

QUESTION BANK

Unit Test-II

Program: - Computer Engineering Group
/CW

Program Code:- CM/IF

Course Title: -Emerging Trends in Computer Technology

Semester: - Sixth

ETI (22618)

Scheme: I

MULTIPLE CHOICE QUESTIONS AND ANSWERS

Chapter 4- Digital Evidence (CO4)

1. A valid definition of digital evidence is:
- A. Data stored or transmitted using a computer
 - B. Information of probative value
 - C. **Digital data of probative value**
 - D. Any digital evidence on a computer

Ans: C

2. What are the three general categories of computer systems that can contain digital evidence?
- A. Desktop, laptop, server
 - B. Personal computer, Internet, mobile telephone
 - C. Hardware, software, networks
 - D. **Open computer systems, communication systems, and embedded systems**

Ans: D

3. In terms of digital evidence, a hard drive is an example of:
- A. **Open computer systems**
 - B. Communication systems
 - C. Embedded computer systems
 - D. None of the above

Ans: A

4. In terms of digital evidence, a mobile telephone is an example of:
- A. Open computer systems
 - B. Communication systems
 - C. **Embedded computer systems**

D. None of the above

Ans: C

5. In terms of digital evidence, a Smart Card is an example of:

- A. Open computer systems
- B. Communication systems
- C. **Embedded computer systems**
- D. None of the above

Ans: C

6. In terms of digital evidence, the Internet is an example of:

- A. Open computer systems
- B. **Communication systems**
- C. Embedded computer systems
- D. None of the above

Ans: B

7. Computers can be involved in which of the following types of crime?

- A. Homicide and sexual assault
- B. Computer intrusions and intellectual property theft
- C. Civil disputes
- D. **All the above**

Ans: D

8. A logon record tells us that, at a specific time:

- A. An unknown person logged into the system using the account
- B. The owner of a specific account logged into the system
- C. **The account was used to log into the system**
- D. None of the above

Ans: C

9. Cyber trails are advantageous because:

- A. They are not connected to the physical world.
- B. Nobody can be harmed by crime on the Internet.
- C. They are easy to follow.
- D. **Offenders who are unaware of them leave behind more clues than they otherwise would have.**

Ans: D

10. Private networks can be a richer source of evidence than the Internet because: A. They retain data for longer periods of time.

- B. Owners of private networks are more cooperative with law enforcement.
- C. **Private networks contain a higher concentration of digital evidence.**

D. All the above.

Ans: C

11. Due to caseload and budget constraints, often computer security professionals attempt to limit the damage and close each investigation as quickly as possible. Which of the following is NOT a significant drawback to this approach?

- A. Each unreported incident robs attorneys and law enforcement personnel of an opportunity to learn about the basics of computer-related crime.
 - B. **Responsibility for incident resolution frequently does not reside with the security professional, but with management.**
 - C. This approach results in under-reporting of criminal activity, deflating statistics that are used to allocate corporate and government spending on combating computer-related crime.
 - D. Computer security professionals develop loose evidence processing habits that can make it more difficult for law enforcement personnel and attorneys to prosecute an offender.
- None of the above

Ans: B

12. The criminological principle which states that, when anyone, or anything, enters a crime scene he/she takes something of the scene with him/her, and leaves something of himself/herself behind, is:

- A. **Locard's Exchange Principle**
- B. Differential Association Theory
- C. Beccaria's Social Contract
- D. None of the above

Ans: A

13. The author of a series of threatening e-mails consistently uses "im" instead of "I'm." This is an example of:

- A. **An individual characteristic**
- B. An incidental characteristic
- C. A class characteristic
- D. An indeterminate characteristic

Ans: A

14. Personal computers and networks are often a valuable source of evidence. Those involved with _____ should be comfortable with this technology.

- A. Criminal investigation
- B. Prosecution
- C. Defense work
- D. All of the above **Ans:**

15. An argument for including computer forensic training computer security specialists is: A. It provides an additional credential.
- B. It provides them with the tools to conduct their own investigations.
 - C. **It teaches them when it is time to call in law enforcement.**
 - D. None of the above. **Ans: C**

16. The digital evidence are used to establish a credible link between_____
- A. **Attacker and victim and the crime scene**
 - B. Attacker and the crime scene
 - C. Victim and the crime scene
 - D. Attacker and Information

Ans: A

17. Digital evidences must follow the requirements of the _____
- A. Ideal Evidence rule
 - B. **Best Evidence rule**
 - C. Exchange rule
 - D. All the mentioned

Ans: B

18. From the two given statements 1 and 2, select the correct option from a-d.
- a. Original media can be used to carry out digital investigation process.
 - b. By default, every part of the victim's computer is considered as unreliable.
- A. a and b both are true
 - B. **a is true and b is false**
 - C. a and b both are false
 - D. a is false and b is true

Ans: B

19. The evidences or proof can be obtained from the electronic source is called the _____
- A. **digital evidence**
 - B. demonstrative evidence
 - C. Explainable evidence
 - D. substantial evidence

Ans: A

20. Which of the following is not a type of volatile evidence?
- A. Routing tables
 - B. Main memory
 - C. **Log files**
 - D. Cached data

Ans: C

21. The evidence must be usable in the court which is called as _____

- A. **Admissible**
- B. Authentic
- C. Complete
- D. **Reliable**

Ans: A

22. Photographs, videos, sound recordings, X-rays, maps drawing, graphs, charts is a a type of _____

- A. **Illustrative evidence**
- B. Electronic evidence
- C. Documented evidence
- D. Explainable evidence

Ans: A

23. Email, hard drives are examples of _____

- A. Illustrative evidence
- B. **Electronic evidence**
- C. Documented evidence
- D. Explainable evidence

Ans: B

24. Blood, fingerprints, DNA these are examples of _____

- A. Illustrative evidence
- B. Electronic evidence
- C. Documented evidence
- D. **Substantial evidence**

Ans: D

25. When an incident takes place, a criminal will leave a hint evidence at the scene and remove a hint from the scene which is called as _____

- A. **Locard's Exchange principle**
- B. Anderson's Exchange principle
- C. Charles's Anthony principle
- D. Kevin Ashton principle

Ans: A

26. Which is not procedure to establish a chain of custody? A. Save the original materials. B. Take photos of physical evidence.

- C. **Don't take screenshots of digital evidence content.**

D. Document date, time, and any other information of receipt.

Ans: C

27. Which is not related with digital evidence?

- A. **Work with the original evidence to develop procedures.**
- B. Use clean collecting media.
- C. Document any extra scope.
- D. Consider safety of personnel at the scene.

Ans: A

28. Which is example of non-volatile memory.

- A. **Flash memory**
- B. Registers and Cache
- C. Process table
- D. Arp cache

Ans: A

29. _____ is known as testimonial.

- A. **Oath affidavit**
- B. DNA samples
- C. Fingerprint
- D. Dried blood

Ans: A

30. The process of ensuring that providing or obtaining the data that you have collected is similar to the data provided or presented in a court is known as _____

- A. **Evidence validation**
- B. Relative evidence
- C. Best evidence
- D. Illustrative evidence

Ans: A

31. When cases got to trial your forensics examiner play one of ____ role.

- A. 2
- B. 4
- C. 3 D. 5

Ans. A

32. Types of digital evidence

- A. Eye witness
- B. Picture and video

- C. Paper work
- D. None of the above

Ans B

33. Rule of evidence is also known as _____

- A. Law of witness
- B. Law of litigation
- C. Law of evidence
- D. All of the above

