Vendor:GIAC

Exam Code:GSEC

Exam Name:GIAC Security Essentials Certification

Version: Demo

QUESTION 1

The TTL can be found in which protocol header?

A. It is found in byte 8 of the ICMP header.

B. It is found in byte 8 of the IP header.

C. It is found in byte 8 of the TCP header.

D. It is found in byte 8 of the DNS header.

Correct Answer: B

QUESTION 2

Your CIO has found out that it is possible for an attacker to clone your company\\'s RFID (Radio Frequency ID) based key cards. The CIO has tasked you with finding a way to ensure that anyone entering the building is an employee. Which of the following authentication types would be the appropriate solution to this problem?

A. Mandatory Access Controls

B. Bell-LaPadula

C. Two-Factor

D. TACACS

Correct Answer: C

QUESTION 3

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He is currently working on his C based new traceroute program. Since, many processes are running together on the system, he wants to give the highest priority to the cc command process so that he can test his program, remove bugs, and submit it to the office in time. Which of the following commands will John use to give the highest priority to the cc command process?

A. nice -n 19 cc -c *.c and

B. nice cc -c *.c and

C. nice -n -20 cc -c *.c and

D. nice cc -c *.c

Correct Answer: C

QUESTION 4

Which of the following tools is used to query the DNS servers to get detailed information about IP addresses, MX records, and NS servers?

A. NBTSTAT

B. NSLOOKUP

C. PING

D. NETSTAT

Correct Answer: B

QUESTION 5

You have been hired to design a TCP/IP-based network that will contain both Unix and Windows computers. You are planning a name resolution strategy. Which of the following services will best suit the requirements of the network?

A. APIPA

B. LMHOSTS

C. DNS

D. DHCP

E. WINS

Correct Answer: C

QUESTION 6

Which of the following tools is also capable of static packet filtering?

A. netstat.exe

B. ipsecpol.exe

C. ipconfig.exe

D. net.exe

Correct Answer: B

QUESTION 7

If the NET_ID of the source and destination address in an IP (Internet Protocol) packet match, which answer BEST describes the routing method the sending host will use?

A. Local (or direct) routing

B. Circuit switch routing

C. Dynamic (or changeable) routing

D. Remote (or indirect) routing

Correct Answer: A

QUESTION 8

Which of the following BEST describes the two job functions of Microsoft Baseline Security Analyzer (MBSA)?

A. Vulnerability scanner and auditing tool

B. Auditing tool and alerting system

C. Configuration management and alerting system

D. Security patching and vulnerability scanner

Correct Answer: D

QUESTION 9

What does an attacker need to consider when attempting an IP spoofing attack that relies on guessing Initial Sequence Numbers (ISNs)?

A. These attacks work against relatively idle servers.

B. These attacks rely on a modified TCP/IP stack to function.

C. These attacks can be easily traced back to the source.

D. These attacks only work against Linux/Unix hosts.

Correct Answer: A

QUESTION 10

Which Windows event log would you look in if you wanted information about whether or not a specific diver was running at start up?

A. Application

B. System

C. Startup

D. Security

Correct Answer: B

QUESTION 11

You are an Intrusion Detection Analyst and the system has alerted you to an Event of Interest (EOI) that appears to be activity generated by a worm. You investigate and find that the network traffic was normal. How would this type of alert be categorized?

A. False Positive

B. True Negative

C. True Positive

D. False Negative

Correct Answer: A

QUESTION 12

Which of the following is generally practiced by the police or any other recognized governmental authority?

A. Spoofing

B. SMB signing

C. Wiretapping

D. Phishing

Correct Answer: C