[Lead2pass Professional Easily Pass SY0-401 Exam By Training Lead2pass Latest VCE Dumps (351-375)

Lead2pass 2017 September New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Lead2pass SY0-401 braindumps including the exam questions and the answer, completed by our senior IT lecturers and the CompTIA product experts, include the current newest SY0-401 exam questions. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 351Ann, an employee, is cleaning out her desk and disposes of paperwork containing confidential customer information in a recycle bin without shredding it first. This is MOST likely to increase the risk of loss from which of the following attacks? A. Shoulder surfingB. Dumpster divingC. TailgatingD. SpoofingAnswer: BExplanation:Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash. QUESTION 352Several bins are located throughout a building for secure disposal of sensitive information.Which of the following does this prevent? A. Dumpster divingB. War drivingC. TailgatingD. War chalking Answer: AExplanation:The bins in this question will be secure bins designed to prevent someone accessing the `rubbish' to learn sensitive information.Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash. QUESTION 353Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this action remediate? A. Shoulder SurfingB. Dumpster DivingC. PhishingD. Impersonation Answer: BExplanation:Incinerating documents (or shredding documents) instead of throwing them into a bin will prevent people being able to read the documents to view sensitive information. Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash. QUESTION 354At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe? A. Shoulder surfingB. TailgatingC. WhalingD. Impersonation Answer: BExplanation:Although Ann is an employee and therefore authorized to enter the building, she does not have her badge and therefore strictly she should not be allowed to enter the building. Just as a driver can tailgate another driver's car by following too closely, in the security sense, tailgating means to compromise physical security by following somebody through a door meant to keep out intruders. Tailgating is actually a form of social engineering, whereby someone who is not authorized to enter a particular area does so by following closely behind someone who is authorized. QUESTION 355Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number.Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent? A. CollusionB. ImpersonationC. PharmingD. Transitive Access Answer: B Explanation: Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. The procedure the users have to go through is to ensure that the technician who will have access to the computer is a genuine

technician and not someone impersonating a technician. QUESTION 356Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor's number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code.Which of the following attack types is this? A. HoaxB. ImpersonationC. Spear phishingD. Whaling Answer: BExplanation:In this question, the impersonator is impersonating a vendor and asking for payment. They have managed to `spoof' their calling number so that their caller ID matches the vendor's number. Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. QUESTION 357A database administrator receives a call on an outside telephone line from a person who states that they work for a well-known database vendor. The caller states there have been problems applying the newly released vulnerability patch for their database system, and asks what version is being used so that they can assist. Which of the following is the BEST action for the administrator to take? A. Thank the caller, report the contact to the manager, and contact the vendor support line to verify any reported patch issues.B. Obtain the vendor's email and phone number and call them back after identifying the number of systems affected by the patch.C. Give the caller the database version and patch level so that they can receive help applying the patch.D. Call the police to report the contact about the database systems, and then check system logs for attack attempts. Answer: AExplanation:Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. In this question, the person making the call may be impersonating someone who works for a well- known database vendor. The actions described in this answer would mitigate the risk. By not divulging information about your database system and contacting the vendor directly, you can be sure that you are talking to the right people. QUESTION 358A security administrator forgets their card to access the server room. The administrator asks a coworker if they could use their card for the day. Which of the following is the administrator using to gain access to the server room? A. Man-in-the-middleB. TailgatingC. ImpersonationD. Spoofing Answer: CExplanation:Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.In this question, by using the coworker's card, the security administrator is `impersonating' the coworker. The server room locking system and any logging systems will `think' that the coworker has entered the server room. QUESTION 359Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST? A. PhishingB. Shoulder surfingC. ImpersonationD. Tailgating Answer: CExplanation:Two attacks took place in this question. The first attack was shoulder surfing. This was the act of Sara recording a person typing in their ID number into a keypad to gain access to the building. The second attack was impersonation. Sara called the helpdesk and used the PIN to impersonate the person she recorded. QUESTION 360Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails? A. WhalingB. ImpersonationC. Privilege escalationD. Spear phishing Answer: A Explanation:A whaling attack is targeted at company executives. Mapping out an organization's staff hierarchy to determine who the people at the top are is also part of a whaling attack. Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. QUESTION 361 Which of the following attacks targets high level executives to gain company information? A. PhishingB. WhalingC. Vishing D. Spoofing Answer: BExplanation:Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. QUESTION 362Users are