Ans. C

True or False Questions

1. Digital evidence is only useful in a court of law.

- A. True
- B. **False**

Ans: B

2. Attorneys and police are encountering progressively more digital evidence in their work.

- A. **True**
- B. False

Ans: A

3. Video surveillance can be a form of digital evidence.

- A. **True**
- B. False

Ans: A

4. All forensic examinations should be performed on the original digital evidence.

- A. True
- B. **False**

Ans: B

5. Digital evidence can be duplicated exactly without any changes to the original data. A. True

B. False

Ans: B

6. Computers were involved in the investigations into both World Trade Center attacks. **A. True**

B. False

Ans: A

7. Digital evidence is always circumstantial.

- A. True
- B. False**

Ans: B

8. Digital evidence alone can be used to build a solid case.

- A. True
- B. False**

Ans: B

9. Computers can be used by terrorists to detonate bombs. **A. True**

- B. False**

Ans: A

10. The aim of a forensic examination is to prove with certainty what occurred. A. True

- B. False**

Ans: B

11. Even digital investigations that do not result in legal action can benefit from principles of forensic science.

- A. True**
- B. False**

Ans: A

12. Forensic science is the application of science to investigation and prosecution of crime or to the just resolution of conflict.

- A. True**
- B. False**

Ans: A

Chapter 5

Basics of Hacking (CO5)

1. Ethical Hacking is also known as _____. A. Black Hat Hacking.
- B. White Hat Hacking.**
 - C. Encryption.
 - D. None of these. **Ans. B**

2. Tool(s) used by ethical hacker _____.
A. Scanner
B. Decoder
C. Proxy
D. **All of these.**

Ans. D

3. Vulnerability scanning in Ethical hacking finds _____. A. Strengths.
- B. Weakness.**
 - C. A & B
 - D. None of these.

Ans. B

4. Ethical hacking will allow to _____ all the massive security breaches. A. Remove.
- B. Measure.**
 - C. Reject.
 - D. None of these.

Ans. B

5. Sequential step hackers use are: _ _ _ . A. Maintaining Access. B. Reconnaissance C. Scanning.

D. Gaining Access.

- A. **B, C, D, A**
- B. B, A, C, D C. A, B, C, D
- D. D, C, B, A

Ans. A

6. _____ is the art of exploiting the human elements to gain access to the authorized user. A. **Social Engineering**. B. IT Engineering.
C. Ethical Hacking.
D. None of the above.

Ans. A

7. Which hacker refers to ethical hacker? A. Black hat hacker.
B. **White hat hacker**.
C. Grey hat hacker.
D. None of the above.

Ans. B

8. The term cracker refers to_____ A. **Black hat hacker**.
B. White hat hacker.
C. Grey hat hacker.
D. None of the above.

Ans. A

9. Who described a dissertation on fundamentals of hacker's attitude? A. G. Palma.
B. **Raymond**.
C. Either.
D. Jhon Browman.

Ans. B

10. Computer Hackers have been in existence for more than a _____. A. Decade.
B. Year.
C. **Century**
D. Era.

Ans. C

11. Hackers do hack for? A. Fame.

- B. Profit.
- C. Revenge.
- D. **All the above**

Ans. D

12. The intent of ethical hacker is to discover vulnerabilities from a _____ point of view to better secure system.

- A. Victims.
- B. **Attackers.**
- C. Both A & B
- D. None of these.

Ans. B

13. Security audits are usually based on ____ A. Entries.

- B. **Checklists.**
- C. Both A & B
- D. None of the above

Ans. B

14. Ethical hacking consist of _____ A.

- Penetration testing.
- B. Intrusion testing.
- C. Red teaming.
- D. **All of the above.**

Ans. D

15. _____ is a person who find and exploits the weakness in computer system.

- A. Victim
- B. **Hacker**
- C. Developer
- D. None of the above.

Ans. B

16. A white hat hacker is the one who _____

- A. **Fix identifies weakness**
- B. Steal the data
- C. Identifies the weakness and leave message to owner
- D. None of the above

Ans. A

17. A black hat hacker is the one who _____

- A. Fix identifies weakness
- B. **Steal the data**

- C. Identifies the weakness and leave message to owner
- D. None of the above. **Ans. B**

18. A grey hat hacker is the one who_____

- A. Fix identifies weakness
- B. Steal the data
- C. **Identifies the weakness and leave message to owner**
- D. None of the above

