[Lead2pass Professional New Lead2pass SY0-401 Dumps PDF Version Released For Free Downloading (401-425)

Lead2pass 2017 September New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! I'm currently studying for CompTIA exam SY0-401. I do enjoy studying for exams. It's hard, but it's an excellent forcing function. I learn bits and pieces here and there now and then about this and that, but when I have an exam schedule for a set date, I have to study! And not only do I put in more hours, but I follow a more systematic approach. In this article, I'm going to share Lead2pass braindumps in case you too are studying and this method works for you. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 401An attacker attempted to compromise a web form by inserting the following input into the username field: admin)(|(password=*))Which of the following types of attacks was attempted? A. SQL injectionB. Cross-site scriptingC. Command injectionD. LDAP injectionAnswer: DExplanation:LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements using a local proxy. This could result in the execution of arbitrary commands such as granting permissions to unauthorized queries, and content modification inside the LDAP tree. The same advanced exploitation techniques available in SQL Injection can be similarly applied in LDAP Injection.In a page with a user search form, the following code is responsible to catch input value and generate a LDAP query that will be used in LDAP database. <input type="text" size=20 name="userName">Insert the username</input> The LDAP query is narrowed down for performance and the underlying code for this function might be the following:String ldapSearchQuery = "(cn=" + $userName + ")";System.out.println(ldapSearchQuery);If the variable $userName is not validated, it could be possible accomplish LDAP injection, as follows:If a user puts "*" on box search, the system may return all the usernames on the LDAP base If a user puts "jonys) (| (password = *))", it will generate the code bellow revealing jonys' password (cn = jonys) (| (password = *)) QUESTION 402Which of the following application attacks is used against a corporate directory service where there are unknown servers on the network? A. Rogue access pointB. Zero day attackC. Packet sniffingD. LDAP injection Answer: DExplanation: A directory service is accessed by using LDAP (Lightweight Directory Access Protocol). LDAP injection is an attack against a directory service. Just as SQL injection attacks take statements that are input by users and exploit weaknesses within, an LDAP injection attack exploits weaknesses in LDAP (Lightweight Directory Access Protocol) implementations. This can occur when the user's input is not properly filtered, and the result can be executed commands, modified content, or results returned to unauthorized queries. The best way to prevent LDAP injection attacks is to filter the user input and to use a validation scheme to make certain that queries do not contain exploits. One of the most common uses of LDAP is associated with user information. Numerous applications exist--such as employee directories--where users find other users by typing in a portion of their name. These queries are looking at the cn value or other fields (those defined for department, home directory, and so on). Someone attempting LDAP injection could feed unexpected values to the query to see what results are returned. All too often, finding employee information equates to finding usernames and values about those users that could be portions of their passwords. QUESTION 403Sara, a hacker, is completing a website form to request a free coupon. The site has a field that limits the request to 3 or fewer coupons. While submitting the form, Sara runs an application on her machine to intercept the HTTP POST command and change the field from 3 coupons to 30.Which of the following was used to perform this attack? A. SQL injectionB. XML injectionC. Packet snifferD. Proxy Answer: BExplanation:When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should. QUESTION 404A malicious individual is attempting to write too much data to an application's memory. Which of the following describes this type of attack? A. Zero-dayB. SQL injectionC. Buffer overflowD. XSRF Answer: CExplanation: A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming

practices supplied the vulnerability. QUESTION 405Data execution prevention is a feature in most operating systems intended to protect against which type of attack? A. Cross-site scriptingB. Buffer overflowC. Header manipulationD. SQL injection Answer: BExplanation:Data Execution Prevention (DEP) is a security feature included in modern operating systems. It marks areas of memory as either "executable" or "nonexecutable", and allows only data in an "executable" area to be run by programs, services, device drivers, etc. It is known to be available in Linux, OS X, Microsoft Windows, iOS and Android operating systems. DEP protects against some program errors, and helps prevent certain malicious exploits, especially attacks that store executable instructions in a data area via a buffer overflow. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability. QUESTION 406Which of the following application attacks is used to gain access to SEH? A. Cookie stealingB. Buffer overflowC. Directory traversalD. XML injection Answer: BExplanation:Buffer overflow protection is used to detect the most common buffer overflows by checking that the stack has not been altered when a function returns. If it has been altered, the program exits with a segmentation fault. Microsoft's implementation of Data Execution Prevention (DEP) mode explicitly protects the pointer to the Structured Exception Handler (SEH) from being overwritten. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability. QUESTION 407While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks? A. Cross-site scriptingB. Buffer overflowC. Header manipulationD. Directory traversal Answer: BExplanation:When the user opens an attachment, the attachment is loaded into memory. The error is caused by a memory issue due to a buffer overflow attack.A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability. QUESTION 408A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe? A. Zero-dayB. Buffer overflowC. Cross site scriptingD. Malicious add-on Answer: BExplanation:This question describes a buffer overflow attack.A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability. QUESTION 409Which of the following was launched against a company based on the following IDS log? 122.41.15.252 - - [21/May/2012:00:17:20 +1200] "GET/index.php?username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA HTTP/1.1" 200 2731 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE

6.0; Windows NT 5.1; Hotbar 4.4.7.0)" A. SQL injectionB. Buffer overflow attackC. XSS attackD. Online password crack Answer: BExplanation:The username should be just a username; instead we can see it's a long line of text with an HTTP command in it. This is an example of a buffer overflow attack. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability. QUESTION 410A security administrator examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90).Which of the following attack types has occurred? A. Buffer overflowB. Cross-site scriptingC. XML injectionD. SQL injection Answer: AExplanation: The hex character 90 (x90) means NOP or No Op or No Operation. In a buffer overflow attack, the buffer can be filled and overflowed with No Op commands. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability. QUESTION 411A security analyst, Ann, is reviewing an IRC channel and notices that a malicious exploit has been created for a frequently used application. She notifies the software vendor and asks them for remediation steps, but is alarmed to find that no patches are available to mitigate this vulnerability.Which of the following BEST describes this exploit? A. Malicious insider threatB. Zero-dayC. Client-side attackD. Malicious add-on Answer: BExplanation:A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. In this question, there are no patches are available to mitigate the vulnerability. This is therefore a zero-day vulnerability. QUESTION 412Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw.Which of the following attacks has MOST likely occurred? A. Cookie stealingB. Zero-dayC. Directory traversalD. XML injection Answer: BExplanation:The vulnerability was unknown in that the IDS and antivirus did not detect it. This is zero day vulnerability.A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. QUESTION 413An attacker used an undocumented and unknown application exploit to gain access to a file server. Which of the following BEST describes this type of attack? A. Integer overflowB. Cross-site scriptingC. Zero-dayD. Session hijackingE. XML injection Answer: CExplanation:The vulnerability is undocumented and unknown. This is zero day vulnerability. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. QUESTION 414Which of the following can only be mitigated through the use of technical controls rather that user security training? A. Shoulder surfingB. Zero-dayC. VishingD. Trojans Answer: BExplanation:A zero day vulnerability is an unknown vulnerability in a software application. This cannot be prevented by user security training.A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the

vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. QUESTION 415The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection.Which of the following has happened on the workstation? A. Zero-day attackB. Known malware infectionC. Session hijackingD. Cookie stealing Answer: AExplanation:The vulnerability was unknown in that the full antivirus scan did not detect it. This is zero day vulnerability.A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. QUESTION 416Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources? A. Zero-dayB. LDAP injectionC. XML injectionD. Directory traversal Answer: AExplanation:The security breaches have NOT yet been identified. This is zero day vulnerability. A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers.Once the vulnerability becomes known, a race begins for the developer, who must protect users. QUESTION 417Which of the following may cause Jane, the security administrator, to seek an ACL work around? A. Zero day exploitB. Dumpster divingC. Virus outbreakD. Tailgating Answer: AExplanation:A zero day vulnerability is an unknown vulnerability so there is no fix or patch for it. One way to attempt to work around a zero day vulnerability would be to restrict the permissions by using an ACL (Access Control List)A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it--this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. QUESTION 418Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection? A. HIPSB. AntivirusC. NIDSD. ACL Answer: AExplanation:Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. A Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. As a zero-day attack is an unknown vulnerability (a vulnerability that does not have a fix or a patch to prevent it), the best defence would be an intrusion prevention system. QUESTION 419Joe, a user, in a coffee shop is checking his email over a wireless network. An attacker records the temporary credentials being passed to Joe's browser. The attacker later uses the credentials to impersonate Joe and creates SPAM messages. Which of the following attacks allows for this impersonation? A. XML injectionB. Directory traversalC. Header manipulationD. Session hijacking Answer: DExplanation:In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. QUESTION 420How often, at a MINIMUM, should Sara, an administrator, review the accesses and rights of

the users on her system? A. AnnuallyB. Immediately after an employee is terminatedC. Every five yearsD. Every time they patch the server Answer: AExplanation:Reviewing the accesses and rights of the users on a system at least annually is acceptable practice. More frequently would be desirable but too frequently would be a waste of administrative time. QUESTION 421Which of the following types of logs could provide clues that someone has been attempting to compromise the SQL Server database? A. EventB. SQL_LOGC. SecurityD. Access Answer: AExplanation:Event logs include Application logs, such as those where SQL Server would write entries. This is where you would see logs with details of someone trying to access a SQL database. QUESTION 422Ann, the security administrator, received a report from the security technician, that an unauthorized new user account was added to the server over two weeks ago. Which of the following could have mitigated this event? A. Routine log auditsB. Job rotationC. Risk likelihood assessmentD. Separation of duties Answer: AExplanation:When a new user account is created, an entry is added to the Event Logs. By routinely auditing the event logs, you would know that an account has been created. QUESTION 423A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check? A. FirewallB. ApplicationC. IDSD. Security Answer: DExplanation:The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrators group in order to turn on, use, and specify which events are recorded in the security log. QUESTION 424The security administrator is analyzing a user's history file on a Unix server to determine if the user was attempting to break out of a rootjail. Which of the following lines in the user's history log shows evidence that the user attempted to escape the rootjail? A. cd ../../../../bin/bashB. whoamiC. ls /rootD. sudo -u root Answer: AExplanation:On modern UNIX variants, including Linux, you can define the root directory on a perprocess basis. The chroot utility allows you to run a process with a root directory other than /. The root directory appears at the top of the directory hierarchy and has no parent: A process cannot access any files above the root directory (because they do not exist). If, for example, you run a program (process) and specify its root directory as /home/sam/jail, the program would have no concept of any files in /home/sam or above: jail is the program's root directory and is labeled / (not jail).By creating an artificial root directory, frequently called a (chroot) jail, you prevent a program from accessing or modifying--possibly maliciously--files outside the directory hierarchy starting at its root. You must set up a chroot jail properly to increase security: If you do not set up the chroot jail correctly, you can actually make it easier for a malicious user to gain access to a system than if there were no chroot jail.The command cd.. takes you up one level in the directory structure. Repeated commands would take you to the top level the root which is represented by a forward slash /. The command /bin/bash is an attempt to run the bash shell from the root level. QUESTION 425A security technician is attempting to improve the overall security posture of an internal mail server. Which of the following actions would BEST accomplish this goal? A. Monitoring event logs dailyB. Disabling unnecessary servicesC. Deploying a content filter on the networkD. Deploy an IDS on the network Answer: BExplanation:One of the most basic practices for reducing the attack surface of a specific host is to disable unnecessary services. Services running on a host, especially network services provide an avenue through which the system can be attacked. If a service is not being used, disable it. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E If you want to prepare for SY0-401 exam in shortest time, with minimum effort but for most effective result, you can use Lead2pass SY0-401 dump which simulates the actual testing environment and allows you to focus on various sections of SY0-401 exam. Best of luck! 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]