QUESTIONS & ANSWERS

Kill your exam at first Attempt

312-38 Dumps
312-38 Braindumps
312-38 Real Questions
312-38 Practice Test
312-38 dumps free

ECCouncil

312-38

EC-Council Network Security Administrator

Answer: D

QUESTION: 319
Which of the following processes helps the business units to understand the impact of a disruptive event?

A. Plan approval and implementation
B. Business continuity plan development
C. Scope and plan initiation
D. Business impact assessment

Answer: D

QUESTION: 320
Which of the following is a network analysis tool that sends packets with nontraditional IP stack parameters?

A. Nessus
B. COPS
C. SAINT
D. HPing

Answer: D

QUESTION: 321
Which of the following protocols is a method of implementing virtual private networks?

A. OSPF
B. PPTP
C. IRDP
D. DHCP

Answer: B

QUESTION: 322
Adam works as a Professional Penetration Tester. A project has been assigned to him to test the vulnerabilities of the CISCO Router of Umbrella Inc. Adam finds out that HTTP Configuration Arbitrary Administrative Access Vulnerability exists in the router.

By applying different password cracking tools, Adam gains access to the router. He analyzes the router config file and notices the following lines:
logging buffered errors logging history critical logging trap warnings logging 10.0.1.103
By analyzing the above lines, Adam concludes that this router is logging at log level 4 to the syslog server 10.0.1.103. He decides to change the log level from 4 to 0. Which of the following is the most likely reason of changing the log level?

A. Changing the log level from 4 to 0 will result in the logging of only emergencies. This way the modification in the router is not sent to the syslog server.
B. By changing the log level, Adam can easily perform a SQL injection attack.
C. Changing the log level grants access to the router as an Administrator.
D. Changing the log level from 4 to 0 will result in the termination of logging. This way the modification in the router is not sent to the syslog server.

Answer: A

Explanation:
The Router Log Level directive is used by the sys log server to specify the level of severity of the log. This directive is used to control the types of errors that are sent to the error log by constraining the severity level. Eight different levels are present in the Log Level directive, which are shown below in order of their descending significance:
Number Level Description
0emergEmergencies - system is unusable
1alertAction must be taken immediately
2critCritical Conditions
3errorError conditions
4warnWarning conditions
5notice Normal but significant condition
6infoInformational
7debug Debug-level messages
Note: When a certain level is specified, the messages from all other levels of higher significance will also be reported. For example, when Log Level crit is specified, then messages with log levels of alert and emerg will also be reported.

QUESTION: 323
Which of the following protocols permits users to enter a user-friendly computer name into the Windows browser and to map network drives and view shared folders?

A. RADIUS
B. NetBEUI
C. VoIP
D. ARP

Answer: B

Explanation:
NetBIOS Extended User Interface (NetBEUI) is a Microsoft proprietary protocol. NetBEUI is usually used in single LANs comprising one to two hundred clients. It is a non-routable protocol. NetBEUI was developed by IBM for its LAN Manager product and has been adopted by Microsoft for its Windows NT, LAN Manager, and Windows for Workgroups products. It permits users to enter a user- friendly computer name into the Windows browser and to map network drives and view shared folders. Answer option C is incorrect. Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms frequently encountered and synonymous with VoIP are IP telephony, Internet telephony, Voice over Broadband (VoBB), broadband telephony, and broadband phone. VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs that encode speech, allowing transmission over an IP network as digital audio via an audio stream. Answer option A is incorrect. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine. RADIUS serves three functions:\
To authenticate users or devices before granting them access to a network
To authorize those users or devices for certain network services To account for usage of those services Answer option D is incorrect. Address Resolution Protocol (ARP) is a computer networking protocol used to determine a network host's Link Layer or hardware address when only its Internet Layer (IP) or Network Layer address is known. This function is critical in local area networking as well as for routing internetworking traffic across gateways (routers) based on IP addresses when the next-hop router must be determined.

QUESTION: 324
Which of the following attacks are computer threats that try to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer? Each correct answer represents a complete solution. Choose all that apply.

A. Buffer overflow
B. Zero-day
C. Spoofing
D. Zero-hour

Answer: B, D

Explanation:
A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks. Answer option C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer option A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application.

QUESTION: 325
Which of the following is the best way of protecting important data against virus attack?

A. Implementing a firewall.
B. Updating the anti-virus software regularly.
C. Taking daily backup of data.
D. Using strong passwords to log on to the network.

Answer: B

Explanation:
Updating the anti-virus software regularly is the best way of protecting important data against virus attack.

QUESTION: 326
Which of the following is a service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration?

A. NTP
B. SLP
C. NNTP
D. DCAP

Answer: B

Explanation:
The Service Location Protocol (SLP, srvloc) is a service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks. Answer option C is incorrect. The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read. Answer option A is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission. Answer option D is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.

QUESTION: 327
Fill in the blanks with the appropriate terms. In L2TP _____ tunnel mode, the ISP must support L2TP, whereas in L2TP tunnel mode, the ISP does not need to su pport L2TP.

Answer: compulsory

Explanation:
The Layer 2 Tunnel Protocol is one of the tunneling protocols that is used in a virtual private network. It contains the functionality of Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling Protocol (PPTP). This protocol is vendor interoperable and supports multihopping.L2TP supports two tunnel modes:
Compulsory tunnel:
In L2TP compulsory tunnel mode, a remote host initiates a connection to its Internet Service Provider (ISP). An L2TP connection is established between the remote user and the corporate network by the ISP. With a compulsory tunnel, the ISP must support L2TP.
Voluntary tunnel:

In L2TP voluntary tunnel mode, the connection is created by the remote user, typically by using an L2TP tunneling client. Then, the remote user sends L2TP packets to its ISP in order to forward them on to the corporate network. With a voluntary tunnel, the ISP does not need to support L2TP.

QUESTION: 328
Jason works as a System Administrator for www.company.com Inc. The company has a Windows- based network. Sam, an employee of the company, accidentally changes some of the applications and system settings. He complains to Jason that his system is not working properly. To troubleshoot the problem, Jason diagnoses the internals of his computer and observes that some changes have been made in Sam's computer registry. To rectify the issue, Jason has to restore the registry. Which of the following utilities can Jason use to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: D, A, C

Explanation:
The resplendent registrar is a tool that offers a complete and safe solution to administrators and power users for maintaining the registry. It can be used for maintaining the registry of desktops and remote computers on the network. It offers a solution for backing up and restoring registries, fast background search and replace, adding descriptions to the registry keys, etc. This program is very attractive and easy to use, as it comes in an explorer-style interface. It can be used for Windows 2003/XP/2K/NT/ME/9x. Reg.exe is a command-line utility that is used to edit the Windows registry. It has the ability to import, export, back up, and restore keys, as well as to compare, modify, and delete keys. It can perform almost all tasks that can be done using the Windows-based Regedit.exe tool. Registry Editor (REGEDIT) is a registry editing utility that can be used to look at information in the registry. REGEDIT.EXE enables users to search for strings, values, keys, and subkeys and is useful to find a specific value or string. Users can also use REGEDIT.EXE to add, delete, or modify registry entries. Answer option B is incorrect. EventCombMT is a multithreaded tool that is used to search the event logs of several different computers for specific events, all from one central location. It is a little- known Microsoft tool to run searches for event IDs or text strings against Windows event logs for systems, applications, and security, as well as File Replication Service (FRS), domain name system (DNS), and Active Directory (AD) logs where applicable. The MT stands for multi-threaded. The program is part of the Account Lockout and Management Tools program package for Windows 2000, 2003, and XP.