Pass Guaranteed 2026 CS0-003: CompTIA Cybersecurity Analyst (CySA+) Certification Exam–Professional Exam Training

BONUS!!! Download part of TroytecDumps CS0-003 dumps for free: https://drive.google.com/open?id=1laKFtms8S4QwlJQnnZBqhp6Rk8_nAcKz

Your life will take place great changes after obtaining the CS0-003 certificate. Many companies like to employ versatile and comprehensive talents. What you have learnt on our CS0-003 study materials will meet their requirements. So you will finally stand out from a group of candidates and get the desirable job. Also, learning our CS0-003 Study Materials will fulfill your dreams. Nothing will stop you as long as you are rich. Also, respect and power is gained through knowledge and skills. If you want to get a higher position in the company, you must have the ability to defeat other excellent colleagues.

Earning the CompTIA CySA+ certification demonstrates to employers that an individual has the knowledge and skills required to analyze and respond to security threats in a fast-paced and constantly evolving cybersecurity landscape. CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification is recognized globally and can help individuals stand out in a competitive job market. In addition, the certification is a prerequisite for several advanced cybersecurity certifications, such as the CompTIA Advanced Security Practitioner (CASP+) and the Certified Information Systems Security Professional (CISSP) certifications.

>> CS0-003 Exam Training <<

CS0-003 Frequent Updates, Pass CS0-003 Rate

It is certain that the pass rate among our customers is the most essential criteria to check out whether our CS0-003 training materials are effective or not. The good news is that according to statistics, under the help of our CS0-003 training materials, the pass rate among our customers has reached as high as 98% to 100%. Our training materials have been honored as the panacea for the candidates for the exam since all of the contents in the CS0-003 Guide materials are the essences of the exam. Consequently, with the help of our study materials, you can be confident that you will pass the exam and get the related certification easily. So what are you waiting for? Just take immediate actions!

The CompTIA Cybersecurity Analyst (CySA+) Certification Exam certification exam is designed to test a candidate's ability to perform cybersecurity analysis and respond to threats. It is a comprehensive exam that evaluates a candidate's knowledge of

cybersecurity concepts, tools, and techniques. CS0-003 exam is composed of multiple-choice questions and performance-based questions. CS0-003 exam is computer-based and can be taken at any Pearson VUE testing center.

The CS0-003 Exam is designed to test the candidate's ability to identify and analyze cybersecurity threats, assess the impact of those threats, and implement effective strategies to mitigate them. CS0-003 exam covers a wide range of topics including threat management, vulnerability management, incident response, security architecture and toolsets. It is a comprehensive exam that requires a thorough understanding of cybersecurity principles and practices.

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Sample Questions (Q111-Q116):