encouraged to click on a link in an email to obtain exclusive access to the newest version of a popular Smartphone. This is an example of. A. ScarcityB. FamiliarityC. IntimidationD. Trust Answer: AExplanation:Scarcity, in the area of social psychology, works much like scarcity in the area of economics. Simply put, humans place a higher value on an object that is scarce, and a lower value on those that are abundant. The thought that we, as humans, want something we cannot have drives us to desire the object even more. This idea is deeply embedded in the intensely popular, "Black Friday" shopping extravaganza that U.S. consumers participate in every year on the day after Thanksgiving. More than getting a bargain on a hot gift idea, shoppers thrive on the competition itself, in obtaining the scarce product. In this question, people want the brand new latest version of a smartphone. The temptation of being one of the first to get the new phone will tempt people into clicking the link in the email. QUESTION 363A computer supply company is located in a building with three wireless networks. The system security team implemented a quarterly security scan and saw the following. SSIDStateChannelLevelComputer AreUs1connected170dbmComputer AreUs2connected580dbmComputer AreUs3connected375dbmComputer AreUs4connected695dbm Which of the following is this an example of? A. Rogue access pointB. Near field communicationC. JammingD. Packet sniffing Answer: AExplanation:The question states that the building has three wireless networks. However, the scan is showing four wireless networks with the SSIDs: Computer AreUs1 , Computer AreUs2 , Computer AreUs3 and Computer AreUs4. Therefore, one of these wireless networks probably shouldn't be there.This is an example of a rogue access point.A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server- client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points. QUESTION 364Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which ofthe following wireless attacks would this address? A. InterferenceB. Man-in-the-middleC. ARP poisoningD. Rogue access point Answer: DExplanation:MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. In this question, a rogue access point would need to be able to connect to the network to provide access to network resources. If the MAC address of the rogue access point isn't allowed to connect to the network port, then the rogue access point will not be able to connect to the network. QUESTION 365Users have been reporting that their wireless access point is not functioning. They state that it allows slow connections to the internet, but does not provide access to the internal network. The user provides the SSID and the technician logs into the company's access point and finds no issues. Which of the following should the technician do? A. Change the access point from WPA2 to WEP to determine if the encryption is too strongB. Clear all access logs from the AP to provide an up-to-date access list of connected usersC. Check the MAC address of the AP to which the users are connecting to determine if it is an imposterD. Reconfigure the access point so that it is blocking all inbound and outbound traffic as a troubleshooting gap Answer: CExplanation:The users may be connecting to a rogue access point. The rogue access point could be hosting a wireless network that has the same SSID as the corporate wireless network. The only way to tell for sure if the access point the users are connecting to is the correct one is to check the MAC address. Every network card has a unique 48-bit address assigned. A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.A network node may have multiple NICs and each NIC must have a unique MAC address. MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64. QUESTION 366Ann, the network administrator, has learned from the helpdesk that employees are accessing

