Vendor: EC-COUNCIL

Exam Code: ECSS

Exam Name: EC-Council Certified Security Specialist Practice Test

Version: Demo

QUESTION 1
Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?

Each correct answer represents a complete solution. Choose all that apply.

A. ICMP packets leaving the network should be allowed.
B. An attacker should know the IP address of the last known gateway before the firewall.
C. There should be a backdoor installed on the network.
D. An attacker should know the IP address of a host located behind the firewall.

Correct Answer: ABD

QUESTION 2
Which of the following security protocols are based on the 802.11i standard?

Each correct answer represents a complete solution. Choose all that apply.

A. WEP
B. WPA2
C. WPA
D. WEP2

Correct Answer: BC

QUESTION 3
Which of the following OSI layers is responsible for protocol conversion, data encryption/decryption, and data compression?

A. Transport layer
B. Presentation layer
C. Data-link layer
D. Network layer

Correct Answer: B

QUESTION 4
You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

A. Vulnerability scanning
B. Manual penetration testing
C. Automated penetration testing
D. Code review

Correct Answer: A

QUESTION 5
Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?

A. Lead investigator
B. Information security representative

C. Technical representative
D. Legal representative

Correct Answer: C

QUESTION 6
Which of the following statements are true about routers?

Each correct answer represents a complete solution. Choose all that apply.

A. Routers are responsible for making decisions about which of several paths network (orInternet)traffic will follow.
B. Routers do not limit physical broadcast traffic.
C. Routers organize addresses into classes, which are used to determine how to move packets fromone network to another.
D. Routers act as protocol translators and bind dissimilar networks.

Correct Answer: ACD

QUESTION 7
Which of the following types of attacks cannot be prevented by technical measures only?

A. Brute force
B. Ping flood attack
C. Smurf DoS
D. Social engineering

Correct Answer: D

QUESTION 8
You work as a Network Administrator for Tech Perfect Inc. The company requires a secure wireless

network. To provide security, you are configuring ISA Server 2006 as a firewall. While configuring

ISA Server 2006, which of the following is NOT necessary?

A. Defining how ISA Server would cache Web contents
B. Defining ISA Server network configuration
C. Setting up of monitoring on ISA Server
D. Configuration of VPN access

Correct Answer: D

QUESTION 9
Which of the following attacks CANNOT be detected by an Intrusion Detection System (IDS)?

Each correct answer represents a complete solution. Choose all that apply.

A. Denial-of-Service (DoS) attack
B. E-mail spoofing
C. Port scan attack
D. Shoulder surfing

Correct Answer: BD

QUESTION 10
Which of the following statements best describes a certification authority?

A. A certification authority is a type of encryption that uses a public key and a private key pair fordata encryption.
B. A certification authority is an entity that issues digital certificates for use by other parties.
C. A certification authority is a technique to authenticate digital documents by using computercryptography.
D. A certification authority is a type of encryption that uses a single key to encrypt and decryp t data.

Correct Answer: B

QUESTION 11
You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement?

Each correct answer represents a complete solution. Choose two.

A. Using WEP encryption
B. Using WPA encryption
C. Not broadcasting SSID
D. MAC filtering the router

Correct Answer: AB

QUESTION 12
Linux traffic monitoring tools are used to monitor and quickly detect faults in the network or a system. Which of the following tools are used to monitor traffic of the Linux operating system? Each correct answer represents a complete solution. Choose all that apply.

A. PsExec
B. IPTraf
C. MRTG
D. PsLogList
E. Ntop

Correct Answer: BCE

QUESTION 13
John works as an Office Assistant in DataSoft Inc. He has received an e-mail from duesoft_lotterygroup@us.com with the following message:

The DueSoft Lottery Incorporation

This is to inform you that you have just won a prize of $7,500.00 for this year's Annual Lottery promotion, which was organized by Msn/Yahoo Lottery in conjunction with DueSoft. We collect active online e-mails and select five people every year as our winners through an electronic balloting machine. Please reply within three days of receiving this e-mail with your full details like Name, Address, Sex, Occupation, Age, State, Telephone number, and Country to claim your prize.

If John replies to this e-mail, which of the following attacks may he become vulnerable to?

A. Salami attack
B. Man-in-the-Middle attack
C. Phishing attack
D. DoS attack

Correct Answer: C

QUESTION 14
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the

tool is as follows:

Which of the following tools is John using to crack the wireless encryption keys?

A. AirSnort
B. Kismet
C. PsPasswd
D. Cain

Correct Answer: A

QUESTION 15
Which of the following proxy servers is also referred to as transparent proxies or forced proxies?

A. Intercepting proxy server
B. Anonymous proxy server
C. Reverse proxy server
D. Tunneling proxy server

Correct Answer: A

QUESTION 16
Which of the following security policies will you implement to keep safe your data when you connect your Laptop to the office network over IEEE 802.11 WLANs?

Each correct answer represents a complete solution. Choose two.

A. Using a protocol analyzer on your Laptop to monitor for risks.
B. Using an IPSec enabled VPN for remote connectivity.
C. Using portscanner like nmap in your network.
D. Using personal firewall software on your Laptop.

Correct Answer: BD

QUESTION 17
Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?

A. I love you
B. Melissa
C. Tequila
D. Brain

Correct Answer: D

QUESTION 18
Which of the following needs to be documented to preserve evidences for presentation in court?

A. Incident response policy
B. Account lockout policy
C. Separation of duties
D. Chain of custody

Correct Answer: D

QUESTION 19
Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme?

Each correct answer represents a complete solution. Choose all that apply.

A. Kerberos requires continuous availability of a central server.
B. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.
C. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject'spasswords.
D. Kerberos requires the clocks of the involved hosts to be synchronized.

Correct Answer: ACD

QUESTION 20
Which of the following is used in asymmetric encryption?

A. Public key and user key
B. SSL
C. Public key and private key
D. NTFS

Correct Answer: C

QUESTION 21
Sam, a malicious hacker, targets the electric power grid of Umbrella Inc. and gains access to the electronic control systems. Which of the following types of cybercrime has Sam performed?

A. Cyber defamation
B. Cybertrespass
C. Cyberterrorism
D. Cybertheft

Correct Answer: C

QUESTION 22
Maria works as a Desktop Technician for PassGuide Inc. She has received an e-mail from the MN

Compensation Office with the following message:

Dear Sir/Madam,

My name is Edgar Rena, the director of compensation here at the MN Compensation Office in Chicago. We receive so many complaints about fraudulent activities that have been taking place in your region for the past few years. Due to the high volume loss of money, the MN compensation department has had an agreement with the appropriate authority to compensate each victim with a sum of USD$500,000.00.

You were selected among the list of people to be paid this sum. To avoid any imperative mood by intending scammers, your payment has been transmuted into an International bank draft which can be cashed at any local bank in your country.

Please fill the below details and send it to our secretary for your compensation bank draft.

Full name:

Address:

Tel:

Fill & Send to:

Dr. Michael Brown

MN Compensation Office, IL

Tel: +1-866-233-8434

Email: micbrown@live.com

Further instructions shall be given to you by our secretary as soon as you contact him. To avoid losing your compensation, you are requested to pay the sum of $350 for Insurance Premium to our secretary.

Thanks and God bless.

If Maria replies to this mail, which of the following attacks may she become vulnerable to?

A. Phishing attack
B. SYN attack
C. CookieMonster attack
D. Mail bombing

Correct Answer: A

QUESTION 23
Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet.

Which of the following security threats may occur if DMZ protocol attacks are performed? Each correct answer represents a complete solution. Choose all that apply.

A. The attacker can exploit any protocol used to go into the internal network or intranet of thecompany.
B. The attacker can gain access to the Web server in a DMZ and exploit the database.
C. The attacker can perform a Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.
D. The attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.

Correct Answer: ABC

QUESTION 24
Which of the following Linux rootkits is installed via stolen SSH keys?

A. Phalanx2
B. Beastkit
C. Adore
D. Linux.Ramen

Correct Answer: A

QUESTION 25
Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Snooping
B. Copyright
C. Utility model

D. Patent

Correct Answer: D

QUESTION 26
Jason works as a System Administrator for Passguide Inc. The company has a Windows-based network. Sam, an employee of the company, accidentally changes some of the applications and system settings. He complains to Jason that his system is not working properly. To troubleshoot the problem, Jason diagnoses the internals of his computer and observes that some changes have been made in Sam's computer registry. To rectify the issue, Jason has to restore the registry.

Which of the following utilities can Jason use to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Reg.exe
B. Resplendent registrar
C. EventCombMT
D. Regedit.exe

Correct Answer: ABD

QUESTION 27
Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the task:

1. Smoothening and decreasing contrast by averaging the pixels of the area where significant

color transitions occurs.

