[Lead2pass Professional Best Lead2pass CompTIA SY0-401 PDF Dumps With New Update Exam Questions (476-500)

Lead2pass 2017 September New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Our PDF dumps of SY0-401 exam is designed to ensure everything which you need to pass your exam successfully. At Lead2pass, we have a completely customer oriented policy. We invite the professionals who have rich experience and expert knowledge of the IT certification industry to guarantee the PDF details precisely and logically. Our customers' time is a precious concern for us. This requires us to provide you the products that can be utilized most efficiently. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 476Ann, a security analyst, is preparing for an upcoming security audit. To ensure that she identifies unapplied security controls and patches without attacking or compromising the system, Ann would use which of the following? A. Vulnerability scanningB. SQL injectionC. Penetration testingD. Antivirus updateAnswer: AExplanation:A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. QUESTION 477Which of the following BEST represents the goal of a vulnerability assessment? A. To test how a system reacts to known threatsB. To reduce the likelihood of exploitationC. To determine the system's security postureD. To analyze risk mitigation strategies Answer: CExplanation:A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. QUESTION 478A security administrator wants to perform routine tests on the network during working hours when certain applications are being accessed by the most people. Which of the following would allow the security administrator to test the lack of security controls for those applications with the least impact to the system? A. Penetration testB. Vulnerability scanC. Load testingD. Port scanner Answer: BExplanation:A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. QUESTION 479Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform? A. Vulnerability assessmentB. Black box testingC. White box testingD. Penetration testing Answer: AExplanation:Vulnerability scanning has minimal impact on network resources due to the passive nature of the scanning.A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database

of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. QUESTION 480A company hires outside security experts to evaluate the security status of the corporate network. All of the company's IT resources are outdated and prone to crashing. The company requests that all testing be performed in a way which minimizes the risk of system failures. Which of the following types of testing does the company want performed? A. Penetration testingB. WAF testingC. Vulnerability scanningD. White box testing Answer: CExplanation:Vulnerability scanning has minimal impact on network resource due to the passive nature of the scanning. A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. QUESTION 481Which of the following tests a number of security controls in the least invasive manner? A. Vulnerability scanB. Threat assessmentC. Penetration test D. Ping sweep Answer: AExplanation:Vulnerability scanning has minimal impact on network resource due to the passive nature of the scanning.A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. QUESTION 482A company is looking to improve their security posture by addressing risks uncovered by a recent penetration test. Which of the following risks is MOST likely to affect the business on a day-to-day basis? A. Insufficient encryption methodsB. Large scale natural disastersC. Corporate espionageD. Lack of antivirus software Answer: DExplanation:The most common threat to computers is computer viruses. A computer can become infected with a virus through day-to-day activities such as browsing web sites or emails. As browsing and opening emails are the most common activities performed by all users, computer viruses represent the most likely risk to a business. QUESTION 483Which of the following is BEST utilized to identify common misconfigurations throughout the enterprise? A. Vulnerability scanningB. Port scanningC. Penetration testingD. Black box Answer: A Explanation:A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. QUESTION 484 Which of the following is an example of a false positive? A. Anti-virus identifies a benign application as malware.B. A biometric iris scanner rejects an authorized user wearing a new contact lens.C. A user account is locked out after the user mistypes the password too many times.D. The IDS does not identify a buffer overflow. Answer: AExplanation:A false positive is an error in some evaluation process in which a condition tested for is mistakenly found to have been detected.In spam filters, for example, a false positive is a legitimate message mistakenly marked as UBE -- unsolicited bulk email, as junk email is more formally known. Messages that are determined to be spam -- whether correctly or incorrectly -- may be rejected by a server or client-side spam filter and returned to the sender as bounce e-mail.One problem with many spam filtering tools is that if they are configured stringently enough to be effective, there is a fairly high chance of getting false positives. The risk of accidentally blocking an important message has been enough to deter many companies from implementing any anti-spam measures at all.False positives are also common in security systems. A host intrusion prevention system (HIPS), for example, looks for anomalies, such as deviations in bandwidth, protocols and ports. When activity varies outside of an acceptable range ?for example, a remote application attempting to open a

normally closed port -- an intrusion may be in progress. However, an anomaly, such as a sudden spike in bandwidth use, does not guarantee an actual attack, so this approach amounts to an educated guess and the chance for false positives can be high. False positives contrast with false negatives, which are results indicating mistakenly that some condition tested for is absent. QUESTION 485Joe a company's new security specialist is assigned a role to conduct monthly vulnerability scans across the network. He notices that the scanner is returning a large amount of false positives or failed audits. Which of the following should Joe recommend to remediate these issues? A. Ensure the vulnerability scanner is located in a segmented VLAN that has access to the company's serversB. Ensure the vulnerability scanner is configured to authenticate with a privileged accountC. Ensure the vulnerability scanner is attempting to exploit the weaknesses it discoversD. Ensure the vulnerability scanner is conducting antivirus scanning Answer: AExplanation:The vulnerability scanner is returning false positives because it is trying to scan servers that it doesn't have access to; for example, servers on the Internet. We need to ensure that the local network servers only are scanned. We can do this by locating the vulnerability scanner in a segmented VLAN that has access to the company's servers. A false positive is an error in some evaluation process in which a condition tested for is mistakenly found to have been detected.In spam filters, for example, a false positive is a legitimate message mistakenly marked as UBE -- unsolicited bulk email, as junk email is more formally known. Messages that are determined to be spam -- whether correctly or incorrectly -- may be rejected by a server or client-side spam filter and returned to the sender as bounce e-mail.One problem with many spam filtering tools is that if they are configured stringently enough to be effective, there is a fairly high chance of getting false positives. The risk of accidentally blocking an important message has been enough to deter many companies from implementing any anti-spam measures at all.False positives are also common in security systems. A host intrusion prevention system (HIPS), for example, looks for anomalies, such as deviations in bandwidth, protocols and ports. When activity varies outside of an acceptable range ?for example, a remote application attempting to open a normally closed port -- an intrusion may be in progress. However, an anomaly, such as a sudden spike in bandwidth use, does not guarantee an actual attack, so this approach amounts to an educated guess and the chance for false positives can be high. False positives contrast with false negatives, which are results indicating mistakenly that some condition tested for is absent. QUESTION 486The Quality Assurance team is testing a new third party developed application. The Quality team does not have any experience with the application. Which of the following is the team performing? A. Grey box testingB. Black box testingC. Penetration testingD. White box testing Answer: BExplanation:Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well. Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place. QUESTION 487Which of the following application security principles involves inputting random data into a program? A. Brute force attackB. SniffingC. FuzzingD. Buffer overflow Answer: CExplanation:Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks. QUESTION 488An IT security technician is actively involved in identifying coding issues for her company.Which of the following is an application security technique that can be used to identify unknown weaknesses within the code? A. Vulnerability scanningB. Denial of serviceC. FuzzingD. Port scanning Answer: CExplanation:Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks. QUESTION 489Which of the following would Jane, an administrator, use to detect an unknown security vulnerability? A. Patch managementB. Application fuzzingC. ID badgeD. Application configuration baseline Answer: BExplanation:Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks. QUESTION 490Which of the following pseudocodes can be used to handle program exceptions? A. If program detects another instance of itself, then kill program instance.B. If user enters invalid input, then restart program.C. If program module crashes, then restart program module.D. If user's input exceeds buffer length, then truncate the input. Answer: CExplanation:Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture all errors and exceptions that could cause the application or its modules to crash. Restarting the application or module would ensure that the application reverts back to a secure state. QUESTION 491Which of the following is an application security coding problem? A. Error and exception handlingB. Patch managementC. Application hardeningD. Application fuzzing Answer: AExplanation:Exception handling is an aspect of secure coding. When errors occur, the

system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application. QUESTION 492Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent? A. Buffer overflowB. Pop-up blockersC. Cross-site scriptingD. Fuzzing Answer: AExplanation:Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits. QUESTION 493Which of the following techniques can be used to prevent the disclosure of system information resulting from arbitrary inputs when implemented properly? A. FuzzingB. Patch managementC. Error handlingD. Strong passwords Answer: CExplanation:Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application. QUESTION 494A program displays: ERROR: this program has caught an exception and will now terminate. Which of the following is MOST likely accomplished by the program's behavior? A. Operating system's integrity is maintainedB. Program's availability is maintainedC. Operating system's scalability is maintainedD. User's confidentiality is maintained Answer: AExplanation:The purpose of error handling is to maintain the security and integrity of the system. Integrity is compromised when unauthorized modification occurs. QUESTION 495Which of the following is a best practice for error and exception handling? A. Log detailed exception but display generic error messageB. Display detailed exception but log generic error messageC. Log and display detailed error and exception messagesD. Do not log or display error or exception messages Answer: AExplanation:A detailed explanation of the error is not helpful for most end users but might provide information that is useful to a hacker. It is therefore better to display a simple but helpful message to the end user and log the detailed information to an access-restricted log file for the administrator and programmer who would need as much information as possible about the problem in order to rectify it. QUESTION 496Which of the following is true about input validation in a client-server architecture, when data integrity is critical to the organization? A. It should be enforced on the client side only.B. It must be protected by SSL encryption.C. It must rely on the user's knowledge of the application.D. It should be performed on the server side. Answer: DExplanation:Client-side validation should only be used to improve user experience, never for security purposes. A client-side input validation check can improve application performance by catching malformed input on the client and, therefore, saving a roundtrip to the server. However, client side validation can be easily bypassed and should never be used for security purposes. Always use server-side validation to protect your application from malicious attacks. QUESTION 497Which of the following is the below pseudo-code an example of? IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT A. Buffer overflow preventionB. Input validationC. CSRF preventionD. Cross-site scripting prevention Answer: BExplanation:Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain. QUESTION 498After Matt, a user enters his username and password at the login screen of a web enabled portal, the following appears on his screen: `Please only use letters and numbers on these fields' Which of the following is this an example of? A. Proper error handlingB. Proper input validationC. Improper input validationD. Improper error handling Answer: BExplanation:Input validation is an aspect of secure coding and is intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain. QUESTION 499In regards to secure coding practices, why is input validation important? A. It mitigates buffer overflow attacks.B. It makes the code more readable.C. It provides an application configuration baseline.D. It meets gray box testing standards. Answer: AExplanation:Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits. QUESTION 500Input validation is an important security defense because it: A. rejects bad or malformed data.B. enables verbose error reporting.C. protects mis-configured web servers.D. prevents denial of service attacks. Answer: AExplanation:Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain. More free Lead2pass SY0-401 exam new questions on Google Drive:

https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E If you want to get more SY0-401 exam preparation material, you can download the free SY0-401 braindumps in PDF files on Lead2pass. It would be great helpful for your exam. All the SY0-401 dumps are updated and cover every aspect of the examination. Welcome to choose. 2017 CompTIA SY0-401 (All 1868 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]