Question #1 *Topic 1*

Sarah works as a Web Developer for XYZ CORP. She is creating a Web site for her company. Sarah wants greater control over the appearance and presentation of Web pages. She wants the ability to precisely specify the display attributes and the appearance of elements on the Web pages. How will she accomplish this?

A. Use the Database Design wizard.

B. Make two templates, one for the index page and the other for all other pages.

C. Use Cascading Style Sheet (CSS).

D. Make a template and use it to create each Web page.

Suggested Answer: *C*

Sarah should use the Cascading Style Sheet (CSS) while creating Web pages. This will give her greater control over the appearance and presentation of the Web pages and will also enable her to precisely specify the display attributes and the appearance of elements on the Web pages.

Community vote distribution

(%100) C

WOODPACKER 7 months, 1 week ago

Selected Answer: C

Edit all ugi

upvoted 1 times

Question #2 *Topic 1*

You work as a Network Administrator for XYZ CORP. The company has a Windows Server 2008 network environment. The network is configured as a Windows
Active Directory-based single forest single domain network. You have installed a Windows Server 2008 computer. You have configured auditing on this server.
The client computers of the company use the Windows XP Professional operating system. You want to audit each event that is related to a user managing an account in the user database on the computer where the auditing is configured. To accomplish the task, you have enabled the Audit account management option on the server.
Which of the following events can be audited by enabling this audit option?

A. Access to an Active Directory object

B. Change of password for a user account

C. Addition of a user account to a group

D. Creation of a user account

Suggested Answer: *BCD*
Audit account management is one of the nine audit settings that can be configured on a Windows computer. This option is enabled to audit each event that is related to a user managing an account in the user database on the computer where the auditing is configured. These events include the following:
⇨ Creating a user account
⇨ Adding a user account to a group
⇨ Renaming a user account
⇨ Changing password for a user account
This option is also used to audit the changes to the domain account of the domain controllers.

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Which of the following types of firewall functions at the Session layer of OSI model?

A. Packet filtering firewall

B. Circuit-level firewall

C. Switch-level firewall

D. Application-level firewall

Suggested Answer: *B*
Circuit-level firewall operates at the Session layer of the OSI model. This type of firewall regulates traffic based on whether or not a trusted connection has been established.

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

You work as a Network Administrator for NetTech Inc. Your computer has the Windows 2000 Server operating system. You want to harden the security of the server.
Which of the following changes are required to accomplish this? (Choose two)

A. Remove the Administrator account.

B. Disable the Guest account.

C. Rename the Administrator account.

D. Enable the Guest account.

Suggested Answer: *BC*
For security, you will have to rename the Administrator account and disable the Guest account. Renaming the Administrator account will ensure that hackers do not break into the network or computer by guessing the password of the Administrator account. You can also create a fake Administrator account that has no privileges and audit its use to detect attacks. Disabling the Guest account will prevent users who do not have a domain or local user account from illegally accessing the network or computer. By default, the Guest account is disabled on systems running Windows 2000 Server. If the Guest account is enabled, you will have to disable it.

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

What does CSS stand for?

A. Cascading Style Sheet

B. Coded System Sheet

C. Cyclic Style Sheet

D. Cascading Style System

Suggested Answer: *A*

A Cascading Style Sheet (CSS) is a separate text file that keeps track of design and formatting information, such as colors, fonts, font sizes, and margins, used in

Web pages. CSS is used to provide Web site authors greater control on the appearance and presentation of their Web pages. It has codes that are interpreted and applied by the browser on to the Web pages and their elements. CSS files have .css extension.

There are three types of Cascading Style Sheets:

⇨ External Style Sheet

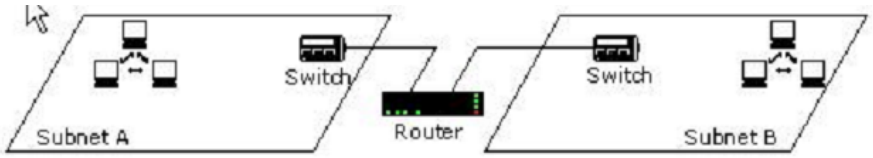
⇨ Embedded Style Sheet

⇨ Inline Style Sheet

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

You work as a Network Administrator for Blue Well Inc. The company has a TCP/IP-based routed network. Two segments have been configured on the network as shown below:



One day, the switch in Subnet B fails. What will happen?

A. Communication between the two subnets will be affected.

B. The whole network will collapse.

C. Workstations on Subnet A will become offline

D. Workstations on Subnet B will become offline.

Suggested Answer: *AD*

According to the question, the network is a routed network where two segments have been divided and each segment has a switch. These switches are connected to a common router. All workstations in a segment are connected to their respective subnet's switches.

Failure of the switch in Subnet B will make all workstations connected to it offline. Moreover, communication between the two subnets will be affected, as there will be no link to connect to Subnet B.

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

You work as the Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are a root user on the Red Hat operating system.
You want to keep an eye on the system log file /var/adm/messages.
Which of the following commands should you use to read the file in real time?

A. tail -n 3 /var/adm/messages

B. tail -f /var/adm/messages

C. cat /var/adm/messages

D. tail /var/adm/messages

Suggested Answer: *B*
Using the -f option causes tail to continue to display the file in real time, showing added lines to the end of the file as they occur.

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to use Kismet as a wireless sniffer to sniff the We-are-secure network.
Which of the following IEEE-based traffic can be sniffed with Kismet?

A. 802.11g

B. 802.11n

C. 802.11b

D. 802.11a

Suggested Answer: *ABCD*
Kismet can sniff IEEE 802.11a, 802.11b, 802.11g, and 802.11n-based wireless network traffic.

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

In which of the following is absolute size of frames expressed?

A. Bits

B. Percentage

C. Inches

D. Pixels

Suggested Answer: *D*

Absolute size of frames is expressed in pixels. Size is expressed in terms of the number of pixels in a frame. Therefore, a change in the screen area of a display device does not affect the absolute frame size of a Web page.

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

What are the different categories of PL/SQL program units?

A. Default

B. Unnamed

C. Primary

D. Named

Suggested Answer: *BD*

A named block is a PL/SQL block that Oracle stores in the database and can be called by name from any application. A named block is also known as a stored procedure. Named blocks can be called from any PL/SQL block. It has a declaration section, which is known as a header. The header may include the name of a block, type of the block, and parameter. The name and list of formal parameters are known as the signature of a subroutine. Once a named PL/SQL block is compiled, it gets permanently stored as p-code after compilation in the shared pool of the system global area. Therefore, the named block gets compiled only once.

An anonymous block is a PL/SQL block that appears in a user's application and is neither named nor stored in the database. This block does not allow any mode of parameter. Anonymous block programs are effective in some situations. They are basically used when building scripts to seed data or perform one-time processing activities. They are also used when a user wants to nest activity in another PL/SQL block's execution section. Anonymous blocks are compiled each time they are executed.

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

You work as a Network Administrator for XYZ CORP. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. 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?

A. Both tasks will be accomplished.

B. The laptop users will be able to use smart cards for getting authenticated.

C. The wireless network communication will be secured.

D. None of the tasks will be accomplished.

Suggested Answer: *C*
As 802.1xand WEP are configured, this step will enable the secure wireless network communication. For authentication, you have configured the PEAP-MS-
CHAP v2 protocol. This protocol can be used for authentication on wireless networks, but it cannot use a public key infrastructure (PKI). No certificate can be issued without a PKI. Smart cards cannot be used for authentication without certificates. Hence, the laptop users will not be able to use smart cards for getting authenticated.

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. 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 take to accomplish the task?

A. Implement the open system authentication for the wireless network.

B. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.

C. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.

D. Implement the IEEE 802.1X authentication for the wireless network.

E. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.

Suggested Answer: *BCD*
In order to enable wireless networking, you have to install access points in various areas of your office building. These access points generate omni directional signals to broadcast network traffic. Unauthorized users can intercept these packets. Hence, security is the major concern for a wireless network. The two primary threats are unauthorized access and data interception.
In order to accomplish the task, you will have to take the following steps:
Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only. This will prevent the sales team members from communicating directly to one another.
Implement the IEEE 802.1X authentication for the wireless network. This will allow only authenticated users to access the network data and resources.
Configure the wireless network to use WEP encryption for data transmitted over a wireless network. This will encrypt the network data packets transmitted over wireless connections.
Although WEP encryption does not prevent intruders from capturing the packets, it prevents them from reading the data inside.

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Anonymizers are the services that help make a user's own Web surfing anonymous. An anonymizer removes all the identifying information from a user's computer while the user surfs the Internet. It ensures the privacy of the user in this manner. After the user anonymizes a Web access with an anonymizer prefix, every subsequent link selected is also automatically accessed anonymously.
Which of the following are limitations of anonymizers?