2. Reducing noise by adjusting color and averaging pixel value.

3. Sharpening, Rotating, Resampling, and Softening the image.

Which of the following Steganography attacks is Victor using?

A. Steg-Only Attack
B. Chosen-Stego Attack
C. Active Attacks
D. Stegdetect Attack

Correct Answer: C

QUESTION 28
What is the major difference between a worm and a Trojan horse?

A. A worm is self replicating, while a Trojan horse is not.
B. A worm is a form of malicious program, while a Trojan horse is a utility.
C. A worm spreads via e-mail, while a Trojan horse does not.
D. A Trojan horse is a malicious program, while a worm is an anti-virus software.

Correct Answer: A

QUESTION 29
John works as a Network Security Administrator for NetPerfect Inc. The manager of the company has told John that the company's phone bill has increased drastically. John suspects that the company's phone system has been cracked by a malicious hacker. Which attack is used by malicious hackers to crack the phone system?

A. Sequence++ attack
B. Phreaking
C. Man-in-the-middle attack
D. War dialing

Correct Answer: B

QUESTION 30
You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Download folder
B. History folder
C. Temporary Internet Folder
D. Cookies folder

Correct Answer: BCD

QUESTION 31
John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system and wants to install an Intrusion Detection System on the We-are-secure server so that he can receive alerts about any hacking attempts. Which of the following tools can John use to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Samhain
B. Tripwire
C. Snort
D. SARA

Correct Answer: AC

QUESTION 32
You manage a Windows Server 2008 server named uCert1 in a domain named PassGuide.com.

uCert1 has the Web Server (IIS) role installed and hosts an intranet Web site named

PassGuideInternal.

You want to ensure that all authentication traffic to the Web site is encrypted securely without the use of SSL. You disable Anonymous Authentication. What else should you do?

A. Enable Windows Authentication and Forms Authentication.
B. Enable Windows Authentication and Digest Authentication.
C. Enable Basic Authentication and Windows Authentication.
D. Enable Digest Authentication and Forms Authentication.

Correct Answer: B

QUESTION 33
Which of the following password cracking attacks does not use any software for cracking e-mail passwords?

Each correct answer represents a complete solution. Choose all that apply.

A. Brute force attack
B. Shoulder surfing
C. Social engineering
D. Dictionary attack

Correct Answer: BC

QUESTION 34
You work as a Sales Manager for NetPerfect Inc. The company has a Windows-based network. You have to often send confidential e-mails and make online payments and purchases. You want to protect transmitted information and also to increase the security of e-mail communications. Which of the following programs or services will you use to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Anonymizer
B. John the Ripper
C. THC Hydra
D. Pretty Good Privacy (PGP)

Correct Answer: AD

QUESTION 35
The IT administrator wants to implement a stronger security policy. What are the four most important security priorities for PassGuide Software Systems Pvt. Ltd.? (Click the Exhibit button on the toolbar to see the case study.)

A. Preventing denial-of-service attacks.
B. Providing two-factor authentication.
C. Ensuring secure authentication.
D. Protecting employee data on portable computers.
E. Implementing Certificate services on Texas office.
F. Preventing unauthorized network access.
G. Providing secure communications between the overseas office and the headquarters.
H. Providing secure communications between Washington and the headquarters office.

Correct Answer: CDFG

QUESTION 36
According to the Internet Crime Report 2009, which of the following complaint categories is on the top?

A. Identity theft
B. Advanced fee fraud
C. Non-delivered merchandise/payment
D. FBI scams

Correct Answer: D

QUESTION 37
Maria works as the Chief Security Officer for PassGuide Inc. She wants to send secret messages to the CEO of the company. To secure these messages, she uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'. What technique is Maria using?

A. Steganography
B. Public-key cryptography
C. Encryption

D. RSA algorithm

Correct Answer: A

QUESTION 38
Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

A. Incident response policy
B. Chain of custody
C. Chain of evidence
D. Evidence access policy

Correct Answer: B

QUESTION 39
Peter works as a System Administrator for TechSoft Inc. The company uses Linux-based systems.

Peter's manager suspects that someone is trying to log in to his computer in his absence. Which of the following commands will Peter run to show the last unsuccessful login attempts, as well as the users who have last logged in to the manager's system?

Each correct answer represents a complete solution. Choose two.

