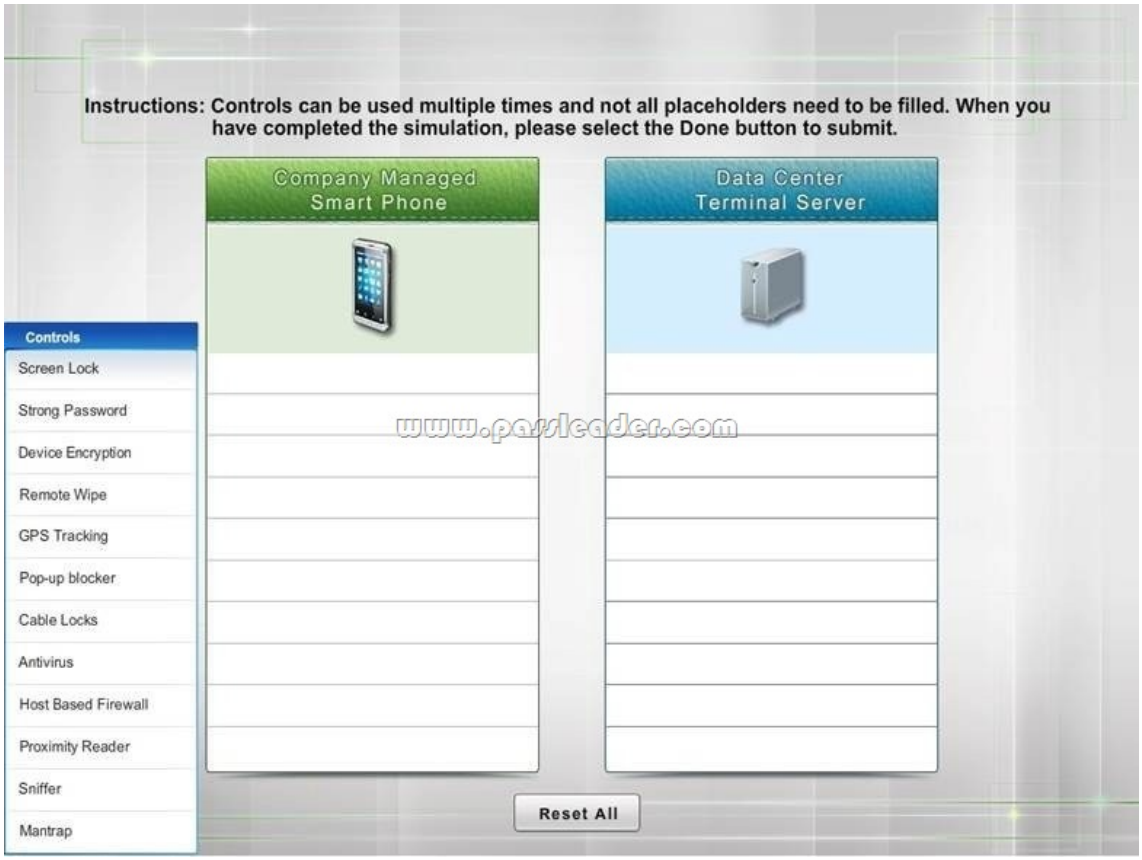
[Nov-2017 Dumps 166q SY0-501 Practice Test from PassLeader Guarantee 100% Passing Exam (Section D)

New Updated SY0-501 Exam Questions from PassLeader SY0-501 PDF dumps! Welcome to download the newest PassLeader SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (166 Q&As) Keywords: SY0-501 exam dumps, SY0-501 exam questions, SY0-501 VCE dumps, SY0-501 PDF dumps, SY0-501 practice tests, SY0-501 study guide, SY0-501 braindumps, CompTIA Security+ Exam P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg QUESTION 91 A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords, The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select TWO.) A.   The portal will function as an identity provider and issue an authentication assertion. B.   The portal will request an authentication ticket from each network that is transitively trusted. C.   The back-end networks will function as an identity provider and issue an authentication assertion. D.   The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store. E.   The back-end networks will verify the assertion token issued by the portal functioning as the identity provider. Answer: BC QUESTION 92 Which of the following would a security specialist be able to determine upon examination of a server's certificate? A.   CA public key B.   Server private key C.   CSR D.   OID Answer: B QUESTION 93 A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system While attempting to determine if an unauthorized user is togged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

www.passleader.com

Hostname	IP Address	MAC	MAC Filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

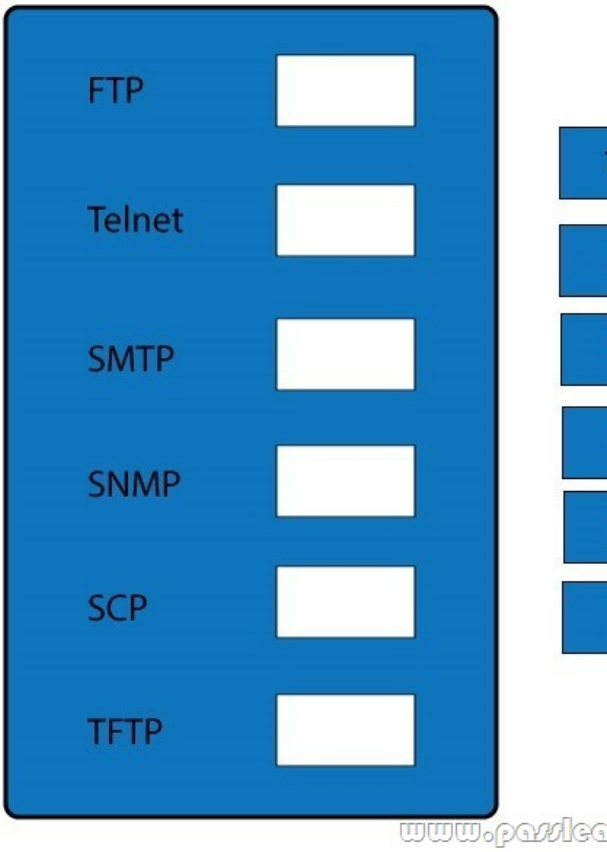
Which of the following should be the NEXT step to determine if there is an unauthorized user on the network? A.   Apply MAC filtering and see if the router drops any of the systems. B.   Physically check each of the authorized systems to determine if they are togged onto the network. C.   Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host. D.   Conduct a ping sweep of each of the authorized systems and see if an echo response is received. Answer: C QUESTION 94 Drag and Drop Question A Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type. Instructions: * Controls can be used multiple times and not all placeholders needs to be filled. * When you have completed the simulation, Please select Done to submit.



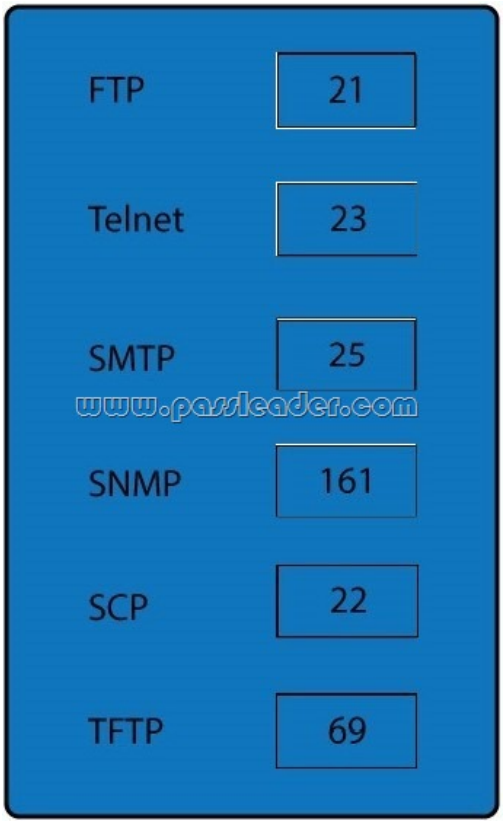
Answer:

QUESTION 95 A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation? A.   An

attacker can access and change the printer configuration. B.   SNMP data leaving the printer will not be properly encrypted. C.   An MITM attack can reveal sensitive information. D.   An attacker can easily inject malicious code into the printer firmware. E.   Attackers can use the PCL protocol to bypass the firewall of client computers. Answer: A QUESTION 96 A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select TWO.) A.   Generate an X.509-complaint certificate that is signed by a trusted CA. B.   Install and configure an SSH tunnel on the LDAP server. C.   Ensure port 389 is open between the clients and the servers using the communication. D.   Ensure port 636 is open between the clients and the servers using the communication. E.   Remove the LDAP directory service role from the server. Answer: AB QUESTION 97 Drag and Drop Question Drag and drop the correct protocol to its default port.

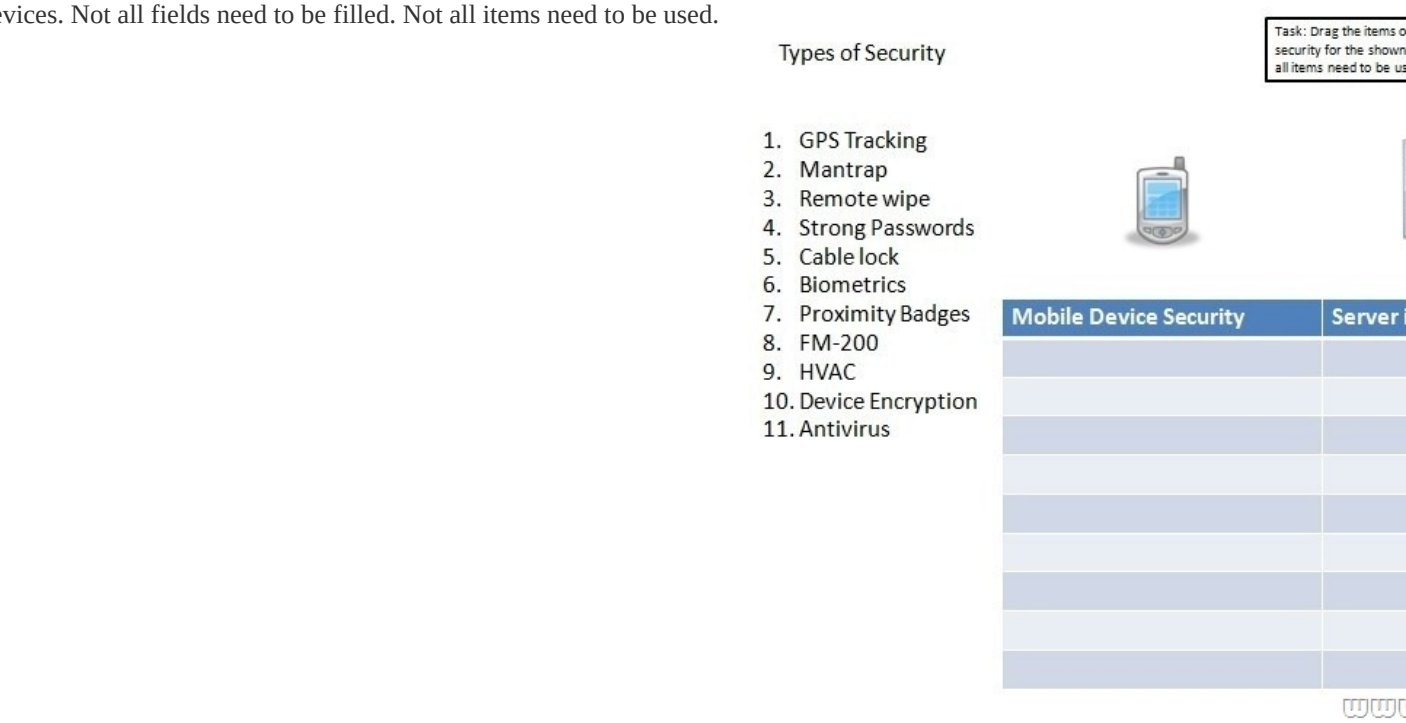


Answer:

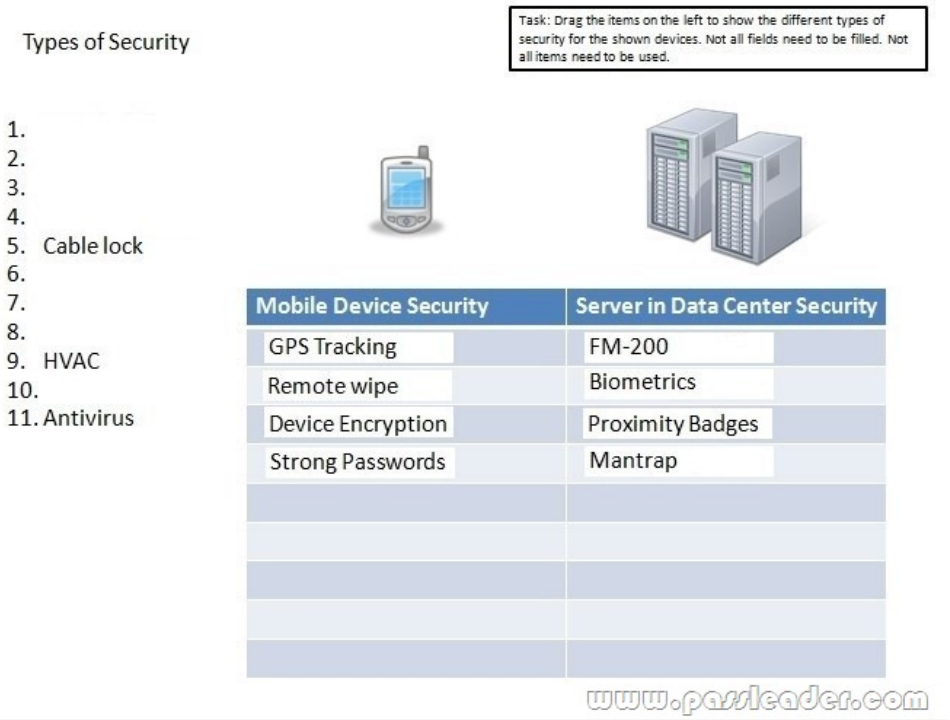


Explanation: - FTP uses TCP port 21. - Telnet uses port 23. - SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). - SMTP uses TCP port 25. - Port 69 is used by TFTP. - SNMP makes use of UDP ports 161 and 162. References: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers QUESTION 98 A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong? A.   SoC B.   ICS C.   IoT D.   MFD Answer: D QUESTION 99 The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device. Which of the following categories BEST describes what she is looking for? A.   ALE B.   MTTR C.   MTBF D.   MTTF Answer: D QUESTION 100 A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet. Which of the following should be used in the code? (Select TWO.) A.   Escrowed keys B.   SSL symmetric encryption key C.   Software code private key D.   Remote server public key E.   OCSP Answer: CE QUESTION 101 A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot. The person is attempting which of the following types of attacks? A.   Jamming B.   War chalking C.   Packet sniffing D.   Near field communication Answer: B QUESTION 102 A system administrator is configuring a site-to-site VPN tunnel. Which of the following should be configured on the VPN concentrator during the IKE phase? A.   RIPEMD B.   ECDHE C.   Diffie-Hellman D.   HTTPS Answer: C QUESTION 103 A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks. Which of the following is the reason the manager installed the racks this way? A.   To lower energy consumption by sharing power outlets B.   To create environmental hot and cold isles C.   To eliminate the potential for electromagnetic interference D.   To maximize fire suppression capabilities Answer: B QUESTION 104

Phishing emails frequently take advantage of high-profile catastrophes reported in the news. Which of the following principles BEST describes the weakness being exploited? A.   Intimidation B.   Scarcity C.   Authority D.   Social proof Answer: D QUESTION 105 Users report the following message appears when browsing to the company's secure site. This website cannot be trusted. Which of the following actions should a security analyst take to resolve these messages? (Select TWO.) A.   Verify the certificate has not expired on the server. B.   Ensure the certificate has a .pfx extension on the server. C.   Update the root certificate into the client computer certificate store. D.   Install the updated private key on the web server. E.   Have users clear their browsing history and relaunch the session. Answer: BD QUESTION 106 Drag and Drop Question Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

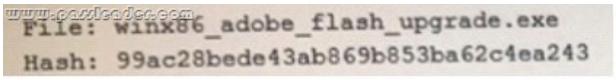


Answer:

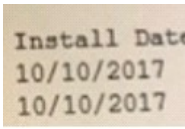


Explanation: For mobile devices, at bare minimum you should have the following security measures in place: Screen lock, Strong password, Device encryption, Remote wipe/Sanitation, Voice encryption, GPS tracking, Application control, Storage segmentation, Asset tracking as well as Device Access control. For servers in a data center your security should include: Fire extinguishers such as FM-200 as part of fire suppression; Biometric, proximity badges, mantraps, HVAC, cable locks; these can all be physical security measures to control access to the server. References: http://bit.ly/sy0-501-dumps (page 369-370) QUESTION 107 A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm? A.   Vulnerability scanning B.   Penetration testing C.   Application fuzzing D.   User permission Answer: A QUESTION 108 Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Winch of the following should be used to sign the users' certificates? A.   CA B.   CRL C.   CSR Answer: C QUESTION 109 Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions: * Shut down all network shares. * Run an email search identifying all employees who received the malicious message. * Reimage all devices belonging to users who opened the attachment. Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process? A.   Eradication B.   Containment C.   Recovery D.   Lessons learned Answer: A QUESTION 110 Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS? A.   Pivoting B.   Process affinity C.   Buffer overflow Answer: A QUESTION 111 Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network. This is MOST likely which of the following types of attacks? A.   Vishing B.   Impersonation C.   Spim D.   Scareware Answer: A QUESTION 112 An administrator discovers the following log entry on a server: Nov 12 2013 00:23:45 httpd[2342]: GET /app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow Which of the following attacks is being attempted? A.   Command injection B.   Password attack C.   Buffer overflow D.   Cross-site scripting Answer: B QUESTION 113 A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures? A.   Table top exercises B.   Lessons learned C.   Escalation procedures D.   Recovery procedures Answer: D QUESTION 114 Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application? A.   Protocol analyzer B.   Vulnerability scan C.   Penetration test D.   Port scanner Answer: B Explanation: 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 115 Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment? A.   Cloud computing B.   Virtualization C.   Redundancy D.   Application control Answer: B Explanation: Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation. QUESTION 116 A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN. Which of the following

protocols should be used? A.   RADIUS B.   Kerberos C.   LDAP D.   MSCHAP Answer: A QUESTION 117 Which of the following types of cloud Infrastructures would allow several organizations with similar structures and interests to realize shared storage and resources? A.   Private B.   Hybrid C.   Public D.   Community Answer: A QUESTION 118 A security administrator has found a hash m the environment known to belong to malware. The administrator then finds this file to be in the preupdate area of the OS, which indicates it was pushed from the central patch system.



The administrator pulls a report from the patch management system with the following output:



Given the above outputs, which of the following MOST likely happened? A.   The file was corrupted after it left the patch system. B.   The file was infected when the patch manager downloaded it. C.   The file was not approved in the application whitelist system. D.   The file was embedded with a logic bomb to evade detection. Answer: D QUESTION 119 Which of the following implements two-factor authentication? A.   A phone system requiring a PIN to make a call. B.   An ATM requiring a credit card and PIN. C.   A computer requiring username and password. D.   A datacenter mantrap requiring fingerprint and iris scan. Answer: D QUESTION 120 A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee? A.   Obtain a list of passwords used by the employee. B.   Generate a report on outstanding projects the employee handled. C.   Have the employee surrender company identification. D.   Have the employee sign an NDA before departing. Answer: A Download the newest PassLeader SY0-501 dumps from passleader.com now! 100% Pass Guarantee! SY0-501 PDF dumps & SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (166 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg