Name: **Enrolment No:**	**UPES**

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

Program: B. Tech CSE+CSF   **Semester: II**
Course: IT System Security and Physical Security   **Code: CSSF 1001**
Time: 2 hours
Max. Marks: 100

Instructions:
1. End semester exam has 60 multiple choice questions, all are mandatory.
2. Exam time limit is 2 hours.
3. There is no negative marking.

UPES

Akashdeep Bhardwaj **48**

My Institution   Courses   Community

Edit Mode is: ● **ON**   **?**

🏠   Tests, Surveys and Pools   Tests   **Test Canvas : Exam: End Semester**

Test Canvas: Exam: End Semester

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	**End Semester Exam**
Instructions	Instructions: 1. End semester exam has 60 multiple choice questions, all are mandatory. 2. Exam time limit is 2 hours. 3. There is no negative marking.
Total Questions	60
Total Points	100
Number of Attempts	103

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

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

☐

1. Multiple Choice: An evil twin attack is described as: Points: **2**

Question	An evil twin attack is described as:
Answer	The impersonation of a senior staff member s email address
	The use of an alternate DHCP server on the corporate LAN
	The interception of DNS requests to provide an alternate response
	✅ The impersonation of a wireless network to attract authentication requests

← **OK**

Points: **1**

☐ **2. Multiple Choice: Which if these is not a type of Phish...**

Question	Which if these is not a type of Phishing Attack?
Answer	Spear Phishing
	✅ Arrow Phishing
	Deceptive Phishing
	CEO Fraud

Points: **1**

☐ **3. Multiple Choice: Which of the following passwords is a...**

Question	Which of the following passwords is a good password to use?
Answer	@#$)*&^%
	akHGksmLN
	✅ UcSc4Evr!
	Password1

Points: **2**

☐ **4. Multiple Choice: Tasks associated with maintaining the...**

Question	Tasks associated with maintaining the user access and requests are known as
Answer	Authorization
	Authentication
	✅ Administration
	Audit

Points: **2**

☐ **5. Multiple Choice: If you wanted to require that a user ...**

Question	If you wanted to require that a user enter an Administrator password to perform administrative tasks, what type of user account should you create for the user?

Answer   Administrator User account

🟢   Standard User account

Power User account

Authenticated User account

☐ **6. Multiple Choice: Which of the following is not a facto...**   Points: **1**

Question	Which of the following is not a factor in securing the environment against an attack on security?
Answer	The level of access provided to employees
	The network architecture
🟢	The business strategy of the company
	The system configuration

☐ **7. Multiple Choice: To hide information inside a picture,...**   Points: **2**

Question	To hide information inside a picture, what technology is used
Answer	Rootkits
	Bitmapping
	Image Rendering
🟢	Steganography

☐

Points: **2**

8. Multiple Choice: Which phase of hacking performs actua...

Question	Which phase of hacking performs actual attack on a network or system?
Answer	Reconnaissance
	Footprinting
	Maintaining Access

Gaining Access ✓

Points: **2**

☐ 9. Multiple Choice: Is there any way to detect malware th...

Question	Is there any way to detect malware that hasn't executed once it's passed through the perimeter and is already resident on the device?
Answer	✓ Yes
	No
	Maybe
	Not possible at all

Points: **1**

☐ 10. Multiple Choice: Which one of the following would resu...

Question	Which one of the following would result in the loss of contact details if it were stolen?
Answer	✓ Mobile Phone
	Landline Phone
	Modem
	USB drive with backup

Points: **2**

☐ 11. Multiple Choice: Which of the following is most likely...

Question	Which of the following is most likely a hoax?
Answer	An email from a friend you have not seen recently
	An email with an attachment sent by a colleague using their personal email address
	✓ An email asking you to go to a website for free computer scan
	An email advertisement from a local shop you subscribe to

☐ **12. Multiple Choice: Which of the following is a SPAM?**

<div align="right">Points: **1**</div>

Question	Which of the following is a SPAM?
Answer	Gathering information about a person or organization without their knowledge
	Performing unauthorized, malicious actions like deleting files
	Putting unnecessary load on network by running multiple PING commands
	✅ Sending unwanted bulk emails

☐ **13. Multiple Choice: Which phase of hacking performs actua...**

<div align="right">Points: **1**</div>

Question	Which phase of hacking performs actual attack on a network or system?
Answer	✅ Gaining Access
	Reconnaissance
	Maintaining Access
	Scanning