A. rwho -a
B. lastb
C. last
D. pwd

Correct Answer: BC

QUESTION 40
John works as a Security Administrator for NetPerfect Inc. The company uses Windows-based

systems. A project has been assigned to John to track malicious hackers and to strengthen the company's security system. John configures a computer system to trick malicious hackers into thinking that it is the company's main server, which in fact is a decoy system to track hackers.

Which system is John using to track the malicious hackers?

A. Honeypot
B. Intrusion Detection System (IDS)
C. Bastion host
D. Honeytokens

Correct Answer: A

QUESTION 41
Which of the following can be used to perform session hijacking?

Each correct answer represents a complete solution. Choose all that apply.

A. ARP spoofing
B. Cross-site scripting
C. Session fixation
D. Session sidejacking

Correct Answer: BCD

QUESTION 42
In which of the following techniques does an attacker take network traffic coming towards a host at one port and forward it from that host to another host?

A. Snooping
B. UDP port scanning
C. Port redirection
D. Firewalking

Correct Answer: C

QUESTION 43
Which of the following is used to authenticate asymmetric keys?

A. Digital signature
B. MAC Address
C. Password
D. Demilitarized zone (DMZ)

Correct Answer: A

QUESTION 44
Which of the following programs is used for bypassing normal authentication for securing remote access to a computer?

A. Worm
B. Adware
C. Backdoor
D. Spyware

Correct Answer: C

QUESTION 45
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright B.
Trademark C.
Trade secret D.
Patent

Correct Answer:

QUESTION 46
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the preattack phase:

·Information gathering
·Determining network range
·Identifying active machines
·Finding open ports and applications
·OS fingerprinting
·Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?

Each correct answer represents a complete solution. Choose all that apply.

A. Traceroute

B. NeoTrace
C. Cheops
D. Ettercap

Correct Answer: ABC

QUESTION 47
John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

A. Replay attack
B. DoS attack
C. ARP spoofing
D. Rainbow attack

Correct Answer: B

QUESTION 48
Which of the following statements are correct about spoofing and session hijacking?

Each correct answer represents a complete solution. Choose all that apply.

A. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the targetand the valid user cannot be active.
B. Session hijacking is an attack in which an attacker takes over the session, and the valid user'ssession is disconnected.
C. Session hijacking is an attack in which an attacker takes over the session, and the valid user'ssession is not disconnected.
D. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the targetbut the valid user can be active.

Correct Answer: CD

QUESTION 49
In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?

A. Fraggle
B. Jolt
C. Teardrop
D. Ping of death

Correct Answer: D

QUESTION 50
John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.

Which of the following worms has attacked the computer?

A. Code red
B. Ramen
C. LoveLetter

D. Nimda

Correct Answer: B

QUESTION 51
Which two technologies should research groups use for secure VPN access while traveling?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose two.

A. SSL
B. Kerberos authentication
C. PPTP
D. Smart cards
E. Encrypting File System (EFS)

Correct Answer: CD

QUESTION 52
Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer?

Each correct answer represents a complete solution. Choose two.

A. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.
B. Attacker can use the Ping Flood DoS attack if WZC is used.
C. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.
D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

Correct Answer: AC

QUESTION 53
Which of the following uses public key cryptography to encrypt the contents of files?

A. EFS
B. DFS
C. NTFS
D. RFS

Correct Answer: A

QUESTION 54
Which of the following softwares is used to perform constant monitoring of the network infrastructure?

A. Logdog
B. THCHydra
C. IPSentry
D. Cain

Correct Answer: C

QUESTION 55
You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest

domain-based network. The company has recently provided fifty laptops to its sales team members. You are required to configure an 802.11 wireless network for the laptops. The sales team members must be able to use their data placed at a server in a cabled network. The planned network should be able to handle the threat of unauthorized access and data interception by an unauthorized user. You are also required to prevent the sales team members from communicating directly to one another. Which of the following actions will you perform to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Implement the open system authentication for the wireless network.
B. Implement the IEEE 802.1X authentication for the wireless network.
C. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.
D. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.
E. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.

Correct Answer: BCD

QUESTION 56
Which of the following statements are true about session hijacking?

Each correct answer represents a complete solution. Choose all that apply.

A. TCP session hijacking is when a hacker takes over a TCP session between two machines.
B. It is used to slow the working of victim's network resources.
C. Use of a long random number or string as the session key reduces session hijacking.
D. It is the exploitation of a valid computer session to gain unauthorized access to informationor services in a computer system.

