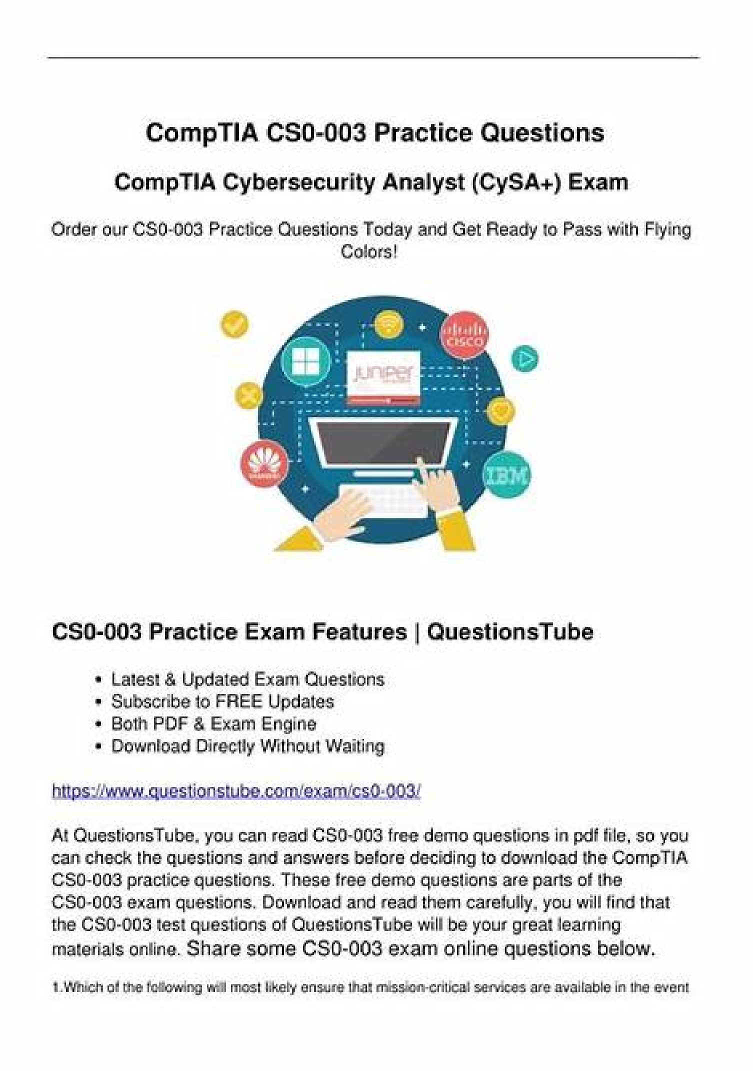
The latest CompTIA certification CS0-003 exam practice questions and answers



CompTIA CS0-003 Practice Questions

CompTIA Cybersecurity Analyst (CySA+) Exam

Order our CS0-003 Practice Questions Today and Get Ready to Pass with Flying Colors!

CS0-003 Practice Exam Features | QuestionsTube

- Latest & Updated Exam Questions
- Subscribe to FREE Updates
- Both PDF & Exam Engine
- Download Directly Without Waiting

https://www.questionstube.com/exam/cs0-003/

At QuestionsTube, you can read CS0-003 free demo questions in pdf file, so you can check the questions and answers before deciding to download the CompTIA CS0-003 practice questions. These free demo questions are parts of the CS0-003 exam questions. Download and read them carefully, you will find that the CS0-003 test questions of QuestionsTube will be your great learning materials online. Share some CS0-003 exam online questions below.

1.Which of the following will most likely ensure that mission-critical services are available in the event

P.S. Free & New CS0-003 dumps are available on Google Drive shared by Lead1Pass: https://drive.google.com/open?id=1c3aUi9DymZxsoSk61JNAhCAEs6R7fFph

We will provide you with three different versions of our CS0-003 exam questions on our test platform. You have the opportunity to download the three different versions from our test platform. The three different versions of our CS0-003 Test Torrent include the PDF version, the software version and the online version. The three different versions will offer you same questions and answers, but they have different functions.