NEW QUESTION # 111
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

- A. File carving
- B. Metadata analysis
- C. Data recovery
- D. Header analysis

Answer: A

NEW QUESTION # 112
An analyst views the following log entries:

```
202.180.158.22   - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5     - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221    - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5     - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5     - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5     - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5      - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5     - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```


The organization has a partner vendor with hosts in the 216.122.5.x range. This partner vendor is required to have access to monthly reports and is the only external vendor with authorized access. The organization prioritizes incident investigation according to the following hierarchy: unauthorized data disclosure is more critical than denial of service attempts.
which are more important than ensuring vendor data access.
Based on the log files and the organization's priorities, which of the following hosts warrants additional investigation?

- A. 134.17.188.5
- B. 202.180.1582
- C. 216.122.5.5
- D. 121.19.30.221

Answer: D

Explanation:
The correct answer is A. 121.19.30.221.
Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.
The log files show the following information:
* The IP addresses of the hosts that accessed the web server
* The date and time of the access
* The file path of the requested resource
* The number of bytes transferred
The organization's priorities are:
* Unauthorized data disclosure is more critical than denial of service attempts
* Denial of service attempts are more important than ensuring vendor data access According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so123. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.
The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two

hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.
The other hosts do not warrant additional investigation based on the log files and the organization's priorities.
Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests45. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.
Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.
Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements.
Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

NEW QUESTION # 113
A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:

Which of the following vulnerabilities Is the security analyst trying to validate?

- A. LFI
- B. CSRF
- C. SQL injection
- D. XSS

Answer: A

Explanation:
The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the "/.../.../.../" in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.
Reference:
According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of Burp Suite, a tool used for testing web application security, in chapter 6. Specifically, it explains the meaning and function of each component in Burp Suite, such as Repeater, which allows the security analyst to modify and resend individual requests1, page 239. Therefore, this is a reliable source to verify the answer to the question.

NEW QUESTION # 114
SIMULATION

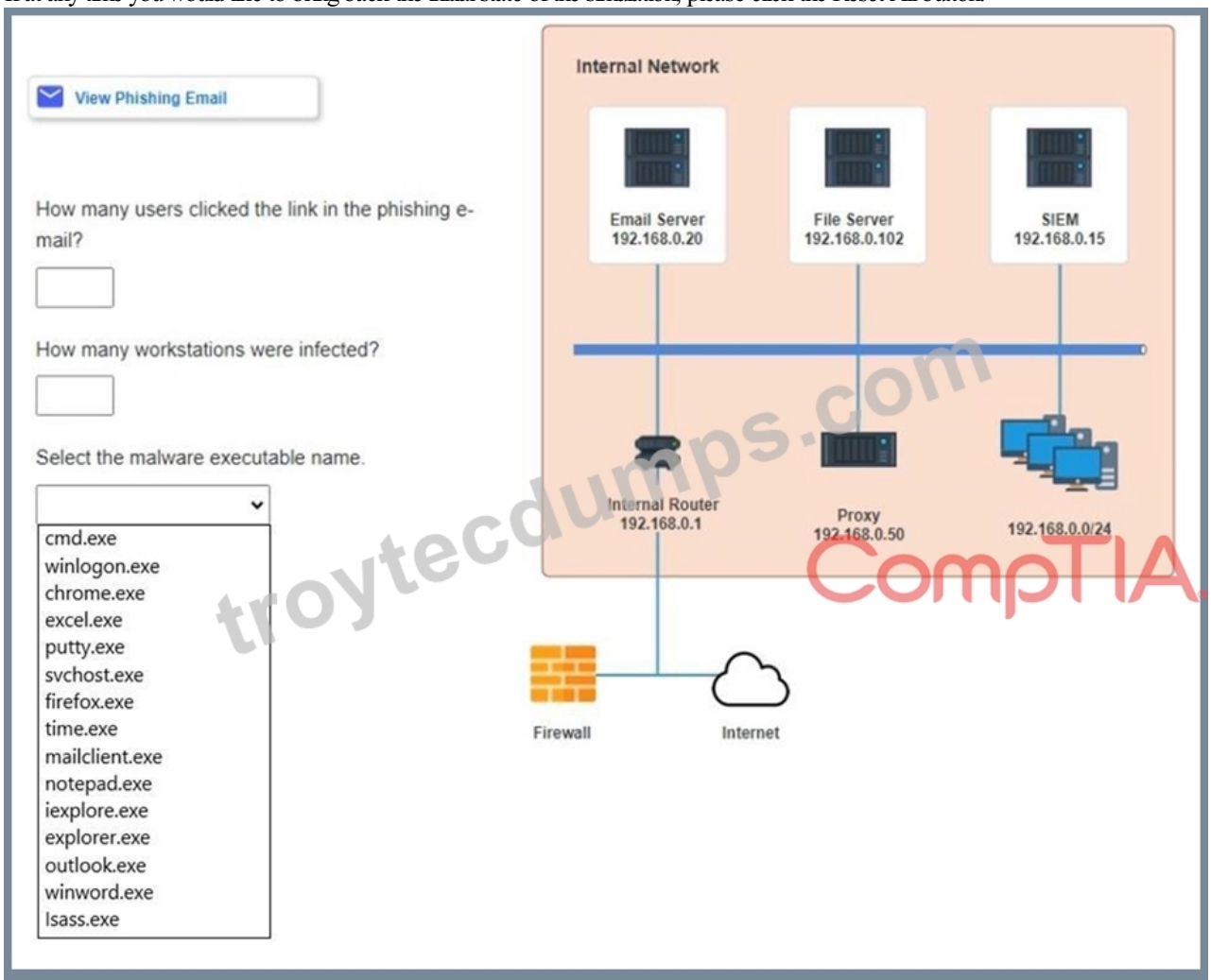
Approximately 100 employees at your company have received a phishing email. As a security analyst, you have been tasked with handling this situation.

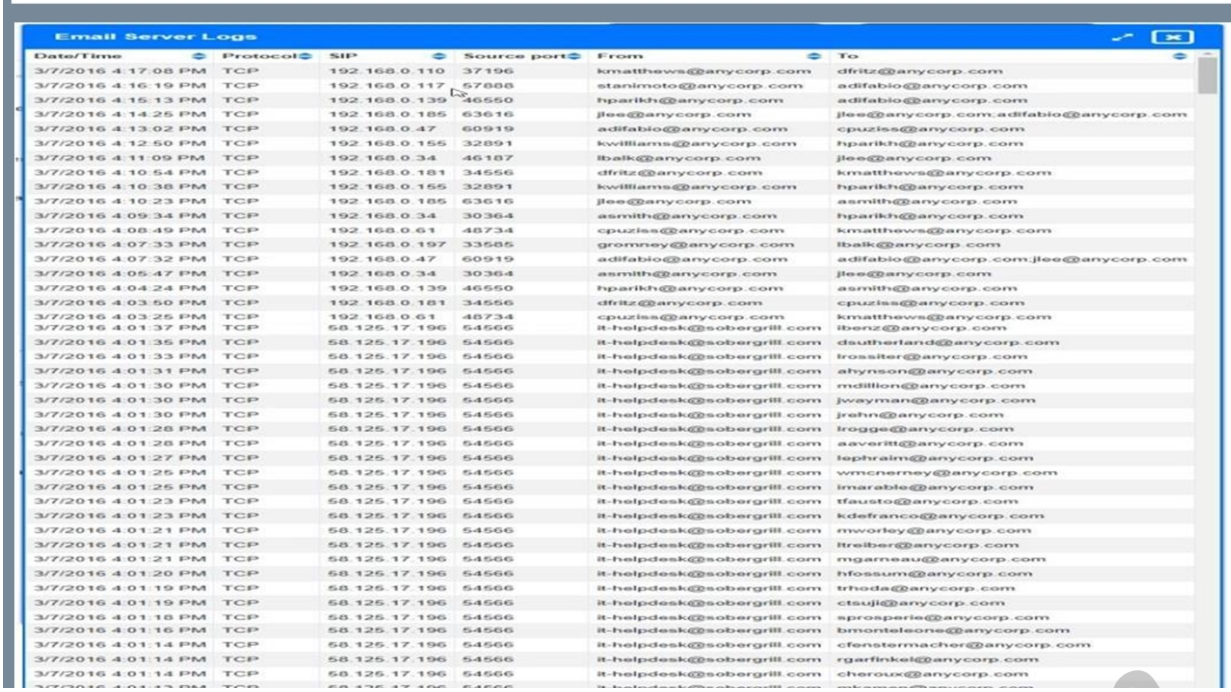
INSTRUCTIONS

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?

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Date/Time	Protocol	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	zdodgen@anycorp.com		
