[2017 Newest Ensure Pass 312-50v9 Exam By Training Lead2pass New PDF Dumps (201-220)

Lead2pass 2017 September New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Lead2pass is constantly updating 312-50v9 exam dumps. We will provide our customers with the latest and the most accurate exam questions and answers that cover a comprehensive knowledge point, which will help you easily prepare for 312-50v9 exam and successfully pass your exam. You just need to spend 20-30 hours on studying the exam dumps. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 201You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.What tool will help you with the task? A. MetagoofilB. ArmitageC. DimitryD. cdpsnarfAnswer: AExplanation:Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.http://www.edge-security.com/metagoofil.php QUESTION 202When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.What command will help you to search files using Google as a search engine? A. site: target.com filetype:xls username password emailB. inurl: target.com filename:xls username password emailC. domain: target.com archive:xls username password emailD. site: target.com file:xls username password email Answer: AExplanation:If you include site: in your query, Google will restrict your search results to the site or domain you specify.If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms "web," "page," "evaluation," and "checklist." http://www.googleguide.com/advanced_operators_reference.html QUESTION 203What is a "Collision attack" in cryptography? A. Collision attacks try to find two inputs producing the same hash.B. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.C. Collision attacks try to get the public key.D. Collision attacks try to break the hash into three parts to get the plaintext value. Answer: AExplanation:A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result.https://learncryptography.com/hash-functions/hash-collision-attack QUESTION 204You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.What testing method did you use? A. Social engineeringB. TailgatingC. PiggybackingD. Eavesdropping Answer: AExplanation:Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.Incorrect Answers:B: Using tailgaiting an attacker, seeking entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access.https://en.wikipedia.org/wiki/Social_engineering_(security) QUESTION 205When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.What nmap script will help you with this task? A. http-methodsB. http enumC. http-headersD. http-git Answer: AExplanation:You can check HTTP method vulnerability using NMAP.Example: #nmap -script=http-methods.nse 192.168.0.25http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/ QUESTION 206When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.What proxy tool will help you find web vulnerabilities? A. BurpsuiteB. MaskgenC. DimitryD. Proxychains Answer: AExplanation:Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

https://portswigger.net/burp/ QUESTION 207You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.What wireshark filter will show the connections from the snort machine to kiwi syslog machine? A. tcp.dstport==514 && ip.dst==192.168.0.150B. tcp.srcport==514 && ip.src==192.168.0.99C. tcp.dstport==514 && ip.dst==192.168.0.0/16D. tcp.srcport==514 && ip.src==192.168.150 Answer: AExplanation:We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.https://wiki.wireshark.org/DisplayFilters QUESTION 208This asymmetry cipher is based on factoring the product of two large prime numbers.What cipher is described above? A. RSAB. SHAC. RC5D. MD5 Answer: AExplanation:RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.
https://en.wikipedia.org/wiki/RSA_(cryptosystem) QUESTION 209Which of the following parameters describe LM Hash (see exhibit): A. I, II, and IIIB. IC. IID. I and II Answer: AExplanation:The LM hash is computed as follows:1. The user's password is restricted to a maximum of fourteen characters.2. The user's password is converted to uppercase.Etc.14 character Windows passwords, which are stored with LM Hash, can be cracked in five seconds.https://en.wikipedia.org/wiki/LM_hash QUESTION 210What is the process of logging, recording, and resolving events that take place in an organization? A. Incident Management ProcessB. Security PolicyC. Internal ProcedureD. Metrics Answer: AExplanation:The activities within the incident management process include:Incident detection and recordingClassification and initial supportInvestigation and analysisResolution and recordIncident closureIncident ownership, monitoring, tracking and communicationEstablish incident framework managementEvaluation of incident framework management
https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure QUESTION 211The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks? A. InjectionB. Cross Site ScriptingC. Cross Site Request ForgeryD. Path disclosure Answer: AExplanation:The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
https://www.owasp.org/index.php/Top_10_2013-Top_10 QUESTION 212You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.What should you do? A. Report immediately to the administratorB. Do not report it and continue the penetration test.C. Transfer money from the administrator's account to another account.D. Do not transfer the money but steal the bitcoins. Answer: AExplanation: QUESTION 213Which of the following describes the characteristics of a Boot Sector Virus? A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBRB. Moves the MBR to another location on the RAM and copies itself to the original location of the MBRC. Modifies directory table entries so that directory entries point to the virus code instead of the actual programD. Overwrites the original MBR and only executes the new virus code Answer: AExplanation:A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.https://www.techopedia.com/definition/26655/boot-sector-virus QUESTION 214You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.Which command-line utility are you most likely to use? A. GrepB. NotepadC. MS ExcelD. Relational Database Answer: AExplanation:grep is a command-line utility for searching plain-text data sets for lines matching a regular expression.https://en.wikipedia.org/wiki/Grep QUESTION 215You've just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.What is one of the first things you should do when given the job? A. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.B. Interview all employees in the company to rule out possible insider threats.C. Establish attribution to suspected attackers.D. Start the wireshark application to start sniffing network traffic. Answer: AExplanation:The goals of penetration tests are:1. Determine feasibility of a particular set of attack vectors2. Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence3.

Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software4. Assess the magnitude of potential business and operational impacts of successful attacks5. Test the ability of network defenders to detect and respond to attacks6. Provide evidence to support increased investments in security personnel and technology https://en.wikipedia.org/wiki/Penetration_test QUESTION 216A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8 A. The host is likely a printer.B. The host is likely a Windows machine.C. The host is likely a Linux machine.D. The host is likely a router. Answer: AExplanation:The Internet Printing Protocol (IPP) uses port 631. https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers QUESTION 217Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company? A. Height and WeightB. VoiceC. FingerprintsD. Iris patterns Answer: AExplanation:There are two main types of biometric identifiers:1. Physiological characteristics: The shape or composition of the body.2. Behavioral characteristics: The behavior of a person.Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice. http://searchsecurity.techtarget.com/definition/biometrics QUESTION 218Which of the following is not a Bluetooth attack? A. BluedrivingB. BluejackingC. BluesmackingD. Bluesnarfing Answer: AExplanation:Incorrect Answers:B: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.C: BlueSmack is a Bluetooth attack that knocks out some Bluetooth-enabled devices immediately. This Denial of Service attack can be conducted using standard tools that ship with the official Linux Bluez utils package.D: Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant.). This allows access to a calendar, contact list, emails and text messages, and on some phones, users can copy pictures and private videos.https://en.wikipedia.org/wiki/Bluejacking http://trifinite.org/trifinite_stuff_bluesmack.htmlhttps://en.wikipedia.org/wiki/Bluesnarfing QUESTION 219This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.What is the most important phase of ethical hacking in which you need to spend a considerable amount of time? A. footprintingB. network mappingC. gaining accessD. escalating privileges Answer: AExplanation:Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html QUESTION 220The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices. A. Wireless Intrusion Prevention SystemB. Wireless Access PointC. Wireless Access Control ListD. Wireless Analyzer Answer: AExplanation:A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention). https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms Lead2pass is no doubt your best choice. Using the EC-Council 312-50v9 exam dumps can let you improve the efficiency of your studying so that it can help you save much more time. 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]