A. ActiveX controls

B. Plugins

C. Secure protocols

D. Java applications

E. JavaScript

Suggested Answer: *ABCDE*
Anonymizers have the following limitations:
1. HTTPS: Secure protocols such as 'https:' cannot be properly anonymized, as the browser needs to access the site directly to properly maintain the secure encryption.
2.Plugins: If an accessed site invokes a third-party plugin, there is no guarantee of an established independent direct connection from the user computer to a remote site.
3.Java: Any Java application accessed through an anonymizer will not be able to bypass the Java security wall.
4.ActiveX: ActiveX applications have almost unlimited access to the user's computer system.
5.JavaScript: The JavaScript scripting language is disabled with URL-based anonymizers.

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You are concerned about the vulnerabilities existing in the network of the company.
Which of the following can be a cause for making the network vulnerable? (Choose two)

A. Use of well-known code

B. Use of uncommon code

C. Use of uncommon software

D. Use of more physical connections

Suggested Answer: *AD*
In computer security, the term vulnerability is a weakness which allows an attacker to reduce a system's Information Assurance. A computer or a network can be vulnerable due to the following reasons:
Complexity: Large, complex systems increase the probability of flaws and unintended access points.
Familiarity: Using common, well-known code, software, operating systems, and/or hardware increases the probability an attacker has or can find the knowledge and tools to exploit the flaw.
Connectivity: More physical connections, privileges, ports, protocols, and services and time each of those are accessible increase vulnerability.
Password management flaws: The computer user uses weak passwords that could be discovered by brute force. The computer user stores the password on the computer where a program can access it. Users re-use passwords between many programs and websites.
Fundamental operating system design flaws: The operating system designer chooses to enforce sub optimal policies on user/program management. For example, operating systems with policies such as default permit grant every program and every user full access to the entire computer. This operating system flaw allows viruses and malware to execute commands on behalf of the administrator.
Internet Website Browsing: Some Internet websites may contain harmful Spyware or Adware that can be installed automatically on the computer systems. After visiting those websites, the computer systems become infected and personal information will be collected and passed on to third party individuals.
Software bugs: The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.
Unchecked user input: The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as Buffer overflows, SQL injection or other non-validated inputs).
Answers B, C are incorrect. Use of common software and common code can make a network vulnerable.

Question #15 *Topic 1*

You work as a Java Programmer for JavaSkills Inc. You are working with the Linux operating system. Nowadays, when you start your computer, you notice that your OS is taking more time to boot than usual. You discuss this with your Network Administrator. He suggests that you mail him your Linux bootup report.
Which of the following commands will you use to create the Linux bootup report?

A. touch bootup_report.txt

B. dmesg > bootup_report.txt

C. dmesg | wc

D. man touch

Suggested Answer: *B*
According to the scenario, you can use dmesg > bootup_report.txt to create the bootup file. With this command, the bootup messages will be displayed and will be redirected towards bootup_report.txt using the > command.

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Adam works on a Linux system. He is using Sendmail as the primary application to transmit e-mails. Linux uses Syslog to maintain logs of what has occurred on the system.
Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?

A. /var/log/mailog

B. /var/log/logmail

C. /log/var/mailog

D. /log/var/logd

Suggested Answer: *A*
/var/log/mailog generally contains the source and destination IP addresses, date and time stamps, and other information that may be used to check the information contained within an e-mail header. Linux uses Syslog to maintain logs of what has occurred on the system. The configuration file /etc/syslog.conf is used to determine where the Syslog service (Syslogd) sends its logs. Sendmail can create event messages and is usually configured to record the basic information such as the source and destination addresses, the sender and recipient addresses, and the message ID of e-mail. The syslog.conf will display the location of the log file for e-mail.

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Which of the following statements about session tracking is true?

A. When using cookies for session tracking, there is no restriction on the name of the session tracking cookie.

B. When using cookies for session tracking, the name of the session tracking cookie must be jsessionid.

C. A server cannot use cookie as the basis for session tracking.

D. A server cannot use URL rewriting as the basis for session tracking.

Suggested Answer: *B*

If you are using cookies for session tracking, the name of the session tracking cookie must be jsessionid. A jsessionid can be placed only inside a cookie header.

You can use HTTP cookies to store information about a session. The servlet container takes responsibility of generating the session ID, making a new cookie object, associating the session ID into the cookie, and setting the cookie as part of response.

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

A Web developer with your company wants to have wireless access for contractors that come in to work on various projects. The process of getting this approved takes time. So rather than wait, he has put his own wireless router attached to one of the network ports in his department. What security risk does this present?

A. None, adding a wireless access point is a common task and not a security risk.

B. It is likely to increase network traffic and slow down network performance.

C. This circumvents network intrusion detection.

D. An unauthorized WAP is one way for hackers to get into a network.

Suggested Answer: *D*
Any unauthorized Wireless Access Point (WAP) is a serious security breach. Its configuration might be very unsecure. For example, it might not use encryption or
MAC filtering, thus allowing anyone in range to get on the network.

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

An auditor assesses the database environment before beginning the audit. This includes various key tasks that should be performed by an auditor to identify and prioritize the users, data, activities, and applications to be monitored.
Which of the following tasks need to be performed by the auditor manually?

A. Classifying data risk within the database systems

B. Monitoring data changes and modifications to the database structure, permission and user changes, and data viewing activities

C. Analyzing access authority

D. Archiving, analyzing, reviewing, and reporting of audit information

Suggested Answer: *AC*
The Internal Audit Association lists the following as key components of a database audit:
Create an inventory of all database systems and use classifications. This should include production and test data. Keep it up-to-date.
Classify data risk within the database systems. Monitoring should be prioritized for high, medium, and low risk data.
Implement an access request process that requires database owners to authorize the "roles" granted to database accounts (roles as in Role Based Access and not the native database roles).
Analyze access authority. Users with higher degrees of access permission should be under higher scrutiny, and any account for which access has been suspended should be monitored to ensure access is denied, attempts are identified.
Assess application coverage. Determine what applications have built-in controls, and prioritize database auditing accordingly. All privileged user access must have audit priority. Legacy and custom applications are the next highest priority to consider, followed by the packaged applications.
Ensure technical safeguards. Make sure access controls are set properly.
Audit the activities. Monitor data changes and modifications to the database structure, permission and user changes, and data viewing activities. Consider using network-based database activity monitoring appliances instead of native database audit trails.
Archive, analyze, review, and report audit information. Reports to auditors and IT managers must communicate relevant audit information, which can be analyzed and reviewed to determine if corrective action is required. Organizations that must retain audit data for long-term use should archive this information with the ability to retrieve relevant data when needed.
The first five steps listed are to be performed by the auditor manually.
Answers B, D are incorrect. These tasks are best achieved by using an automated solution.

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Which of the following is Microsoft's implementation of the file and application server for the Internet and private intranets?

A. Internet Server Service (ISS)

B. Internet Server (IS)

C. WWW Server (WWWS)

D. Internet Information Server (IIS)

Suggested Answer: *D*

Microsoft Internet Information Server (IIS)is a Web Application server for the Internet and private intranets. IIS receives requests from users on the network using the World Wide Web (WWW) service and transmits information using the Hypertext Transport Protocol (HTTP). IIS uses Microsoft Transaction Server (MTS) to provide security, performance, and scalability with server side packages.

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Which of the following statements about a perimeter network are true? (Choose three)

A. It has a connection to the Internet through an external firewall and a connection to an internal network through an interior firewall.

B. It has a connection to a private network through an external firewall and a connection to an internal network through an interior firewall.

C. It is also known as a demilitarized zone or DMZ.

D. It prevents access to the internal corporate network for outside users.

Suggested Answer: *ACD*

A perimeter network, also known as a demilitarized zone or DMZ, is a small network that lies in between the Internet and a private network. It has a connection to the Internet through an external firewall and a connection to the internal network through an interior firewall. It allows outside users access to the specific servers located in the perimeter network while preventing access to the internal corporate network. Servers, routers, and switches that maintain security by preventing the internal network from being exposed on the Internet are placed in a perimeter network. A perimeter network is commonly used for deploying e-mail and Web servers for a company.

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

You work as the Project Engineer for XYZ CORP. The company has a Unix-based network. Your office consists of one server, seventy client computers, and one print device. You raise a request for printing a confidential page. After 30 minutes, you find that your print request job is not processed and is at the seventh position in the printer queue. You analyze that it shall take another one hour to print. You decide to remove your job from the printer queue and get your page printed outside the office.
Which of the following Unix commands can you use to remove your job from the printer queue?

A. tunelp

B. pr

C. lprm

D. gs

Suggested Answer: *C*
The basic Unix printing commands are as follows:
banner: It is used to print a large banner on a printer.
lpr: It is used to submit a job to the printer.
lpc: It enables one to check the status of the printer and set its state. lpq: It shows the contents of a spool directory for a given printer. lprm: It is used to remove a job from the printer queue. gs: It works as a PostScript interpreter. pr: It is used to print a file. tunelp: It is used to set various parameters for the lp device.

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

An executive in your company reports odd behavior on her PDA. After investigation you discover that a trusted device is actually copying data off the PDA. The executive tells you that the behavior started shortly after accepting an e-business card from an unknown person.
What type of attack is this?

A. Session Hijacking

B. Bluesnarfing

C. Privilege Escalation

D. PDA Hijacking

Suggested Answer: *B*
Bluesnarfing is a rare attack in which an attacker takes control of a bluetooth enabled device. One way to do this is to get your PDA to accept the attacker's device as a trusted device.

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which of the following is a technique for creating Internet maps? (Choose two)

A. AS PATH Inference

B. Object Relational Mapping

C. Active Probing

D. Network Quota

Suggested Answer: *AC*

There are two prominent techniques used today for creating Internet maps:

Active probing: It is the first works on the data plane of the Internet and is called active probing. It is used to infer Internet topology based on router adjacencies.

AS PATH Inference: It is the second works on the control plane and infers autonomous system connectivity based on BGP data.

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

You work as a Network Administrator for XYZ CORP. The company has a Linux-based network. The company needs to provide secure network access. You have
configured a firewall to prevent certain ports and applications from forwarding the packets to the company's intranet.
What does a firewall check to prevent these ports and applications from forwarding the packets to the intranet?

A. The network layer headers and the session layer port numbers

B. The application layer port numbers and the transport layer headers

C. The transport layer port numbers and the application layer headers

D. The presentation layer headers and the session layer port numbers

Suggested Answer: *C*
A firewall stops delivery of packets that are not marked safe by the Network Administrator. It checks the transport layer port numbers and the application layer
headers to prevent certain ports and applications from forwarding the packets to an intranet.

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

You work as a Web Deployer for UcTech Inc. You write the <security constraint> element for an application in which you write the <auth-constraint> sub-element as follows: <auth-constraint> <role-name>*</role-name> </auth-constraint> Who will have access to the application?

A. Only the administrator

B. No user

C. All users

D. It depends on the application.

Suggested Answer: *C*

The <auth-constraint> element is a sub-element of the <security-constraint> element. It defines the roles that are allowed to access the Web resources specified by the <web-resource-collection> sub-elements.

The <auth-constraint> element is written in the deployment descriptor as follows:

<security-constraint> <web-resource-collection> ---------- </web-resource-collection> <auth-constraint> <role-name>Administrator</role-name> </auth- constraint> </security-constraint>

Writing Administrator within the <role-name> element will allow only the administrator to have access to the resource defined within the <web-resource-collection> element.

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Patricia joins XYZ CORP., as a Web Developer. While reviewing the company's Web site, she finds that many words including keywords are misspelled.
How will this affect the Web site traffic?

A. Leave a bad impression on users.

B. Search engine relevancy may be altered.

C. Link exchange with other sites becomes difficult.

D. The domain name cannot be registered.

Suggested Answer: *B*
Web site traffic depends upon the number of users who are able to locate a Web site. Search engines are one of the most frequently used tools to locate Web sites. They perform searches on the basis of keywords contained in the Web pages of a Web site. Keywords are simple text strings that are associated with one or more topics of a Web page. Misspelled keywords prevent Web pages from being displayed in the search results.

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

You work as a Network Administrator for BetaTech Inc. You have been assigned the task of designing the firewall policy for the company. Which of the following statements is unacceptable in the 'acceptable use statement' portion of the firewall policy?

A. The computers and their applications should be used for organizational related activities only.

B. Computers may not be left unattended with a user account still logged on.

C. Applications other than those supplied or approved by the company can be installed on any computer.

D. The installed e-mail application can only be used as the authorized e-mail service.

Suggested Answer: *C*
stand true in the 'acceptable use statement' portion of the firewall policy.

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

In which of the following CAATs (Computer Assisted Auditing Techniques) does an auditor perform tests on computer files and databases?

A. Parallel Simulation

B. Generalized Audit Software (GAS)

C. Test Data

D. Custom Audit Software (CAS)

Suggested Answer: *B*
CAATs (Computer Assisted Auditing Techniques) are used to test application controls as well as perform substantive tests on sample items.
Following are the types of CAATs:
Generalized Audit Software (GAS): It allows the auditor to perform tests on computer files and databases.
Custom Audit Software (CAS): It is generally written by auditors for specific audit tasks. CAS is necessary when the organization's computer system is not compatible with the auditor's GAS or when the auditor wants to conduct some testing that may not be possible with the GAS.
Test Data: The auditor uses test data for testing the application controls in the client's computer programs. The auditor includes simulated valid and invalid test data, used to test the accuracy of the computer system's operations. This technique can be used to check data validation controls and error detection routines, processing logic controls, and arithmetic calculations, to name a few.
Parallel Simulation: The auditor must construct a computer simulation that mimics the client's production programs.
Integrated TestFacility: The auditor enters test data along with actual data in a normal application run.

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He successfully performs a brute force attack on the We-are-secure server. Now, he suggests some countermeasures to avoid such brute force attacks on the We-are-secure server.
Which of the following are countermeasures against a brute force attack?

A. The site should use CAPTCHA after a specific number of failed login attempts.

B. The site should increase the encryption key length of the password.

C. The site should restrict the number of login attempts to only three times.

D. The site should force its users to change their passwords from time to time.

Suggested Answer: *AC*
Using CAPTCHA or restricting the number of login attempts are good countermeasures against a brute force attack.

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 2*

You work as a Software Developer for Cinera Softwares Inc. You create a DHTML page that contains ten TextBox controls to get information from the users who use your application. You want all the components placed on the DHTML page to be repositioned dynamically, when a user resizes the browser window.
Which of the following will you use for this?

A. Use the position attribute of the Cascading Style Sheet.

B. Use the OnResize event for the DHTML page object.

C. Use the Resize event of the Document object.

D. Use the OnResize event of the Cascading Style Sheet.

Suggested Answer: *A*
position attribute of the Cascading Style Sheet. The DHTML page object modal gives access to styles and style sheets. Therefore, you can easily set and change the position of an element. Reference: MSDN, Index "Dynamic HTML(DHTML), in DHTML Applications", "Elements Positioning in DHTML Application", Search
"Positioning", "Dynamic HTML"

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 2*

Which of the following are the limitations for the cross site request forgery (CSRF) attack?

A. The attacker must determine the right values for all the form inputs.

B. The attacker must target a site that doesn't check the referrer header.

C. The target site should have limited lifetime authentication cookies.

D. The target site should authenticate in GET and POST parameters, not only cookies.

Suggested Answer: *AB*
Following are the limitations of cross site request forgeries to be successful:
1. The attacker must target either a site that doesn't check the Referer header (which is common) or a victim with a browser or plugin bug that allows Referer spoofing (which is rare).
2. The attacker must find a form submission at the target site that does something useful to the attacker (e.g., transfers money, or changes the victim's e-mail address or password).
3. The attacker must determine the right values for all the form inputs: if any of them are required to be secret authentication values or IDs that the attacker can't guess, the attack will fail.
4. The attacker must lure the victim to a Web page with malicious code while the victim is logged in to the target site. Since, the attacker can't see what the target
Web site sends back to the victim in response to the forged requests, unless he exploits a cross- site scripting or other bug at the target Web site.
Similarly, the attacker can only "click" any links or submit any forms that come up after the initial forged request, if the subsequent links or forms are similarly predictable. (Multiple "clicks" can be simulated by including multiple images on a page, or by using JavaScript to introduce a delay between clicks). from cross site request forgeries (CSRF) by applying the following countermeasures available:
Requiring authentication in GET and POST parameters, not only cookies.
Checking the HTTP Referer header.
Ensuring there's no crossdomain.xml file granting unintended access to Flash movies.
Limiting the lifetime of authentication cookies.
Requiring a secret, user-specific token in all form submissions prevents CSRF; the attacker's site can't put the right token in its submissions.
Individual Web users can do relatively little to prevent cross-site request forgery.
Logging out of sites and avoiding their "remember me" features can mitigate CSRF risk; not displaying external images or not clicking links in "spam" or unreliable e-mails may also help.

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 2*

Which of the following are attributes of the <TABLE> tag? (Choose three)

A. BORDER

B. ALIGN

C. TD

D. WIDTH

Suggested Answer: *ABD*
The WIDTH attribute of the <TABLE> tag is used to set the width of a table. Width can be specified in pixels and percentage. For example, if a table of the same width as that of the parent object has to be created, the WIDTH attribute must be set to 100%. The ALIGN attribute aligns the table within the text flow. By default alignment is set to left. The BORDER attribute of the <TABLE> tag is used to set the width of the table border.
Answer C is incorrect. <TD> is not an attribute of the <TABLE> tag. It is a tag used to specify cells in a table.

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 2*

You have been assigned a project to develop a Web site for a construction company. You have to develop a Web site and want to get more control over the appearance and presentation of your Web pages. You also want to increase the ability to precisely specify the location and appearance of the elements on a page and create special effects. You plan to use Cascading style sheets (CSS). You want to apply the same style consistently throughout your Web site.
Which type of style sheet will you use?