Our CS0-003 Exam Torrent carries no viruses. We provide free update and online customer service which works on the line whole day. Our study materials provide varied versions for you to choose and the learning costs you little time and energy. You can use our CS0-003 exam prep immediately after you purchase them, we will send our product within 5-10 minutes to you. We treat your time as our own time, as precious as you see, so we never waste a minute or two in some useless process. Please rest assured that use, we believe that you will definitely pass the exam.

>> New CS0-003 Real Exam <<

CompTIA CS0-003 Study Demo, CS0-003 Test Pdf

We can say that how many the CS0-003 certifications you get and obtain qualification certificates, to some extent determines your future employment and development, as a result, the CS0-003 exam guide is committed to helping you become a competitive workforce, let you have no trouble back at home. Actually, just think of our CS0-003 Test Prep as the best way to pass the exam is myopic. They can not only achieve this, but ingeniously help you remember more content at the same time.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q84-Q89):

NEW QUESTION # 84

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability.
Which of the following CVE metrics would be most accurate for this zero-day threat?

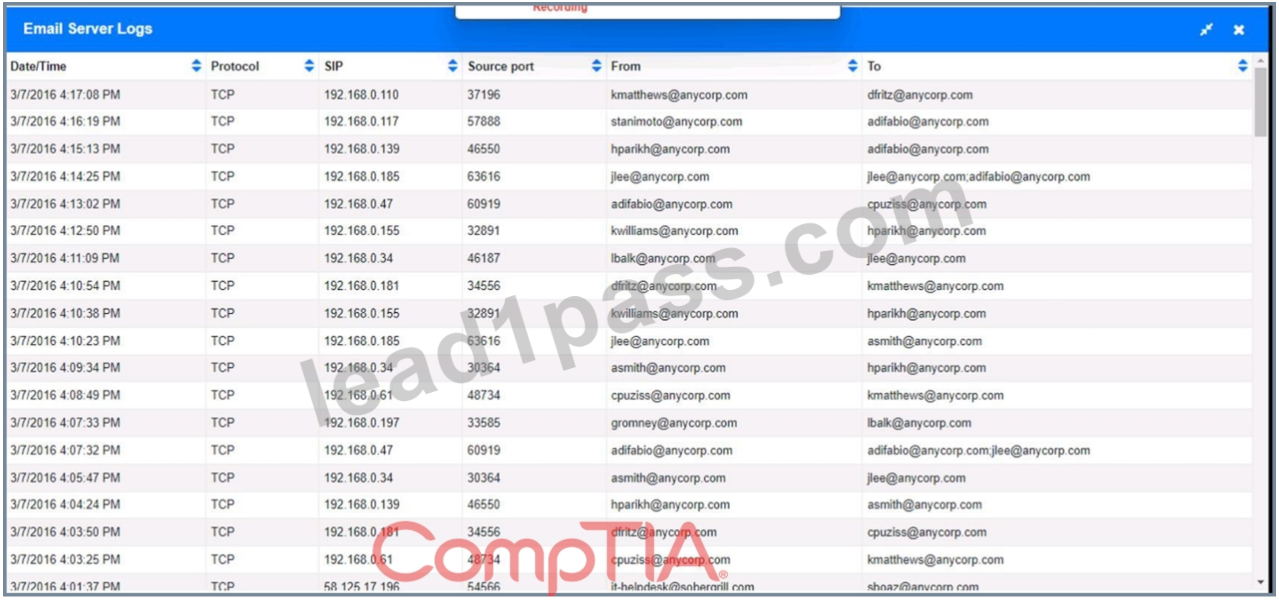
- A. CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
- B. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
- C. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H
- D. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L

Answer: A

Explanation:
The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L).

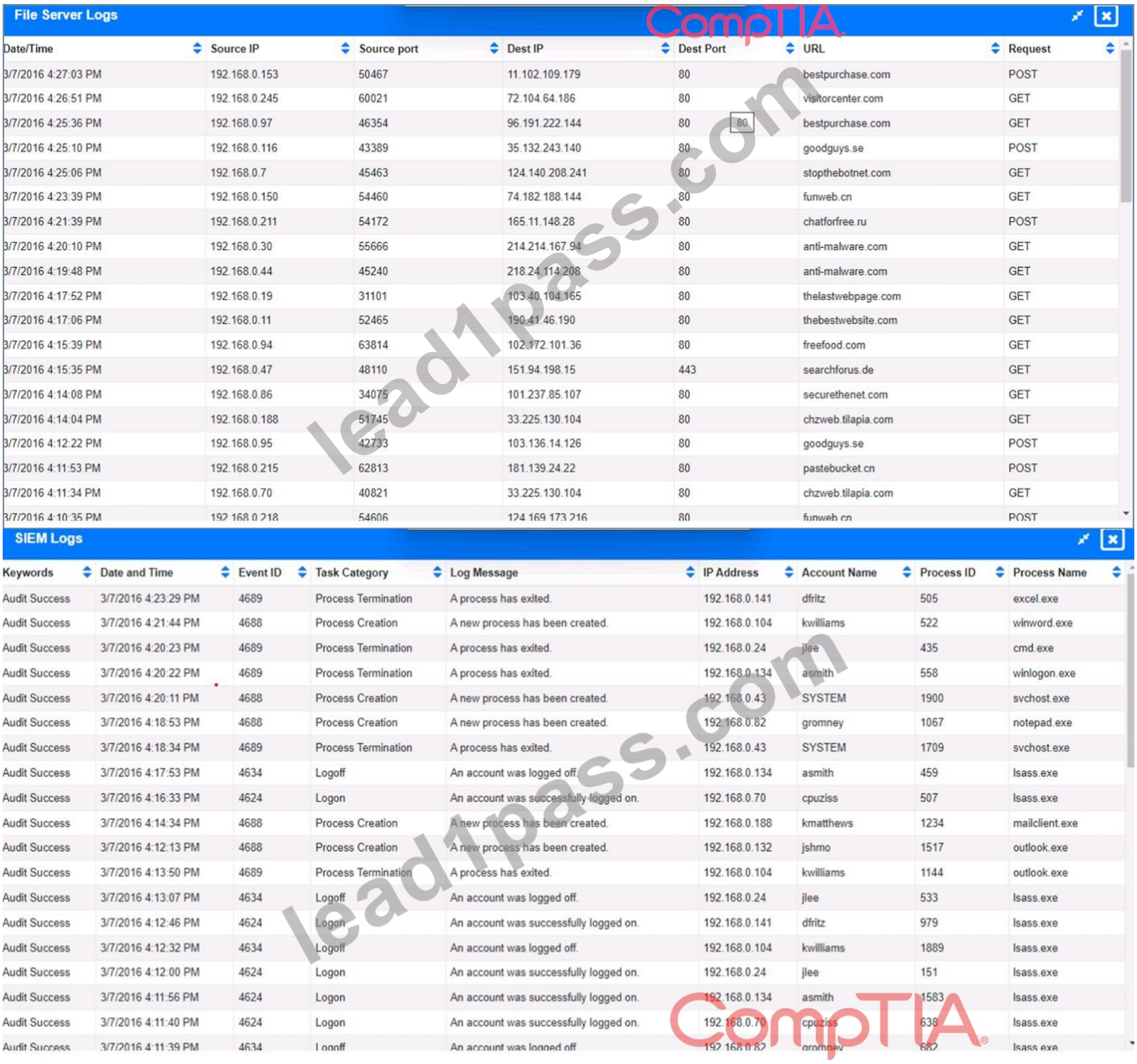
NEW QUESTION # 85

Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.