Ans. C

19. Keeping information secured can protect an organization image and save an organization lot of money

- A. **True**
- B. False

Ans. A

20. Information is one of the most valuable assets of an organization

- A. **True**
- B. False

Ans. A

21. To catch a thief, think like _____

- A. Police
- B. Forensics
- C. **Thief**
- D. Hacker

Ans. C

22. _____ can create a false feeling of safety

- A. Firewall
- B. Encryption
- C. VPNs
- D. **All the above**

Ans. D

23. _____ exploits that involve manipulating people and users even your self are the greatest vulnerability within any computer

- A. **Nontechnical attacks**
- B. Network infrastructure attack
- C. Operating system attack
- D. Application and other specialized attack

Ans. A

24. Connecting into network through a rogue modem attached to computer behind a firewall is an example of ____ -

- A. Nontechnical attacks
- B. **Network infrastructure attack**
- C. Operating system attack
- D. Application and other specialized attack

Ans. B

25. _____ comprise of large portion of hacker attacks simply because every computer has one and _____ so well know exploits can be used against them

- A. Nontechnical attacks
- B. Network infrastructure attack
- C. **Operating system attack**
- D. Application and other specialized attack

Ans. C

26. _____ should be done before ethical hacking process. A.

- Data gathering.
- B. Attacking
- C. **Planning**
- D. Research

Ans. C

27. Which permission is necessary before ethical hacking? A.

- Written permission.**
- B. Decision maker permission
- C. Privacy permission
- D. Risk permission.

Ans. A

28. Which tool is used to crack the password?

- A. Nmap
- B. **LC4**
- C. ToneLOC
- D. Nessus

Ans. B

29. Which tool is used for depth analysis of a web application?

- A. **Whisker**
- B. Super scan

- C. Nikto
- D. Kismet **Ans. A**

30. Which tool is used to encrypt Email?

- A. WebInspect
- B. QualyGuard
- C. **PGP (pretty good privacy)**
- D. None of the above.

Ans. C

31. Malicious attacker often think like?

- A. Thieves
- B. Kidnapper
- C. **Both A & B**
- D. None of the above

Ans. C

32. Which hacker try to distribute political or social message through their work?

- A. Black hat hacker
- B. **Hactivist**
- C. Script kiddes
- D. White hat hacker

Ans. B

33. _____ are part of organized crime on internet.

- A. Criminal
- B. Antinationalist
- C. **Hacker for hire**
- D. None of the above

Ans. C

34. Which magazines releases the latest hacking methods?

- A. 2600
- B. Hackin9
- C. PHRACK
- D. **All the above**

Ans. D

35. Performing a shoulder surfing in order to check other's password is _____ ethical practice.

- A. a good
- B. not so good

- C. very good social engineering practice
- D. **a bad Ans. D**

36. _____ has now evolved to be one of the most popular automated tools for unethical hacking.

- A. Automated apps
- B. Database software
- C. **Malware**
- D. Worms

Ans. C

37. Leaking your company data to the outside network without prior permission of senior authority is a crime.

- A. **True**
- B. False

Ans. A

38. A penetration tester must identify and keep in mind the _____ & _____ requirements of a firm while evaluating the security postures.

- A. **privacy and security**
- B. rules and regulations
- C. hacking techniques
- D. ethics to talk to seniors

Ans. A

39. The legal risks of ethical hacking include lawsuits due to _____ of personal data. A. stealing

- B. disclosure**
- C. deleting
- D. hacking

Ans. B

40. Before performing any penetration test, through legal procedure, which key points listed below is not mandatory?

- A. Know the nature of the organization
- B. Characteristics of work done in the firm
- C. System and network
- D. **Type of broadband company used by the firm**

Ans. D

Chapter-6

Types of Hacking (CO6)

1. SNMP stands for_____
- A. Simple Network Messaging Protocol
 - B. Simple Network Mailing Protocol
 - C. **Simple Network Management Protocol**
 - D. Simple Network Master Protocol

Ans: C

2. Which of the following tool is used for Network Testing and port Scanning_____
- A. NetCat
 - B. SuperScan
 - C. NetScan
 - D. **All of above**

Ans: D

3. Banner grabbing is used for
- A. **White Hat Hacking**
 - B. Black Hat Hacking
 - C. Grey Hat Hacking
 - D. Script Kiddies

Ans: A

4. An attacker can create an_____attack by sending hundreds or thousands of e-mails a with very large attachments.
- A. Connection Attack
 - B. **Auto responder Attack**
 - C. Attachment Overloading Attack
 - D. All the above

Ans: B

5. Which of the following tool is used for Windows for network queries from DNS lookups to trace routes?
- A. **Sam Spade**
 - B. SuperScan
 - C. NetScan
 - D. Netcat

Ans: A

6. Which tool is used for ping sweeps and port scanning?

- A. Netcat
- B. SamSpade
- C. **SuperScan**
- D. All the above

Ans: C

7. Which of the following tool is used for security checks as port scanning and firewall testing?

- A. **Netcat**
- B. Nmap
- C. Data communication
- D. Netscan

Ans: A

8. What is the most important activity in system cracking? A. Information gathering

- B. **Cracking password**
- C. Escalating privileges
- D. Covering tracks

Ans: B

9. Which Nmap scan is does not completely open a TCP connection?

- A. **SYN stealth scan**
- B. TCP scan
- C. XMAS tree scan
- D. ACK scan

Ans: A

10. Key loggers are form of

- A. **Spyware**
- B. Shoulder surfing
- C. Trojan
- D. Social engineering

Ans: A

11. Nmap is abbreviated as Network Mapper.

- A. **True**
- B. False

Ans: A

12. _____ is a popular tool used for discovering network as well as security auditing.

- A. **Ettercap**

- B. Metasploit
 - C. Nmap
 - D. Burp Suit
- Ans: C**

13. Which of this Nmap do not check?
- A. Services different hosts are offering
 - B. On what OS they are running.
 - C. What kind of firewall in use?
 - D. **What type of antivirus in use?**

Ans: D

14. What is purpose of Denial of Service attacks? A. Exploit weakness in TCP/IP attack. B. To execute a trojan horse on a system.
- C. **To overload a system so it is no longer operational.**
 - D. To shutdown services by turning them off.

Ans: C

15. What are the some of the most common vulnerabilities that exist in a network system? A. Changing manufacturer, or recommended settings of newly installed application.
- B. **Additional unused feature on commercial software package.**
 - C. Utilizing open source application code.
 - D. Balancing security and ease of use of system.

Ans: B

16. Which of the following is not a characteristic of ethical hacker? A. Excellent knowledge of Windows.
- B. Understands the process of exploiting network vulnerabilities.
 - C. Patience, persistence and perseverance.
 - D. **Has the highest level of security for the organization.**

Ans: D

17. Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking.
- A. **Local networking**
 - B. Social engineering
 - C. Physical entry
 - D. Remote networking

Ans: A

18. The first phase of hacking an IT system is compromise of which foundation of security?
- A. Availability
 - B. **Confidentiality**
 - C. Integrity

D. Authentication **Ans: B**

19. Why would a ping sweep be used?

A. To identify live systems

B. To locate live systems

C. To identify open ports

D. To locate firewalls

Ans: A

20. What are the port states determined by Nmap?

A. Active, inactive, standby

B. Open, half-open, closed

C. Open, filtered, unfiltered

D. Active, closed, unused

Ans: C

21. What port does Telnet use?

A. 22 **B.** 80

C. 20

D. 23

Ans: D

22. Which of the following will allow foot printing to be conducted without detection?

A. PingSweep

B. Traceroute

C. War Dialers

D. ARIN

Ans: D

23. Performing hacking activities with the intent on gaining visibility for an unfair situation is called _____.

A. Cracking

B. Analysis

C. Hactivism

D. Exploitation

Ans: C

24. Why would a hacker use a proxy server?

A. To create a stronger connection with the target.

B. To create a ghost server on the network.

C. To obtain a remote access connection

D. To hide malicious activity on the network **Ans: A**

25. Which phase of hacking performs actual attack on a network or system?

- A. Reconnaissance
- B. Maintaining Access
- C. Scanning
- D. **Gaining Access**

Ans: D

26. Sniffing is used to perform _____ fingerprinting.

- A. **Passive stack**
- B. Active stack
- C. Passive banner grabbing
- D. Scanned

Ans: A

27. Services running on a system are determined by _____.

- A. The system's IP address
- B. The Active Directory
- C. The system's network name
- D. **The port assigned**

Ans: D

28. What are the types of scanning? A. Port, network, and services

- B. **Network, vulnerability, and port**
- C. Passive, active, and interactive
- D. Server, client, and network

Ans: B

29. Enumeration is part of what phase of ethical hacking?

- A. Reconnaissance
- B. Maintaining Access
- C. **Gaining Access**
- D. Scanning

Ans: C

30. _____ framework made cracking of vulnerabilities easy like point and click.

- A. Net
- B. **Metasploit**
- C. Zeus
- D. Ettercap

Ans: B

31. _____ is a popular IP address and port scanner.

- A. Cain and Abel
- B. Snort
- C. **Angry IP Scanner**

D. Ettercap

Ans: C

32. _____ is a popular tool used for network analysis in multiprotocol diverse network

- A. Snort
- B. SuperScan
- C. Burp Suit
- D. **EtterPeak**

Ans: D

33. _____ scans TCP ports and resolves different hostnames.

- A. **SuperScan**
- B. Snort
- C. Ettercap
- D. QualysGuard .

Ans: A

34. What tool can be used to perform SNMP enumeration?

- A. DNSlookup
- B. Whois
- C. Nslookup
- D. **IP Network Browser**

Ans: D

35. Wireshark is a _____ tool.

- A. **network protocol analysis**
- B. network connection security
- C. connection analysis
- D. defending malicious packet-filtering

Ans: A

36. Aircrack-ng is used for _____

- A. Firewall bypassing
- B. **Wi-Fi attacks**
- C. Packet filtering
- D. System password cracking

Ans: B

37. Phishing is a form of _____.

- A. Spamming
- B. Identify Theft
- C. **Impersonation**
- D. Scanning

Ans: C

38. What are the types of scanning?
- A. Port, network, and services
 - B. Network, vulnerability, and port**
 - C. Passive, active, and interactive
 - D. Server, client, and network

Ans: B

- 39 _____ is used for searching of multiple hosts in order to target just one specific open port.
- A. Ping Sweep**
 - B. Port scan
 - C. Ipconfig
 - D. Spamming

Ans: A

40. ARP spoofing is often referred to as _____
- A. Man-in-the-Middle attack**
 - B. Denial-of-Service attack
 - C. Sniffing
 - D. Spoofing

Ans: A

41. _____ is a tool that allows you to look into network and analyze data going across the wire for network optimization, security and troubleshooting purposes.
- A. Network analyzer**
 - B. Crypt tool
 - C. John-the -Ripper
 - D. Back track

Ans: A

42. _____ is not a function of network analyzer tool.
- A. Captures all network traffic
 - B. Interprets or decodes what is found into a human-readable format.
 - C. Displays it all in chronological order.
 - D. Banner grabbing**

43. _____ protocol is used for network monitoring.
- A. FTP SNMP**
 - B.
 - C. RELNET
 - D. ARP

Ans: A

44. What is the attack called “evil twin”? **A. rouge access point**

- B. ARP poisoning
- C. session hijacking
- D. MAC spoofing

Ans: A

45. What is the primary goal of an ethical hacker?

- A. avoiding detection
- B. testing security controls
- C. **resolving security vulnerabilities**
- D. determining return on investment for security measures

Ans: C

46. What are the forms of password cracking technique?

- A. Attack syllable
- B. Attack brute forcing
- C. Attacks hybrid
- D. **All the above**

Ans: D

45. Which type of hacker represents the highest risk to your network?

- A. black-hat hackers
- B. grey-hat hackers
- C. script kiddies
- D. **disgruntled employees**

Ans: D

46. Hacking for a cause is called _____

- A. **hacktivism**
- B. black-hat hacking
- C. active hacking
- D. activism

Ans: A

47. When a hacker attempts to attack a host via the internet it is known as what type of attack? A. local access

- B. **remote attack**
- C. internal attack
- D. physical access

Ans: B

49. A type of attack that overloads the resources of a single system to cause it to crash or hang.

- A. Resource Starvation
- B. Active Sniffing

- C. **Passive Sniffing**
- D. Session Hijacking

Ans. C

50. In computer networking, _____ is any technical effort to manipulate the normal behavior of network connections and connected systems.

- A. Hacking
- B. Evidence
- C. Tracing
- D. None of above

Ans:-A

51. _____ generally refers to unauthorized intrusion into a computer or a network.

- A. Hacking
- B. Evidence
- C. Tracing
- D. None of above

Ans:-A

52. We can eliminate many well-known network vulnerabilities by simply patch-ing your network hosts with their latest _____ and _____.

- A. Hckers and Prackers
- B. Vendor software and firmware patches
- C. Software amd Hardware
- D. None of above

Ans:-B

53. Network consist devices such as routers, firewalls, hosts that you must assess as a part of _____ process.

- A. Prackers
- B. Black hat hacking
- C. Grey hat hacking process
- D. Ethical hacking process.

Ans:-D

54. Network infrastructure vulnerabilities are the foundation for most technical security issues in your information systems.

- A. Operating system vulnerabilities
- B. Web vulnerabilities
- C. Wireless network vulnerabilities
- D. Network infrastructure vulnerabilities

Ans:-D

55. ____ attack, which can take down your Internet connection or your entire network.

- A. MAC
- B. DOS
- C. IDS
- D. None of above

Ans:-B

56. DOS stands for A. Detection of system

- B. Denial of Service
- C. Detection of service
- D. None of above

Ans:-B

57. IDS stands for ____

- A. Intrusion detection system
- B. Information documentation service
- C. Intrusion documentation system
- D. None of above

Ans:-A

58. Which protocols are in use is vulnerable

- A. TCL
- B. SSL
- C. FTP
- D. SMTP

Ans:-B

59. SSL stands for ____ A. Secure Sockets Layer

- B. Software Security Layer
- C. Socket security layer
- D. System software layer

Ans:-A

60. ____ include phishing, SQL injection, hacking, social engineering, spamming, denial of service attacks, Trojans, virus and worm attacks.

- A. Operating system vulnerabilities
- B. Web vulnerabilities
- C. Wireless network vulnerabilities
- D. Network infrastructure vulnerabilities

Ans:-D

61. Who invented worm attack ____

- A. Brightn Godfrey
- B. Alan yeung
- C. Robert Morris
- D. None of above

Ans:-C

62. Which of the following is not a typical characteristic of an ethical hacker? A. Excellent knowledge of Windows.

- B. Understands the process of exploiting network vulnerabilities.
- C. Patience, persistence and perseverance.
- D. Has the highest level of security for the organization.

Ans:-D

63. What is the purpose of a Denial of Service attack?

- A. Exploit a weakness in the TCP/IP stack
- B. To execute a Trojan on a system
- C. To overload a system so it is no longer operational
- D. To shutdown services by turning them off

Ans:- C

64. What are some of the most common vulnerabilities that exist in a network or system?

- A. Changing manufacturer, or recommended, settings of a newly installed application.
- B. Additional unused features on commercial software packages.
- C. Utilizing open source application code
- D. Balancing security concerns with functionality and ease of use of a system. Ans:B

65. What is the sequence of a TCP connection?

- A. SYN-ACK-FIN
- B. SYN-SYN ACK-ACK
- C. SYN-ACK
- D. SYN-SYN-ACK

Ans:B

66. Why would a ping sweep be used?

- A. To identify live systems
- B. To locate live systems
- C. To identify open ports
- D. To locate firewalls

Ans:-A

67. A packet with no flags set is which type of scan?

- A. TCP
- B. XMAS
- C. IDLE
- D. NULL

Ans:-D

Happy Learning! cwipedia.in

Cwipedia.in