A. Internal Style Sheet

B. External Style Sheet

C. Inline Style Sheet

D. Embedded Style Sheet

Suggested Answer: *B*
To apply the same style consistently throughout your Web site you should use external style sheet. Cascading style sheets (CSS) are used so that the Web site authors can exercise greater control on the appearance and presentation of their Web pages. And also because they increase the ability to precisely point to the location and look of elements on a Web page and help in creating special effects.
Cascading Style Sheets have codes, which are interpreted and applied by the browser on to the Web pages and their elements.
There are three types of cascading style sheets.

External Style Sheets -
▪
⇨ Embedded Style Sheets
⇨ Inline Style Sheets
External Style Sheets are used whenever consistency in style is required throughout a Web site. A typical external style sheet uses a .css file extension, which can be edited using a text editor such as a Notepad.
Embedded Style Sheets are used for defining styles for an active page.
Inline Style Sheets are used for defining individual elements of a page.
Reference: TechNet, Contents: Microsoft Knowledgebase, February 2000 issue PSS ID Number: Q179628

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 2*

You configure a wireless router at your home. To secure your home Wireless LAN (WLAN), you implement WEP. Now you want to connect your client computer to the WLAN.
Which of the following is the required information that you will need to configure the client computer? (Choose two)

A. SSID of the WLAN

B. WEP key

C. IP address of the router

D. MAC address of the router

Suggested Answer: *AB*
In order to connect a client computer to a secured Wireless LAN (WLAN), you are required to provide the following information:
SSID of the WLAN WEP key rticlesItemsReportsHelp

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 2*

Which of the following is an example of penetration testing?

A. Configuring firewall to block unauthorized traffic

B. Implementing HIDS on a computer

C. Simulating an actual attack on a network

D. Implementing NIDS on a network

Suggested Answer: *C*

Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat
Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration testing is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security of penetration testing.

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 2*

Which of the following commands can you use to search a string 'pwd' in all text files without opening them? (Choose two)

A. vi

B. grep

C. sed

D. locate

Suggested Answer: *BC*
sed and grep are the two commands that can be used to search a specified string in all text files without opening them. sed is a stream editor that is used to perform basic text transformations on an input stream (a file or input from a pipeline).

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 2*

You work as a Database Administrator for Dolliver Inc. The company uses Oracle 11g as its database. You have used the LogMiner feature for auditing purposes.
Which of the following files store a copy of the data dictionary? (Choose two)

A. Online redo log files

B. Operating system flat file

C. Dump file

D. Control file

Suggested Answer: *AB*
LogMiner requires a dictionary to translate object IDs into object names when it returns redo data to you. You have the following three options to retrieve the data dictionary:
The Online catalog: It is the most easy and efficient option to be used. It is used when a database user have access to the source database from which the redo log files were created. The other condition that should qualify is that there should be no changes to the column definitions in the desired tables.
The Redo Log Files: This option is used when a database user does not have access to the source database from which the redo log files were created and if there are any chances of changes to the column definitions of the desired tables.
An operating system flat file: Oracle does not recommend to use this option, but it is retained for backward compatibility. The reason for not preferring the option is that it does not guarantee transactional consistency. LogMiner is capable to access the Oracle redo logs. It keeps the complete record of all the activities performed on the database, and the associated data dictionary, which is used to translate internal object identifiers and types to external names and data formats.
For offline analysis, LogMiner can be run on a separate database, using archived redo logs and the associated dictionary from the source database.

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 2*

You work as a Network Administrator for XYZ CORP. The company's Windows 2000 network is configured with Internet Security and Acceleration (ISA) Server
2000. ISA Server is configured as follows: The server uses the default site and content rule and default IP packet filters. Packet filtering is enabled. The server has two protocol rules:

Name of the Rule	Scope	Action	Protocol	Applies To	Schedule
Web-Secure	Array	Allow	HTTPS	Any request	Always
Web	Array	Allow	HTTPS	Any request	Always

Users in the network complain that they are unable to access secure Web sites. However, they are able to connect to Web sites in which secure transmission is not required.
What is the most likely cause?

A. A protocol rule that allows the use of HTTP has not been created.

B. An IP packet filter that allows the use of network traffic on port 80 has not been created.

C. An IP packet filter that allows the use of network traffic on port 443 has not been created.

D. A protocol rule that allows the use of HTTPS has not been created.

Suggested Answer: *C*
The default IP packet filter allows HTTP protocol (for non-secure communication) at port 80 to access the Internet. However, to allow users to access secure Web sites, you will have to create an additional packet filter to allow communication on port 443.

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 2*

Which of the following statements about packet filtering is true?

A. It allows or restricts the flow of specific types of packets to provide security.

B. It is used to send confidential data on the public network.

C. It allows or restricts the flow of encrypted packets to provide security.

D. It is used to store information about confidential data.

Suggested Answer: *A*

Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet.

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 2*

You work as a Security Administrator in Tech Perfect Inc. The company has a TCP/IP based network. The network has a vast majority of Cisco Systems routers and Cisco network switches. You have implemented four VPN connections in the network. You use the Cisco IOS on the network. Which feature will you enable to maintain a separate routing and forwarding table for each VPN?

A. Intrusion Prevention System

B. VRF-aware firewall

C. Virtual Private Network

D. Stateful firewall

Suggested Answer: *B*
In this scenario, the company's network has a vast majority of Cisco Systems routers and Cisco network switches. The security administrator of the company has implemented four VPN connections in the network and uses the Cisco IOS on the network. He needs to maintain a separate routing and forwarding table for each
VPN in order to provide more secure communication. To accomplish this task, he should enable the VRF-aware firewall feature on the Cisco IOS routers.

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 2*

Which of the following commands can be used to intercept and log the Linux kernel messages?

A. syslogd

B. klogd

C. sysklogd

D. syslog-ng

Suggested Answer: *BC*

The klogd and sysklogd commands can be used to intercept and log the Linux kernel messages.

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 2*

Which of the following are the reasons for implementing firewall in any network?

A. Create a choke point

B. Log Internet activity

C. Log system activity

D. Limit access control

E. Implementing security policy

F. Limit network host exposure

Suggested Answer: *ABEF*

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria. The four important roles of a firewall are as follows:

1. Implement security policy: A firewall is a first step in implementing security policies of an organization. Different policies are directly implemented at the firewall.

A firewall can also work with network routers to implement Types-Of-Service (ToS) policies.

2. Creating a choke point: A firewall can create a choke point between a private network of an organization and a public network. With the help of a choke point the firewall devices can monitor, filter, and verify all inbound and outbound traffic.

3. Logging Internet activity: A firewall also enforces logging of the errors and faults. It also provides alarming mechanism to the network.

4. Limiting network host exposure: A firewall can create a perimeter around the network to protect it from the Internet. It increases the security by hiding internal information.

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 2*

Samantha works as a Web Developer for XYZ CORP. She is designing a Web site for the company. In a Web page, she uses the HTTP-EQUIV attribute to control the page cache.
Which of the following HTTP-EQUIV values controls the page cache in the browser folder?

A. Window-target

B. Status-code

C. Content-type

D. Pragma

Suggested Answer: *D*
HTTP-EQUIV is an attribute of the META tag. It sets or retrieves information used to bind the META tag's content to an HTTP response header. The pragma value of HTTP-EQUIV controls the page cache.

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 2*

You work as a Software Developer for Mansoft Inc. You create an application and use it to create users as members of the local Users group. Which of the following code snippets imperatively demands that the current user is a member of the local Users group?

A. System.AppDomain.CurrentDomain.SetPrincipalPolicy(PrincipalPolicy.WindowsPrincipal); PrincipalPermission MyPermission = new PrincipalPermission(null, @"BUILTIN\Users", true); MyPermission.Demand();

B. PrincipalPermission MyPermission = new PrincipalPermission(null, @"BUILTIN\Users", true); MyPermission.Demand();

C. System.AppDomain.CurrentDomain.SetPrincipalPolicy(PrincipalPolicy.WindowsPrincipal); PrincipalPermission MyPermission = newPrincipalPermission(null, @"Users", true); MyPermission.Demand();

D. PrincipalPermission MyPermission = new PrincipalPermission(null, @"Users", true); MyPermission.Demand();

Suggested Answer: *AC*

The PrincipalPermission class allows security checks against the active principal. This is done by using the language constructs that are defined for both imperative and declarative security actions. To perform an imperative security demand for membership in a built-in Microsoft Windows group, you must first set the default principal policy to the Windows principal by calling the SetPrincipalPolicy (PrincipalPolicy.WindowsPrincipal) statement. Construct a PrincipalPermission object specifying the group name. To specify the group name, you can provide just the group name, or you can preface the group name with either "BUILTIN\" or the computer name and a backslash. Finally, call the PrincipalPermission.Demand method. There is another method of identifying group membership, i.e. by using the PrincipalPermissionclass or the PrincipalPermissionAttribute attribute derived from the System.Security.Permissions namespace. The PrincipalPermission object identifies that the identity of the active principal should match its information with the identity information that is passed to its constructor. The identity information contains the user's identity name and role.

