[2017 New Free Downloading SY0-401 Exam Dumps PDF From Lead2pass (301-325)

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! I have already passed CompTIA SY0-401 certification exam today! Scored 989/1000 in Australia. SO MANY new added exam questions which made me headache?.. Anyway, I finally passed SY0-401 exam with the help of Lead2pass! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 301A company recently experienced data loss when a server crashed due to a midday power outage.Which of the following should be used to prevent this from occurring again? A. Recovery proceduresB. EMI shieldingC. Environmental monitoringD. RedundancyAnswer: DExplanation:Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction (in this case a power outage). Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. QUESTION 302Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure? A. Hardware load balancingB. RAIDC. A cold siteD. A host standby Answer: BExplanation:Fault tolerance is the ability of a system to sustain operations in the event of a component failure. Fault-tolerant systems can continue operation even though a critical component, such as a disk drive, has failed. This capability involves overengineering systems by adding redundant components and subsystems. RAID can achieve fault tolerance using software which can be done using the existing hardware and software. QUESTION 303After a company has standardized to a single operating system, not all servers are immune to a well-known OS vulnerability. Which of the following solutions would mitigate this issue? A. Host based firewallB. Initial baseline configurationsC. Discretionary access controlD. Patch management system Answer: DExplanation:A patch is an update to a system. Sometimes a patch adds new functionality; in other cases, it corrects a bug in the software. Patch Management can thus be used to fix security problems discovered within the OS thus negating a known OS vulnerability. QUESTION 304A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls? A. IntegrityB. AvailabilityC. ConfidentialityD. Safety Answer: DExplanation:Fencing is used to increase physical security and safety. Locks are used to keep those who are unauthorized out. QUESTION 305A cafe provides laptops for Internet access to their customers. The cafe is located in the center corridor of a busy shopping mall. The company has experienced several laptop thefts from the cafe during peak shopping hours of the day. Corporate has asked that the IT department provide a solution to eliminate laptop theft. Which of the following would provide the IT department with the BEST solution? A. Attach cable locks to each laptopB. Require each customer to sign an AUPC. Install a GPS tracking device onto each laptopD. Install security cameras within the perimeter of the caf? Answer: AExplanation:All laptop cases include a built-in security slot in which a cable lock can be inserted to prevent it from easily being removed from the premises. QUESTION 306Which of the following malware types may require user interaction, does not hide itself, and is commonly identified by marketing pop-ups based on browsing habits? A. BotnetB. RootkitC. AdwareD. Virus Answer: CExplanation:Adware is free software that is supported by advertisements. Common adware programs are toolbars, games and utilities. They are free to use, but require you to watch advertisements as long as the programs are open. Adware typically requires an active Internet connection to run. QUESTION 307A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program? A. Zero-dayB. TrojanC. VirusD. Rootkit Answer: CExplanation:A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs. QUESTION 308A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download? A. BackdoorB. SpywareC. Logic bombD. DDoSE. Smurf Answer: BExplanation:Spyware is software that is used to gather information about a person or organization without their knowledge and sends that information to another entity. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. QUESTION 309Which of the following malware types typically allows an attacker to monitor a user's computer, is characterized by a drive-by download, and requires no user interaction? A. VirusB. Logic bombC. SpywareD. Adware Answer: CExplanation:Spyware is software that is used to gather information about a person or organization without their knowledge and sends that information to another entity. QUESTION 310Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware? A. Logic bombB. WormC. TrojanD. Adware Answer: CExplanation:In computers, a Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus. QUESTION 311During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running. Which of the following has MOST likely been installed on the server? A. SPIMB. BackdoorC. Logic bombD. Rootkit Answer: DExplanation:A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user- level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection. The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network. QUESTION 312A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an: A. Logic bomb.B. Backdoor.C. Adware application.D. Rootkit. Answer: BExplanation:There has been a security breach on a computer system. The security administrator should now check for the existence of a backdoor.A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.Although the number of backdoors in systems using proprietary software (software whose source code is not publicly available) is not widely credited, they are nevertheless frequently exposed. Programmers have even succeeded in secretly installing large amounts of benign code as Easter eggs in programs, although such cases may involve official forbearance, if not actual permission. Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as DRM measures--and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers. QUESTION 313Two programmers write a new secure application for the human resources department to store personal identifiable information. The programmers make the application available to themselves using an uncommon port along with an ID and password only they know. This is an example of which of the following? A. Root KitB. SpywareC. Logic BombD. Backdoor Answer: DExplanation:A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.Although the number of backdoors in systems using proprietary software (software whose source code is not publicly available) is not widely credited, they are nevertheless frequently exposed. Programmers have even succeeded in secretly installing large amounts of benign code as Easter eggs in programs, although such cases may involve official forbearance, if not actual permission. Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as

DRM measures--and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers. QUESTION 314The Chief Information Officer (CIO) receives an anonymous threatening message that says "beware of the 1st of the year". The CIO suspects the message may be from a former disgruntled employee planning an attack.Which of the following should the CIO be concerned with? A. Smurf AttackB. TrojanC. Logic bombD. Virus Answer: CExplanation:A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. QUESTION 315Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO). A. RootkitB. Logic BombC. BotnetD. BackdoorE. Spyware Answer: BDExplanation:This is an example of both a logic bomb and a backdoor. The logic bomb is configured to `go off' or activate one week after her account has been disabled. The reactivated account will provide a backdoor into the system.A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system. QUESTION 316Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company? A. RootkitB. Logic bombC. WormD. Botnet Answer: BExplanation:This is an example of a logic bomb. The logic bomb is configured to `go off' or when Jane has left the company.A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. QUESTION 317Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware? A. Viruses are a subset of botnets which are used as part of SYN attacks.B. Botnets are a subset of malware which are used as part of DDoS attacks.C. Viruses are a class of malware which create hidden openings within an OS.D. Botnets are used within DR to ensure network uptime and viruses are not. Answer: BExplanation:A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules. QUESTION 318A user, Ann, is reporting to the company IT support group that her workstation screen is blank other than a window with a message requesting payment or else her hard drive will be formatted. Which of the following types of malware is on Ann's workstation? A. TrojanB. SpywareC. AdwareD. Ransomware Answer: DExplanation:Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive), while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a trojan like a conventional computer worm, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program will then run a payload: such as one that will begin to encrypt personal files on the hard drive. More sophisticated ransomware may hybrid-encrypt the victim's plaintext with a random symmetric key and a fixed public key. The malware author is the only party that knows the needed private decryption key. Some ransomware payloads do not use encryption. In these cases, the payload is simply an application designed to restrict interaction with the system, typically by setting the Windows Shell to itself, or even modifying the master boot record and/or partition table (which prevents the operating system from booting at all until it is repaired)Ransomware payloads utilize elements of scareware to extort money from the system's user. The payload may, for example, display notices purportedly issued by companies or law enforcement agencies which falsely claim that the system had been used for illegal activities, or contains illegal content such as pornography and pirated software or media. Some ransomware payloads imitate Windows' product activation notices, falsely claiming that their computer's Windows installation is counterfeit or requires re-activation. These tactics coax the user into paying the malware's author to remove the ransomware, either by supplying a program which can decrypt the files, or by sending an unlock code that undoes the changes the payload has made. QUESTION 319Which of the following describes a type of malware which is difficult to reverse engineer in a virtual lab? A. Armored virusB. Polymorphic malwareC. Logic bombD. Rootkit Answer: AExplanation:An armored virus is a type of virus that has been designed to thwart attempts by analysts from examining its code by using various methods to make tracing, disassembling and reverse engineering more difficult. An Armored Virus may also protect itself from antivirus programs, making it more difficult to trace. To do this, the Armored Virus attempts to trick the antivirus program into believing its location is somewhere other than where it really is on the system. QUESTION 320Hotspot QuestionSelect the appropriate attack from each drop down list to label the corresponding illustrated attackInstructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit. Answer: Explanation: http://searchsecurity.techtarget.com/definition/spear-phishing http://www.webopedia.com/TERM/V/vishing.html http://www.webopedia.com/TERM/P/phishing.htmlhttp://www.webopedia.com/TERM/P/pharming.html QUESTION 321Drag and Drop Question Task: Determine the types of attacks below by selecting an option from the dropdown list. Answer: Explanation:A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page. B: 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. C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit. D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS). E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques. http://www.webopedia.com/TERM/P/phishing.htmlhttp://www.techopedia.com/definition/28643/whaling http://www.webopedia.com/TERM/V/vishing.htmlhttp://searchsecurity.techtarget.com/definition/social-engineering QUESTION 322A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IPs: 10.10.3.1610.10.3.23212.178.24.26217.24.94.83 These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring? A. XSSB. DDoSC. DoSD. Xmas Answer: BExplanation:A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer.One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack. QUESTION 323A distributed denial of service attack can BEST be described as: A. Invalid characters being entered into a field in a database application.B. Users attempting to input random or invalid data into fields within a web browser application.C. Multiple computers attacking a single target in an organized attempt to deplete its resources.D. Multiple attackers attempting to gain elevated privileges on a target system. Answer: CExplanation:A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer.One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack. QUESTION 324An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that: A. it is being caused by the presence of a rogue access point.B. it is the beginning of a DDoS attack.C. the IDS has been compromised.D. the internal DNS tables have been poisoned. Answer: BExplanation:A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer.One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack. QUESTION 325A security technician at a small business is worried about the Layer 2 switches in the network suffering from a DoS style attack caused by staff incorrectly cabling network connections between switches.Which of the following will BEST mitigate the risk if implemented on the switches? A.   Spanning treeB.   Flood guardsC.   Access control listsD.   Syn flood Answer: AExplanation:Spanning Tree is designed to eliminate network `loops' from incorrect cabling between switches. Imagine two switches named switch 1 and switch 2 with two network cables connecting the switches. This would cause a network loop. A network loop between two switches can cause a `broadcast storm' where a broadcast packet is sent out of all ports on switch 1 which includes two links to switch 2. The broadcast packet is then sent out of all ports on switch 2 which includes links back to switch 1. The broadcast packet will be sent out of all ports on switch 1 again which includes two links to switch 2 and so on thus flooding the network with broadcast traffic. The Spanning-Tree Protocol (STP) was created to overcome the problems of transparent bridging in redundant networks. The purpose of STP is to avoid and eliminate loops in the network by negotiating a loop-free path through a root bridge. This is done by determining where there are loops in the network and blocking links that are redundant. Spanning-Tree Protocol executes an algorithm called the Spanning-Tree Algorithm (STA). In order to find redundant links, STA will choose a reference point called a Root Bridge, and then determines all the available paths to that reference point. If it finds a redundant path, it chooses for the best path to forward and for all other redundant paths to block. This effectively severs the redundant links within the network.All switches participating in STP gather information on other switches in the network through an exchange of data messages. These messages are referred to as Bridge Protocol Data Units (BPDUs). The exchange of BPDUs in a switched environment will result in the election of a root switch for the stable spanning-tree network topology, election of designated switch for every switched segment, and the removal of loops in the switched network by placing redundant switch ports in a backup state. Lead2pass SY0-401 PDF dumps is perfect! Totally! Thanks so much! SY0-401 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWExUbFM0YU0 **2017 CompTIA SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]