the wireless network without entering their domain credentials upon connection. Once the connection is made, they cannot reach any internal resources, while wired network connections operate smoothly. Which of the following is MOST likely occurring? A. A user has plugged in a personal access point at their desk to connect to the network wirelessly.B. The company is currently experiencing an attack on their internal DNS servers.C. The company's WEP encryption has been compromised and WPA2 needs to be implemented instead.D. An attacker has installed an access point nearby in an attempt to capture company information. Answer: DExplanation:The question implies that users should be required to enter their domain credentials upon connection to the wireless network. The fact that they are connecting to a wireless network without being prompted for their domain credentials and they are unable to access network resources suggests they are connecting to a rogue wireless network. A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server- client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points. QUESTION 367Which of the following is where an unauthorized device is found allowing access to a network? A. BluesnarfingB. Rogue access pointC. HoneypotD. IV attack Answer: BExplanation:A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server- client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points. QUESTION 368Which of the following attacks would cause all mobile devices to lose their association with corporate access points while the attack is underway? A. Wireless jammingB. Evil twinC. Rogue APD. Packet sniffing Answer: AExplanation:When most people think of frequency jamming, what comes to mind are radio, radar and cell phone jamming. However, any communication that uses radio frequencies can be jammed by a strong radio signal in the same frequency. In this manner, Wi-Fi may be attacked with a network jamming attack, reducing signal quality until it becomes unusable or disconnects occur. With very similar methods, a focused and aimed signal can actually break access point hardware, as with equipment destruction attacks. QUESTION 369The system administrator has been notified that many users are having difficulty connecting to the company's wireless network. They take a new laptop and physically go to the access point and connect with no problems. Which of the following would be the MOST likely cause? A. The certificate used to authenticate users has been compromised and revoked.B. Multiple war drivers in the parking lot have exhausted all available IPs from the pool to deny access.C. An attacker has gained access to the access point and has changed the encryption keys.D. An unauthorized access point has been configured to operate on the same channel. Answer: DExplanation:Wireless Access Points can be configured to use a channel. If you have multiple access points within range of each other, you should configure the access points to use different channels. Different channels use different frequencies. If you have two access points using the same channel, their wifi signals will interfere with each other. The question states that that many users are having difficulty connecting to the company's wireless network. This is probably due to the signal being weakened by interference from another access point using the same channel. When the administrator takes a new laptop and physically goes to the access point and connects with no problems, he is able to connect because he is near the access point and therefore has a strong signal. QUESTION 370After viewing wireless traffic, an attacker notices the following networks are being broadcasted by local access points: CorpnetCoffeeshop FreePublicWifi Using this information the attacker spoofs a response to make nearby laptops connect back to a malicious device. Which of the following has the attacker created? A. Infrastructure as a ServiceB. Load balancerC. Evil twinD. Virtualized network Answer: CExplanation:In this question, the attacker has created another wireless network that is impersonating one of more of the three wireless networks listed in the question. This is known as an Evil Twin. An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.For example, a hacker using an evil twin exploit may be

positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits. QUESTION 371After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output: MAC SSID ENCRYPTION POWER BEACONS00:10:A1:36:12:CC MYCORP WPA2 CCMP 60 120200:10:A1:49:FC:37 MYCORP WPA2 CCMP 70 9102 FB:90:11:42:FA:99 MYCORP WPA2 CCMP 40 303100:10:A1:AA:BB:CC MYCORP WPA2 CCMP 55 202100:10:A1:FA:B1:07 MYCORP WPA2 CCMP 30 6044 Given that the corporate wireless network has been standardized, which of the following attacks is underway? A. Evil twinB. IV attackC. Rogue APD. DDoS Answer: AExplanation:The question states that the corporate wireless network has been standardized. By `standardized' it means the wireless network access points are running on hardware from the same vendor. We can see this from the MAC addresses used. The first half of a MAC address is vendor specific. The second half is network adapter specific. We have four devices with MAC addresses that start with 00:10:A1.The "odd one out" is the device with a MAC address starting FB:90:11. This device is from a different vendor. The SSID of the wireless network on this access point is the same as the other legitimate access points. Therefore, the access point with a MAC address starting FB:90:11 is impersonating the corporate access points. This is known as an Evil Twin. An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits. QUESTION 372Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users? A. IV attackB. Evil twin C. War drivingD. Rogue access point Answer: BExplanation:An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits. QUESTION 373Matt, an administrator, is concerned about the wireless network being discovered by war driving.Which of the following can be done to mitigate this? A. Enforce a policy for all users to authentic through a biometric device.B. Disable all SSID broadcasting.C. Ensure all access points are running the latest firmware.D. Move all access points into public access areas. Answer: BExplanation:B: War driving is the act of using a detection tool to look for wireless networking signals. The setting making a wireless network closed (or at least hidden) is the disabling of service set identifier (SSID) broadcasting. Thus by disabling all SSID broadcasting you can mitigate the risk of war driving. QUESTION 374 Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device? A. Man-in-the-middleB. BluejackingC. BluesnarfingD. Packet sniffing Answer: BExplanation: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 375Joe, an employee is taking a taxi through a busy city and starts to receive unsolicited files sent to his Smartphone. Which of the following is this an example of? A. VishingB. BluejackingC. War DrivingD. SPIME. Bluesnarfing Answer: BExplanation: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. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E If you use Lead2pass braindump as your SY0-401 exam prepare material, we guarantee your success in the first attempt. Lead2pass SY0-401 dump provides you everything you will need to take your SY0-401 Exam. 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]