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 2*

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You have configured a firewall on the network. A filter has been applied to block all the ports. You want to enable sending and receiving of emails on the network.
Which of the following ports will you open? (Choose two)

A. 25

B. 20

C. 80

D. 110

Suggested Answer: *AD*
In order to enable email communication, you will have to open ports 25 and 110. Port 25 is used by SMTP to send emails. Port 110 is used by POP3 to receive emails.

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 2*

What is the purpose of Cellpadding attribute of <Table> tag?

A. Cellpadding is used to set the width of cell border and its content.

B. Cellpadding is used to set the width of a table.

C. Cellpadding is used to set the space between the cell border and its content.

D. Cellpadding is used to set the space between two cells in a table.

Suggested Answer: *C*
Cellpadding attribute is used to set the space, in pixels, between the cell border and its content. If you have not set the value of Cellpadding attribute for a table, the browser takes the default value as 1.

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 2*

You are the Network Administrator for a company. You have decided to conduct a user access and rights review.
Which of the following would be checked during such a review? (Choose three)

A. Access Control Lists

B. Encryption Methods

C. User Roles

D. Firewalls

E. Group Membership

Suggested Answer: *ACE*
A user access and rights review must check all users, what groups they belong to, what roles they have, and what access they have. Furthermore, such a review should also check logs to see if users are appropriately utilizing their system rights and privileges.

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 2*

Which of the following statements are true about KisMAC?

A. It scans for networks passively on supported cards.

B. It cracks WEP and WPA keys by Rainbow attack or by dictionary attack.

C. It is a wireless network discovery tool for Mac OS X.

D. Data generated by KisMAC can also be saved in pcap format.

Suggested Answer: *ACD*

KisMAC is a wireless network discovery tool for Mac OS X. It has a wide range of features, similar to those of Kismet, its Linux/BSD namesake and far exceeding those of NetStumbler, its closest equivalent on Windows. The program is geared toward network security professionals, and is not as novice-friendly as similar applications. KisMAC will scan for networks passively on supported cards - including Apple's AirPort, and AirPort Extreme, and many third-party cards, and actively on any card supported by Mac OS X itself. Cracking of WEP and WPA keys, both by brute force, and exploiting flaws such as weak scheduling and badly generated keys is supported when a card capable of monitor mode is used, and packet reinjection can be done with a supported card. GPS mapping can be performed when an NMEA compatible GPS receiver is attached. Data can also be saved in pcap format and loaded into programs such as Wireshark.

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 2*

Which of the following methods will free up bandwidth in a Wireless LAN (WLAN)?

A. Change hub with switch.

B. Deploying a powerful antenna.

C. Disabling SSID broadcast.

D. Implement WEP.

Suggested Answer: *C*

Disabling SSID broadcast will free up bandwidth in a WLAN environment. It is used to enhance security of a Wireless LAN (WLAN). It makes difficult for attackers to find the access point (AP). It is also used by enterprises to prevent curious people from trying to access the WLAN.

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 2*

You work as the Network Technician for XYZ CORP. The company has a Linux-based network. You are working on the Red Hat operating system.
You want to view only the last 4 lines of a file named /var/log/cron.
Which of the following commands should you use to accomplish the task?

A. tail -n 4 /var/log/cron

B. tail /var/log/cron

C. cat /var/log/cron

D. head /var/log/cron

Suggested Answer: *A*
The tail -n 4 /var/log/cron command will show the last four lines of the file /var/log/cron.

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 2*

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You want to use multiple security countermeasures to protect the integrity of the information assets of the company. To accomplish the task, you need to create a complex and multi-layered defense system.
Which of the following components can be used as a layer that constitutes 'Defense in depth'? (Choose three)

A. Backdoor

B. Firewall

C. Antivirus software

D. Intrusion detection

Suggested Answer: *BCD*
The components of Defense in depth include antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection, and biometric verification. In addition to electronic countermeasures, physical protection of business sites along with comprehensive and ongoing personnel training enhances the security of vital data against compromise, theft, or destruction.
Answer A is incorrect. A backdoor is any program that allows a hacker to connect to a computer without going through the normal authentication process. The main advantage of this type of attack is that the network traffic moves from inside a network to the hacker's computer. The traffic moving from inside a network to the outside world is typically the least restrictive, as companies are more concerned about what comes into a network, rather than what leaves it. It, therefore, becomes hard to detect backdoors.

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 2*

Which of the following statements are true about SSIDs?

A. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.

B. SSIDs are case insensitive text strings and have a maximum length of 64 characters.

C. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.

D. SSID is used to identify a wireless network.

Suggested Answer: *ACD*
SSID stands for Service SetIdentifier. It is used to identify a wireless network. SSIDs are case sensitive text strings and have a maximum length of 32 characters.
All wireless devices on a wireless network must have the same SSID in order to communicate with each other. The SSID on computers and the devices in WLAN can be set manually and automatically. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict. A network administrator often uses a public SSID that is set on the access point. The access point broadcasts SSID to all wireless devices within its range. Some newer wireless access points have the ability to disable the automatic SSID broadcast feature in order to improve network security.

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 2*

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You want to configure the ACL with a Cisco router.
Which of the following router prompts can you use to accomplish the task?

A. router(config-if)#

B. router(config)#

C. router(config-ext-nacl)#

D. router#

Suggested Answer: *C*
The auditor of a Cisco router should be familiar with the variety of privilege modes. The current privilege mode can be quickly identified by looking at the current router prompt. The prime modes of a Cisco router are as follows:
⇨ #Nonprivileged mode: router>
⇨ #Priviledged mode: router#
⇨ #Global configuration mode: router(config)#
⇨ #Interface configuration mode: router(config-if)#
⇨ #ACL configuration mode: router(config-ext-nacl)#
⇨ #Boot loader mode: router(boot)
⇨ #Remote connectivity config mode: router(config-line)#

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 2*

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He has a data.txt file in which each column is separated by the TAB character. Now, he wants to use this file as input for a data mining software he has created. The problem preventing him from accomplishing his task is that with his data mining software, he has used TAB as a delimiter to distinguish between columns. Hence, he is unable to use this file as input for the software. However, if he somehow replaces the TAB characters of the file with SPACE characters, he can use this file as an input file for his data mining software.
Which of the following commands will John use to replace the TAB characters of the file with SPACE characters?

A. expand -t 1 data.txt > data.txt

B. cat data.txt

C. chmod 755 data.txt

D. touch data.txt

Suggested Answer: *A*
According to the scenario, John can replace the TAB characters with single space characters with the expand command. With the expand -t 1 data.txt > data.txt command, the TABs of data.txt are changed into single spaces and are redirected by using the > command into the data.txt file. Now, John can use the data.txt file as the input file for his data mining software.

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 2*

You are concerned about possible hackers doing penetration testing on your network as a prelude to an attack.
What would be most helpful to you in finding out if this is occurring?

A. Examining your antivirus logs

B. Examining your domain controller server logs

C. Examining your firewall logs

D. Examining your DNS Server logs

Suggested Answer: *C*
Firewall logs will show all incoming and outgoing traffic. By examining those logs, you can do port scans and use other penetration testing tools that have been used on your firewall.

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 2*

Which of the following applications work as mass-emailing worms? (Choose two.)

A. Chernobyl virus

B. I LOVE YOU virus

C. Nimda virus

D. Melissa virus

Suggested Answer: *BC*

The Nimda and I LOVE YOU viruses work as mass-emailing worms.

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 2*

Which of the following commands can be used to find out where commands are located?

A. type

B. which

C. env

D. ls

Suggested Answer: *AB*

The which and type commands can be used to find out where commands are located.

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 2*

Data mining is a process of sorting through data to identify patterns and establish relationships. Which of the following data mining parameters looks for patterns where one event is connected to another event?

A. Sequence or path analysis

B. Forecasting

C. Clustering

D. Association

Suggested Answer: *D*

Data mining is a process of sorting through data to identify patterns and establish relationships. Following are the data mining parameters:

☞ Association: Looking for patterns where one event is connected to another event.

☞ Sequence or path analysis: Looking for patterns where one event leads to another later event.

☞ Classification: Looking for new patterns (may result in a change in the way the data is organized but is acceptable).

☞ Clustering: Finding and visually documenting groups of facts not previously known.

☞ Forecasting: Discovering patterns in data that can lead to reasonable predictions about the future (This area of data mining is known as predictive analytics).

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 3*

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. Rick, your assistant, is configuring some laptops for wireless access. For security, WEP needs to be configured for wireless communication. By mistake, Rick configures different WEP keys in a laptop than that is configured on the Wireless Access Point (WAP).
Which of the following statements is true in such situation?

A. The laptop will be able to access the wireless network but the security will be compromised.

B. The WAP will allow the connection with the guest account's privileges.

C. The laptop will be able to access the wireless network but other wireless devices will be unable to communicate with it.

D. The laptop will not be able to access the wireless network.

Suggested Answer: *D*
In order to communicate with WAP, a wireless device needs to be configured with the same WEP key. If there is any difference in the key, the device will not be able to access and communicate with the wireless network.

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 3*

Which of the following internal control components provides the foundation for the other components and encompasses such factors as management's philosophy and operating style?

