





+ BASIC

CYBER



SECURITY Wan + + + + + + + + + + + + **OUR PROFESSIONAL**

CYBER ____SECURITY



1.	are tiny files which get downloaded to your system when you visit a website A) Cookies B) Caches	5.	is an anti-malware tool found in newer OS which is designed for protecting computers from viruses, spyware & other malware
2.	C) Bots D) Crawlers gets propagated through networks and technologies like SMS, Bluetooth, wireless medium, USBs and infrared to affect mobile phones	6.	A) Norton Antivirus B) Windows Defender C) Anti-malware D) Microsoft Security Essentials technique is also used in product advertisement
	A) Worms B) Antivirus C) Malware D) Multimedia files	الله الله الله	A) Phishing B) e-Banners C) Cookies D) Spamming is a network reliability
3.	are essential because they frequently comprise of critical patches to security holes.	Phy	A) The number of users B) The type of transmission medium
	A) System software B) Utility software C) Software executables D) Software updates	8.	C) The frequency of failure D) Unauthorized accessmonitors user activity on internet and transmit that
4.	is populating the inbox of any target victim with unsolicited or junk		information in the background to someone else A) Malware
	A) Phishing B) Spamming C) Hooking D) DoS		B) Spyware C) Adware D) None of these
		9.	"Cyberspace" was coined by





- A) Richard Stallman
- B) William Gibson
- C) Andrew Tannenbaum
- D) Scott Fahlman
- 10. A ______ is a method in which a computer security mechanism is bypassed untraceable for accessing the computer or its information
 - A) front-door
 - B) backdoor
 - C) clickjacking
 - D) key-logging
- 11. A ______ is a small malicious program that runs hidden on infected system.
 - A) Virus
 - B) Trojan
 - C) Shareware
 - D) Adware
- 12. A _______ is a process of breaking a password protected system or server by simply & automatically entering every word in a dictionary as a password
 - A) Dictionary attack
 - B) Phishing attack
 - C) Social engineering attack
 - D) MiTM attack
- 13. A company requires each employee to power off his

- computer at the end of the day. This rule was implemented to make the network
- A) perform better
- B) more reliable
- C) more secure
- D) more error-free

14. A digital signature is

- A) a bit string giving identity of a correspondent
- B) a unique identification of a sender
- C) an authentication of an electronic record by tying it uniquely to a key only a sender knows
- D) an encrypted signature of a sender

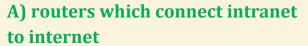
15. A Firewall is a

- A) wall built to prevent fires from damaging a corporate intranet
- B) security device deployed at the boundary of a company to prevent unauthorized physical access
- C) security device deployed at the boundary of a corporate intranet to protect it from unauthorized access
- D) device to prevent all accesses from the internet to the corporate intranet
- 16. A firewall may be implemented in









- B) bridges used in an intranet
- C) expensive modem
- D) user's application programs
- 17. A_____is illicitly introduced code that damages a network device
 - A) Protocol
 - **B) Virus**
 - C) Catastrophe
 - D) Medium
- 18. All of the following are examples of real security and privacy threats except
 - A) Hackers
 - B) Virus
 - C) Spam
 - D) Worm
- 19. Attackers could steal _____ to achieve illegitimate accessing to online accounts & disturbs the personal information
 - A) plug-ins
 - B) cache
 - C) cookies
 - D) history
- 20. BIOS is abbreviated as
 - A) Basic Input Output Server
 - B) Basic Internet Output Systems

- C) Basic Input Output System
- D) Battery-based Input Output System
- 21. Browser _____ are impermanent internet files which helps the browsers download web images, data & documents for rapid performance & viewing in the future
 - A) plug-ins
 - B) Cache
 - C) ad-on
 - D) history
- 22. Brute force attack is
 - A) fast
 - B) inefficient
 - C) slow
 - D) complex to understand
- 23. Certification of Digital signature by an independent authority is needed because
 - A) it is safe
 - B) it gives confidence to a business
 - C) the authority checks and assures customers that the public key indeed belongs to the business which claims ita ownership
 - D) private key claimed by a sender may not be actually his









- A) Bug
- **B)** Threat
- C) Vulnerability
- D) Attack

25. Conversion of Cypher text to plain text

- A) Encryption
- **B)** Decryption
- C) None of these answers
- D) Simple Text

26. EDI (Electronic Data Interchange) use

- A) required an extranet
- B) requires value added network
- C) can be done on internet
- D) requires a corporate intranet

27. For secure EDI(Electronic Data Interchang) transmission on internet

- A) MIME is used
- B) S/MIME is used
- C) PGP is used
- D) TCP/IP is used
- 28. Governments hired some highly skilled hackers for providing cyber security for the country or state.

