[Lead2pass Professional New Lead2pass SY0-401 Dumps PDF Version Released For Free Downloading (451-475)

Lead2pass 2017 September New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Good news, Lead2pass has updated the SY0-401 exam dumps. With all the questions and answers in your hands, you will pass the CompTIA SY0-401 exam easily. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 451Which of the following would a security administrator implement in order to identify a problem between two applications that are not communicating properly? A. Protocol analyzerB. Baseline reportC. Risk assessmentD. Vulnerability scanAnswer: AExplanation: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 and analyzing the packets sent between applications on systems that are not communicating properly could help determine the cause of the issue.Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal). QUESTION 452Which of the following tools would allow Ann, the security administrator, to be able to BEST quantify all traffic on her network? A. HoneypotB. Port scannerC. Protocol analyzerD. Vulnerability scanner Answer: CExplanation: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. By capturing and analyzing the packets sent between the systems on the network, Ann would be able to quantify the amount of traffic on the network.Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal). QUESTION 453Joe, the security administrator, has determined that one of his web servers is under attack. Which of the following can help determine where the attack originated from? A. Capture system imageB. Record time offsetC. ScreenshotsD. Network sniffing Answer: DExplanation:Network sniffing is the process of capturing and analyzing the packets sent between systems on the network. A network sniffer is also known as a Protocol Analyzer. 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 and analyzing the packets sent to the web server will help determine the source IP address of the system sending the packets.Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal). QUESTION 454Which of the following BEST allows Pete, a security administrator, to determine the type, source, and flags of the packet traversing a network for troubleshooting purposes? A. SwitchesB. Protocol analyzersC. RoutersD. Web security gateways 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. By capturing and analyzing the packets, Pete will be able to determine the type, source, and flags of the packets traversing a network for troubleshooting purposes.Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal). QUESTION 455Which of the following security architecture elements also has sniffer functionality? (Select TWO). A. HSMB. IPSC. SSL acceleratorD. WAPE. IDS Answer: BEExplanation:Sniffer functionality means the ability to capture and analyze the content of data packets as they are transmitted across the network.IDS and IPS systems perform their functions by capturing and analyzing the content of data packets. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content. QUESTION 456Which of the following would a security administrator implement in order to discover comprehensive security threats on a network? A. Design reviewsB. Baseline reportingC. Vulnerability scanD. Code review Answer: CExplanation:A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. Vulnerabilities include computer systems that do not have the latest security patches installed.The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities.A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise. QUESTION 457An administrator is concerned that a company's web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform? A. Vulnerability scanB. Risk assessmentC. Virus scanD. Network sniffer Answer: AExplanation:A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. Vulnerabilities include computer systems that do not have the latest security patches installed.The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities.A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise. QUESTION 458Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses? A. Penetration testB. Code reviewC. Vulnerability scanD. Brute Force scan Answer: CExplanation:A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise. QUESTION 459Which of the following should an administrator implement to research current attack methodologies? A. Design reviewsB. HoneypotC. Vulnerability scannerD. Code reviews Answer: BExplanation:A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes: The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers. There are two main types of honeypots:Production - A production honeypot is one used within an organization's environment to help mitigate risk.Research ?A research honeypot add value to research in computer security by providing a platform to study the threat. QUESTION 460Based on information leaked to industry websites, business management is concerned that unauthorized employees are accessing critical project information for a major, well-known new product. To identify any such users, the security administrator could: A. Set up a honeypot and place false project documentation on an unsecure share.B. Block access to the project documentation using a firewall.C. Increase antivirus coverage of the project servers.D. Apply security updates and harden the OS on all project servers. Answer: AExplanation:In this scenario, we would use a honeypot as a `trap' to catch unauthorized employees who are accessing critical project information.A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes: The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers. There are two main types of honeypots:Production - A production honeypot is one used within an organization's environment to help mitigate risk.Research ?A research honeypot add value to research in computer security by providing a platform to study the threat. QUESTION 461Joe, an administrator, installs a web server on the Internet that performs credit card transactions for customer payments. Joe also sets up a second web server that looks like the first web server.However, the second server contains fabricated files and folders made to look like payments were processed on this server but really were not. Which of the following is the second server? A. DMZB. HoneynetC. VLAND. Honeypot Answer: DExplanation:In this scenario, the second web server is a `fake' webserver designed to attract attacks. We can then monitor the second server to view the attacks and then ensure that the `real' web server is secure against such attacks. The second web server is a honeypot.A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes: The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers. There are two main types of honeypots:Production - A production honeypot is one used within an organization's environment to help mitigate risk.Research ?A research honeypot add value to research in computer security by providing a platform to study the threat. QUESTION 462Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network? A. Security logsB. Protocol analyzerC. Audit logsD. Honeypot Answer: DExplanation:A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes: The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers. There are two main types of honeypots:Production - A production honeypot is one used within an organization's environment to help mitigate risk. Research - A research honeypot add value to research in computer security by providing a platform to study the threat. QUESTION 463What is a system that is intended or designed to be broken into by an attacker? A. HoneypotB. HoneybucketC. DecoyD. Spoofing system Answer: AExplanation:A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies. According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes: The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers. There are two main types of honeypots:Production - A production honeypot is one used within an organization's environment to help mitigate risk.Research - A research honeypot add value to research in computer security by providing a platform to study the threat. QUESTION 464Several users report to the administrator that they are having issues downloading files from the file server. Which of the following assessment tools can be used to determine if there is an issue with the file server? A. MAC filter listB. Recovery agentC. BaselinesD. Access list Answer: CExplanation:The standard configuration on a server is known as the baseline. In this question, we can see if anything has changed on the file server by comparing its current configuration with the baseline. The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline.A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline). QUESTION 465One of the servers on the network stops responding due to lack of available memory. Server administrators did not have a clear definition of what action should have taken place based on the available memory. Which of the following would have BEST kept this incident from occurring? A. Set up a protocol analyzerB. Set up a performance baselineC. Review the systems monitor on a monthly basisD. Review the performance monitor on a monthly basis Answer: BExplanation:A performance baseline provides the input needed to design, implement, and support a secure network. The performance baseline would define the actions that should be performed on a server that is running low on memory. QUESTION 466Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release? A. Product baseline reportB. Input validationC. Patch regression testingD. Code review Answer: DExplanation:The problems listed in this question can be caused by problems with the application code.Reviewing the code will help to prevent the problems.The purpose of code review is to look at all custom written code for holes that may exist. The review needs also to examine changes that the code--most likely in the form of a finished application--may make: configuration files, libraries, and the like. During this examination, look for threats such as opportunities for injection to occur (SQL, LDAP, code, and so on), cross-site request forgery, and authentication. Code review is often conducted as a part of gray box testing. Looking at source code can often be one of the easiest ways to find weaknesses within the application. Simply reading the code is known as manual assessment, whereas using tools to scan the code is known as automated assessment. QUESTION 467Which of the following assessment techniques would a security administrator implement to ensure that systems and software are developed properly? A. Baseline reportingB. Input validationC. Determine attack surfaceD. Design reviews Answer: DExplanation:When implementing systems and software, an important step is the design of the systems and software. The systems and software should be designed to ensure that the system works as intended and is secure.The design review assessment examines the ports and protocols used, the rules, segmentation, and access control in the system or application. A design review is basically a check to ensure that the design of the system meets the security requirements. QUESTION 468A financial company requires a new private network link with a business partner to cater for realtime and batched data flows.Which of the following activities should be performed by the IT security staff member prior to establishing the link? A. Baseline reportingB. Design reviewC. Code reviewD. SLA reporting Answer: BExplanation:This question is asking about a new private network link (a VPN) with a business partner. This will provide access to the local network from the business partner. When implementing a VPN, an important step is the design of the VPN. The VPN should be designed to ensure that the security of the network and local systems is not compromised. The design review assessment examines the ports and protocols used, the rules, segmentation, and access control in the systems or applications. A design review is basically a check to ensure that the design of the system meets the security requirements. QUESTION 469Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place? A. Code reviewB. Penetration testC. Protocol analyzerD. Vulnerability scan Answer: BExplanation:Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. Pen test strategies include: Targeted testingTargeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out. External testingThis type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access. Internal testingThis test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause. Blind testingA blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive. Double blind testingDouble blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures. QUESTION 470Which of the following is the MOST intrusive type of testing against a production system? A. White box testingB. War dialingC. Vulnerability testingD. Penetration testing Answer: DExplanation:Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. Pen test strategies include: Targeted testingTargeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out. External testingThis type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access. Internal testingThis test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause. Blind testingA blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive. Double blind testingDouble blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures. QUESTION 471During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges? A. All users have write access to the directory.B. Jane has read access to the file.C. All users have read access to the file.D. Jane has read access to the directory. Answer: CExplanation:The question states that Jane was able to download a document from the spool directory. To view and download the document, Jane must have at least Read access to the file. The fact that the document belonged to someone else suggests that all users have read access to the file. QUESTION 472During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR). A. 21B. 22C. 23D. 69E. 3389F. SSHG. Terminal servicesH. RloginI. RsyncJ. Telnet Answer: BCFJExplanation:The question states that Jane was able to establish a connection to an internal router. Typical ports and protocols used to connect to a router include the following:B, F: Port 22 which is used by SSH (Secure Shell).C, J: Port 23 which is used by Telnet.SSH and Telnet both provide command line interfaces for administering network devices such as routers and switches. QUESTION 473Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate? A. War dialingB. War chalkingC. War drivingD. Bluesnarfing Answer: AExplanation:War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network. QUESTION 474Which of the following is BEST utilized to actively test security controls on a particular system? A. Port scanningB. Penetration testC. Vulnerability scanningD. Grey/Gray box Answer: BExplanation:Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. Pen test strategies include: Targeted testingTargeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out. External testingThis type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access. Internal testingThis test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause. Blind testingA blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive. Double blind testingDouble blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures. QUESTION 475A security administrator is aware that a portion of the company's Internet-facing network tends to be non-secure due to poorly configured and patched systems. The business owner has accepted the risk of those systems being compromised, but the administrator wants to determine the degree to which those systems can be used to gain access to the company intranet. Which of the following should the administrator perform? A. Patch management assessmentB. Business impact assessmentC. Penetration testD. Vulnerability assessment Answer: CExplanation:Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system. It is also used to determine the degree to which the systems can be used to gain access to the company intranet (the degree of access to local network resources).Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. Pen test strategies include: Targeted testingTargeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out. External testingThis type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access. Internal testingThis test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause. Blind testingA blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive. Double blind testingDouble blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Once there are some changes on SY0-401 exam questions, we will update the study materials timely to make sure that our customer can download the latest edition. 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]