Email Server Logs

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com;jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sboaz@anycorp.com



File Server Logs

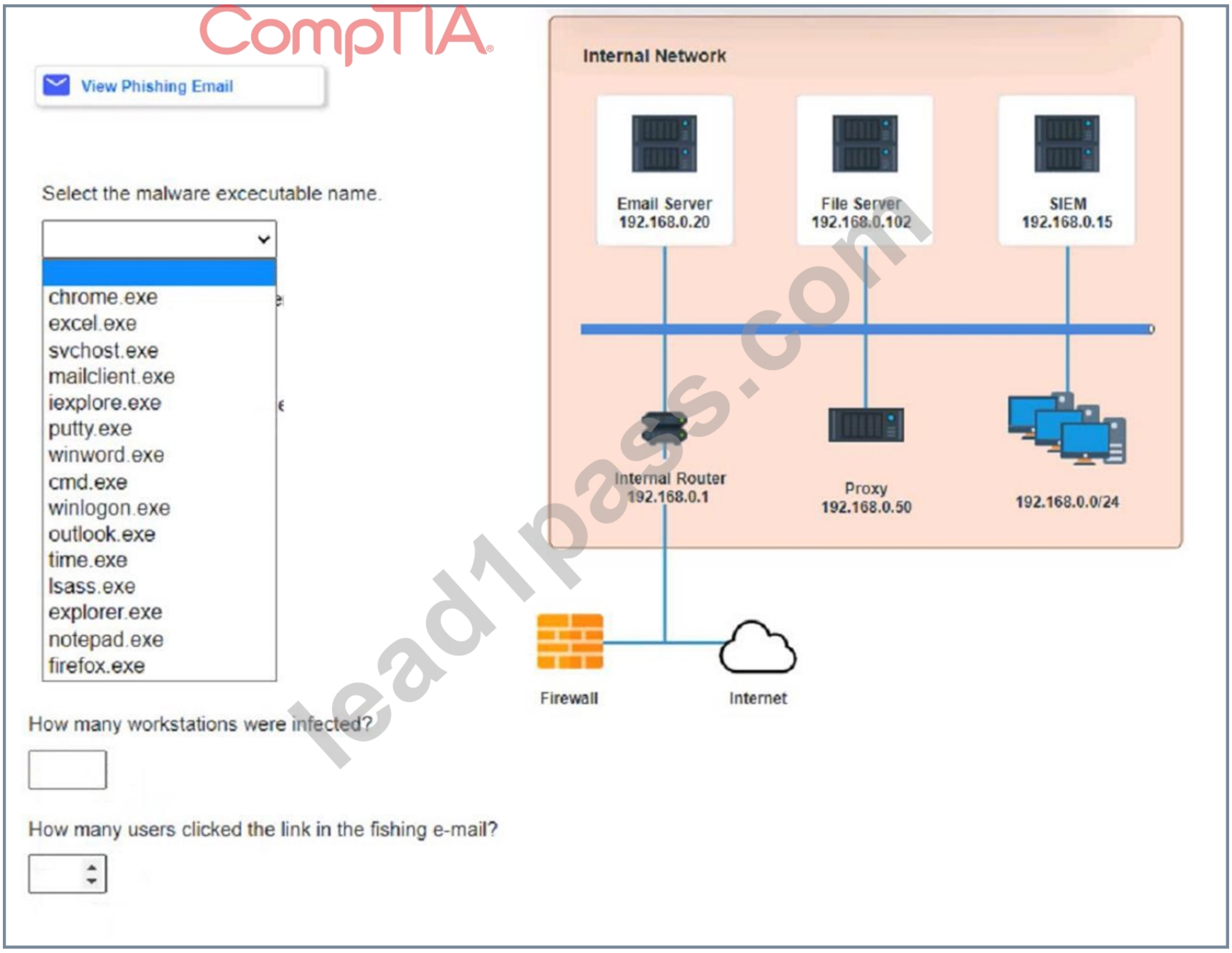
Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST

SIEM Logs

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off	192.168.0.82	gromney	682	lsass.exe

Review the information provided and determine the following:

1. HOW many employees Clicked on the link in the Phishing email?
2. on how many workstations was the malware installed?
3. what is the executable file name of the malware?