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhammonds@anycorp.com		
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	onorth@anycorp.com		
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mroanes@anycorp.com		
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kbowling@anycorp.com		
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nrachal@anycorp.com		
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jdegenhardt@anycorp.com		
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wracette@anycorp.com		
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lhammond@anycorp.com		
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dmilazzo@anycorp.com		
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kneubauer@anycorp.com		
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bboyko@anycorp.com		
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dcrofoot@anycorp.com		
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmemmott@anycorp.com		
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	chodgin@anycorp.com		
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aholler@anycorp.com		
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	abattaglia@anycorp.com		
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	halberti@anycorp.com		
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	myeoman@anycorp.com		
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wbobadilla@anycorp.com		
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lkam@anycorp.com		
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jcooks@anycorp.com		
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpolice@anycorp.com		
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mwagener@anycorp.com		
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com		
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com		
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dstivers@anycorp.com		
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	msistrunk@anycorp.com		
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com		
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com		
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com		
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com		
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com		
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com		
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenware@anycorp.com		
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgalipeau@anycorp.com		
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com		
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com		
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com		
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com		
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com		
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckrooker@anycorp.com		
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com		
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuziss@anycorp.com		
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com		
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com		
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com		
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com		
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morwig@anycorp.com		
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com		
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com		
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com		
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com		
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com		
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrains@anycorp.com		
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nnavarro@anycorp.com		
3/7/2016 4:00:08 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbalk@anycorp.com		
3/7/2016 4:00:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgulyas@anycorp.com		
3/7/2016 4:00:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	praso@anycorp.com		
3/7/2016 4:00:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tspiegel@anycorp.com		
3/7/2016 4:00:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rbettencourt@anycorp.com		
3/7/2016 4:00:02 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	asmith@anycorp.com		
3/7/2016 4:00:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mleeds@anycorp.com		
3/7/2016 4:00:00 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kpolasek@anycorp.com		
3/7/2016 4:00:00 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com		
3/7/2016 3:59:11 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com		
3/7/2016 3:57:58 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com		
3/7/2016 3:56:04 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com		
3/7/2016 3:54:28 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com		
3/7/2016 3:52:59 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com		
3/7/2016 3:52:15 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com		
3/7/2016 3:50:39 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com		
3/7/2016 3:49:07 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com		
3/7/2016 3:48:40 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com		
3/7/2016 3:48:35 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com;jlee@anycorp.com		
3/7/2016 3:47:27 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com		
3/7/2016 3:46:06 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com		
3/7/2016 3:46:05 PM	TCP	192.168.0.60	31498	dfritz@anycorp.com	cpuziss@anycorp.com		
3/7/2016 3:44:45 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com		
3/7/2016 3:44:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com		
3/7/2016 3:43:36 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com		
3/7/2016 3:41:56 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com		
3/7/2016 3:41:43 PM	TCP	192.168.0.139	53876	hparikh@anycorp.com	adifabio@anycorp.com		
3/7/2016 3:40:50 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com		
3/7/2016 3:39:13 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com		
3/7/2016 3:38:44 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com		
3/7/2016 3:38:22 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com		
3/7/2016 3:38:00 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com		
3/7/2016 3:36:24 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com		
3/7/2016 3:35:03 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@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	35.132.243.120	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

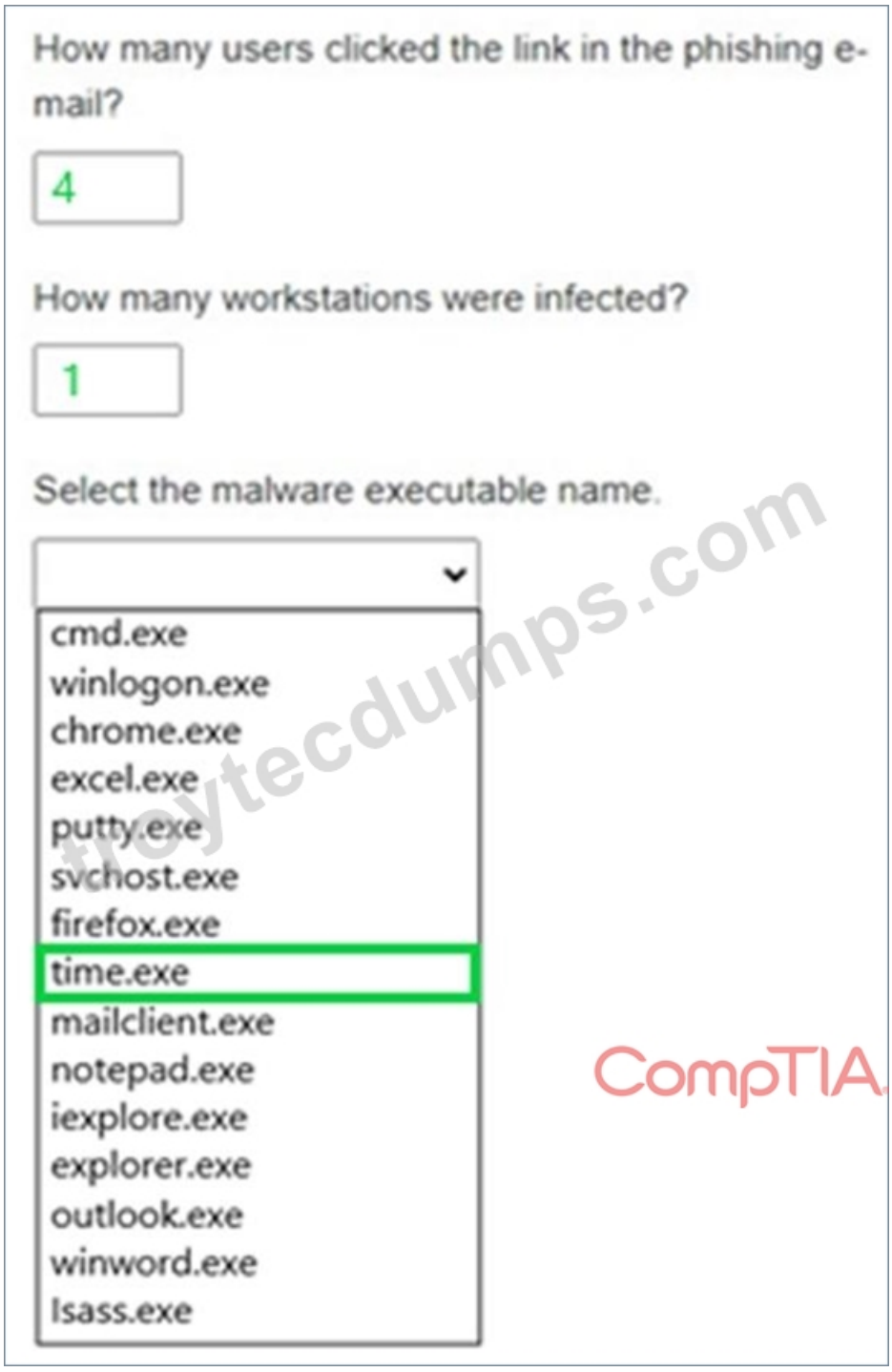
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55947	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.190.57.150	80	freefood.com	POST
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET
3/7/2016 3:57:59 PM	192.168.0.59	33145	209.240.152.67	80	bestpurchase.com	GET
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.83.170.116	80	goodguys.se	POST
3/7/2016 3:55:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET
3/7/2016 3:54:31 PM	192.168.0.152	30520	141.217.181.243	80	goodguys.se	POST
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.201.191	80	pastebucket.cn	POST
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.192	80	funweb.cn	POST
3/7/2016 3:49:54 PM	192.168.0.126	40815	171.140.162.96	80	stopthebotnet.com	GET
3/7/2016 3:49:07 PM	192.168.0.9	47625	18.23.47.44	80	stopthebotnet.com	GET
