Verified GCIH dumps Q&As - 2023 Latest GCIH Download [Q123-Q138

Verified GCIH dumps Q&As - 2023 Latest GCIH Download
Dumps Questions [2023] Pass for GCIH Exam

NO.123 Which of the following is the difference between SSL and S-HTTP?
* SSL operates at the application layer and S-HTTP operates at the network layer.
* SSL operates at the application layer and S-HTTP operates at the transport layer.
* SSL operates at the network layer and S-HTTP operates at the application layer.
* SSL operates at the transport layer and S-HTTP operates at the application layer.

NO.124 You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?
* Containment
* Preparation
* Recovery
* Identification

Section: Volume C

NO.125 Which of the following languages are vulnerable to a buffer overflow attack?

Each correct answer represents a complete solution. Choose all that apply.
* Java
* C++
* C
* Action script

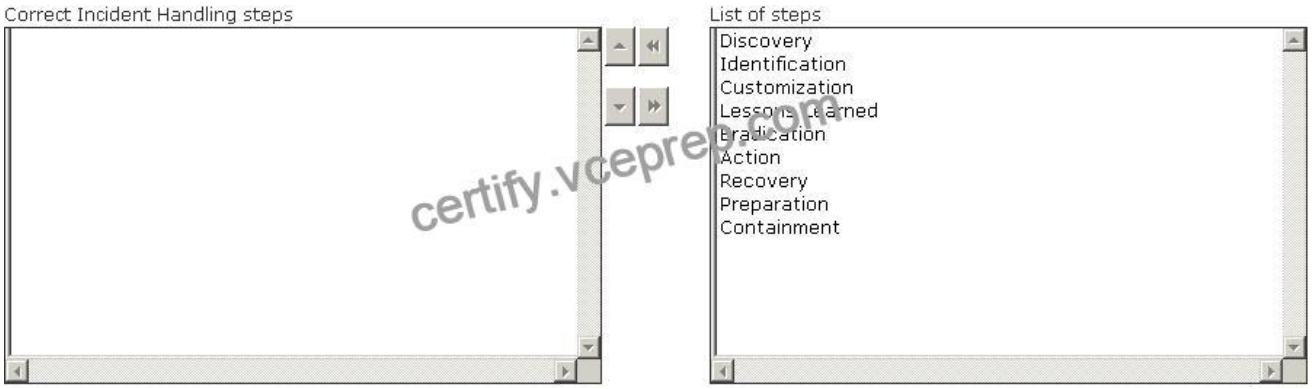
NO.126 Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms.

In order to use this tool on the Windows platform a user must install a packet capture library.

What is the name of this library?
* PCAP
* SysPCap
* WinPCap
* libpcap

NO.127 In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?
* Dos
* DDoS
* Backscatter
* SQL injection

NO.128 Choose and reorder the steps of an incident handling process in their correct order.



NO.129 Which of the following tools can be used for stress testing of a Web server?

Each correct answer represents a complete solution. Choose two.
* Internet bots
* Scripts
* Anti-virus software
* Spyware

Section: Volume A

Explanation

NO.130 SIMULATION

Fill in the blank with the appropriate word.

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft’s /GS option use

_____ defense against buffer overflow attacks.
canary

NO.131 Which of the following statements about Ping of Death attack is true?
* In this type of attack, a hacker sends more traffic to a network address than the buffer can handle.
* This type of attack uses common words in either upper or lower case to find a password.
* In this type of attack, a hacker maliciously cuts a network cable.
* In this type of attack, a hacker sends ICMP packets greater than 65,536 bytes to crash a system.

NO.132 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.
* The attacker must determine the right values for all the form inputs.
* The attacker must target a site that doesn’t check the referrer header.
* The target site should have limited lifetime authentication cookies.
* The target site should authenticate in GET and POST parameters, not only cookies.

Section: Volume C

NO.133 Which of the following attacks can be overcome by applying cryptography?
* Buffer overflow
* Web ripping
* Sniffing
* DoS

Section: Volume B

NO.134 Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network

security of the company. He created a webpage to discuss the progress of the tests with employees who were

interested in following the test. Visitors were allowed to click on a company’s icon to mark the progress of the test.

Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the

network well and allows strict Internet access.

How was security compromised and how did the firewall respond?
* The attack was social engineering and the firewall did not detect it.
* Security was not compromised as the webpage was hosted internally.
* The attack was Cross Site Scripting and the firewall blocked it.
* Security was compromised as keylogger is invisible for firewall.

NO.135 A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows:

l Saturation of network resources

l Disruption of connections between two computers, thereby preventing communications between services

l Disruption of services to a specific computer

l Failure to access a Web site l Increase in the amount of spam

Which of the following can be used as countermeasures against DoS attacks?

Each correct answer represents a complete solution. Choose all that apply.
* Blocking undesired IP addresses
* Applying router filtering
* Disabling unneeded network services
* Permitting network access only to desired traffic

NO.136 Which of the following functions can be used as a countermeasure to a Shell Injection attack?

Each correct answer represents a complete solution. Choose all that apply.
* escapeshellarg()
* mysql_real_escape_string()
* regenerateid()
* escapeshellcmd()

NO.137 Which of the following is the most common vulnerability that can affect desktop applications written in native code?
* SpyWare
* DDoS attack
* Malware
* Buffer overflow

Section: Volume C

NO.138 Which of the following statements are true about tcp wrappers?

Each correct answer represents a complete solution. Choose all that apply.
* tcp wrapper provides access control, host address spoofing, client username lookups, etc.
* When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
* tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access

control purposes.
* tcp wrapper protects a Linux server from IP address spoofing.
Section: Volume A

Explanation/Reference: