Vendor: EC-Council

Exam Code: 312-49v9

Exam Name: Computer Hacking Forensic Investigator v9 Exam

Version: DEMO

QUESTION 1
You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

```
http://172.168.4.131/level/99/exec/show/config
```

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. URL Obfuscation Arbitrary Administrative Access Vulnerability
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
D. HTTP Configuration Arbitrary Administrative Access Vulnerability Answer:

Answer: D

QUESTION 2
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block access to TCP port 171
B. Change the default community string names
C. Block all internal MAC address from using SNMP
D. Block access to UDP port 171

Answer: B

QUESTION 3
When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Time-Sync Protocol
B. SyncTime Service
C. Network Time Protocol
D. Universal Time Set

Answer: C

QUESTION 4
When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Avoid over-saturation of wireless signals

B. So that the access points will work on different requencies
C. Avoid cross talk
D. Multiple access points can be set up on the same channel without any issues

Answer: C

QUESTION 5
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords.
A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour.
Why were these passwords cracked so Quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked are local accounts on the Domain Controller

Answer: A

QUESTION 6
Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Filtered
B. Closed
C. Open
D. Stealth

Answer: C

QUESTION 7
What is the target host IP in the following command?

```
C:\> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP
```

A. 10.10.150.1
B. This command is using FIN packets, which cannot scan target hosts
C. Firewalk does not scan target hosts
D. 172.16.28.95

Answer: D

QUESTION 8
Terri works for a security consulting firm that is currently performing a penetration test on First

National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Poison the switch's MAC address table by flooding it with ACK bits
B. Crash the switch with aDoS attack since switches cannot send ACK bits
C. Enable tunneling feature on the switch
D. Trick the switch into thinking it already has a session with Terri's computer Answer:

Answer: D

QUESTION 9
When is it appropriate to use computer forensics?

A. If copyright and intellectual property theft/misuse has occurred
B. If employees do not care for their boss?management techniques
C. If sales drop off for no apparent reason for an extended period of time
D. If a financial institution is burglarized by robbers

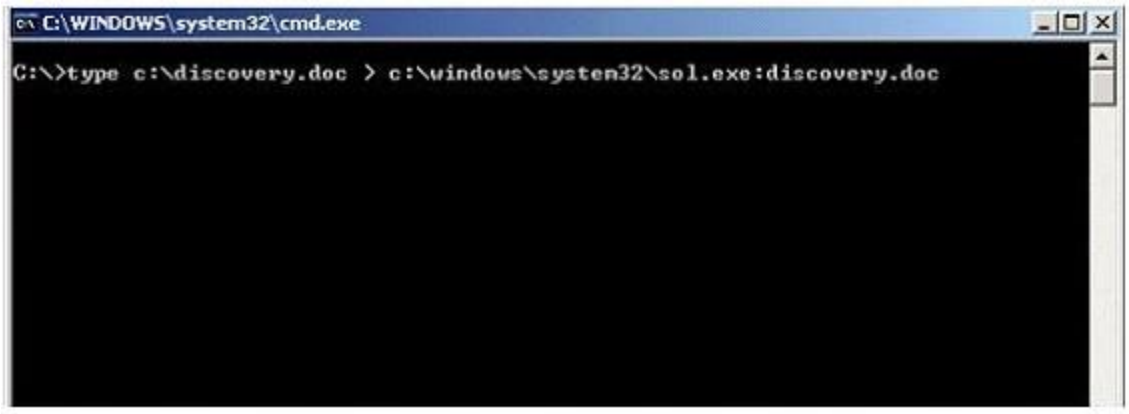
Answer: A

QUESTION 480
You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different.
What area of the law is the employee violating?

A. Copyright law
B. Brandmark law
C. Trademark law
D. Printright law

Answer: C

QUESTION 11
What feature of Windows is the following command trying to utilize?



A. White space
B. AFS
C. ADS
D. Slack file

Answer: C

QUESTION 12
You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as other members of your team collect it.
Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive.
How will these forms be stored to help preserve the chain of custody of the case?

A. All forms should be placed in an approved secure container because they are now primary evidence in the case
B. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be
placed in the report file
C. All forms should be placed in the report file because they are now primary evidence in the case
D. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an
approved secure container

Answer: D

QUESTION 13
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to _____

A. Automate collection from image files
B. Avoiding copying data from the boot partition
C. Acquire data from the host-protected area on a disk
D. Prevent contamination to the evidence drive

Answer: D

QUESTION 14
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, reQuested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Social Validation
B. Friendship/Liking
C. Reciprocation
D. Scarcity

Answer: C

QUESTION 15
You are working as a computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact local law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject computer. You inform the officer that you will not be able to comply with thatnetwork sniffer on your network and monitor all traffic to the subject? computer. You inform the officer that you will not be able to comply with that request because doing so would:

A. Violate your contract
B. Cause network congestion
C. Make you an agent of law enforcement
D. Write information to the subject hard drive Write information to the subject hard drive

Answer: C

QUESTION 16
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. IAS account names and passwords
B. Service account passwords in plain text
C. Local store PKI Kerberos certificates
D. Cached password hashes for the past 20 users

Answer: B

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **BDNT2014**