3/7/2016 3:47:38 PM	192.168.0.131	44579	139.58.55.91	80	funweb.cn	GET
3/7/2016 3:45:58 PM	192.168.0.186	62683	31.133.137.225	80	chatforfree.ru	POST
3/7/2016 3:44:05 PM	192.168.0.181	38937	150.119.71.249	80	anti-malware.com	GET
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:35:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:35:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	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 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe
Audit Success	3/7/2016 4:10:46 PM	4688	Process Creation	A new process has been created.	192.168.0.9	lbalk	907	mailclient.exe
Audit Success	3/7/2016 4:10:42 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	520	iexplore.exe
Audit Success	3/7/2016 4:10:01 PM	4689	Process Termination	A process has exited.	192.168.0.70	cpuziss	392	chrome.exe
Audit Success	3/7/2016 4:13:02 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	724	svchost.exe
Audit Success	3/7/2016 4:11:03 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	1398	putty.exe
Audit Success	3/7/2016 4:09:23 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	410	lsass.exe
Audit Success	3/7/2016 4:09:15 PM	4688	Process Creation	A new process has been created.	192.168.0.24	jlee	1566	mailclient.exe
Audit Success	3/7/2016 4:07:37 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	864	lsass.exe
Audit Success	3/7/2016 4:10:27 PM	4688	Process Creation	A new process has been created.	192.168.0.141	dfritz	895	explorer.exe
Audit Success	3/7/2016 4:10:23 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	87	svchost.exe
Audit Success	3/7/2016 4:09:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.82	gromney	162	lsass.exe
Audit Success	3/7/2016 4:08:08 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	638	lsass.exe
Audit Success	3/7/2016 4:06:51 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	886	lsass.exe
Audit Success	3/7/2016 4:06:26 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	127	lsass.exe
Audit Success	3/7/2016 4:05:46 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	847	lsass.exe
Audit Success	3/7/2016 4:04:24 PM	4624	Logon	An account was successfully logged on.	192.168.0.82	gromney	718	lsass.exe
Audit Success	3/7/2016 4:02:47 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	730	firefox.exe
Audit Success	3/7/2016 4:02:04 PM	4688	Process Creation	A new process has been created.	192.168.0.132	asmith	127	mailclient.exe
Audit Success	3/7/2016 4:00:26 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	1481	time.exe
Audit Success	3/7/2016 3:58:43 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	645	svchost.exe
Audit Success	3/7/2016 3:58:40 PM	4688	Process Creation	A new process has been created.	192.168.0.141	dfritz	1992	outlook.exe
Audit Success	3/7/2016 3:57:15 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	654	lsass.exe
Audit Success	3/7/2016 3:56:13 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	1323	lsass.exe
Audit Success	3/7/2016 3:55:04 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	1034	lsass.exe

Answer:

Explanation:



NEW QUESTION # 115
An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:
* created the initial evidence log.
* disabled the wireless adapter on the device.
* interviewed the employee, who was unable to identify the website that was accessed
* reviewed the web proxy traffic logs.
Which of the following should the analyst do to remediate the infected device?

- A. Delete the user profile and restore data from backup.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Update the system firmware and reimage the hardware.

Answer: D

Explanation:
Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

NEW QUESTION # 116
.....