☐ **14. Multiple Choice: Why would a ping sweep be used?**

<div align="right">Points: **2**</div>

Question	Why would a ping sweep be used?
Answer	Locate dead systems
	Identify open ports
	Locate firewalls
	✅ Identify live systems

☐ **15. Multiple Choice: Process of verifying the identity of ...**

<div align="right">Points: **2**</div>

Question	Process of verifying the identity of the user requesting the access is
Answer	Authorization

Authentication

Administration

Audit

Points: **2**

☐ **16. Multiple Choice: Intention to inflict pain, injury, da...**

Question	Intention to inflict pain, injury, damage, or other hostile action is know as
Answer	Asset
	Employee
	Vulnerability
	✅ Threat

Points: **2**

☐ **17. Multiple Choice: Situation when a program misbehaves o...**

Question	Situation when a program misbehaves only when certain conditions are met, otherwise it works like a genuine program is know as
Answer	Virus
	Worm
	Trojan
	✅ Logic Bomb

Points: **1**

☐ **18. Multiple Choice: Program installed on user system that...**

Question	Program installed on user system that obtains information in covert manner is know as
Answer	Virus
	✅ Spyware
	Malware

Rootkit

□ 19. Multiple Choice: Program has security holes in its cod...

Points: **2**

Question	Program has security holes in its code to perform illegal action or bypass security without knowledge of user is known as
Answer	✅ Trap Door
	Main Door
	Side Door
	Open Door

□ 20. Multiple Choice: What is the primary reason that organ...

Points: **2**

Question	What is the primary reason that organizations continue to use endpoint protection suites?
Answer	✅ Virus Blocking Effectiveness
	Low cost
	Ability to stop an APT
	Compliance Mandate

□ 21. Multiple Choice: Why do traditional malware detection ...

Points: **2**

Question	Why do traditional malware detection techniques have trouble with advanced malware?
Answer	Attack kits available on the Internet
	✅ Polymorphic malware
	Cloud-based signature repositories
	Command and control network traffic

□ **22. Multiple Choice: Why did host intrusion prevention (HI...**

Points: **2**

Question	Why did host intrusion prevention (HIPS) technology achieve limited adoption for endpoint security?
Answer	✓ Too many false positives
	Missed attacks
	Too hard to manage
	High cost

□ **23. Multiple Choice: If you choose not to trust all of you...**

Points: **2**

Question	If you choose not to trust all of your endpoints (assume compromised), which of these controls would not help you ensure your data is not exfiltrated?
Answer	Highly segmented network
	✓ Network-based sandbox device on perimeter
	Vulnerability Scanning
	Network Packet Capture

□ **24. Multiple Choice: When Auto-Protect is enabled, protect...**

Points: **2**

Question	When Auto-Protect is enabled, protection is optional for which type of file access?
Answer	access
	modify
	✓ backup
	restore

□ **25. Multiple Choice: Activities performed to satisfy compl...**

Points: **2**

Question	Activities performed to satisfy compliance and check if rules, best practices and standards being followed is...
Answer	Authorization
	Authentication
	Administration
	✅ Audit

Points: **2**

26. Multiple Choice: Process which can choke (clog) system...

Question	Process which can choke (clog) system performance by using system resources to extreme levels are known as
Answer	Memory Hoggers
	✅ Worm
	Trojan
	Virus

Points: **2**

□ 27. Multiple Choice: Process to provide appropriate level ...

Question	Process to provide appropriate level of access to the authenticated user is
Answer	✅ Authorization
	Authentication
	Administration
	Audit

Points: **1**

□ 28. Multiple Choice: Which of the following is not a typic...

Question	Which of the following is not a typical characteristic of an ethical hacker?

Answer	✅	Has highest level of security for the organization
		Excellent knowledge of Windows
		Understands the process of exploiting network vulnerabilities
		Patience, persistence and perseverance

Points: **2**

☐
29. Multiple Choice: Which one of the following should you...

Question	Which one of the following should you do to ensure that your USB storage device is kept safe and secure?
Answer	Only use it in private surroundings
	Do not access it using a Bluetooth device
	Use firewall software
	✅ Never leave it unattended

☐ **30. Multiple Choice: Which one of the following describes ...**

Points: **1**

Question	Which one of the following describes why you should follow guidelines and procedures while using IT resources in an organization?
Answer	To ensure easy access to information on your computer.
	✅ To ensure the secure use of IT resources.
	To ensure the secure use of IT resources.
	To ensure the secure use of IT resources.