Correct Answer: ACD

QUESTION 57
Which of the following Linux rootkits allows attackers to hide files, processes, and network connections?

Each correct answer represents a complete solution. Choose all that apply.

A. Phalanx2
B. Adore
C. Knark
D. Beastkit

Correct Answer: BC

QUESTION 58
Who among the following are security experts who specialize in penetration testing and other testing methodologies to ensure that their company's information systems are secure?

Each correct answer represents a complete solution. Choose all that apply.

A. Black hat hackers
B. White hat hackers
C. Script Kiddies
D. Ethical hackers

Correct Answer: BD

QUESTION 59
You work as a Network Administrator for ABC Inc. The company uses a secure wireless network.

John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

A. Independent audit
B. Operational audit
C. Non-operational audit
D. Dependent audit

Correct Answer: A

QUESTION 60
Fill in the blank with the appropriate word is software that is a subcategory of malware and refers to unwanted software that performs malicious actions on a user's computer. Some its examples are Trojan, adware, and spyware.

Correct Answer: Crimeware

Exam B

QUESTION 1
In a complex network, Router transfers data packets by observing some form of parameters or metrics provided in the routing table. Which of the following metrics is NOT included in the routing table?

A. Bandwidth
B. Delay
C. Load
D. Frequency

Correct Answer: D

QUESTION 2
A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. Stunnel
B. IPTables
C. OpenSSH
D. IPChains

Correct Answer: B

QUESTION 3
Which of the following terms is used for the process of securing a system or a device on a network infrastructure?

A. Hardening
B. Sanitization
C. Authentication
D. Cryptography

Correct Answer: A

QUESTION 4
Which of the following Intrusion Detection Systems (IDS) is used to monitor rogue access points and the use of wireless attack tools?

A. Snort 2.1.0
B. WIDS
C. NFR security
D. LogIDS 1.0

Correct Answer: B

QUESTION 5
Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses 'Faulkner' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone. Which of the following methods has the attacker used to crack Andrew's password?

Each correct answer represents a complete solution. Choose all that apply.

A. Zero-day attack
B. Social engineering

C. Rainbow attack
D. Buffer-overflow attack
E. Brute force attack
F. Dictionary-based attack
G. Denial-of-service (DoS) attack
H. Password guessing

Correct Answer: BCEFGH

QUESTION 6
Which of the following software helps in protecting the computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software?

Each correct answer represents a complete solution. Choose all that apply.

A. BitDefender
B. Windows Defender
C. John the Ripper
D. THC Hydra

Correct Answer: AB

QUESTION 7
A digital signature is a type of public key cryptography. Which of the following statements are true about digital signatures?

Each correct answer represents a complete solution. Choose all that apply.

A. In order to digitally sign an electronic record, a person must use his/her public key.
B. In order to verify a digital signature, the signer's private key must be used.
C. In order to verify a digital signature, the signer's public key must be used.
D. In order to digitally sign an electronic record, a person must use his/her private key.

Correct Answer: CD

QUESTION 8
Andrew works as a Forensic Investigator for Passguide Inc. The company has a Windows-based environment. The company's employees use Microsoft Outlook Express as their e-mail client program. E-mails of some employees have been deleted due to a virus attack on the network.

Andrew is therefore assigned the task to recover the deleted mails. Which of the following tools can Andrew use to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. FINALeMAIL
B. eMailTrackerPro
C. EventCombMT
D. R-mail

Correct Answer: AD

QUESTION 9
Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Eradication phase
B. Preparation phase

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

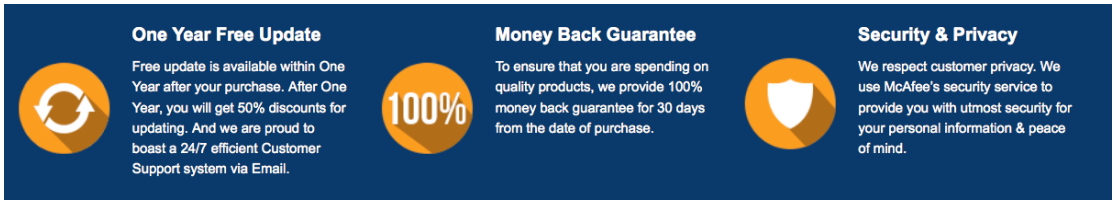
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

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

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions