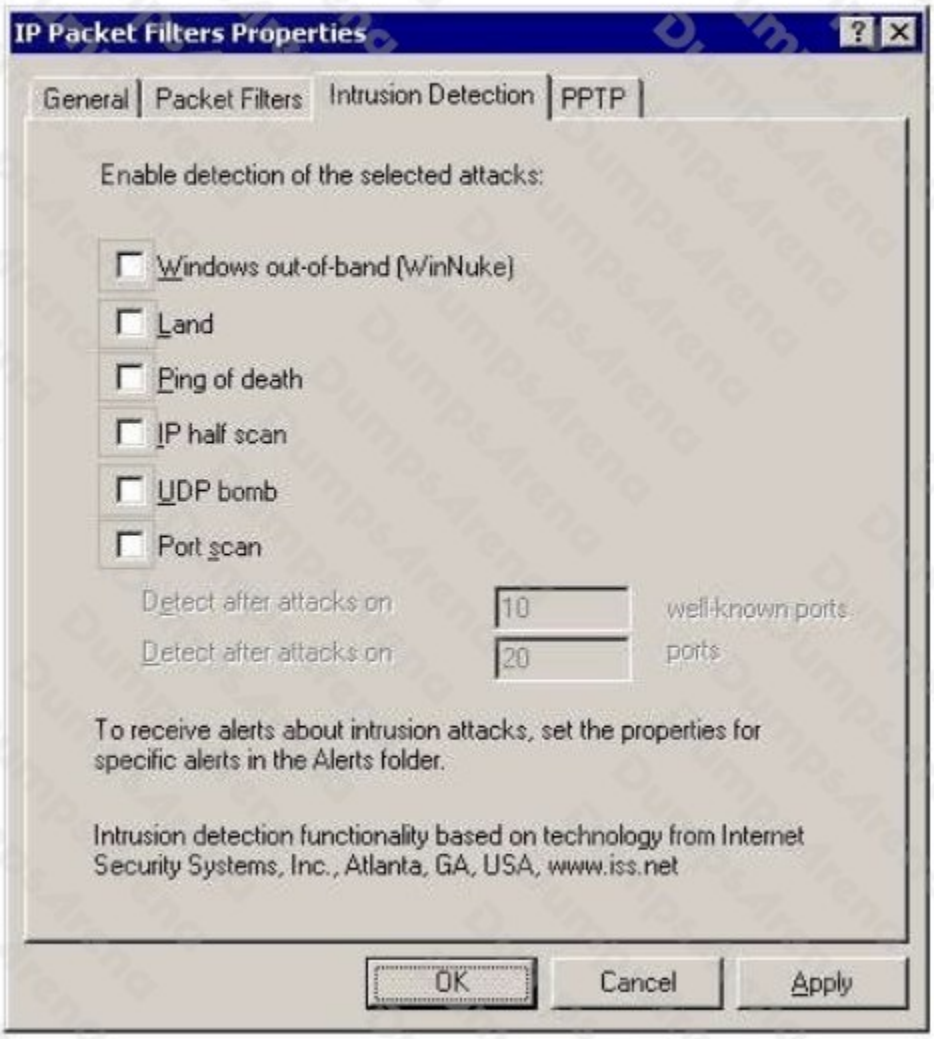
QUESTION NO: 12 - (HOTSPOT)