☐ **31. Multiple Choice: Which one of the following describes ...**

Points: **1**

Question	Which one of the following describes why users should lock their computer when leaving their desk?
Answer	✅ To prevent unauthorized access to data

To prevent waste of electricity

To prevent data from getting corrupted

To prevent computer from malfunctioning

---

32. Multiple Choice: Which one of the following describes ...

Points: **1**

Question	Which one of the following describes how to find out about an organization's IT Security policy?
Answer	By reading the office newsletter
	✅ By reading the organization's policy manual
	By speaking to the IT Asset Manager
	By speaking to the Technical Support Head

---

33. Multiple Choice: Which one of the following could be t...

Points: **1**

Question	Which one of the following could be the unexpected outcome of deleting a large group of files?
Answer	The files would be hidden
	✅ Any important file may be accidently deleted
	The files would become read only
	A delete file confirmation window will appear

---

34. Multiple Choice: Which one of the following is the rec...

Points: **2**

Question	Which one of the following is the recommended action to prevent the risk of access to a network by other users?
Answer	Disconnect the computer from the network
	Complain to the IT Helpdesk
	✅ Change the default WEP or WPA access key

Adjust the Internet Security settings to HIGH

☐ **35. Multiple Choice: Which one of the following describes ...**   Points: **1**

Question	Which one of the following describes what you should do if you receive a chain letter email?
Answer	Forward the email
	Download it onto your system
	✅ Delete that email
	Send a read receipt

☐ **36. Multiple Choice: Which one of the following describes ...**   Points: **2**

Question	Which one of the following describes why it is important to have a secure off-site backup copy of files?
Answer	To improve accessibility of files from other locations
	To speed up the process of accessing files anytime
	✅ To prevent loss of data in event of fire
	To reduce possibility of data theft

☐
Points: **2**

37. Multiple Choice: Which of the following is NOT a commo...

Question	Which of the following is NOT a common challenge with vulnerability scanning?
Answer	Vulnerability scans often generate large amounts of traffic.
	Vulnerability scan report often have false positives.
	✓ Vulnerability scans can notify external parties to system weaknesses.
	Vulnerability scanners are often blamed for system outage if run during business hours.

38. Multiple Choice: A webshell can be described as:

Points: **2**

Question	A webshell can be described as:
Answer	✓ A script that facilitates commands on a compromised web server
	A command injection attack on a web application
	An alternate shell program on a Unix command line written in HTML
	A shell command hidden in a JSON file

39. Multiple Choice: Why must any final security report be...

Points: **2**

Question	Why must any final security report be encrypted when delivered?
Answer	To ensure that the report is not altered
	To ensure that the customer does not share the report with competing penetration testers
	✓ To ensure that customer sensitive information is protected in transit
	To comply with penetration test audit compliance

40. Multiple Choice: In which section are details of the r...

Points: **2**

Question	In which section are details of the risk related to vulnerabilities included?
Answer	Method overview
	✓ Summary of findings

	Method
	Conclusion

☐ **41. Multiple Choice: The first phase of hacking an IT Syst...**

Points: **2**

Question	The first phase of hacking an IT System is Compromise of which foundation of Security?
Answer	Availability
	Integrity
	Authentication
✅	Confidentiality

☐ **42. Multiple Choice: A friend sends an electronic Hallmark...**

Points: **2**

Question	A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card. What should you do?
Answer	Reply back with another Hallmark greeting card
	Reply back with a polite 'Thank you'
✅	Delete the email
	Ignore your friend

☐ **43. Multiple Choice: We saw a case a while back where some...**

Points: **2**

Question	We saw a case a while back where someone used their yahoo account at a computer lab on campus. She made sure her yahoo account was no longer open in the browser window before leaving the lab. Someone came in behind her and used the same browser to re-access her account. They started sending emails from it and caused all sorts of mayhem. What do you think might be going on here?
Answer	Brute Force Attack

The first person didn't log out of her account, so the new person could just go to history and access her account.

✅ She did log out, but didn t clear her web cache.

