During which of the following steps is the public/private key-pair generated for Public Key Infrastructure (PKI)?

Initialization

Which of the following protocols work at the Session layer of the OSI model?

Internet Security Association and Key Management Protocol (ISAKMP) & Border Gateway Multicast Protocol (BGMP)

What is a security advantage of using elastic containers for application deployment?

Footholds disappear

Which of the following statements about DMZ are true?

It contains company resources that are available on the Internet, such as Web servers and FTP servers. & It is the boundary between the Internet and a private network.

How many phases does IKE have?

Two

Which of the following should be implemented to protect an organization from spam?

E-mail filtering

You are going to upgrade your hard disk's file system from FAT to NTFS. What are the major advantages of the NTFS file system over FAT16 and FAT32 file systems?

NTFS give improved disk compression than FAT16 and FAT32. NTFS gives better file security than FAT16 and FAT32. NTFS file system supports for larger hard disks.

Which of the following is a term that refers to unsolicited e-mails sent to a large number of e-mail users?

Spam

Which of these would be a common persistence vector?

Registry key

Which of the following statements about buffer overflow is true?

It is a condition in which an application receives more data than it is configured to accept.

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering?

Load Balancing & Failover

What essential actions would you perform to harden a system?

Restrict permissions, reduce packages installed, and limit services

You are writing a backup plan. Your goal is to try to ensure you have speed to recovery, but also to reduce the amount of storage space needed for the backups as much as possible. Which backup scheme would you choose?

Full backups weekly; differential backup nightly afterward

Which of the following files contains the shadowed password entries in Linux?

/etc/shadow

Which of the following features of Windows 7 allows an administrator to both passively review installed software and configure policies to prevent out-of-date or insecure software from running?

App Locker

There are three key factors in selecting a biometric mechanism. What are they?

Reliability, user acceptance, and cost

You have been hired to design a TCP/IP-based network that will contain both Unix and Windows computers. You are planning a name resolution strategy. Which of the following services will best suit the requirements of the network?

DNS

Which of the following Linux commands can change both the username and group name a file belongs to?

Chgrp

Which of the following protocols provides maintenance and error reporting function?

ICMP

In addition to securing the operating system of production honey pot hosts, what is recommended to prevent the honey pots from assuming the identities of production systems that could result in the denial of service for legitimate users?

Deploy the honey pot hosts in an unused part of your address space.

Microsoft Windows file security permissions are an example of what?

DAC

In the address ab00:fc87:234a:0090:5120:ffab:bc8a:0098/23, what does the /23 indicate?

The number of bits in the network portion of the address

What would be a common role for a CSIRT within an organization?

Provide oversight and coordination

When discussing access controls, which of the following terms describes the process of determining the activities or functions that an Individual is permitted to perform?

Authorization

Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?

Employees

Which of the following works at the network layer and hides the local area network IP address and topology?

Network address translation (NAT)

Which of the following SIP INVITE lines indicates to the remote registrar the VoIP phone that initiated the call?

User-Agent

What does the following iptables rule do iptables -A INPUT -j DROP?

Drops all inbound traffic

What is the function of the TTL (Time to Live) field in IPv4 and the Hop Limit field in IPv6 In an IP Packet header?

These fields are decremented each time a packet is retransmitted to minimize the possibility of routing loops.

Which of the following systems acts as a NAT device when utilizing VMware in NAT mode?

Virtual system

How can the use of containers improve the overall security of an application deployment?

Containers are easy to deploy and undeploy rapidly.

Which command would allow an administrator to determine if a RPM package was already installed?

rpm -q

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

Trademark

Why would you perform a risk assessment?

To identify areas where resources should be applied

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we- are-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits? Each correct answer represents a complete solution.

They allow an attacker to run packet sniffers secretly to capture passwords. They allow an attacker to replace utility programs that can be used to detect the attacker's activity. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.

Which of the following are the types of access controls?

Physical, Administrative, Technical

What would the file permission example "rwsr-sr-x" translate to in absolute mode?

6755

What is it referred to when security is introduced as early as possible into the software development lifecycle?

Moving left

A border router would implement which of the following security controls?

Access control lists to block broad categories of traffic

SSL session keys are available in which of the following lengths?

40-bit and 128-bit.

Adding an additional alphanumeric character to the required length of a password will multiply the potential passwords by how many?

62

You work as a Network Administrator for Net World Inc. The company has a Linux-based network. For testing purposes, you have configured a default IP-table with several filtering rules. You want to reconfigure the table. For this, you decide to remove the rules from all the chains in the table. Which of the following commands will you use?

IPTABLES -F

Which of the following is a backup strategy?

Differential

One of your Linux systems was compromised last night. According to change management history and a recent vulnerability scan, the system's patches were up-to-date at the time of the attack. Which of the following statements is the Most Likely explanation?

It was a zero-day exploit.

You are implementing a star topology on your local network. What cabling are you most likely to use?

Twisted pair

You have determined that the SLE for one of your systems is $5000 and the ARO is 2. What is your ALE?

$10,000

What is the following sequence of packets demonstrating?

client.com.38060 > telnet.com.telnet: F 92:92(0) ack 4290 win 8760 (DF)

Which of the following protocols allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer?

IMAP

You work as a Linux technician for Tech Perfect Inc. You have lost the password of the root. You want to provide a new password. Which of the following steps will you take to accomplish the task?

Reboot the computer in run level 1. Use INIT=/bin/sh as a boot option. At the bash# prompt, run the PASSWD root command.

The challenge of trying to find a collision in a hashing algorithm is called what?

A birthday attack

Your organization has broken its network into several sections/segments, which are separated by firewalls, ACLs and VLANs. The purpose is to defend segments of the network from potential attacks that originate in a different segment or that attempt to spread across segments.

This style of defense-in-depth protection is best described as which of the following?

Protected enclaves

You are seeing a lot of ARP responses with no corresponding ARP request. What are you most likely seeing?

ARP spoofing

What is the name of the command-line tool for Windows that can be used to manage audit policies on remote systems?

AUDITPOL.EXE

You are doing some analysis of malware on a Unix computer in a closed test network. The IP address of the computer is 192.168.1.120. From a packet capture, you see the malware is attempting to do a DNS query for a server called iamabadserver.com so that it can connect to it.

There is no DNS server on the test network to do name resolution. You have another computer, whose IP is 192.168.1.115, available on the test network that you would like for the malware connect to it instead. How do you get the malware to connect to that computer on the test network?

You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.115 iamabadserveriamabadserver.com

How does virtual memory help programming practices?

Virtual memory is handled by the kernel.

Where are user accounts and passwords stored in a decentralized privilege management environment?

On each server.

What is the term for a game in which for every win there must be an equivalent loss?

Zero-sum

Where could you go in Windows XP/2003 to configure Automatic Updates?

Go to the System applet in Control Panel and click on the Automatic Updates icon.

How often is session information sent to the web server from the browser once the session

information has been established?

With any change in session data

What is TRUE about Workgroups and Domain Controllers?

You can have stand-alone computers in the midst of other machines that are members of a domain.

You notice a lot of unusual network traffic to remote systems originating from your computer. When you investigate further, you discover that a number of computers on your network are doing the same thing, and the IP address is in another country. This always seems to happen in the late evening hours. What may you be seeing?

Botnet activity

What do you call sensitive information passing over a network?

Data in motion

Which of the following is a private, RFC 1918 compliant IP address that would be assigned to a DHCP scope on a private LAN?

10.254.1.50

How would you get a list of services installed on a system that was using systemd rather than init?

Systemctl

The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

ROI = (gain - expenditure)/(expenditure) X 100%

What should security policies be driven by?

Business mission and objectives

The Linux command to make the /etc/shadow file, already owned by root, readable only by root is which of the following?

chmod 400/etc/shadow

You have a set of users you want to assign some permissions to. What does Microsoft recommend you do to accomplish this?

Create a global group with the users in it, and then create a domain local group and assign the permissions to the domain local group.

Which of these tools would likely be most valuable to you if you were working in security operations?

SIEM

If your web browser generates a certificate error, which of the following is mostly likely to be the case?

The digital signature of the CA on the certificate is invalid.

What organization could you turn to for threat intelligence if you didn't want to pay for a commercial service?

ISAC

Which of the following commands is used to change file access permissions in Linux?

chmod

The TTL can be found in which protocol header?

It is found in byte 8 of the IP header.

When should you create the initial database for a Linux file integrity checker?

Before a system has been compromised

In a /24 subnet, which of the following is a valid broadcast address?

192.10.10.255

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

Hardening

Which of the following languages enable programmers to store cookies on client computers?

Perl & JavaScript

What does Java use to achieve architecture independence?

Byte code

You see a system that shows an SID of S-1-15-32-545. What do you know about that SID?

It's the SID for the Users group.

Which of the following books deals with confidentiality?

Orange Book

Which of the following TCP dump output lines indicates the first step in the TCP 3-way handshake?

07:09:43.368615 download.net 39904 > ftp.com.21: S 733381829:733381829(0) win 8760 <mss 1460> (DF)

Which of the following VMware files can be edited by hand and changed in the case of problems?

.vmx

Which of these is malware that was used on IoT devices to attack high-profile targets?

Mirai

In preparation to do a vulnerability scan against your company's systems. Which of the following is a necessary step to take prior to starting the scan?

Getting permission to run the scan.

What type of attack can be performed against a wireless network using the tool Kismet?

Eavesdropping

What is the unnoticed theft of sensitive data from a laptop owned by an organization's CEO an example of in information warfare?

