[2017 Newest Lead2pass 312-50v9 Exam Dumps New Updated By EC-Council Official Exam Center (221-240)

Lead2pass 2017 September New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Test your preparation for EC-Council 312-50v9 with these actual 312-50v9 new questions below. Exam questions are a sure method to validate one's preparation for actual certification exam. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 221The NMAP command above performs which of the following? > NMAP -sn 192.168.11.200-215 A. A ping scanB. A trace sweepC. An operating system detectD. A port scanAnswer: AExplanation:NMAP -sn (No port scan)This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run.https://nmap.org/book/man-host-discovery.html QUESTION 222You are using NMAP to resolve domain names into IP addresses for a ping sweep later.Which of the following commands looks for IP addresses? A. >host -t a hackeddomain.comB. >host -t soa hackeddomain.comC. >host -t ns hackeddomain.comD. >host -t AXFR hackeddomain.com Answer: AExplanation:The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.https://en.wikipedia.org/wiki/List_of_DNS_record_types QUESTION 223Which of the following is a command line packet analyzer similar to GUI-based Wireshark? A. tcpdumpB. nessusC. etherealD. Jack the ripper Answer: AExplanation:tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/ IP and other packets being transmitted or received over a network to which the computer is attached. https://en.wikipedia.org/wiki/Tcpdump QUESTION 224The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive.Which of the following is being described? A. promiscuous modeB. port forwardingC. multi-cast modeD. WEM Answer: AExplanation:Promiscuous mode refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting. https://www.tamos.com/htmlhelp/monitoring/ QUESTION 225Which of the following is an extremely common IDS evasion technique in the web world? A. unicode charactersB. spywareC. port knockingD. subnetting Answer: AExplanation:Unicode attacks can be effective against applications that understand it. Unicode is the international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion.Unicode characters are normally represented with two bytes, but this is impractical in real life.One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded.What is worse is multiple representations of each character can exist. Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-chp-10-sect-8.html QUESTION 226Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange? A. PKIB. single sign onC. biometricsD. SOA Answer: AExplanation:A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e- commerce, internet banking and confidential email.https://en.wikipedia.org/wiki/Public_key_infrastructure QUESTION 227Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications? A. Service Oriented ArchitectureB. Object Oriented ArchitectureC. Lean CodingD. Agile Process Answer: AExplanation:A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. https://en.wikipedia.org/wiki/Service-oriented_architecture QUESTION 228Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN? A. ESP transport modeB. AH permiscuousC. ESP confidentialD. AH Tunnel mode Answer: AExplanation:When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.Incorrect Answers:B: Authentication Header (AH) provides authentication, integrity, and anti-replay protection for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means that it does not encrypt the data.

https://technet.microsoft.com/en-us/library/cc739674(v=ws.10).aspx QUESTION 229Which of the following is assured by the use of a hash? A. IntegrityB. ConfidentialityC. AuthenticationD. Availability Answer: AExplanation:An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event). https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages QUESTION 230Which of the following is the greatest threat posed by backups? A. A backup is the source of Malware or illicit information.B. A backup is unavailable during disaster recovery.C. A backup is incomplete because no verification was performed.D. An un-encrypted backup can be misplaced or stolen. Answer: DExplanation:If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.http://resources.infosecinstitute.com/backup-media-encryption/ QUESTION 231An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.What is the most likely cause? A. The network devices are not all synchronized.B. Proper chain of custody was not observed while collecting the logs.C. The attacker altered or erased events from the logs.D. The security breach was a false positive. Answer: AExplanation:Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5619315&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5619315 QUESTION 232In Risk Management, how is the term "likelihood" related to the concept of "threat?" A. Likelihood is the probability that a threat-source will exploit a vulnerability.B. Likelihood is a possible threat-source that may exploit a vulnerability.C. Likelihood is the likely source of a threat that could exploit a vulnerability.D. Likelihood is the probability that a vulnerability is a threat-source. Answer: AExplanation:The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.
http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on- assessing-threat-attack-likelihood.pdf QUESTION 233The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%). What is the closest approximate cost of this replacement and recovery operation per year? A. $146B. $1320C. $440D. $100 Answer: AExplanation:The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.https://en.wikipedia.org/wiki/Annualized_loss_expectancy QUESTION 234 A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.What kind of vulnerability must be present to make this remote attack possible? A. File system permissionsB. Privilege escalationC. Directory traversalD. Brute force login Answer: AExplanation:To upload files the user must have proper write file permissions.http://codex.wordpress.org/Hardening_WordPress QUESTION 235While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.What Web browser-based security vulnerability was exploited to compromise the user? A. Cross-Site Request ForgeryB. Cross-Site ScriptingC. ClickjackingD. Web form input validation Answer: AExplanation:Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.Example and characteristicsIf an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.Incorrect Answers:C: Clickjacking (User Interface redress attack, UI

redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.https://en.wikipedia.org/wiki/Cross-site_request_forgery QUESTION 236A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate? A.   Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.B.   Attempts by attackers to access the user and password information stored in the company's SQL database.C.   Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.D.   Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long. Answer: AExplanation:Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content. https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft QUESTION 237A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.What kind of Web application vulnerability likely exists in their software? A.   Cross-site scripting vulnerabilityB.   Cross-site Request Forgery vulnerabilityC.   SQL injection vulnerabilityD.   Web site defacement vulnerability Answer: AExplanation:Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, <b>very</b> large), output encoding (such as <b>very</b> large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "<b>very</b> large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code. https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input QUESTION 238Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities? A.   Use cryptographic storage to store all PIIB.   Use encrypted communications protocols to transmit PIIC.   Use full disk encryption on all hard drives to protect PIID.   Use a security token to log into all Web applications that use PII Answer: B QUESTION 239 Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications? A.   Validate and escape all information sent to a serverB.   Use security policies and procedures to define and implement proper security settingsC.   Verify access right before allowing access to protected information and UI controlsD.   Use digital certificates to authenticate a server prior to sending data Answer: AExplanation:Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input QUESTION 240An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.Which AAA protocol is most likely able to handle this requirement? A.   RADIUSB.   DIAMETERC.   KerberosD.   TACACS+ Answer: AExplanation:Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e- mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.https://en.wikipedia.org/wiki/RADIUS More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms These EC-Council 312-50v9 exam questions are all a small selection of questions. If you want to practice more questions for actual 312-50v9 exam, use the links at the end of this document. Also you can find links for 312-50v9 VCE software that is great for preparation and self-assessment for EC-Council 312-50v9 exam. 2017 EC-Council 312-50v9 (All 589 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/312-50v9.html [100% Exam Pass Guaranteed]