 These types of hackers are termed as _____

- A) Nation / State sponsored hackers
- B) CIA triad
- C) Special Hackers
- D) Government Hackers
- 29. Identify the oldest phone hacking technique used by hackers to make free calls
 - A) Spamming
 - **B)** Phreaking
 - C) Cracking
 - D) Phishing
- 30. If you set up a BUS network, what is the major disadvantage?
 - A) It is entirely wireless and open to wifi-based attacks
 - B) It is daisy-chained together with several cables
 - C) It is linked with a single cable which can be a major vulnerability
 - D) It is connected in a star pattern and can be disabled by disrupting one data center
- 31. In ______ session hijacking, hackers gain session ID for taking control of existing session or even create a new unauthorized session
 - A) network level
 - B) physical level
 - C) application level
 - D) data level



CYBER ____SECURITY



as A)	Increase your security for social edia account by always syou step away from the system signing in logging out	C) using an algorithm to implement DES instead of using hardware D) designing DES with high securand not publicizing algorithm usit	rity
C)	signing up	36. Mobile Phone OS contains o	pen
D)	logging in	APIs that may be at	tack
33.	Many social media sites and	A) useful for	
se	ervices provide for	B) vulnerable to	
le	gitimate account verification	C) easy to	
4.7	Dating agains	D) meant for	
-	Retina scanning	27 Mobile constitute also know	o
_	2-step verification	37. Mobile security is also know	VII as
-	Fingerprint scanning		
נט) CAPTCHA	A) OS Security	
34.	Message can be sent more	B) Wireless security	
se	curely using DES by	C) Cloud security	
A)	Phishing Phishing	D) Database security	
B)	Cookies	38. Once activated can	
C)	e-Banners	enableto spy on the	
D)) Spamming	victim, steal their sensitive	
35.	Message can be sent more	information & gain backdoor	
	ecurely using DES by	access to the system.	
4.7	de la companie de la	A) virus, cyber-criminals	
	encrypting plain text by a different	B) malware, penetration testers	
randomly selected key for each transmission		C) trojans, cyber-criminals	
		D) virus, penetration testers	
_	encrypting plain text by a	20 Part of the social modic site	
	fferent random key for each	39. Part of the social media site	
m	essage transmission and sending	are the various games & 3rd p	arty

the key to the receiver using a

public key system

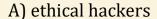
data

applications which helps

_ to get access to your







- B) penetration testers
- C) security auditors
- D) cyber-criminals

40. Password are used to improve the of a Network

- A) Performance
- B) Reliability
- C) Application Security
- D) All of the above

41. Possible threat to any information cannot be

- A) reduced
- B) transferred
- C) protected
- D) ignored

42. Saving passwords in the browser is a good habit

- A) True
- B) False
- C) nan
- D) nan

43.	Since most
0	ccur at the very beginning of the
T	CP session, this allows hackers to
σ	ain access to any system

- A) authentications
- B) breaches
- C) integrations
- D) associations

44. TCP is used for what three main functions

A) Connect to the Web, deliver email, and transfer files

- B) Connect to the Web, compress data, encrypt mail
- C) Connect to the Web, conceal data, transfer files
- D) Connect to the Web, encrypt data, transmit information

45. The full form of EDR is _____

- A) Endpoint Detection and recovery
- B) Early detection and response
- C) Endpoint Detection and response
- D) Endless Detection and Recovery

46.	The	e threat	of back	doors started	ł
W	hen	পেশ্ৰ	&	OSs	
b	ecan	ie widel	ly accep	oted	

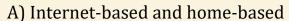
- A) single-user, Windows
- B) multiuser, networked
- C) single-user, UNIX
- D) multiuser, UNIX

47. There are _____ types of session hijacking

- A) 2
- B) 3
- C) Longevity
- D) Security
- 48. There are two types of firewalls. What are they







B) Hardware and software

- C) Remote and local
- D) Digital and electronic

49. There are two types of firewalls. What are they

- A) Internet-based and home-based
- B) Hardware and software
- C) Remote and local
- D) Digital and electronic