Denial of Service Attack

Points: **1**

☐ **44. Multiple Choice: Which of the following is primarily a...**

Question	Which of the following is primarily a confidentiality concern?
Answer	✅ Eavesdropping
	Impersonation
	Destruction
	Altering

Points: **1**

☐ **45. Multiple Choice: Which of the following BEST describes...**

Question	Which of the following BEST describes the practice of providing user credentials when logging onto the network?
Answer	Output
	Storage
	✅ Input
	Processing

Points: **1**

☐ **46. Multiple Choice: Which of the following BEST describes...**

Question	Which of the following BEST describes an application running on a typical operating system?
Answer	✅ Process
	Thread

Function

Task

Points: **2**

47. Multiple Choice: A user is getting an error message wh...

Question	A user is getting an error message when trying to go to a website. A technician asks the user a few questions to find out more about the issue. The technician opens a browser locally and browses to the same site as the user. Which of the following troubleshooting steps is the technician using by browsing to the same site?
Answer	Establish plan of action
	Gather information
	✅ Duplicate the problem
	Find the root cause

Points: **2**

48. ☐ Multiple Choice: A user is buying a laptop. The user w...

Question	A user is buying a laptop. The user will have a lot of personal and confidential information on the laptop. The user wants to ensure data cannot be accessed by anyone, even if the laptop is stolen. Which of the following should be set up to accomplish this?
Answer	Permissions
	Decryption
	Auditing
	✅ Encryption

Points: **2**

49. Multiple Choice: Your supervisor is very busy and asks...

Question	Your supervisor is very busy and asks you to log into the HR Server using her user-ID and password to retrieve some reports. What should you do?
Answer	Ask the Supervisor to send the request in email/writing and then and finish request

It s your boss, so it s okay to do this.

Ignore the request and hope she forgets.

✅ Decline the request and remind your supervisor that it is against the security policy

☐ **50. Multiple Choice: One of your friend subscribes to a nu...**

Points: **2**

Question	One of your friend subscribes to a number of free IT magazines. Among the questions she was asked in order to activate her subscriptions, one magazine asked for her month of birth, a second asked for her year of birth, and a third asked for her mother's maiden name. What do you think might be going on here?
Answer	Trackback Spamming
	Email Spamming
	Comment Spamming
	✅ Phishing

☐ **51. Multiple Choice: The mouse on your office computer scr...**

Points: **2**

Question	The mouse on your office computer screen starts to move around on its own and click on things on your desktop. What do you do?
Answer	Call your co-workers over so they can see
	✅ Disconnect your computer from the network & Call IT/Tell your supervisor
	Unplug your mouse and Run anti-virus
	Turn your computer off

☐ **52. Multiple Choice: Physical Security does not manages an...**

Points: **2**

Question	Physical Security does not manages and protects assets in form of

Answer		Administrative Security Control
		Technical Security Control
		Process Security Control ✅
		Physical Security Control

☐ **53. Multiple Choice: Which is not an example of Technical ...**

Question	Which is not an example of Technical Control?
Answer	Access Control Systems
	Auditing Systems
	Intrusion Detection Systems
	Taking Manual Attendance ✅

☐ **54. Multiple Choice: Which is not an example of Administra...**

Question	Which is not an example of Administrative Control?
Answer	Site Location
	Facility Design
	Building Construction
	Building Material ✅

☐ **55. Multiple Choice: Which of the following is not an exam...**

Question	Which of the following is not an example of Physical Control?
Answer	Proxy Server ✅
	Perimeter Security

Wiring & Fences

Locks & Guards

Points: **2**

56. Multiple Choice: Physical Security Threats do not incl...

Question	Physical Security Threats do not include threats due to
Answer	Natural Environment
	Supply Systems
✅	Cybersecurity & Internet
	Man Made

Points: **2**

57. Multiple Choice: Categories of Physical Security do NO...

Question	Categories of Physical Security do NOT include
Answer	Security in Layers
	Perception as Physical Security
	Technical Controls
✅	Non-Technical Controls

Points: **1**

58. Multiple Choice: Security in Layers has the following ...

Question	Security in Layers has the following layers
Answer	Locks and Keys
	Fences and Walls
✅	Outer and Inner

Technical and Non Technical

Points: **2**

59. Multiple Choice: Examples of Technical Controls are Ma...

Question	Examples of Technical Controls are Mantraps, Turnstiles, Biometrics, CCTV Surveillance
Answer	Only first two are correct
	Only second and third are correct
✅	All are correct
	Only first and third are correct

Points: **2**

60. Multiple Choice: Fire Extinguishers are A for Paper/Wo...

Question	Fire Extinguishers are A for Paper/Wood, B for Flammable Liquids, C for Electrical and D for Flammable Metals
Answer	Only first two are correct
	Only second and third are correct
✅	All are correct
	Only first and third are correct

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

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