PUNE VIDYARTHI GRIHA'S

COLLEGE OF SCIENCE AND TECHNOLOGY

Affiliated to University of Mumbai

Question Bank

Class: T.Y.B. Sc.CS **Semester: VI**

Subject: Ethical Hacking

UNIT I

1. What is the ethics behind training how to hack a system?
a) To think like hackers and know how to defend such attacks
b) To hack a system without the permission
c) To hack a network that is vulnerable
d) To corrupt software or service using malware

2. 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

3. ----------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

4. Leaking your company data to the outside network without prior permission of senior authority is a crime.
a) True
b) False

5. ---------- is the technique used in business organizations and firms to protect IT assets.
a) Ethical hacking
b) Unethical hacking
c) Fixing bugs
d) Internal data-breach

6. The legal risks of ethical hacking include lawsuits due to ---------- of personal data.
a) stealing
b) disclosure
c) deleting
d) hacking

7. An ethical hacker must ensure that proprietary information of the firm does not get leaked.
a) True
b) False

8. ---------- helps to classify arguments and situations, better understand a cyber-crime and helps to determine appropriate actions.
a) Cyber-ethics
b) Social ethics
c) Cyber-bullying
d) Corporate behaviour

9. In which year the first popular hacker conference took place?
a) 1994
b) 1995
c) 1993
d) 1992

10. What is the name of the first hacker's conference?
a) DEFCON
b) OSCON
c) DEVCON
d) SECCON

11. _____ is the oldest phone hacking techniques used by hackers to make free calls
a) Phishing
b) Spamming
c) Phreaking
d) Cracking

12.Which is the legal form of hacking based on which jobs are provided in IT industries and firms?
a) Cracking
b) Non ethical Hacking
c) Ethical hacking
d) Hacktivism

13. Governments hired some highly skilled hackers. These types of hackers are termed as _____
a) Special Hackers
b) Government Hackers
c) Cyber Intelligence Agents
d) Nation / State sponsored hackers

14.The security, functionality, and ease of use triangle illustrates which concept?

a) As security increases, functionality and ease of use increase.
b) As security decreases, functionality and ease of use increase.
c) As security decreases, functionality and ease of use decrease.
d) Security does not affect functionality ease of use.

15. _---------- are programs to execute a series of operation automatically
a) bots
b) robots
c) machine
d) helper

16. What is the first step in a SQL injection attack?
a) Enter arbitrary commands at a user prompt
b) Locate a user field on a web page
c) Locate the return pointer
d) Enter a series of NOPs

17. ---------- Testing involves performing a security evaluation and testing with no previous knowledge of the network infrastructure or system to be tested
a) Black-box
b) White-box
c) Gray-box
d) Green-box

18. ---------- is a small piece of malicious program that runs hidden on an infected system.
a) Virus
b) Trojan
c) Shareware
d) Worm

19. ---------- of information means only authorized users are capable of accessing the information.
a) Confidentiality
b) Integrity
c) Non-repudiation
d) Availability

20. What does availability of data mean?
a) Assurance that data exists.
b) Assurance that data will be restricted and available to authorize People.
c) Assurance that data will be accurate and trustworthy.
d) The level of assurance that data will be available to people who need it, when they need it

21.When you use the word --------- it means you are protecting your data from getting disclosed.

a) Confidentiality
b) Integrity
c) Authentication
d) Availability

22.What does the CIA stand for?

a) Confidentiality, Integrity, Availability
b) Central Intelligence Agency
c) Cybersecurity Investigation Agency
d) Cybersecurity, Internet, Accessibility

23.Integrity assuring____
a) Trust
b) Completeness
c) Accuracy of data
d) All of the above

24.Which of this is an example of physical hacking?
a) Remote Unauthorised access
b) Inserting malware loaded USB to a system
c) SQL Injection on SQL vulnerable site
d) DDoS (Distributed Denial of Service) attack

25. ---------- is a weakness that can be exploited by attackers.
a) System with Virus
b) System without firewall
c) System with vulnerabilities
d) System with a strong password

26.Hacking for a cause is called .....
a) Hacktivism
b) Black-hat hacking
c) Active hacking
d) Activism

27.BOTs are computer program or software applications design to execute a series of operations automatically

a) True
b) False

28. ---------- means verifying a claim of identity

a) availability
b) authorization
c) identification
d) Authentication

29. How does a Denial of Service attack work?

a) Cracks passwords, causing the system to crash
b) Imitates a valid user
c) Prevents a legitimate user from using a system or service
d) Attempts to break the authentication method

30.What is a rootkit?
a) A simple tool to gain access to the root of the Windows system
b) A Trojan that sends information to an SMB relay
c) An invasive program that affects the system files, including the kernel and libraries
d) A tool to perform a buffer overflow

31.---------- is the recommended password-change interval?
a) 30 days
b) 20 days
c) 1 day
d) 7 days

32.What is the difference between a backdoor and a Trojan?
a) A Trojan usually provides a backdoor for a hacker.
b) A backdoor must be installed first.
c) A Trojan is not a way to access a system.
d) A backdoor is provided only through a virus, not through a Trojan.