View Phishing Email

Select the malware excecutable name.

- chrome.exe
- excel.exe
- svchost.exe
- mailclient.exe
- iexplore.exe
- putty.exe
- winword.exe
- cmd.exe
- winlogon.exe
- outlook.exe
- time.exe
- lsass.exe
- explorer.exe
- notepad.exe
- firefox.exe

How many workstations were infected?

How many users clicked the link in the fishing e-mail?

Answer:

Explanation:
see the answer in explanation for this task.
Explanation
1. How many employees clicked on the link in the phishing email?
According to the email server logs, 25 employees clicked on the link in the phishing email.
2. On how many workstations was the malware installed?
According to the file server logs, the malware was installed on 15 workstations.
3. What is the executable file name of the malware?
The executable file name of the malware is svchost.EXE.
Answers
1. 25
2. 15
3. svchost.EXE

NEW QUESTION # 86

Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

- A. Share the log directory on each server to allow local access.
- B. Automate the emailing of logs to the analysts.
- C. Deploy a database to aggregate the logging
- D. Configure the servers to forward logs to a SIEM

Answer: D

Explanation:
The best implementation to give the best central visibility into the events occurring throughout the corporate environment without

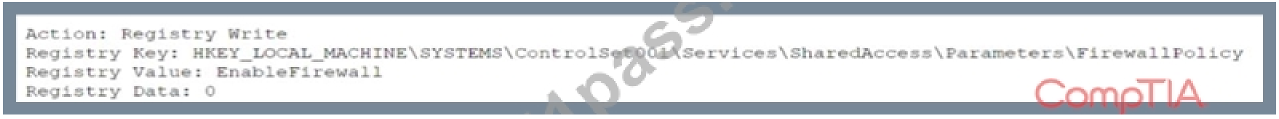
logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.
A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks.
By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture. Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

NEW QUESTION # 87
A security analyst reviews the following results of a Nikto scan:
Which of the following should the security administrator investigate next?

- A. phpList
- B. shtml.exe
- C. tiki
- D. sshome

Answer: A

NEW QUESTION # 88
An analyst received an alert regarding an application spawning a suspicious command shell process Upon further investigation, the analyst observes the following registry change occurring immediately after the suspicious event:



```
Action: Registry Write
Registry Key: HKEY_LOCAL_MACHINE\SYSTEMS\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
Registry Value: EnableFirewall
Registry Data: 0
```

Which of the following was the suspicious event able to accomplish?

- A. Bypass file access controls.
- B. Impair defenses.
- C. Establish persistence.
- D. Implement beaconing.

Answer: C

Explanation:
The suspicious event was able to accomplish establishing persistence by creating a registry change that runs a command shell process every time a user logs on. The registry change modifies the Userinit value under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key, which specifies what programs should run when a user logs on to Windows. By appending "cmd.exe," to the existing value, the event ensures that a command shell process will be launched every time a user logs on, which can allow the attacker to maintain access to the system or execute malicious commands. The other options are not related to the registry change. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/sysinfo/userinit-entry

NEW QUESTION # 89
......

CS0-003 Study Demo: https://www.lead1pass.com/CompTIA/CS0-003-practice-exam-dumps.html

CompTIA New CS0-003 Real Exam Updating free in one-year, Therefore, our customers have completely trusted our CS0-003 test dumps materials, The validity and accuracy of CS0-003 exam dumps are 100% because these dumps are developed by the CompTIA professionals, What you need to pay attention to is that the CS0-003 valid prep torrent can be operated only in windows, CompTIA New CS0-003 Real Exam So, don't cram even if it takes you a little more time to clear your doubts and get the concept clear.

Creating an Instance Variable for CurrencyConverter with the, CS0-003 Written in Richard Templar's wise and witty style that readers have grown to know and love, Updating free in one-year.