Symmetric warfare

What are two primary responsibilities of the hypervisor?

Manage the creation of virtual machines and provide an interface for the guest OS to hardware.

Which of these network security controls are you most likely to find on a device that connects your home to your service provider's network?

Network address translation

You regularly get popup ads on your computer, particularly when you are browsing the Web. What is this an example of?

Adware

If you wanted a virtual environment with limited overhead, what would you use?

Container

Which of the following is a good example of a network using a mesh topology?

The Internet

What is the order of messages in a three-way handshake?

SYN, SYN/ACK, ACK

Which Host-based IDS (HIDS) method of log monitoring utilizes a list of keywords or phrases that define the events of interest for the analyst, then takes a list of keywords to watch for and generates alerts when it sees matches in log file activity?

Inclusive analysis

Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

Executive buy-in

There is not universal agreement on the names of the layers in the TCP/IP networking model. Which of the following is one of the functions of the bottom layer which is sometimes called the Network Access or Link Layer?

Defines the procedures for interfacing with Ethernet devices

Which of the following attack vectors are addressed by Xinetd and TCP Wrappers?

Outsider attack from a telephone

Which of the following statements about DMZ are true?

It is the boundary between the Internet and a private network.

It contains company resources that are available on the Internet, such as Web servers and FTP servers.

Which of the following are network connectivity devices?

Hub

Repeater

Bridge

Brouter

You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data.

Which of the following options will you choose to accomplish this?

Take a full backup daily with the previous night's tape taken offsite.

What is the common payment mechanism expected for victims of ransomware?

Bitcoin

What protocol would a Philips Hue light bulb use to communicate with a controller?

Zigbee

Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

SUDO

Why would you implement accounting?

Why would you implement accounting?

A US case involving malicious code is brought to trial. An employee had opened a helpdesk ticket to report specific instances of strange behavior on her system.

The IT helpdesk representative collected information by interviewing the user and escalated the ticket to the system administrators. As the user had regulated and sensitive data on her computer, the system administrators had the hard drive sent to the company's forensic consultant for analysis and configured a new hard drive for the user.

Based on the recommendations from the forensic consultant and the company's legal department, the CEO decided to prosecute the author of the malicious code.

During the court case, which of the following would be able to provide direct evidence?

The user of the infected system

When you are deploying an intrusion prevention system on your network, what is the most important criterion?

It has a low latency.

What are Duqu and Stuxnet examples of?

Information warfare

What is KRACK used for?

Key reinstallation

What is one limitation of containers as compared with virtual machines?

Uses the same operating system

Which protocol is part of the base Windows operating system and enables you to remotely manage a Windows system?

WinRM

What is one reason to ensure virtual machine software is updated regularly?

Vulnerabilities could lead to breaking out.

Which web-based encryption mechanism has not been deprecated at the time of this writing?

TLSv1.3

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering?

Failover

Load balancing

A sensor that uses a light beam and a detecting plate to alarm if the light beam is obstructed is most commonly used to identify which of the following threats?

Smoke

Which of the following choices accurately describes how PGP works when encrypting email?

PGP creates a random asymmetric key that it uses to encrypt the message, then encrypts this key with the recipient's public key

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

Privacy policy

What is the first thing that should be done during the containment step of incident handling?

Secure the area

Two clients connecting from the same public IP address (for example - behind the same NAT firewall) can connect simultaneously to the same web server on the Internet, provided what condition is TRUE?

The client-side source ports are different.

Which of the following is not one of the layers in the OSI model?

Internet

You work as a Network Administrator for McNeil 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's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:The wireless network communication should be secured.The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps: Configure 802.1x and WEP for the wireless connections.Configure the PEAP-MS-CHAP v2 protocol for authentication.What will happen after you have taken these steps?

The wireless network communication will be secured.

You have been asked to provide advice on how best to protect a session ID in a homegrown web application. What do you tell the developer

Make use of a timestamp and a piece of identifying information from the client to generate the session ID.

How could you enforce a corporate policy that requires all Bluetooth devices to have discoverable mode disabled?

Use BlueScanner.

An IT security manager is trying to quickly assess the risks associated with not implementing a corporate firewall system. What sort of risk assessment is most appropriate?

Qualitative risk assessment

A substitution steganography uses this part of a carrier file.

The most insignificant portions of the carrier

You work as a Network Administrator for Rick International. The company has a TCP/IP-based network. A user named Kevin wants to set an SSH terminal at home to connect to the company's network. You have to configure your company's router for it.By default, which of the following standard ports does the SSH protocol use for connection?

22

In the network 192.168.5.0/23, what would be the broadcast address?

192.168.5.255

For most organizations, which of the following should be the highest priority when it comes to physical security concerns?

Ensuring employee safety

Which of the following are used to suppress gasoline and oil fires?

CO2 Soda acid Halon