33.How do you remove a Trojan from a system?
a) Search the Internet for freeware removal tools.
b) Purchase commercially available tools to remove the Trojan.
c) Reboot the system.
d) Uninstall and reinstall all applications.

34.What is a zombie?
a) A compromised system used to launch a DDoS attack
b) The hacker's computer
c) The victim of a DDoS attack
d) A compromised system that is the target of a DDoS attack

35.What is the objective of ethical hacking from the hacker's perspective?
a) Determine the security posture of the organization.
b) B. Find and penetrate invalid parameters.
c) Find and steal available system resources.
d) Leave marks on the network to prove they gained access.

36.This term is not used in hacking circles.
a) Vulnerabilities
b) Exploits
c) Integrity
d) Zero-day attack

37.Ethical hacking cannot:

a) Perform security analysis

b) Prioritize threats

c) Test resources

d) Exploit vulnerabilities

38.Which of the following is not the key term of the CIA triad?

a) Exploits

b) Availability

c) Confidentiality

d) Integrity

39. _____ to access information and other computing series begins with administrative policies and procedures

a) Authentication
b) Verification
c) Authorization
d) Validation

40. Choose the one that doesn't belong.

A. Zero-day attacks

B. Natural threat

C. Exploits

D. Malware

41.The _____ Attack consist of exploitation of the web session control mechanism, which is normally managed for a session token

a) Man-in-the middle
b) Session Hijacking
c) Waterhole
d) Cookie Theft

42. ---------- attack is a trial-and- error method used to obtain information such as User Password.

a) Brute Force
b) DoS
c) Phishing
d) Clickjacking

43. ---------- is Sneaky program that tracks reports your computing activity without consent.

a) Rootkits
b) Virus
c) Trojan
d) Spyware

44. _____ is a weakness which can be exploited by a Threat
a) Weakness
b) Vulnerability
c) Virus
d) Threat

45. An --------- is any attempt or tries to expose, alter, disable, destroy, steal or gain unauthorize access to or make unauthorized use of an asset
a) Attack
b) Asset
c) Alter
d) Attempt

46. The Open Web Application Security Project (OWASP) is a ----------organisation
a) commercial
b) non-profit
c) free
d) banking

47. Cross-site scripting (XSS) flaws give attacker the capability to inject ----------_____ scripts into the application
a) server-side
b) client-side
c) victim-side
d) attacker-side

48. _____ is a cyber-attack that uses disguised email as a weapon
a) Backtrack
b) Phishing
c) DOS
d) brute force

49. A ---------- is a computer connected to the Internet that has been compromised by a hacker
a) Botnets
b) zombie
c) malware
d) infected

50. The Rabbit virus makes multiple copies of itself on a single computer
a) Trojan
b) worm
c) Rabbit

d) Malware

Unit II

1. 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

2. After performing _____ the ethical hacker should never disclose client information to other parties.
   a) hacking
   b) cracking
   c) penetration testing
   d) exploiting

3. _____ is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.
   a) Social ethics
   b) Ethics in cyber-security
   c) Corporate ethics
   d) Ethics in black hat hacking

4. 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

5. What is the preferred communications method used with systems on a bot-net?
   a) IRC
   b) E-mail
   c) ICMP
   d) TFTP

6. Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as _____

a) Black Hat hackers
b) White Hat Hackers
c) Grey Hat Hackers
d) Red Hat Hackers

7. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber-crimes. Who are "they" referred to here?
   a) Gray Hat Hackers
   b) White Hat Hackers
   c) Hactivists
   d) Black Hat Hackers

8. _____ are the combination of both white as well as black hat hackers.
   a) Grey Hat hackers
   b) Green Hat hackers
   c) Blue Hat Hackers
   d) Red Hat Hackers

9. The amateur or newbie in the field of hacking who don't have many skills about coding and in-depth working of security and hacking tools are called _____

   a) Sponsored Hackers
   b) Hactivists
   c) Script Kiddies
   d) Whistle Blowers

10. Suicide Hackers are those _____

    a) who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity
    b) individuals with no knowledge of codes but an expert in using hacking tools
    c) who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints
    d) who are employed in an organization to do malicious activities on other firms

11. 43. Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____
    a) State sponsored hackers
    b) Blue Hat Hackers
    c) Cyber Terrorists
    d) Red Hat Hackers

12. What is the next step to be performed after footprinting?
    a) Enumeration
    b) scanning
    c) System hacking

d) Active information gathering

13. 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

14. Which of the following tool/s is/are used for footprinting?
    a) Whois
    b) Sam Spade
    c) SuperScan
    d) NCC

15. Which of the following statements best describes a white-hat hacker?
    a) Security professional
    b) Former black hat
    c) Former grey hat
    d) Malicious hacker

16. Which of the following is a tool for performing footprinting undetected?
    a) Whois search
    b) Traceroute
    c) Ping sweep
    d) Host scanning

17. What is the next step to be performed after footprinting?
    a) Scanning
    b) Enumeration
    c) System hacking
    d) Active information gathering

18. What is footprinting?
    a) Measuring the shoe size of an ethical hacker
    b) Accumulation of data by gathering information on a target
    c) Scanning a target network to detect operating system types
    d) Mapping the physical layout of a target's network

19. Why would hackers want to cover their tracks?
    a) To prevent another person from using the programs they have installed on a target system
    b) To prevent detection or discovery
    c) To prevent hacking attempts
    d) To keep other hackers from using their tools

20. How do you remove a Trojan from a system?
    a) Search the Internet for freeware removal tools.
    b) Purchase commercially available tools to remove the Trojan.
    c) Reboot the system.
    d) Uninstall and reinstall all applications.

21. What is sniffing?

a) Sending corrupted data on the network to trick a system
b) Capturing and deciphering traffic on a network
c) Corrupting the ARP cache on a target system
d) Performing a password-cracking attack

22. What is the first step of a pen test?
a) Create a map of the network by scanning.
b) Locate the remote access connections to the network.
c) Sign a scope of work, NDA, and liability release document with the client.
d) Perform a physical security audit to ensure the physical site is secure.

23. Someone (from outside) who tests security issues for bugs before launching a system or application, and who is not a part of that organization or company are _____
a) Black Hat hacker
b) External penetration tester
c) Blue Hat hacker
d) White Hat Hacker

24.A hacker needs to be a good programmer as many hacking software programs have ready-made exploits that can be launched against a computer system or network. Identify the uses of exploits.
(Choose which is not applicable.)
a)Initial attack
b)Expose vulnerability
c)Steal data
d)Gain privilege escalation

25.From discovery until disclosure, it is a:
a) Black risk
b) White risk
c) Gray risk
d) Red risk

26.Who are self-proclaimed ethical hackers?
a) Black hat hackers
b) White hat hackers
c) Gray hat hackers
d) Red hat hackers

27.Pen testers will use _____ to protect the possibility of data leakage and add another layer of security.

a) code review

b)vulnerability scan

c) manual testing

d) planning

28. What type of testing is the best option for an organization that can benefit from the experience of a security professional?

a) Automated testing tools
b) White-hat and black-hat testing
c) Manual testing
d) Automated testing

29. What is the purpose of a pen test?

a) To simulate methods that intruders take to gain escalated privileges
b) To see if you can get confidential network data
c) To test the security posture and policies and procedures of an organization
d) To get passwords

30. What is enumeration?

a) Identifying active systems on the network
b) Cracking passwords
c) Identifying users and machine names
d) Identifying routers and firewalls

31. Which tool can be used to perform a DNS zone transfer on Windows?

a) nslookup
b) DNSlookup
c) whois
d) ipconfig

32. Which step comes after enumerating users in the CEH hacking cycle?

a) Crack password
b) Escalate privileges
c) Scanning
d) Covering tracks

33. What is the proper command to perform and NMAP SYN scan every 5 minutes?

a) nmap -ss - paranoid
b) nmap -Ss -paranoid
c) nmap -Ss -fast
d) namp -Ss -sneaky

34. A packet with all flags set is which type of scan?

a) Full Open
b) Syn scan
c) XMAS
d) TCP connect

35. What are the three types of scanning?

a) Port, network, and vulnerability
b) Port, network, and services
c) Grey, black, and white hat
d) Server, client, and network

36. Banner grabbing is an example of what?

a) Passive operating system fingerprinting
b) Active operating system fingerprinting
c) Footprinting
d) Application analysis

37. What is war dialing used for?

a) Testing firewall security
b) Testing remote access system security
c) Configuring a proxy filtering gateway
d) Configuring a firewall