A. Information and communication

B. Risk assessment

C. Control activities

D. Control environment

Suggested Answer: *D*
COSO defines internal control as, "a process, influenced by an entity's board of directors, management, and other personnel, that is designed to provide reasonable assurance in the effectiveness and efficiency of operations, reliability of financial reporting, and the compliance of applicable laws and regulations".
The auditor evaluates the organization's control structure by understanding the organization's five interrelated control components, which are as follows:
1. Control Environment: It provides the foundation for the other components and encompasses such factors as management's philosophy and operating style.
2. Risk Assessment: It consists of risk identification and analysis.
3. Control Activities: It consists of the policies and procedures that ensure employees carry out management's directions.
The types of control activities an organization must implement are preventative controls (controls intended to stop an error from occurring), detective controls
(controls intended to detect if an error has occurred), and mitigating controls (control activities that can mitigate the risks associated with a key control not operating effectively).
4. Information and Communication: It ensures the organization obtains pertinent information, and then communicates it throughout the organization.
5. Monitoring: It involves reviewing the output generated by control activities and conducting special evaluations. In addition to understanding the organization's control components, the auditor must also evaluate the organization's General and Application controls. There are three audit risk components: control risk, detection risk, and inherent risk.

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 3*

Brutus is a password cracking tool that can be used to crack the following authentications: HTTP (Basic Authentication) HTTP (HTML Form/CGI) POP3 (Post
Office Protocol v3) FTP (File Transfer Protocol) SMB (Server Message Block) Telnet Which of the following attacks can be performed by Brutus for password cracking?

A. Man-in-the-middle attack

B. Hybrid attack

C. Replay attack

D. Brute force attack

E. Dictionary attack

Suggested Answer: *BDE*
Brutus can be used to perform brute force attacks, dictionary attacks, or hybrid attacks.

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 3*

Andrew works as a Network Administrator for Infonet Inc. The company has a Windows 2003 domain-based network. The network has five Windows 2003 member servers and 150 Windows XP Professional client computers. One of the member servers works as an IIS server. The IIS server is configured to use the
IP address 142.100.10.6 for Internet users and the IP address 16.5.7.1 for the local network. Andrew wants the server to allow only Web communication over the
Internet. He also wants to enable the local network users to access the shared folders and other resources.
How will Andrew configure the IIS server to accomplish this? (Choose three)

A. Enable the IP packet filter.

B. Permit all the ports on the network adapter that uses the IP address142.100.10.6.

C. Permit only port 25 on the network adapter that uses the IP address 142.100.10.6.

D. Permit all the ports on the network adapter that uses the IP address 16.5.7.1.

E. Permit only port 80 on the network adapter that uses the IP address 142.100.10.6.

Suggested Answer: *ADE*
In order to configure the IIS server to allow only Web communication over the Internet, Andrew will have to use IP packet filtering to permit only port 80 on the network adapter that uses the IP address 142.100.10.6 for connecting to the Internet. This is because Web communication uses the Hyper Text Transfer Protocol
(HTTP) that uses the TCP port 80. IP packet filtering restricts the IP traffic received by the network interface by controlling the TCP or UDP port for incoming data.
Furthermore, Andrew wants to allow local users to access shared folders and all other resources. Therefore, Andrew will have to enable all the ports on the network adapter that uses the IP address 16.5.7.1 for the local network.

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 3*

What will be the output of the following command? echo $(date %M) > date.txt

A. The current time (Month) will be written in the date.txt file.

B. It will create a variable $(date %M).

C. It will print a string "date %M".

D. The current time (Minutes) will be written in the date.txt file.

Suggested Answer: *D*
The date command with the %M specifier prints the current time (Minutes). Since the output is redirected towards the date.txt file, the current time (Minutes) will be printed in the date.txt file.

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 3*

Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

A. Tiny

B. NetBus

C. Trojan Man

D. EliteWrap

Suggested Answer: *C*
The Trojan Man is a Trojan wrapper that not only combines two programs, but also encrypts the resulting package in an attempt to foil antivirus programs.

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 3*

You have been assigned a project to develop a Web site for a construction company. You plan to develop a Web site and want to get more control over the appearance and presentation of the Web pages. You also want to increase your ability to precisely specify the position and appearance of the elements on a page and create special effects. You plan to use cascading style sheets (CSS). You want to define styles only for the active page.
Which type of style sheet will you use?

A. Embedded Style Sheet

B. Inline Style Sheet

C. Internal Style Sheet

D. External Style Sheet

Suggested Answer: *A*
To define styles only for the active page you should use embedded style sheet. Cascading style sheets (CSS) are used so that the Website authors can exercise greater control on the appearance and presentation of their Web pages. And also because they increase the ability to precisely point to the location and look of elements on a Web page and help in creating special effects. Cascading Style Sheets have codes, which are interpreted applied by the browser on to the Web pages and their elements. There are three types of cascading style sheets. External Style Sheets Embedded Style Sheets Inline Style Sheets External Style
Sheets are used whenever consistency in style is required throughout a Web site. A typical external style sheet uses a .css file extension, which can be edited using a text editor such as a Notepad. Embedded Style Sheets are used for defining styles for an active page. Inline Style Sheets are used for defining individual elements of a page.
Reference: TechNet, Contents: Microsoft Knowledgebase, February 2000 issue PSS ID Number: Q179628 You want to enable Host A to access the Internet. For this, you need to configure the default gateway settings. Choose the appropriate address to accomplish the task.

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 3*

John works as a Network Administrator for Perfect Solutions Inc. The company has a Debian Linux-based network. He is working on the bash shell in which he creates a variable VAR1. After some calculations, he opens a new ksh shell. Now, he wants to set VAR1 as an environmental variable so that he can retrieve
VAR1 into the ksh shell.
Which of the following commands will John run to accomplish the task?

A. echo $VAR1

B. touch VAR1

C. export VAR1

D. env -u VAR1

Suggested Answer: *C*
Since John wants to use the variable VAR1 as an environmental variable, he will use the export command to accomplish the task.

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 3*

You are the project manager of a Web development project. You want to get information about your competitors by hacking into their computers. You and the project team determine should the hacking attack not be performed anonymously, you will be traced. Hence, you hire a professional hacker to work on the project.
This is an example of what type of risk response?

A. Transference

B. Mitigation

C. Acceptance

D. Avoidance

Suggested Answer: *A*
Whenever the risk is transferred to someone else, it is an example of transference risk response. Transference usually has a fee attached to the service provider that will own the risk event.

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 3*

Which of the following statements is true about COLSPAN attribute?

A. COLSPAN is used to create columns in a table.

B. COLSPAN is used to divide one column into many columns.

C. COLSPAN is used to span one column across many rows.

D. COLSPAN is used to span one column across many columns.

Suggested Answer: *D*
COLSPAN attribute is used to span one column across many columns. COLSPAN is an attribute of <TD> and <TH> tags that allow a singlecolumn in a table to take space that is occupied by several columns. If the specified COLSPAN value is greater than the number of columns in the table, then a new column is created at the end of the row.
Reference: MSDN, Contents: COLSPAN

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 3*

Which of the following statements about URL rewriting are true?

A. If cookies are supported by the browser, URL rewriting will return the URL unchanged.

B. The request.encodeRedirectURL() method is used to add a session id info to the URL and send the request to another URL.

C. The request.encodeURL() method is used to add a session id info to the URL.

D. URL rewriting is used in cases where cookies are not supported by the browser.

Suggested Answer: *AD*
By default, session tracking uses cookies to associate a session identifier with a unique user. URL rewriting is used in cases where cookies are not supported by the browser.

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 3*

You work as a Database Administrator for BigApple Inc. The Company uses Oracle as its database. You enabled standard database auditing. Later, you noticed that it has a huge impact on performance of the database by generating a large amount of audit data.
How will you keep control on this audit data?

A. By implementing principle of least privilege.

B. By removing some potentially dangerous privileges.

C. By setting the REMOTE_LOGIN_PASSWORDFILE instance parameter to NONE.

D. By limiting the number of audit records generated to only those of interest.

Suggested Answer: *D*
Auditing is the process of monitoring and recording the actions of selected users in a database. Auditing is of the following types:
⇨ Mandatory auditing
⇨ Standard auditing
⇨ Fine-grained auditing
By focusing the audits as narrow as possible, you will get audit records for events that are of significance. If it is possible then try doing audit by session, not by access. When auditing a database the SYS.AUD$ table may grow many gigabytes. You may delete or truncate it periodically to control the load of audit data. minimum set of privileges that are just sufficient to accomplish their requisite roles, so that even if the users try, they cannot perform those actions that may critically endanger the safety of data in the event of any malicious attacks. It is important to mention that some damage to data may still be unavoidable. Therefore, after identifying the scope of their role, users are allocated only those minimal privileges just compatible with that role. This helps in minimizing the damage to data due to malicious attacks. Grant of more privileges than necessary may make data critically vulnerable to malicious exploitation. The principle of least privilege is also known as the principle of minimal privilege and is sometimes also referred to as POLA, an abbreviation for the principle of least authority. The principle of least privilege is implemented to enhance fault tolerance, i.e. to protect data from malicious attacks. While applying the principle of least privilege, one should ensure that the parameter 07_DICTIONARY_ACCESSIBILITY in the data dictionary is set to FALSE, and revoke those packages and roles granted to a special pseudo-user known as Public that are not necessary to perform the legitimate actions, after reviewing them. This is very important since every user of the database, without exception, is automatically allocated the Public pseudo-user role.
Some of the packages that are granted to the special pseudo-user known as Public are as follows: UTL_TCP UTL_SMTP UTL_HTTP UTL_FILE
REMOTE_LOGIN_PASSWORDFILE is an initialization parameter used to mention whether or not Oracle will check for a password file and by which databases a password file can be used.
The various properties of this initialization parameter are as follows: Parameter type: String Syntax: REMOTE_LOGIN_PASSWORDFILE = {NONE | SHARED |
EXCLUSIVE} Default value: NONE Removing some potentially dangerous privileges is a security option.
All of the above discussed options are security steps and are not involved in standard database auditing.