HOTSPOT

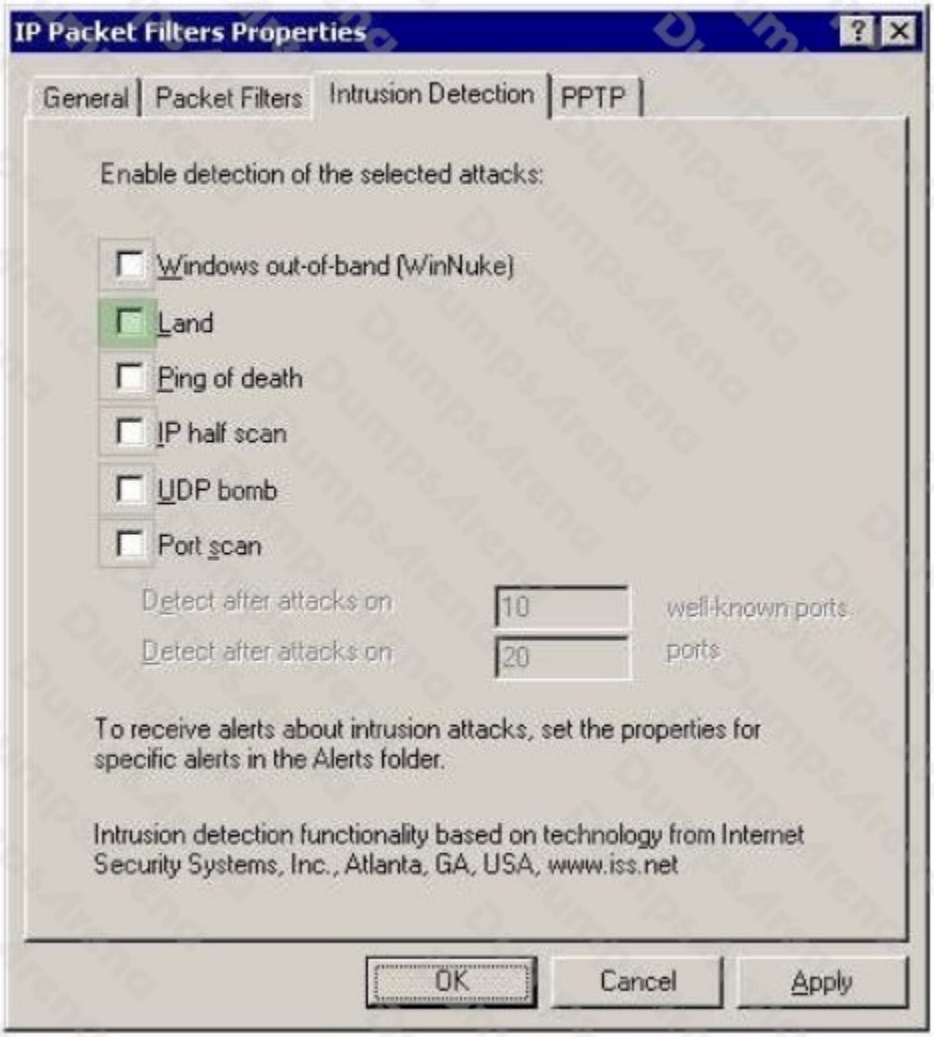
You work as a Network Administrator for McRobert Inc. The company's Windows 2000-based network is configured with Internet Security and Acceleration (ISA) Server 2000. You are configuring intrusion detection on the server. You want to get

notified when a TCP SYN packet is sent with a spoofed source IP address and port number that match the destination IP address and port number. Mark the alert that you will enable on the Intrusion Detection tab page of the IP Packet Filters Properties dialog box to accomplish the task.

Hot Area:



ANSWER:



Explanation:

QUESTION NO: 13

Which of the following NETSH commands for interface Internet protocol version 4 (IPv4) is used to delete a DNS server or all DNS servers from a list of DNS servers for a specified interface or for all interfaces?

A. alter dnsserver

B. delete dnsserver

C. disable dnsserver

D. remove dnsserver

ANSWER: B

QUESTION NO: 14

Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?

Each correct answer represents a complete solution. Choose all that apply.

A. portsentry

B. libnids

C. nmap

D. scanlogd

ANSWER: A B D

QUESTION NO: 15

Adam, an expert computer user, doubts that virus named love.exe has attacked his computer. This virus acquires hidden and read-only attributes, so it is difficult to delete it. Adam decides to delete virus file love.exe from the command line. He wants to use del command for this purpose. Which of the following switches will he use with del command to delete hidden and read onlyfiles?

A. del /f /ah

B. del /q /ar

C. del /p /ar

D. del /q

ANSWER: A

QUESTION NO: 16

Which of the following IP packet elements is responsible for authentication while using IPSec?

A. Internet Key Exchange (IKE)

B. Authentication Header (AH)

C. Layer 2 Tunneling Protocol (L2TP)

D. Encapsulating Security Payload (ESP)

ANSWER: B

QUESTION NO: 17

Which of the following statements about a host-based intrusion prevention system (HIPS) are

true?

Each correct answer represents a complete solution. Choose two.

A. It can detect events scattered over the network.

B. It can handle encrypted and unencrypted traffic equally.

C. It cannot detect events scattered over the network.

D. It is a technique that allows multiple computers to share one or more IP addresses.

ANSWER: B C

QUESTION NO: 18

Which of the following components are usually found in an Intrusion detection system (IDS)? Each correct answer represents a complete solution. Choose two.

A. Sensor

B. Gateway

C. Firewall

D. Modem

E. Console

ANSWER: A E

QUESTION NO: 19

Which of the following ports is used by NTP for communication?

A. 143

B. 123

C. 161

D. 53

ANSWER: B

QUESTION NO: 20

Which of the following are default ports for the FTP service?

Each correct answer represents a complete solution. Choose two.

A. 80

B. 21

C. 20

D. 443

ANSWER: B C