38. Dumpster diving can be considered which type of social engineering attack?

a) Human-based
b) Computer-based
c) Physical access
d) Paper-based

39. Nslookup can be used to gather information regarding which of the following?

a) Host names and IP addresses
b) Whois information
c) DNS server locations
d) Name server types and operating systems

40. What is footprinting?

a) Measuring the shoe size of an ethical hacker
b) Accumulation of data by gathering information on a target
c) Scanning a target network to detect operating system types
d) Mapping the physical layout of a target's network

41. Faking a website for the purpose of getting a user's password and username is which type of social engineering attack?

a) Human-based
b) Computer-based

c) Web-based
d) User-based

42. What is it called when a hacker pretends to be a valid user on the system?

a) Impersonation
b) Third-person authorization
c) Help desk
d) Valid User

43. What is the best reason to implement a security policy?

a) It increases security.
b) It makes security harder to enforce
c) It removes the employee's responsibility to make judgments
d) It decreases security

44. When a hacker attempts to attack a host via the Internet it is known as what type of attack?

a) Remote attack
b) Physical access
c) Local Access
d) Internal Attack

45. In_____testing extensive implementation knowledge is required

a) Black box
b) White box
c) Blue box
d) Grey box

46. If the information is leaked, the injured person can claim ____ of contract

a) end
b) suspension
c) violation
d) breach

47. NDA stands for _____

a) National Defence Academy
b) Non-disclosure agreement
c) Non-developed asset
d) national digital agency

48. ____is the process of exploiting weakness int the system and gaining unauthorized access to data

a) Attack
b) Hijacking
c) Hacking

d) Threat

49. White hat hackers are also called as ethical hacker or _____

a) security
b) Kerberos
c) watchdog
d) pen testers

50. In _____ testing data domains and internal boundaries can be tested

a) Blue box
b) Glass box
c) Black box
d) White box

UNIT III

1. Which of them is not a disadvantage of active online attack?
a) Takes a long time
b) Easily and automatically detected
c) Need high network bandwidth
d) Need the patience to crack

2. In which year, first practical technology hacking came into origin?
a) 1878
b) 1890
c) 1895
d) 1876

3. In which year, hacking became a practical crime and a matter of concern in the field of technology?
a) 1971
b) 1973
c) 1970
d) 1974

4. Which one of the following is not a part of Metasploit interface?
a) msfgui
b) msfconsole
c) msfcli
d) msfpayload

5. Ehtical hacking is the process of finding the vulnerabilities in a system through____procedures.
a)Unlafuk
b)Legal
c)Illegal
d)Screte

6. 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

7. What is the first phase of hacking?

a) Maintaining access
b) Gaining access
c) Reconnaissance
d) Scanning

8. In which attack attacker changes the MAC address
   a) DNS poisoning
   b) Buffer overflow
   c) IOT attack
   d) ARP poisoning

9. What is the best way to prevent a social-engineering attack?
   a) Installing a firewall to prevent port scans
   b) Configuring an IDS to detect intrusion attempts
   c) Increasing the number of help-desk personnel
   d) Employee training and education

10._____ is the process of hiding text within an image called?
   a) Steganography
   b) Encryption
   c) Spyware
   d) Keystroke logging

11.What is necessary in order to install a hardware keylogger on a target system?
   a) The IP address of the system
   b) The Administrator username and password
   c) Physical access to the system
   d) Telnet access to the system

12.What is cryptography?
   a) The study of computer science
   b) The study of mathematics
   c) The study of encryption
   d) The creation of encryption algorithms

13.Hackers and ethical hackers use the same tools and techniques.

a) True

b) False

14. _____flaws give attackers the capability to inject client-side scripts into applications.

   a) Cross Site Scripting (XSS)
   b) SQL Injection (SQLI)
   c) IDS/IPS
   d) SMTP

15._____ is decoy computer system for trapping hackers or tracking unconventional or new hacking methods.

a) Encryption
b) Denial of Service
c) Spoofing
d) Honeypot

16. ---------- hacking involves gaining access of the system as well as changing the integrity of the system

a) system
b) black hat
c) grey hat
d) white hat

17. A_____ can refer to any good computer programmer

a) security
b) developer
c) hacker
d) tester

18. Linux is ___ operating system

a) open source
b) expensive
c) difficult
d) automated

19. Windows is ___ operating system

a) open source
b) expensive
c) difficult
d) automated

20. ____ kernel is used in Windows

a) Monolithic kernel
b) Micro kernel
c) simple kernel
d) complex kernel

21. ____ kernel is used in Linux

a) Monolithic kernel
b) Micro kernel
c) simple kernel
d) complex kernel

22. In Windows separation of the directories using _____

a) Back slash
b) Forward slash
c) dot
d) underscore

23. In Linux separation of the directories using _____

a) Back slash
b) Forward slash
c) dot
d) underscore

24. In _____ file naming is case sensitive

a) Solarise
b) Mac
c) Linux
d) Windows

25. In _____ file naming is case insensitive

a) Solarise
b) Mac
c) Linux
d) Windows

26. _____ framework is a collection of shellcodes, exploits, fuzzing tools, encoders, payloads