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 3*

Which of the following listeners need not be configured in the deployment descriptor? (Choose two)

A. HttpSessionBindingListener

B. HttpSessionAttributeListener

C. HttpSessionListener

D. HttpSessionActivationListener

Suggested Answer: *AD*
Except for the HttpSessionActivationListener and the HttpSessionBindingListener, all other listeners must be configured in the deployment descriptor.
HttpSessionBindingListener has methods that notify the object when it is added to or removed from a session. It has methods that informs the attributes when the session is about to be activated or passivated. These methods are related to the attributes and not to the complete session. Hence, the container takes care of them and need not be configured in the deployment descriptor.

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 3*

Which of the following statements are true about MS-CHAPv2?

A. It is a connectionless protocol.

B. It provides an authenticator-controlled password change mechanism.

C. It is subject to offline dictionary attacks.

D. It can be replaced with EAP-TLS as the authentication mechanism for PPTP.

Suggested Answer: *BCD*
MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the
Success packet. MS-CHAPv2 has various features such as:
It is enabled by negotiating CHAP Algorithm 0x80 (0x81 for MS-CHAPv2) in LCP option 3, Authentication Protocol.
It provides an authenticator-controlled password change mechanism.
It provides an authenticator-controlled authentication retry mechanism.
It defines failure codes returned in the Failure packet message field.
With weak passwords, MS-CHAPv2 is subject to offline dictionary attacks; hence, it can be replaced with EAP-TLS as the authentication mechanism for PPTP.

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 3*

Mark works as a Web Developer for XYZ CORP. He is developing a Web site for the company. The Manager of the company requires Mark to use tables instead of frames in the Web site.
What is the major advantage that a table-structured Web site has over a frame-structured Web site?

A. Easy maintenance

B. Speed

C. Better navigation

D. Capability of being bookmarked or added to the Favorites folder

Suggested Answer: *D*
The major advantage that a table-structured Web site has over a frame-structured Web site is that users can bookmark the pages of a table-structured Web site, whereas pages of a frame-structured Web site cannot be bookmarked or added to the Favorites folder. Non-frame Web sites also give better results with search engines.
Better navigation: Web pages can be divided into multiple frames and each frame can display a separate Web page. It helps in providing better and consistent navigation.
Easy maintenance: Fixed elements, such as a navigation link and company logo page, can be created once and used with all the other pages. Therefore, any change in these pages is required to be made only once.

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 3*

Which of the following statements are true about the Enum tool?

A. It uses NULL and User sessions to retrieve user lists, machine lists, LSA policy information, etc.

B. It is capable of performing brute force and dictionary attacks on individual accounts of Windows NT/2000.

C. One of the countermeasures against the Enum tool is to disable TCP port 139/445.

D. It is a console-based Win32 information enumeration utility.

Suggested Answer: *ABCD*
Enum is a console-based Win32 information enumeration utility. It uses null sessions to retrieve user lists, machine lists, share lists, namelists, group and member lists, passwords, and LSA policy information. It is also capable of performing brute force and dictionary attacks on individual accounts. Since the Enum tool works on the NetBIOS NULL sessions, disabling the NetBIOS port can be a good countermeasure against the Enum tool.

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 3*

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He has recently backed up his entire Linux hard drive into the my_backup.tgz file. The size of the my_backup.tgz file is 800MB. Now, he wants to break this file into two files in which the size of the first file named my_backup.tgz.aa should be 600MB and that of the second file named my_backup.tgz.ab should be
200MB.
Which of the following commands will John use to accomplish his task?

A. split --verbose -b 200m my_backup.tgz my_backup.tgz

B. split --verbose -b 200m my_backup.tgz my_backup.tgz

C. split --verbose -b 600m my_backup.tgz my_backup.tgz

D. split --verbose -b 600m my_backup.tgz my_backup.tgz

Suggested Answer: *D*
According to the scenario, John wants to break the my_backup.tgz file into two files in which thesize of the first file named my_backup.tgz.aa should be 600MB and that of the second file named my_backup.tgz.ab should be 200MB. Hence, he will use the the split --verbose -b 600 my_backup.tgz my_backup.tgz. command, which will automatically break the first file into 600MB named my_backup.tgz.aa, and the rest of the data (200MB) will be assigned to the second file named my_backup.tgz.ab. The reason behind the names is that the split command provides suffixes as 'aa', 'ab', 'ac', ..., 'az', 'ba', 'bb', etc. in the broken file names by default. Hence, both conditions, the file names as well as the file sizes, match with this command.
Note: If the size of the tar file my_backup.tgz is 1300MB, the command split --verbose -b 600 my_backup.tgz my_backup.tgz. breaks the my_backup.tgz file into three files,i.e., my_backup.tgz.aa of size 600MB, my_backup.tgz.ab of size 600MB, and my_backup.tgz.ac of size 100MB.

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 3*

What are the purposes of audit records on an information system? (Choose two)

A. Upgradation

B. Backup

C. Troubleshooting

D. Investigation

Suggested Answer: *CD*

The following are the purposes of audit records on an information system:

⇨ Troubleshooting

⇨ Investigation

An IT audit is the process of collecting and evaluating records of an organization's information systems, practices, and operations. The evaluation of records provides evidence to determine if the information systems are safeguarding assets, maintaining data integrity, and operating effectively and efficiently enough to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement. Audit records are also used to troubleshoot system issues.

Answers A, B are incorrect. The audit records cannot be used for backup and upgradation purposes.

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 3*

Which of the following statements are true about WPA?

A. WPA-PSK requires a user to enter an 8-character to 63-character passphrase into a wireless client.

B. Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used.

C. WPA-PSK converts the passphrase into a 256-bit key.

D. WPA provides better security than WEP.

Suggested Answer: *ABCD*
WPA stands for Wi-Fi Protected Access. It is a wireless security standard. It provides better security than WEP (Wired Equivalent Protection).
Windows Vista supports both WPA-PSK and WPA-EAP. Each of these is described as follows:
WPA-PSK: PSK stands for Preshared key. This standard is meant for home environment. WPA-PSK requires a user to enter an 8- character to 63-character passphrase into a wireless client. The WPA converts the passphrase into a 256-bit key.
WPA-EAP: EAP stands for Extensible Authentication Protocol. This standard relies on a back-end server that runs Remote AuthenticationDial-In User Service for user authentication. Note: Windows Vista supports a user to use a smart card to connect to a WPA-EAP protected network.
Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used. To protect against a brute force attack, a truly random passphrase of
13 characters (selected from the set of 95 permitted characters) is probably sufficient.

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 3*

Sarah works as a Web Developer for XYZ CORP. She develops a Web site for the company. She uses tables in the Web site. Sarah embeds three tables within a table.
What is the technique of embedding tables within a table known as?

A. Nesting tables

B. Stacking tables

C. CSS tables

D. Horned tables

Suggested Answer: *A*
In general, nesting means embedding a construct inside another. Nesting tables is a technique in which one or more tables are embedded within a table.

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 3*

You work as a Network Administrator for Net World International. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. There are ten Sales Managers in the company. The company has recently provided laptops to all its Sales
Managers. All the laptops run Windows XP Professional. These laptops will be connected to the company's network through wireless connections. The company's management wants to implement Shared Key authentication for these laptops. When you try to configure the network interface card of one of the laptops for
Shared Key authentication, you find no such option. What will you do to enable Shared Key authentication?

A. Install PEAP-MS-CHAP v2

B. Enable WEP

C. Install Service Pack 1

D. Install EAP-TLS.

Suggested Answer: *B*
Shared Key authentication requires the use of the Wired Equivalent Privacy (WEP) algorithm. If the WEP is not implemented, then the option for Shared Key authentication is not available. In order to accomplish the task, you will have to enable the WEP on all the laptops.

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 3*

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He executes the following command in the terminal: echo $USER, $UID.
Which of the following will be displayed as the correct output of the above command?