50. TPM is abbreviated as _____

- A) Trusted Platform Mode
- **B) Trusted Platform Module**
- C) Trusted Privacy Module
- D) True Platform Module

51. Transit time and response time measure the of a network

- A) Performance
- B) Reliability
- C) Security
- D) Longevity

52. Trojan creators do not look for

- A) Credit card information
- B) Confidential data
- C) Securing systems with such programs
- D) Important documents

53. True or False? Malware exists which affects both Windows and Linux systems.

A) True

- B) False
- C) Vulnerability
- D) Threat

54 .	Try not to keep
pa	asswords, especially fingerprint
fo	r your smart-phone, because it
Ca	nn lead to physical hacking if
V	ou're not aware or asleep.

A) Biometric

- B) PIN-based
- C) Alphanumeric
- D) Short

55. Unsolicited commercial email is known as____

- A) Spam
- B) Malware
- C) Virus
- D) Spyware

56. What is a captcha?

- A) A spam email that attempts to "capture" information and then use that information to cause damage; the second phase is often referred to as the "gotcha" phase.
- B) A SPAM email written in all caps
- C) It is a tool website often use to prevent automated spammer bots







from posting or registering on a website by forcing the user to do a task, often entering in letters or numbers based on a picture or audio, which verifies that they are human.

- D) A group of characters in hidden in an email that often includes code used in malware
- 57. What is a Joe Job?
 - A) A virus
 - B) An antivirus
 - C) A spam attacks
 - D) An antispam
- 58. What is another name for Internet Layer
 - A) TCP Layer
 - B) Interwebs
 - C) SSL Layer
 - D) IP Layer
- 59. What is DHA
 - A) Directory Harvest Attack
 - B) DNS Harvest Attack
 - C) Direct Harvest Attack
 - D) Dictionary Harvest Attack
- 60. What is one way that a web browser is vulnerable to breaching?
 - A) A browser can be infected by closing it

- B) A virus can be sent through the monitor
- C) A browser plugin can be exploited
- D) Web browsers are impervious to exploitation
- 61. What is the difference between a worm and Virus?
 - A) A worm does not replicate itself like a virus does, but rather moves from computer to computer
 - B) A virus infects files, while a worm eats them
 - C) A worm is a virus created for a very specific purpose
 - D) Unlike a virus, a worm does not need to attach itself to a program to spread
- 62. What is the existence of weakness in a system or network is known as?
 - A) Attack
 - B) Exploit
 - C) Threat
 - D) Vulnerability
- 63. What is the top method an attacker might infect a target
 - A) Social engineering or psychological manipulation
 - B) SQL injection
 - C) Buffer overflow
 - D) Hacking via the Internet







- 64. What Security tradeoff occurs while using IDS(Intrusion Detection System)?
 - A) Change in permission
 - B) Login Failures
 - C) Change in privilege
 - D) Performance degradation
- 65. When a person is harrassed repeatedly by being followed, called or be written to he/she is a target of
 - A) Bullying
 - **B) Stalking**
 - C) Identity theft
 - D) Phishing
- 66. When is encrypted data the safest
 - A) When it is being trasferred via usb stick
 - B) When it is in transit
 - C) When it is being written. When it is at rest
 - D) When it is being written
- 67. Where might a spammer get your personal information from
 - A) Facebook
 - B) MySpace
 - C) LinkedIn
 - D) All of these
- 68. Which Key is used to decrypt the message in PKI?

- A) Public Key
- **B)** Private Key
- C) Pre-shared Secret Key
- D) Hybrid Key
- 69. Which of the following act violates cyber security?
 - A) Exploit
 - B) Attack
 - C) security auditors
 - D) cyber-criminals
- 70. Which of the following actions compromise cyber security?
 - A) Vulnerability
 - B) Attack
 - C) Threat
 - D) Exploit
- 71. Which of the following are different categories of viruses
 - A) Parasitic
 - B) Bootstrap sector
 - C) Companion
 - D) All of the above
- 72. Which of the following are direct hars caused by spam
 - A) Loss of productivity
 - B) Increased downloading costs
 - C) Increased infrastructure costs
 - D) All of the above





- 73. Which of the following can diminish the chance of data leakage?
 - A) Steganography
 - B) Chorography
 - C) Cryptography
 - D) Authentication
- 74. Which of the following comes under the advantage of dictionary attack?
 - A) Time-consuming
 - B) Moderate efficient
 - C) Very fast
 - D) Complex to carry-out
- 75. Which of the following enables secure and private data exchange/transfer on an unsecure public network
 - A) Public Key Infrastucture
 - B) Virtual Key Infrastucture
 - C) Private Key Infrastucture
 - D) All of the given options are correct
- 76. Which of the following is a component of cyber security
 - A) Internet Of Things
 - B) AI
 - C) Database
 - D) Attacks
- 77. Which of the following is a session hijacking tool

- A) T-Sight
- B) Wireshark
- C) Maltego
- D) Nessus
- 78. Which of the following is a Stuxnet?
 - A) Trojan
 - B) Antivirus
 - C) Worm
 - D) Virus
- 79. Which of the following is a type of cyber-attack?
 - A) Phishing
 - B) SQL Injections
 - C) Password Attack
 - D) All of the above
- 80. Which of the following is a type of cyber security?
 - A) Cloud Security
 - B) Network Security
 - C) Application Security
 - D) All of the above
- 81. Which of the following is a type of cyber security?
 - A) Cloud Security
 - B) Network Security
 - C) nan
 - D) nan
- 82. Which of the following is an anti-virus program







- A) Norton
- B) K7
- C) Quick heal
- D) All of these
- 83. Which of the following is an objective of network security?
 - A) Confidentiality
 - B) Integrity
 - C) Availability
 - D) All of the above
- 84. Which of the following is not a step followed by cyber-criminals in data breaching?
 - A) Exfiltration
 - B) Research and info-gathering
 - C) Attack the system
 - D) Fixing the bugs
- 85. Which of the following is not a technique used by spanners
 - A) Spoofing the domain
 - B) Sending attached virus in spams
 - C) Junk tags associated with spamemails
 - D) Making important deals through such emails
- 86. Which of the following is not a well-known anti-virus program
 - A) AVAST
 - B) SMAG
 - C) AVG
 - D) McAFee

- 87. Which of the following is not an advantage of dictionary attack?
 - A) Very fast
 - B) Time-saving
 - C) Easy to perform
 - D) Very tough and inefficient
- 88. Which of the following is not an appropriate way of targeting a mobile phone for hacking?
 - A) Target mobile hardware vulnerabilities
 - B) Target apps' vulnerabilities
 - C) Setup Keyloggers and spyware in smart-phones
 - D) Snatch the phone
- 89. Which of the following is not an email-related hacking tool?
 - A) Mail Password
 - B) Email Finder Pro
 - C) Mail PassView
 - D) Sendinc
- 90. Which of the following is the hacking approach where cybercriminals design fake websites or pages for tricking or gaining additional traffic?
 - A) Pharming
 - B) Website-Duplication
 - C) Mimicking
 - D) Spamming





- 91. Which of the following is the most viral section of the internet?
 - A) Chat Messenger
 - B) Social networking sites
 - C) Tutorial sites
 - D) Chat-rooms
- 92. Which of the following online service's privacy cannot be protected using Tor?
 - A) Browsing data
 - B) Instant messaging
 - C) Login using ID
 - D) Relay chats
- 93. Which of the following spam filtering techniques has the highest potential for generating false positives
 - A) Community Filtering
 - B) Bayesian Filtering
 - C) Challenge-Response Filtering
 - D) Keyword Filtering
- 94. Which of the following term refers to a group of hackers who are both white and black hat?
 - A) Yellow Hat hackers
 - B) Grey Hat hackers
 - C) Red Hat Hackers
 - D) White-Black Hat Hackers
- 95. Which of the following type of attack can actively modify communications or data

- A) Both Active and Passive attack
- B) Neither Active nor Passive attack
- C) Active attack
- D) Passive attack
- 96. Which of them is not an objective of sniffing for hackers?
 - A) Fetching passwords
 - B) Email texts
 - C) Types of files transferred
 - D) Geographic location of a user
- 97. While sending a signed message, a sender
 - A) sends message key using public key encryption using DES and hashed message using public key encryption
 - B) sends message using public key encryption and hashed message using DES
 - C) sends both message and hashed message using DES
 - D) sends both message and hashed message using public key encryption



Unlock Your Potential with Students' Professional Courses



Advance Excel



Web Development

Kids Coding



5 Graphic Design

ChatGPT & Al Tools Training