a) Simple
b) Complex
c) .Net
d) Metasploit

27. ____ Linux is based on a rolling release model

a) Red hat
b) Kali
c) Ubuntu
d) Dolphin

28. The process of gathering information about your target is known as_____

a) enumeration
b) Hacking
c) data gathering
d) hijacking

29. What is common port number of HTTP?

a) 40
b) 81
c) 80

d) 21

30. What is common port number of FTP?

a) 40
b) 80
c) 81
d) 21

31. A _____ is a sequential segment of the memory location that is allocated for containing some data such as a character string or an array of integers.
a) stack
b) queue
c) external storage
d) buffer

32. In a _____ attack, the extra data that holds some specific instructions in the memory for actions is projected by a cyber-criminal or penetration tester to crack the system.
a) Phishing
b) MiTM
c) Buffer-overflow
d) Clickjacking

33. Let suppose a search box of an application can take at most 200 words, and you've inserted more than that and pressed the search button; the system crashes. Usually this is because of limited _____
a) buffer
b) external storage
c) processing power
d) local storage

34. The full form of Malware is _____
a) Malfunctioned Software
b) Multipurpose Software
c) Malicious Software
d) Malfunctioning of Security

35. Who deploy Malwares to a system or network?
a) Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
b) Criminal organizations, White hat hackers, malware developers, cyber-terrorists
c) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
d) Criminal organizations, gray hat hackers, Malware developers, Penetration testers

36. When there is an excessive amount of data flow, which the system cannot handle, _____ attack takes place.
a) Database crash attack

b) DoS (Denial of Service) attack
c) Data overflow Attack
d) Buffer Overflow attack

37. Compromising a user's session for exploiting the user's data and do malicious activities or misuse user's credentials is called _____
a) Session Hijacking
b) Session Fixation
c) Cookie stuffing
d) Session Spying

38. Which method of hacking will record all your keystrokes?
a) Keyhijacking
b) Keyjacking
c) Keylogging
d) Keyboard monitoring

39. _____ are the special type of programs used for recording and tracking user's keystroke.
a) Keylogger
b) Trojans
c) Virus
d) Worms

40. These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actions over a digital medium.
a) Malware
b) Remote Access Trojans
c) Keyloggers
d) Spyware

41. A Web site that allows users to enter text, such as a comment or a name, and then stores it and later display it to other users, is potentially vulnerable to a kind of attack called a ----------attack.
a) Two-factor authentication
b) Cross-site request forgery
c) Cross-site scripting
d) Cross-site scoring scripting

42. ---------- is an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated.
a) Two-factor authentication
b) Cross-site request forgery
c) Cross-site scripting
d) Cross-site scoring scripting

43. Many applications use ---------- where two independent factors are used to identify a user.
a) Two-factor authentication
b) Cross-site request forgery

c) Cross-site scripting
d) Cross-site scoring scripting

44. Even with two-factor authentication, users may still be vulnerable to_____attacks.
a) Radiant
b) Cross attack
c) scripting
d) Man-in-the-middle

45. Point out the wrong statement.
a) SQL injection vulnerabilities occur whenever input is used in the construction of an SQL query without being adequately constrained or sanitized
b) SQL injection allows an attacker to access the SQL servers and execute SQL code under the privileges of the user used to connect to the database
c) The use of PL-SQL opens the door to these vulnerabilities
d) None of the mentioned

46. ---------- is time based SQL injection attack.
a) Quick detection
b) Initial Exploitation
c) Blind SQL Injection
d) Inline Comments

47. QL injection is an attack in which --------- code is inserted into strings that are later passed to an instance of SQL Server.
a) malicious
b) redundant
c) clean
d) non malicious

48. In ---------- attacks an attacker do not contact with authorizing party for stealing password.
a) passive online
b) active online
c) offline
d) non-electronic

49.Which of the following is an example of passive online attack?
a) Phishing
b) Social Engineering
c) Spamming
d) Wire sniffing

50. Which of the following is not an example of a passive online attack?
a) MiTM
b) Reply Attack
c) Phishing
d) Wire sniffing