

[FREEBraindump2go SY0-401 Exam PDF Download (151-160)]

COMPTIA NEWS: SY0-401 Exam Questions has been Updated Today! Get Latest SY0-401 VCE and SY0-401 PDF Instantly! Welcome to Download the Newest Braindump2go SY0-401 VCE&SY0-401 PDF Dumps:

<http://www.braindump2go.com/sy0-401.html> (1220 Q&As) Braindump2go New Released SY0-401 CompTIA Exam Dumps Free Download Today! All 1220q SY0-401 Exam Questions are the new updated from CompTIA Official Exam Center.Braindump2go Offers SY0-401 PDF Dumps and SY0-401 VCE Dumps for free Download Now! 100% pass SY0-401 Certification Exam! Exam Code: SY0-401Exam Name: CompTIA Security+Certification Provider: CompTIACorresponding Certification: CompTIA Security+SY0-401 Dump,SY0-401 PDF,SY0-401 VCE,SY0-401 Braindump,SY0-401 Study Guide,SY0-401 Study Guide PDF,SY0-401 Objectives,SY0-401 Practice Test,SY0-401 Practice Exam,SY0-401 Performance Based Questions,SY0-401 Exam Questions,SY0-401 Exam Dumps,SY0-401 Exam PDF,SY0-401 Dumps Free,SY0-401 Dumps PDF

CompTIA Security+ Certification



Questions and Answers : 1220 Q&As
Updated: Nov 2, 2015
~~\$129.99~~ **\$99.99**
[PDF DEMO](#)
[CHECK OUT](#)

Product Description

Exam Number/Code: SY0-401

"CompTIA Security+ Certification. With the comprehensive exam resources, you will be ready for your success."

Free Demo Download

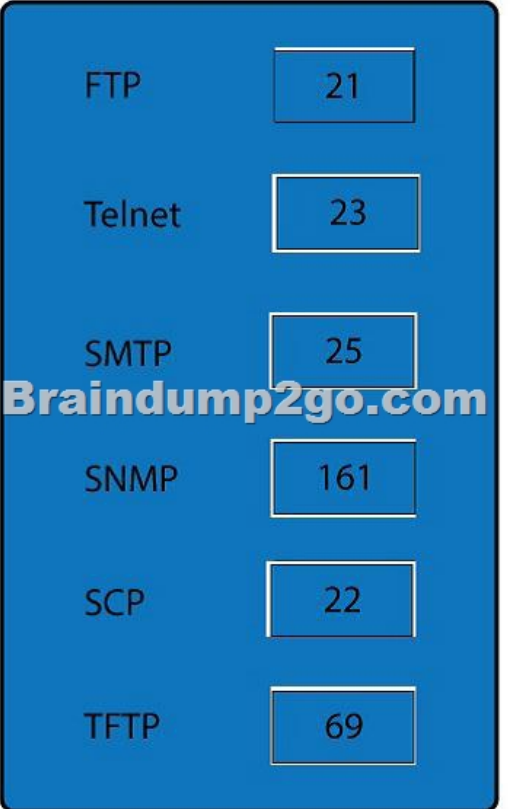
Braindump2go offers free demo. You can check out the interface and decide to buy it.

☒ Printable PDF ☒ PDF

QUESTION 151Drag and Drop QuestionsDrag and drop the correct protocol to its default port.

FTP	<input type="text"/>	161
Telnet	<input type="text"/>	22
SMTP	<input type="text"/>	21
SNMP	<input type="text"/>	25
SCP	<input type="text"/>	23
TFTP	<input type="text"/>	

Answer:



FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

Explanation: When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts. Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation. QUESTION 152 Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools? A. Identify user habits B. Disconnect system from network C. Capture system image D. Interview witnesses Answer: C Explanation: Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. Very much as helpful in same way that a virus sample is kept in laboratories to study later after a breakout. Also you should act in the order of volatility which states that the system image capture is first on the list of a forensic analysis. QUESTION 153 Computer evidence at a crime is preserved by making an exact copy of the hard disk. Which of the following does this illustrate? A. Taking screenshots B. System image capture C. Chain of custody D. Order of volatility Answer: B Explanation: A system image would be a snapshot of what exists at the moment. Thus capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. QUESTION 154 To ensure proper evidence collection, which of the following steps should be performed FIRST? A. Take hashes from the live system B. Review logs C. Capture the system image D. Copy all compromised files Answer: C Explanation: Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. This is essential since the collection of evidence process may result in some mishandling and changing the exploited state. QUESTION 155 A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive? A. `cp /dev/sda /dev/sdb bs=8kB` B. `tail -f /dev/sda > /dev/sdb bs=8kB` C. `dd in=/dev/sda out=/dev/sdb bs=4kB` D. `locate /dev/sda /dev/sdb bs=4k` Answer: C Explanation: `dd` is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files. `dd` can duplicate data across files, devices, partitions and volumes On Unix, device drivers for hardware (such as hard disks) and special device files (such as `/dev/zero` and `/dev/random`) appear in the file system just like normal files; `dd` can also read and/or write from/to these files, provided that function is implemented in their respective driver. As a result, `dd` can be used for tasks such as backing up the boot sector of a hard drive, and obtaining a fixed amount of random data. The `dd` program can also perform conversions on the data as it is copied, including byte order swapping and conversion to and from

the ASCII and EBCDIC text encodings. An attempt to copy the entire disk using cp may omit the final block if it is of an unexpected length; whereas dd may succeed. The source and destination disks should have the same size. QUESTION 156A security technician wishes to gather and analyze all Web traffic during a particular time period. Which of the following represents the BEST approach to gathering the required data? A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443. B. Configure a proxy server to log all traffic destined for ports 80 and 443. C. Configure a switch to log all traffic destined for ports 80 and 443. D. Configure a NIDS to log all traffic destined for ports 80 and 443. Answer: B Explanation: A proxy server is in essence a device that acts on behalf of others and in security terms all internal user interaction with the Internet should be controlled through a proxy server. This makes a proxy server the best tool to gather the required data. QUESTION 157A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used? A. Detective B. Deterrent C. Corrective D. Preventive Answer: C Explanation: A corrective control would be any corrective action taken to correct any existing control that were faulty or wrongly installed ?as in this case the cameras were already there, it just had to be adjusted to perform its function as intended. QUESTION 158Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity? A. Place a full-time guard at the entrance to confirm user identity. B. Install a camera and DVR at the entrance to monitor access. C. Revoke all proximity badge access to make users justify access. D. Install a motion detector near the entrance. Answer: B Explanation: Tailgating is a favorite method of gaining entry to electronically locked systems by following someone through the door they just unlocked. With a limited budget installing a camera and DVR at the entrance to monitor access to the restricted areas is the most feasible solution. The benefit of a camera (also known as closed-circuit television, or CCTV) is that it is always running and can record everything it sees, creating evidence that can be admissible in court if necessary. QUESTION 159The incident response team has received the following email message. From: monitor@ext-company.com To: security@company.com Subject: Copyright infringement A copyright infringement alert was triggered by IP address 13.10.66.5 at 09: 50: 01 GMT. After reviewing the following web logs for IP 13.10.66.5, the team is unable to correlate and identify the incident. 09: 45: 33 13.10.66.5 http:

//remote.site.com/login.asp?user=john 09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne 10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov 11: 02: 45 13.10.65.5 http: //remote.site.com/download.asp?movie.mov=ok Which of the following is the MOST likely reason why the incident response team is unable to identify and correlate the incident? A. The logs are corrupt and no longer forensically sound. B. Traffic logs for the incident are unavailable. C. Chain of custody was not properly maintained. D. Incident time offsets were not accounted for. Answer: D Explanation: It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system. QUESTION 160A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that: A. HDD hashes are accurate. B. the NTP server works properly. C. chain of custody is preserved. D. time offset can be calculated. Answer: D Explanation: It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system. Guaranteed 100% CompTIA SY0-401 Exam Pass OR Full Money Back! Braindump2go Provides you the latest SY0-401 Dumps PDF & VCE for Instant Download!

CompTIA Security+ Certification Exam: SY0-401



Questions and Answers : 1220
Q&As

Updated: Nov 2, 2015

~~\$129.99~~ **\$99.99**

PDF DEMO

CHECK OUT

Product Description Exam Number/Code: SY0-401

Exam Number/Code: SY0-401

"CompTIA Security+ Certification Exam", also known as SY0-401 exam, is a CompTIA Certification. With the complete collection of questions and answers, Braindump2go has assembled to take you through 1220 Q&As to your SY0-401 Exam preparation. In the SY0-401 exam resources, you will cover every field and category in CompTIA CompTIA Security+ helping to ready you for your successful CompTIA Certification.

Free Demo Download

Braindump2go offers free demo for SY0-401 exam (CompTIA Security+ Certification Exam). You can check out the interface, question quality and usability of our practice exams before you decide to buy it.

☒ **Printable PDF** ☒ **Premium VCE + VCE Simulator**

FREE DOWNLOAD: NEW UPDATED SY0-401 PDF Dumps & SY0-401 VCE Dumps from Braindump2go:

<http://www.braindump2go.com/sy0-401.html> (1220 Q&A)