ETI 22618 Unit 4 to 6 - lecture notes

Diploma in information technology (University of Mumbai)

QUESTION BANK

Program: - Computer Engineering Group Program Code:- CO

Course Title: -Emerging Trends in Computer Technology Semester: - Sixth

Course Abbr & Code:-ETI (22618) Scheme: I

MULTIPLE CHOICE QUESTIONS AND ANSWERS

Chapter 4- Digital Forensics (CO4)

1............. pays vital role in criminal justice systems

a) Forensics science
b) Digital evidences
c) Volatile Evidence
d) All of the Above

2. Federal Bureau of Investigation program is currently referred to as…………….

a) Magnet Media Program
b) Computer Analysis and Response Team (CART)
c) INTERPOL
d) Computer Forensic Laboratory

3. Digital forensics is all of them except:

a) Extraction of computer data.
b) Preservation of computer data.
c) Interpretation of computer data.
d) Manipulation of computer data.

4. Which of following are rule of digital forensics?

a) An examination should never be performed on the original data
b) The copy of the evidence must be an exact, bit-by-bit copy
c) The chain of custody of all evidence must be clearly maintained
d) The examination must be conducted in such a way as to prevent any modification of the evidence.
e) All of the Above

5. Which of following is not a rule of digital forensics?

a) An examination should be performed on the original data
b) A copy is made onto forensically sterile media
c) The copy of the evidence must be an exact, bit-by-bit copy
d) The chain of custody of all evidence must be clearly maintained

6. IDIP stands for:

a) Integrated Digital Investigation Process.
b) Integrated Data Investigator Process.
c) Integrated Digital Investigator Process.
d) Independent Digital Investigator Process.

7. Who is the father of Computer Forensics?
a) G.Palmar
b) Michael Anderson
c) S.Ciardhuain
d) Carrier and Safford

8. Who proposed Abstract Digital Forensic model (ADFM)
a) Reith, Carr, Gunsh
b) S.Ciardhuain
c) Carrier and Safford
d) G.Palmar

9. Which model of Investigation proposed by S.Ciardhuain?
a) Extended Model of Cybercrime Investigation (EMCI)
b) Integrated Digital Investigation Process(IDIP)
c) Road Map for Digital Forensic Research (RMDFR)
d) Extended Model of Cybercrime Investigation (EMCI)

10. Which Forensic Model is more likely the most comprehensive till date?
a) Abstract Digital Forensic model (ADFM)
b) Integrated Digital Investigation Process(IDIP)
c) Extended Model of Cybercrime Investigation (EMCI)
d) Road Map for Digital Forensic Research (RMDFR)

11. Which phase record the physical scene and duplicate digital evidence using standardized and accepted procedures?
a) Identification
b) Preservation
c) Collection
d) Examination
e) Analysis

12. Which phase provides a mechanism for an incident to be detected and confirmed?
a) Readiness phase
b) Deployment phase
c) Physical Crime Investigation phase
d) Digital Crime Investigation phase
e) Review phase

13. Which phase includes putting the pieces of a digital puzzle together and developing investigative hypotheses?
a) Preservation phase
b) Survey phase
c) Documentation phase
d) Reconstruction phase

14. Which phase investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location?
a) Preservation phase
b) Survey phase
c) Documentation phase
d) Reconstruction phase
e) Presentation phase

15. Which phase entails a review of the whole investigation and identifies area of improvement?

a) Physical crime investigation
b) Digital crime investigation.
c) Review phase.
d) Deployment phase

16. Ethical decision making in digital forensic work consist which of the following:

a) Honesty towards the investigation
b) Prudence means carefully handling the digital evidences
c) Compliance with the law and professional norms.
d) All of the Above

17. Which of following is/are general Ethical norm for Investigator?

a) To contribute to society and human being.
b) To avoid harm to others.
c) To be honest and trustworthy.
d) All of above
e) None of above

18. Which of following is/are Unethical norms for Investigator?

a) Uphold any relevant evidence.
b) Declare any confidential matters or knowledge.
c) Distort or falsify education, training, credentials.
d) All of above
e) None of above

19. Which of following is not general ethical norm for Investigator?

a) To contribute to society and human being.
b) **To express an opinion on the guilt or innocence belonging to any party**
c) To be honest and trustworthy.
d) To honor confidentially.