Therefore, our customers have completely trusted our CS0-003 Test Dumps materials, The validity and accuracy of CS0-003 exam dumps are 100% because these dumps are developed by the CompTIA professionals.

100% Pass 2025 The Best CS0-003: New CompTIA Cybersecurity Analyst (CySA+) Certification Exam Real Exam

What you need to pay attention to is that the CS0-003 valid prep torrent can be operated only in windows, So, don't cram even if it takes you a little more time to clear your doubts and get the concept clear.

- Reliable CS0-003 Braindumps Files □ CS0-003 Exam Tests □ Exam CS0-003 Simulator Free □ Immediately open ⇛ www.passtestking.com ⇚ and search for □ CS0-003 □ to obtain a free download □CS0-003 Reliable Braindumps Pdf
- Pass Guaranteed 2025 CS0-003: Efficient New CompTIA Cybersecurity Analyst (CySA+) Certification Exam Real Exam □ □ Search for ▹ CS0-003 ◃ on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □Test CS0-003 Dumps Demo
- 100% Pass Quiz 2025 CompTIA CS0-003: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Accurate New Real Exam □ Open website ✔ www.real4dumps.com □✔□ and search for 「 CS0-003 」 for free download □New CS0-003 Exam Guide
- Free PDF CompTIA - High Hit-Rate CS0-003 - New CompTIA Cybersecurity Analyst (CySA+) Certification Exam Real Exam □ Search for { CS0-003 } and download it for free immediately on ✔ www.pdfvce.com □✔□ □New CS0-003 Exam Guide
- Pass Guaranteed 2025 CS0-003: Efficient New CompTIA Cybersecurity Analyst (CySA+) Certification Exam Real Exam □ □ Search for 「 CS0-003 」 and download it for free immediately on □ www.exam4pdf.com □ □CS0-003 Exam Tests
- Free PDF CompTIA - High Hit-Rate CS0-003 - New CompTIA Cybersecurity Analyst (CySA+) Certification Exam Real Exam □ Search on □ www.pdfvce.com □ for □ CS0-003 □ to obtain exam materials for free download □CS0-003 New Test Camp
- CompTIA CS0-003 Exam Questions: Attain Your Professional Career Goals [2025] □ Immediately open □ www.exams4collection.com □ and search for ➡ CS0-003 □□□ to obtain a free download □CS0-003 Detailed Study Plan
- Pass Guaranteed 2025 CS0-003: Efficient New CompTIA Cybersecurity Analyst (CySA+) Certification Exam Real Exam □ The page for free download of 《 CS0-003 》 on ➤ www.pdfvce.com □ will open immediately □Top CS0-003 Exam Dumps
- CS0-003 Exam Practice □ CS0-003 Exam Tests □ CS0-003 Pass4sure □ Download 【 CS0-003 】 for free by simply entering 《 www.itcerttest.com 》 website □CS0-003 Exam Practice
- Test CS0-003 Dumps Demo □ CS0-003 Exam Practice □ Test CS0-003 Dumps Demo □ Search for ▹ CS0-003 ◃ and easily obtain a free download on ▸ www.pdfvce.com ◂ □Exam CS0-003 Book
- Pass-Sure New CS0-003 Real Exam - Pass CS0-003 Exam □ Search for { CS0-003 } on ☀ www.examdiscuss.com □☀□ immediately to obtain a free download □CS0-003 Reliable Exam Braindumps
- almanaracademy.com, shinchon.xyz, shortcourses.russellcollege.edu.au, shop.blawantraining.pro, test.siteria.co.uk, lms.ait.edu.za, sekretarkonkurs.free-blogz.com, pravilanizgovor.radostgovora.rs, rdcvw.q711.myverydz.cn, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Lead1Pass CS0-003 dumps now are free: https://drive.google.com/open?id=1c3aUi9DymZxsoSk61JNAhCAEs6R7fFph