A. John, 0

B. root, 0

C. root, 500

D. John, 502

Suggested Answer: *B*
According to the scenario, John is a root user. Hence, the value of the environmental variables $USER and $UID will be root and 0, respectively.

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 3*

Which of the following methods can be helpful to eliminate social engineering threat? (Choose three)

A. Data encryption

B. Data classification

C. Password policies

D. Vulnerability assessments

Suggested Answer: *BCD*
The following methods can be helpful to eliminate social engineering threat:

Password policies -

Vulnerability assessments -

Data classification -
Password policy should specify that how the password can be shared. Company should implement periodic penetration and vulnerability assessments. These assessments usually consist of using known hacker tools and common hacker techniques to breach a network security. Social engineering should also be used for an accurate assessment. Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees know and follow. Data classification assigns level of sensitivity of company information. Each classification level specifies that who can view and edit data, and how it can be shared.

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 3*

You work as the Network Administrator for a company. You configure a Windows 2000-based computer as the Routing and Remote Access server, so that users can access the company's network, remotely. You want to log a record of all the users who access the network by using Routing and Remote Access.
What will you do to log all the logon activities?

A. On the Routing and Remote Access server, enable log authentication requests in auditing, and define the path for the log file in Remote Access Logging.

B. On the Routing and Remote Access server, enable log authentication requests in Remote Access Logging.

C. On the Routing and Remote Access server, enable log authentication requests in auditing.

D. Do nothing as the Windows 2000-based Routing and Remote Access server automatically creates a log record for each connection attempt.

Suggested Answer: *B*
The Routing and Remote Access service can log all the records of authentication and accounting information for connection attempts when Windows authentication or accounting is enabled. This can be done by enabling the log authentication requests in the properties of the RemoteAccess Logging folder, in the
Routing and Remote Access snap-in, where you can configure the type of activity to log, i.e., accounting or authentication activity and log file settings. This information is stored in the form of a log file in '%SystemRoot%System32LogFiles' folder. For each authentication attempt, the name of the remote access policy, that either accepted or rejected the connection attempt, is recorded. The logged information is useful to track remote access usage, and authentication attempts.

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 3*

What is the extension of a Cascading Style Sheet?

A. .hts

B. .cs

C. .js

D. .css

Suggested Answer: *D*

A Cascading Style Sheet (CSS) is a separate text file that keeps track of design and formatting information, such as colors, fonts, font sizes, and margins, used in

Web pages. CSS is used to provide Web site authors greater control on the appearance and presentation of their Web pages. It has codes that are interpreted and applied by the browser on to the Web pages and their elements. CSS files have .css extension.

There are three types of Cascading Style Sheets:

⇨ External Style Sheet

⇨ Embedded Style Sheet

⇨ Inline Style Sheet

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 3*

Which of the following is a basic feature of the Unix operating system? (Choose three)

A. It is highly portable across hardware.

B. All files can be individually protected using read, write, and execute permissions for the user, group, and others.

C. It allows all the modules to be loaded into memory.

D. A user can execute multiple programs at the same time from a single terminal.

Suggested Answer: *ABD*

The basic features of Unix are as follows:

⇨ Multi-user: It supports more than one user to access the system simultaneously through a set of terminals attached to a system.

⇨ Multi-tasking: A user can execute multiple programs at the same time from a single terminal.

⇨ Time sharing: The operating system shares CPU time among tasks.

⇨ Portability: It is highly portable across hardware.

⇨ Modularity: It allows only needed modules to be loaded into the memory.

⇨ File structure: It has an inverted tree like file structure, with files and directories created within the file structure.

⇨ Security: All files can be individually protected using read, write, and execute permissions for the user, group, and others.

⇨ Network support: It uses the TCP/IP protocol.

Advanced graphics: CAD-CAM applications perform the best in a Unix System with its varied support for graphics card.

▪

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 3*

Which of the following statements are true about a hot site?

A. It is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.

B. It is the most inexpensive backup site.

C. It can be used within an hour for data recovery.

D. It is cheaper than a coldsite but more expensive than a worm site.

Suggested Answer: *AC*

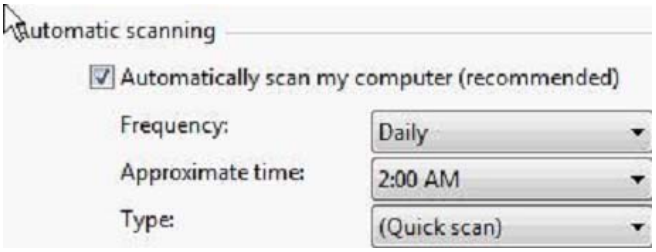
A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. A hot site can be used within an hour for data recovery. The capacity of the hot site may or may not match the capacity of the original site depending on the organization's requirements.

This type of backup site is the most expensive to operate. Hot sites are popular with organizations that operate real time processes such as financial institutions, government agencies, and ecommerce providers. the original site. A cold site is the most inexpensive type of backup site for an organization to operate since it does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. A warm site is, quite logically, a compromise between hot and cold in terms of resources and cost.

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 3*

You have purchased a laptop that runs Windows Vista Home Premium. You want to protect your computer from malicious applications, such as spyware, while connecting to the Internet. You configure Windows Defender on your laptop to schedule scan daily at 2 AM as shown in the image below:



You want Windows Defender to scan the laptop for all the known spyware and other potentially unwanted software, including the latest one. You do not want to manually perform this task.
Which of the following actions will you perform to accomplish the task?

A. Create a scheduled task to download definition files for Windows Defender every Sunday.

B. Configure Windows Defender to use the definition file placed on the Microsoft Update site for scanning the laptop.

C. Select the Check for updated definitions before scanning check box in the Automatic Scanning section.

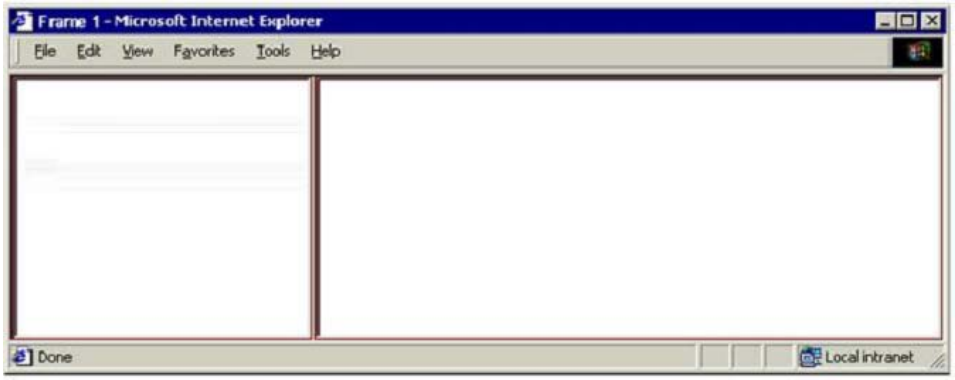
D. Click the arrow beside the Help button Click the Check for updates option.

Suggested Answer: *C*
According to the question, Windows Defender should scan the laptop for all the known spyware and other potentially unwanted software, including the latest one.
Windows Defender uses definitions to scan the system. Definitions are files that include the information of known spyware and potentially unwanted software. To scan a computer for the latest spyware, Windows Defender requires the latest definition files available on the Internet. For this, you have to configure Windows
Defender to check for the latest definitions and download them, if available, before scanning the computer. Furthermore, the question also states that the task must be performed automatically. In order to accomplish the task, you will have to select the Check for updated definitions before scanning check box in the
Automatic Scanning section.

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 3*

Which of the following tags will create two vertical frames, as given in the image below, where the left frame is half as wide as the right one?



A. <FRAMESET ROWS = "*, *"><FRAME SRC = "cell1.htm"><FRAME SRC = "cell2.htm"></FRAMESET>

B. <FRAMESET ROWS = "1,2"><FRAME SRC = "cell1.htm"><FRAME SRC = "cell2.htm"></FRAMESET>

C. <FRAMESET COLS = "*, *"><FRAME SRC = "cell1.htm"><FRAME SRC = "cell2.htm"></FRAMESET>

D. <FRAMESET ROWS = "*, 2*"><FRAME SRC = "cell1.htm"><FRAME SRC = "cell2.htm"></FRAMESET>

E. <FRAMESET COLS = "*, 2*"><FRAME SRC = "cell1.htm"><FRAME SRC = "cell2.htm"></FRAMESET>

Suggested Answer: *E*

<FRAMESET> tag specifies a frameset used to organize multiple frames and nested framesets in an HTML document. It defines the location, size, and orientation of frames. An HTML document can either contain a <FRAMESET> tag or a <BODY> tag.

The COLS attribute of the <FRAMESET> tag defines the width of the vertical frames. The ROWS attribute defines the height of the horizontal frames. The code in answer option E will create two identical frames. The left frame will be half as wide as the right frame because of the relative size attributes given in the

<FRAMESET> tag, i.e., <FRAMESET COLS = "*, 2*">.

Currently there are no comments in this discussion, be the first to comment!