20. Which of following is a not unethical norm for Digital Forensics Investigation?

a) Uphold any relevant evidence.
b) Declare any confidential matters or knowledge.
c) Distort or falsify education, training, credentials.
d) Should be fair and take action not to discriminate.

21. In the past, the method for expressing an opinion has been to frame a ....question based on available factual evidence.

a) Hypothetical
b) Nested
c) Challenging
d) Contradictory

22. More subtle because you are not aware that you are running these macros (the document opens and the application automatically runs); spread via email

a) The purpose of copyright
b) Danger of macro viruses
c) Derivative works
d) computer-specific crime

23. There are three c's in computer forensics. Which is one of the three?

a) Control
b) Chance
c) Chains
d) Core

24. What is Digital Forensic?

a) Process of using scientific knowledge in analysis and presentation of evidence in court
b) The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation
c) process where we develop and test hypotheses that answer questions about digital events
d) Use of science or technology in the investigation and establishment of the facts or evidence in a court of law

25. Digital Forensics entails ………………

a) Accessing the system's directories viewing mode and navigating through the various systems files and folders
b) Undeleting and recovering lost files
c) Identifying and solving computer crimes
d) The identification, preservation, recovery, restoration and presentation of digital evidence from systems and devices

26. Which of the following is FALSE?

a) The digital forensic investigator must maintain absolute objectivity
b) It is the investigator's job to determine someone's guilt or innocence.
c) It is the investigator's responsibility to accurately report the relevant facts of a case.
d) The investigator must maintain strict confidentiality, discussing the results of an investigation on only a "need to know"

27. What is the most significant legal issue in computer forensics?

a) Preserving Evidence
b) Seizing Evidence
c) Admissibility of Evidence
d) Discovery of Evidence

28. Which of the following is not a property of computer evidence?

a) Authentic and Accurate.
b) Complete and Convincing.
c) Duplicated and Preserved.
d) Conform and Human Readable.

29............. can breaks investigation.

a) Crime
b) Security
c) Digital Forensic
d) Evidence

30. 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

31. Digital evidences must follow the requirements of the …………….

a) Ideal Evidence rule
b) Best Evidence rule
c) Exchange rule
d) All of the above

32. The true or real copy of the evidence media which is given by victim/client.

a) Superior evidence
b) Best Evidence
c) Original Evidence
d) All of the Above

33. Which property defines evidence must be usable in the court.

a) Admissible
b) Authentic
c) Complete
d) Reliable

34. From the two given statements 1 and 2, select the correct option from a-d.

1. Original media can be used to carry out digital investigation process.
2. By default, every part of the victim's computer is considered as unreliable.

a) 1 and 2 both are true
b) 1 is true and 2 is false
c) 1 and 2 both are false
d) 1 is false and 2 is true

35. Which of following is/are sources of digital evidence?

a) Internet-based
b) Stand-alone computers
c) Mobile devices
d) All of the Above

36. 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

37. When an incident takes place, a criminal will leave 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

38. Evidence transfer in the physical and digital dimensions helps investigators establish connections between…………

a) Victims and offenders
b) Victims and crime scenes
c) Offenders and crime scenes
d) Victims, offenders and crime scenes

39. Digital evidence is also defined as Information and data of value to an investigation that is ………..

a) Stored on electronic device
b) Transmitted by an electronic device
c) Received by an electronic device
d) All of the above

40. The evidences or proof that can be obtained from the electronic source is called as………..

a) Digital evidence
b) Demonstrative evidence
c) Explainable evidence
d) Substantial evidence

41. Photographs, videos, sound recordings, graphs, and charts are examples of which type of evidence.

a) Demonstrative evidence
b) Explainable Evidence
c) Substantial Evidence
d) Testimonial

42. Dried blood, fingerprints, DNA samples, casts of footprints at the crime scene are examples which type of evidence.

a) Illustrative evidence
b) Explainable Evidence
c) Documented evidence
d) Substantial evidence

43. The evidence spoken by the spectator under the oath is which type of evidence.

a) Demonstrative evidence
b) Documented Evidence
c) Substantial Evidence
d) Testimonial

44. For an evidence to be admissible, it is necessary that it should be……………..

a) Complete
b) Authenticated
c) Reliable
d) Believable

45. Which is the important to establish a chain of custody?

a) Save the original materials.
b) Take photos of physical evidence.
c) Take screenshots of digital evidence content.
d) Document date, time, and any other information of receipt.
e) All of the Above

46. 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.

47. The process of ensuring that providing the data that you have collected is similar to the data presented in a court is known as……………

a) Evidence verification
b) Evidence validation
c) Evidence authentication
d) Best evidence

48. Which of following is a most volatile evidence source?
a) Main memory
b) Temporary file systems
c) Registers and cache
d) Secondary memory

49. Which of the following is not a type of volatile evidence?
a) Routing tables
b) Main memory
c) Log files
d) Cached data

50. 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

Chapter 5: Basics of Hacking (CO5)

- -

1. Ethical Hacking is also known as …………….
a) Black Hat Hacking.
b) White Hat Hacking.
c) Gray Hat Hacking
d) Script kiddies

2. Tool(s) used by ethical hacker…………
a) Scanner
b) Decoder
c) Proxy
d) All of these.

3. Vulnerability scanning in Ethical hacking finds……...
a) Strengths.
b) Weakness.
c) Both a and b
d) None of these.

4. Ethical hacking will allow to…..............all the massive security breaches.
a) Remove.
b) Measure.
c) Reject.
d) None of these.

5. Sequential step hacker's use are ______.
1. Maintaining Access.
2. Reconnaissance
3. Gaining Access.

4. Scanning
a) 2, 3, 4,1
b) 4, 2, 3, 1
c) 2, 4, 3, 1
d) 4, 3, 2, 1

6. What is social engineering?

a) A technique to identify vulnerabilities in a system or network
b) A technique to exploit vulnerabilities in a system or network
c) A technique to manipulate people into giving up sensitive information
d) A technique to fix vulnerabilities in a system or network

7. The term cracker refers to……….
a) **Black hat hacker**.
b) White hat hacker.
c) Grey hat hacker.
d) None of the above.

8. Who described a dissertation on fundamentals of hacker's attitude?
a) G. Palma.
b) Raymond.
c) Either.
d) Jhon Browman.

9. The term refers hackers with unlawful intentions.
a) Black Hat Hacker
b) White Hat Hacker
c) Gray Hat Hacker
d) Script kiddies

10. Which type of hackers hack systems to discover vulnerabilities to protect against unauthorized access, abuse, and misuse?
a) Black Hat Hacker.
b) Gray Hat Hacker
c) Ethical Hacker
d) Script kiddies

11. Which type of hackers uses hacking to send social, religious, and political, etc. messages?
a) White Hat Hacker
b) Black Hat Hacker
c) Hacktivist
d) Script kiddies

12. Which type of hacker hacks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner?
a) White Hat Hacker
b) Black Hat Hacker
c) Gray Hat Hacker
d) Hacktivist
e) Script kiddies

13. 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 and b
d) None of these.

14. Security audits are usually based on………..
a) Entries.
b) Checklists.
c) Both a and b
d) None of the above

15. Ethical hacking is also known as …………
a) Penetration testing.
b) Intrusion testing.
c) Red teaming.
d) All of the above.

16. What is main goal of ethical hacking?
a) To cause damage to system
b) To gain unauthorized access to a system
c) To identify and fix security vulnerabilities
d) To steal sensitive information

17............. is a person who find and exploits the weakness in computer system.
a) Victim
b) Hacker
c) Developer
d) None of the above.

18……is similar to a backup, but it is a complete image of a protected system, including data and system files.
a) Replication
b) Backup
c) Snapshots
d) DPLR

19...........assure that user privileges are applied correctly.
a) Authentication
b) Authorization
c) Replication
d) All of the Above

20. Data subjects can ask data controllers to "forget" their personal data is……….
a) Right to erasure
b) Automated decision making
c) Transferring data outside the EU
d) Right to Control

21. Which entity that holds or processes personnel data on behalf of another organization?
a) GDPR Data Controller
b) GDPR Data Processor
c) Data Protection Officer
d) All of the Above

22 .... is a set of strategies and processes you can use to secure the privacy, availability, and integrity of your data.

a) Data privacy
b) Data protection
c) Data security
d) Both b and c

23 .... involves automating the transmission of critical data to offline and online storage.

a) Data availability
b) Data lifecycle management
c) Information lifecycle management
d) All of the Above

24. Which of following is/are goal of ethical hacker?

a) Hack your systems in a non-destructive fashion.
b) Enumerate vulnerabilities and, if necessary, prove to upper management that vulnerabilities exist.
c) Apply results to remove vulnerabilities and better secure your systems.
d) All of the Above

25 ....can creates false feeling of safety.

a) Firewall
b) Encryption
c) VNPs
d) All the above

26. Which of following rule must obey by ethical hacker?

a) Get written permission from the owner of the computer system and/or computer network before hacking.
b) Protect the privacy of the organization been hacked.
c) Transparently report all the identified weaknesses in the computer system to the organization.
d) Inform hardware and software vendors of the identified weaknesses.
e) All of the Above

27. To connecting into network through a rogue modem attached to computer behind a firewall is an example of which type of attack?

a) Nontechnical attacks
b) Network infrastructure attack
c) Operating system attack
d) Application and other specialized attack

28. Breaking file system security is an example of which type of attack?

a) Nontechnical attacks
b) Network infrastructure attack
c) Operating system attack
d) Application and other specialized attack

29. Malicious software includes………..

a) Viruses
b) Worms,
c) Trojan horses
d) All of the Above

30 ....should be done before ethical hacking process.

a) Data gathering.
b) Attacking
c) Planning
d) Research

31. Which permission is necessary before ethical hacking?
a) Written permission.
b) Decision maker permission
c) Privacy permission
d) Risk permission.

32. Ethical Hacker must obey which of following ethical hacking principle
a) Working ethically
b) Respecting privacy
c) Not crashing your systems
d) All of the Above

33. Which tool is used to crack password?
a) Ethereal
b) Nmap
c) Whisker
d) LC4

34. Which tool is used for depth analysis of a web application?
e) Ethereal
f) Nmap
g) Whisker
h) LC4

35. Which tool is used to encrypt Email?
a) WebInspect
b) QualyGuard
c) PGP (pretty good privacy)
d) None of the above.

36. What is vulnerability scanner?
a) A tool used to identify weaknesses in a system or network
b) A tool used to exploit vulnerabilities in a system or network
c) A tool used to monitor network traffic
d) A tool used to block email spam

37. The Information Technology Act 2000 is an Act of Indian Parliament notified on………..
a) 27th October 2000
b) 15th December 2000
c) 17th November 2000
d) 17th October 2000

38. The offense "Receiving stolen computer or communication device" comes under ……section of Cyber security Act 2000.
a) 66B
b) 67A
c) 66E
d) 66C

39. The offense “Failure /refusal to decrypt data” comes under ....section of Cyber security Act 2000.

a) 68
b) 69
c) 70
d) 71

40. Which section penalized sending "offensive messages"?

a) Section 66A
b) Section 66B
c) Section 66C
d) Section 66D

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

2. Which of the following tool is used for Network Testing and port Scanning…………..

a) NetCat
b) SuperScan
c) NetScan
d) All of above

3. Banner grabbing is mostly used for…….

a) White Hat Hacking
b) Black Hat Hacking
c) Grey Hat Hacking
d) Script Kiddies

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

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

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

a) Netcat

b) SamSpade
c) SuperScan
d) All the above

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

8. What is the most important activity in windows vulnerabilities?
a) Information gathering
b) Cracking password
c) Escalating privileges
d) Covering tracks

9. 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.

10. 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

11. What port does Telnet use?
a) 22
b) 80
c) 20
d) 23

12. An excessive amount of ARP requests can be a sign of an................attack on your network.
a) ARP poisoning attack
b) ARP Sniffing attack
c) MAC-address poisoning
d) MAC-address Sniffing

13. ARP spoofing is often referred to as………..

a) Denial-of-Service attack
b) Man-in-the-Middle attack
c) Sniffing attack
d) Flooding attack

14……………..watch out for unauthorized Access Points and wireless clients attached to your network that are running in ad-hoc mode

a) Rogue Network
b) ARP Poisoning
c) Session Hijacking
d) MAC spoofing

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

a) MAC
b) DOS
c) IDS
d) None of above

16. What are the port states determined by Nmap?
a) Active, inactive, standby
b) Open, half-open, closed
c) Open, closed, filtered
d) Active, closed, unused

17 .... include phishing, SQL injection, hacking, social engineering, spamming, denial ofservice attacks, Trojans, virus and worm attacks.

a) Operating system vulnerabilities
b) Web vulnerabilities
c) Wireless network vulnerabilities
d) Network infrastructure Vulnerabilities

18. What are some examples of hacker attacks against messaging system?

a) Transmitting malware
b) Crashing servers
c) Obtaining remote control of workstations
d) All of the Above

19. Which protocol plays important role in MAC –daddy attack?

a) ARP
b) FTP
c) SMTP
d) SNMP

20. What is one of the potential problems you may face if a hacker compromises your WLAN?

a) Loss of network access

b) Loss of confidential information

c) Legal liabilities

d) All of the above

21. “allintitle“ Google dork operator returns

a) results for pages that meet all of the keyword criteria

b) pages with specific text in their HTML title
c) matches for URLs that meet all the matching criteria
d) specific files containing title

22................. is a technique used by hackers to find the information exposed accidentally to the internet.

a) Buffer overflow
b) Google Dorking
c) Google Shadow
d) GDPR

23. In …………, your hacker corrupts data within the ...., and that code change forces your system to overwrite important data.

a) Stack Based, heap
b) Stack Based, stack
c) Heap-based, heap
d) Heap-based, stack

24. What is ARP poisoning or spoofing?
a) It is a method of stealing personal data
b) It is a type of man-in-the-middle (MITM) attack
c) It is a way to bypass firewalls
d) It is a technique used to perform DDoS attacks

25. How can hackers modify ARP tables?
a) By using a proxy server
b) By running a program such as dsniff or Cain & Abel
c) By brute-forcing the network password
d) By launching a phishing attack

26. What happens when a program or system process places more data than was originally allocated to be stored in a buffer?
a) The data is compressed to fit within the buffer
b) The extra data overflows and corrupts or overwrites other data in adjacent buffers
c) The data is automatically deleted
d) The buffer expands to accommodate the extra data

27. What is a buffer-overflow attack?
a) An attack that causes a program to stop functioning
b) An attack that fills up the hard drive with useless data
c) An attack that sends extra data to a program's buffer to corrupt or overwrite adjacent data
d) An attack that steals personal data from a program's buffer

28. What are the two methods that an attacker can use to take over a program's buffer and initiate a buffer-overflow attack?
a) Stack-based and heap-based
b) Stack-based and queue-based
c) Heap-based and list-based
d) Queue-based and tree-based

29. How does a stack-based buffer-overflow attack work?
a) The attacker corrupts data within the heap

b) **The attacker sends data to a too-small stack buffer and inserts malicious code by using a "push" or "pop" function**
c) The attacker floods the buffer with a large amount of data to cause it to crash
d) The attacker sends a virus to the buffer to infect the program

30. What is a heap-based buffer-overflow attack?
a) An attack that targets the stack buffer of a program
b) An attack that floods a buffer with a large amount of data
c) An attack that corrupts data within the heap and forces the system to overwrite important data
d) An attack that steals personal data from the program's buffer

31. What are database management systems?
a) Complex software systems for managing database
b) Simple software systems for management database
c) Hardware systems for managing databases
d) Network systems for managing databases

32. What is the role of a security professional in managing potential security problem in database management systems?
a) To ignore the potential security problems
b) To asses and manage the potential security problems
c) To create more security problems
d) To delegate the security problems to someone else

33. What is one of the vulnerabilities in database management systems?
a) Strong access permissions
b) Implementation of cryptography as an access control
c) Keeping sensitive data for a short time
d) **Loose access permissions**

34. What is the impact of excessive retention of sensitive data in database management systems?
a) It reduces the impact of a security breach
b) It increases the impact of a security breach
c) It has no impact on the security breach
d) It helps prevent security breaches

35. What is aggregation of personally identifiable information in database management systems?

a) The practice of collecting only non-sensitive data
b) The practice of keeping data in separate data warehouses
c) The practice of combining data about citizens from various sources into a data warehouse
d) The practice of deleting all sensitive data

36. What is SQL injection?

a) A technique to identify vulnerabilities in a system or network
b) **A technique to exploit vulnerabilities in a system or network**
c) A technique to fix vulnerabilities in a system or network
d) A technique to steal sensitive information from a system or network

37. Email bomb can crash a server and provide..............administrator access
a) Authorized
b) Unauthorized

c) Both A and B
d) None of the above

38. Hackers attacks against insecure Web Application via…….

a) HTTP
b) FTP
c) HTTPS
d) UDP

39. SQL Injection is which type of vulnerability?

a) Web Application vulnerability
b) Security vulnerability
c) Windows vulnerability
d) All of the above

40. Google Dorking is also known as…….

a) Google Tracking
b) Google Hacking
c) Google fetching
d) None of the above

41. Which of the following is/are Google Dork operator?

a) intitle
b) allintitle
c) inurl
d) All of the above

42. What is the intitle operator in Google Dorks?

a) It allows a hacker to search for pages based on the text contained in the URL
b) It searches for specific text in the HTML title of a page
c) It helps a hacker narrow down search results to specific file types
d) It searches for files based on their file extension.

43. What is the inurl operator in Google Dorks?

a) It allows a hacker to search for pages based on the text contained in the URL
b) It searches for specific text in the HTML title of a page
c) It helps a hacker narrow down search results to specific file types
d) It searches for files based on their file extension

.

44. What is the purpose of the filetype operator in Google Dorks?

a) To search for pages with specific text in their HTML title
b) To search for pages based on the text contained in the URL
c) To help a hacker narrow down search results to specific file types
d) To search for files based on their file extension

45. What is the purpose of the ext operator in Google Dorks?

a) To search for pages with specific text in their HTML titl

b) To search for pages based on the text contained in the URL

c) To help a hacker narrow down search results to specific file type

d) To search for files based on their file extension

46. What is the intext operator in Google Dorks?

a) It allows a hacker to search for pages based on the text contained in the URL

b) It searches for specific text in the HTML title of a page

c) It helps a hacker narrow down search results to specific file types

d) **It searches the entire content of a given page for keywords supplied by the hacker**

47. Which operator allows a hacker to search for pages based on the text contained in the URL?

a) intitle

b) allintitle

c) inurl

d) allinurl

48. Which operator searches the entire content of a given page for keywords supplied by the hacker?

a) intitle

b) allintitle

c) intext

d) allintext

49. Which operator requires a page to match all of the given keywords?

a) intext

b) allintext

c) inurl

d) allinurl

50. Which operator limits the scope of a query to a single website?

a) intitle

b) allintitle

c) site

d) inurl

51. What are some common vulnerability found in all versions of Windows?

a) DoS, Remote Code Execution, and SQL Injection

b) Buffer Overflow, Cross-site Scripting, and Directory Traversal.

c) CSRF File Inclusion, Http Response Splitting, and Gain Information/Privileges.

d) All of the above.

52. Why is Microsoft Windows OS the most widely hacked?

a) Because Microsoft doesn't care about security as much as other OS vendors.

b) Because it has the most vulnerabilities.

c) Because it is the most widely used OS in the world.

d) None of the above.

53. What is the one positive thing about hackers?

a) **They are driving the requirement for better security**.
b) They are exposing vulnerabilities in operating systems.
c) They are making it easier for software vendors to fix their products.
d) None of the above.

54. What type of vulnerability has the maximum impact on confidentiality and integrity?

a) DoS.
b) Remote Code Execution.
c) Memory Corruption.
d) **Gaining Privileges**.

55. What type of vulnerability was used by the Blaster worm in UNIX and Linux systems?

a) DoS.
b) Remote Code Execution.
c) Remote Procedure Call
d) SQL Injection.

56. What is the primary purpose of email attacks?

a) To damage Internet-connected computers.
b) To violate the privacy of email users.
c) To render Internet services inoperable.
d) All of the above.

57. Why has email become a major vulnerability to users and organizations?

a) Because it is a universal service used by a large number of people worldwide.
b) Because it is not secure and can be easily hacked.
c) Because it contains sensitive information that can be exploited.
d) None of the above.

58. What are the basic hacking methodologies used in some email attacks?

a) Gathering public information, scanning, and enumerating your systems.
b) Capturing network traffic and exploiting vulnerabilities.
c) Brute-force password cracking and phishing.
d) All of the above.