# [Lead2pass Professional New Lead2pass SY0-401 Dumps PDF Version Released For Free Downloading (376-400)

Lead2pass 2017 September New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! We are all well aware that a major problem in the IT industry is that there is a lack of quality study materials. Our exam preparation material provides you everything you will need to take a certification examination. Our CompTIA SY0-401 Exam will provide you with exam questions with verified answers that reflect the actual exam. These questions and answers provide you with the experience of taking the actual test. High quality and value for the SY0-401 Exam. 100% guarantee to pass your CompTIA SY0-401 exam and get your CompTIA certification. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 376A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place? A. War chalkingB. BluejackingC. War drivingD. BluesnarfingAnswer: BExplanation:The question states that the `attack' took place on public transport and was received on a smartphone. Therefore, it is most likely that the image was sent using Bluetooth. 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.Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters. Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames. QUESTION 377Which of the following is characterized by an attack against a mobile device? A. Evil twinB. Header manipulationC. Blue jackingD. Rogue AP Answer: CExplanation:A bluejacking attack is where unsolicited messages are sent to mobile devices using Bluetooth. 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.Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters. Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames. QUESTION 378Which of the following attacks allows access to contact lists on cellular phones? A. War chalkingB. Blue jackingC. Packet sniffingD. Bluesnarfing Answer: DExplanation:Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled. QUESTION 379An administrator has advised against the use of Bluetooth phones due to bluesnarfing concerns.Which of the following is an example of this threat? A. An attacker using the phone remotely for spoofing other phone numbersB. Unauthorized intrusions into the phone to access dataC. The Bluetooth enabled phone causing signal interference with the networkD. An attacker using exploits that allow the phone to be disabled Answer: BExplanation:Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled. QUESTION 380After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings? A. IV attackB. War dialingC. Rogue access pointsD. War chalking Answer: DExplanation:War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The

open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot. QUESTION 381The practice of marking open wireless access points is called which of the following? A. War dialingB. War chalkingC. War drivingD. Evil twin Answer: BExplanation:War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot. QUESTION 382Which of the following types of attacks involves interception of authentication traffic in an attempt to gain unauthorized access to a wireless network? A. Near field communicationB. IV attackC. Evil twinD. Replay attack Answer: BExplanation:An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session.An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack.A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "I" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "I" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance. WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets. QUESTION 383Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway? A. IV attackB. InterferenceC. Blue jackingD. Packet sniffing Answer: AExplanation:In this question, it's likely that someone it trying to crack the wireless network security. An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session.An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack.A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "I" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "I" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance. WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets. QUESTION 384Maintenance workers find an active network switch hidden above a dropped-ceiling tile in the CEO's office with various connected cables from the office. Which of the following describes the type of attack that was occurring? A. Spear phishingB. Packet sniffingC. ImpersonationD. MAC flooding Answer: BExplanation:A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing packets sent from a computer system is known as packet sniffing. However, packet sniffing requires a physical connection to the network. The switch hidden in the ceiling is used to provide the physical connection to the network.Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal). A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a

particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. QUESTION 385Which statement is TRUE about the operation of a packet sniffer? A. It can only have one interface on a management network.B. They are required for firewall operation and stateful inspection.C. The Ethernet card must be placed in promiscuous mode.D. It must be placed on a single virtual LAN interface. Answer: CExplanation:A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. QUESTION 386Which of the following network devices is used to analyze traffic between various network interfaces? A. ProxiesB. FirewallsC. Content inspectionD. Sniffers Answer: DExplanation:A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. QUESTION 387Which of the following software allows a network administrator to inspect the protocol header in order to troubleshoot network issues? A. URL filterB. Spam filterC. Packet snifferD. Switch Answer: CExplanation:Every data packet transmitted across a network has a protocol header. To view a protocol header, you need to capture and view the contents of the packet with a packet sniffer.A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer. QUESTION 388A security administrator discovered that all communication over the company's encrypted wireless network is being captured by savvy employees with a wireless sniffing tool and is then being decrypted in an attempt to steal other employee's credentials. Which of the following technology is MOST likely in use on the company's wireless? A. WPA with TKIPB. VPN over open wirelessC. WEP128-PSKD. WPA2-Enterprise Answer: CExplanation:WEP's major weakness is its use of static encryption keys. When you set up a router with a WEP encryption key, that one key is used by every device on your network to encrypt every packet that's transmitted. But the fact that packets are encrypted doesn't prevent them from being intercepted, and due to some esoteric technical flaws it's entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is. This problem used to be something you could mitigate by periodically changing the WEP key (which is why routers generally allow you to store up to four keys). But few bother to do this because changing WEP keys is inconvenient and time-consuming because it has to be done not just on the router, but on every device that connects to it. As a result, most people just set up a single key and then continue using it ad infinitum.Even worse, for those that do change the WEP key, new research and developments reinforce how even changing WEP keys frequently is no longer sufficient to protect a WLAN. The process of 'cracking' a WEP key used to require that a malicious hacker intercept millions of packets plus spend a fair amount of time and computing power. Researchers in the computer science department of a German university recently demonstrated the capability to compromise a WEP- protected network very quickly. After spending less than a minute intercepting data (fewer than 100,000 packets in all) they were able to compromise a WEP key in just three seconds. QUESTION 389Which of the following protocols is vulnerable to man-in-the-middle attacks by NOT using end to end TLS encryption? A. HTTPSB. WEPC. WPAD. WPA 2 Answer: BExplanation:WEP offers no end-to-end TLS encryption.The WEP process consists of a series of steps as follows:The wireless client sends an authentication request.The Access Point (AP) sends an authentication response containing clear-text (uh-oh!) challenge text.The client takes the challenge text received and encrypts it using a static WEP key. The

client sends the encrypted authentication packet to the AP. The AP encrypts the challenge text using its own static WEP key and compares the result to the authentication packet sent by the client. If the results match, the AP begins the association process for the wireless client. The big issue with WEP is the fact that it is very susceptible to a Man in the Middle attack. The attacker captures the clear-text challenge and then the authentication packet reply. The attacker then reverses the RC4 encryption in order to derive the static WEP key. Yikes! As you might guess, the designers attempted to strengthen WEP using the approach of key lengths. The native Windows client supported a 104-bit key as opposed to the initial 40-bit key. The fundamental weaknesses in the WEP process still remained however. QUESTION 390Which of the following wireless protocols could be vulnerable to a brute-force password attack? (Select TWO). A. WPA2-PSKB. WPA - EAP - TLSC. WPA2-CCMPD. WPA -CCMPE. WPA - LEAPF. WEP Answer: AFExplanation:A brute force attack is an attack that attempts to guess a password. WPA2-PSK and WEP both use a "Pre-Shared Key". The pre-shared key is a password and therefore is susceptible to a brute force attack. QUESTION 391A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of 192.168.1.1. The victim is logged into their router administrative interface in one tab and clicks a forum link in another tab. Due to clicking the forum link, the home router reboots. Which of the following attacks MOST likely occurred? A. Brute force password attackB. Cross-site request forgeryC. Cross-site scriptingD. Fuzzing Answer: BExplanation:Cross-Site Request Forgery--also known as XSRF, session riding, and one-click attack--involves unauthorized commands coming from a trusted user to the website. This is often done without the user's knowledge, and it employs some type of social networking to pull it off. For example, assume that Evan and Spencer are chatting through Facebook. Spencer sends Evan a link to what he purports is a funny video that will crack him up. Evan clicks the link, but it actually brings up Evan's bank account information in another browser tab, takes a screenshot of it, closes the tab, and sends the information to Spencer. The reason the attack is possible is because Evan is a trusted user with his own bank. In order for it to work, Evan would need to have recently accessed that bank's website and have a cookie that had yet to expire. The best protection against cross- site scripting is to disable the running of scripts (and browser profi les). QUESTION 392A security administrator develops a web page and limits input into the fields on the web page as well as filters special characters in output. The administrator is trying to prevent which of the following attacks? A. SpoofingB. XSSC. FuzzingD. Pharming Answer: BExplanation:Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.By validating user input and preventing special characters, we can prevent the injection of client- side scripting code. QUESTION 393Pete, the security administrator, has been notified by the IDS that the company website is under attack. Analysis of the web logs show the following string, indicating a user is trying to post a comment on the public bulletin board. INSERT INTO message `<script>source=http://evilsite</script> This is an example of which of the following? A. XSS attackB. XML injection attackC. Buffer overflow attackD. SQL injection attack Answer: AExplanation:The <script> </script> tags indicate that script is being inserted. Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. QUESTION 394Which of the following BEST describes a protective countermeasure for SQL injection? A. Eliminating cross-site scripting vulnerabilitiesB. Installing an IDS to monitor network trafficC. Validating user input in web applicationsD. Placing a firewall between the Internet and database servers Answer: CExplanation:By validating user input and preventing special characters, we can prevent the injection of client- side scripting code.SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be

used to attack any type of SQL database. QUESTION 395A security administrator looking through IDS logs notices the following entry: (where email=joe@joe.com and passwd= `or 1==1')Which of the following attacks had the administrator discovered? A. SQL injectionB. XML injectionC. Cross-site scriptD. Header manipulation Answer: AExplanation:The code in the question is an example of a SQL Injection attack. The code `1==1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. QUESTION 396Which of the following types of application attacks would be used to specifically gain unauthorized information from databases that did not have any input validation implemented? A. SQL injectionB. Session hijacking and XML injectionC. Cookies and attachmentsD. Buffer overflow and XSS Answer: AExplanation:To access information in databases, you use SQL. To gain unauthorized information from databases, a SQL Injection attack is used.SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. QUESTION 397The string: ` or 1=1-- - Represents which of the following? A. BluejackingB. Rogue access pointC. SQL InjectionD. Client-side attacks Answer: CExplanation:The code in the question is an example of a SQL Injection attack. The code `1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. QUESTION 398When an order was submitted via the corporate website, an administrator noted special characters (e.g., ";--" and "or 1=1 --") were input instead of the expected letters and numbers.Which of the following is the MOST likely reason for the unusual results? A. The user is attempting to highjack the web server session using an open-source browser.B. The user has been compromised by a cross-site scripting attack (XSS) and is part of a botnet performing DDoS attacks.C. The user is attempting to fuzz the web server by entering foreign language characters which are incompatible with the website.D. The user is sending malicious SQL injection strings in order to extract sensitive company or customer data via the website. Answer: DExplanation:The code in the question is an example of a SQL Injection attack. The code `1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. QUESTION 399Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server? A. SQL InjectionB. Theft of the physical database serverC. CookiesD. Cross-site scripting Answer: AExplanation:The question discusses a very secure environment with disk and transport level encryption and access control lists restricting access. SQL data in a database is accessed by SQL queries from an application on the application server. The data can still be compromised by a SQL injection attack.SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. QUESTION 400Which of the following BEST describes a SQL Injection attack? A. The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.B. The attacker attempts to

have the receiving server run a payload using programming commonly found on web servers.C. The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage.D. The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload. Answer: AExplanation:SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E The CompTIA SY0-401 questions and answers in PDF on Lead2pass are the most reliable study guide for SY0-401 exam. Comparing with others', our SY0-401 dump is more authoritative and complete. We provide the latest full version of SY0-401 PDF and VCE dumps with new real questions and answers to ensure your SY0-401 exam 100% pass. 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]