[Mar-2024 GCIH Free PDF from ValidExam [Q34-Q51

Mar-2024 Latest ValidExam GCIH Exam Dumps with PDF and Exam Engine Free Updated Today! Following are some new GCIH Real Exam Questions! Q34. Which of the following can be used as a Trojan vector to infect an information system?

Each correct answer represents a complete solution. Choose all that apply.
* NetBIOS remote installation
* Any fake executable
* Spywares and adware
* ActiveX controls, VBScript, and Java scripts

Q35. In which of the following malicious hacking steps does email tracking come under?
* Reconnaissance
* Gaining access
* Maintaining Access
* Scanning
Section: Volume B

Q36. Which of the following is a type of computer security vulnerability typically found in Web applications that allow code injection by malicious Web users into the Web pages viewed by other users?

* SID filtering
* Cookie poisoning
* Cross-site scripting
* Privilege Escalation

Q37. In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target

system?
* Ping of death
* Jolt
* Fraggle
* Teardrop

Q38. Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish

this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered

only when the algorithm compares the changed cover with the original cover. Which of the following Steganography

methods is Victor using to accomplish the task?
* The distortion technique
* The spread spectrum technique
* The substitution technique
* The cover generation technique

Q39. Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?
* Signature-based IDS
* Network-based IDS
* Passive IDS
* Active IDS

Q40. You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries. But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution?

Each correct answer represents a part of the solution. Choose all that apply.
* Eradication
* Contamination
* Preparation
* Recovery
* Identification

Q41. Jason, a Malicious Hacker, is a student of Baker university. He wants to perform remote hacking on the server of DataSoft Inc. to hone his hacking skills. The company has a Windows-based network. Jason successfully enters the target system remotely by using the advantage of vulnerability. He places a Trojan to maintain future access and then disconnects the remote session. The employees of the company complain to Mark, who works as a Professional Ethical Hacker for DataSoft Inc., that some computers are very slow. Mark diagnoses the network and finds that some irrelevant log files and signs of Trojans are present on the computers. He suspects that a malicious hacker has accessed the network. Mark takes the help from Forensic Investigators and catches Jason.

Which of the following mistakes made by Jason helped the Forensic Investigators catch him?
* Jason did not perform a vulnerability assessment.
* Jason did not perform OS fingerprinting.
* Jason did not perform foot printing.
* Jason did not perform covering tracks.
* Jason did not perform port scanning.

Q42. Which of the following netcat parameters makes netcat a listener that automatically restarts itself when a connection is dropped?
* -u
* -l
* -p
* -L

Q43. In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with

the purpose of concealing the identity of the sender or impersonating another computing system?
* Rainbow attack
* IP address spoofing
* Cross-site request forgery
* Polymorphic shell code attack

Q44. Which of the following characters will you use to check whether an application is vulnerable to an SQL injection attack?
* Dash (-)
* Double quote (&#8220;)
* Single quote (&#8216;)
* Semi colon (;)

Q45. Which of the following attacks is specially used for cracking a password?
* PING attack
* Dictionary attack
* Vulnerability attack
* DoS attack

Q46. Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?

Each correct answer represents a complete solution. Choose two.
* Land attack
* SYN flood attack
* Teardrop attack
* Ping of Death attack

Q47. Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether.

The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. What steps can be used as a countermeasure of ARP spoofing?

Each correct answer represents a complete solution. Choose all that apply.
* Using smash guard utility
* Using ARP Guard utility
* Using static ARP entries on servers, workstation and routers
* Using ARP watch utility
* Using IDS Sensors to check continually for large amount of ARP traffic on local subnets

Q48. In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system?
* Rainbow attack
* IP address spoofing
* Cross-site request forgery
* Polymorphic shell code attack

Q49. Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration. The tool uses raw IP packets to determine the following:

What ports are open on our network systems.

▪

What hosts are available on the network.

▪

Identify unauthorized wireless access points.

▪

What services (application name and version) those hosts are offering.

▪

What operating systems (and OS versions) they are running.

▪

What type of packet filters/firewalls are in use.

▪

Which of the following tools is Victor using?
* Nessus
* Kismet
* Nmap
* Sniffer

Q50. You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic. What is this most likely to be an indicator of?
* Virus

* Syn flood
* Misconfigured router
* DoS attack

Q51. Which of the following are the automated tools that are used to perform penetration testing?

Each correct answer represents a complete solution. Choose two.
* Pwdump
* Nessus
* EtherApe
* GFI LANguard
Section: Volume B