ETHICS MCQ

LECTURE 1:

…….. are a structure of standards and practices that influence how people lead their lives

a) Ethics

b) Law

ANSWAR: a

Ethics are like laws that legally mandate what is right or wrong.

a) true

b) false

ANSWAR: b

Explanation : Ethics are unlike laws that legally mandate what is right or wrong.

….. illustrate society's views about what is right and what is wrong

a) **Ethics**
b) **Law**

ANSWAR: a

What is the primary difference between ethics and laws?

a) Ethics are legally binding, while laws are guidelines.

b) Ethics govern personal conduct, while laws mandate legal behavior.

c) Ethics and laws are interchangeable terms.

d) Ethics are only applicable to computer-related activities.

ANSWAR: b

Privacy concerns, intellectual property rights and effects on the society are some of the common issues of ……

a) **Ethics**
b) **Law**
c) **Computer ethics**

ANSWAR: c

It is not strictly implemented to follow these ethics, but it is basically for the benefit of everyone that we do.

a) True
b) False

ANSWAR: a

…….. are a set of moral standards that govern the use of computers. It is society's views about the use of computers, both hardware and software

a) Ethics
b) Computer ethics
c) Law

ANSWAR: b

Privacy concerns, intellectual property rights and effects on the society are some of the common issues of computer ethics.

a) True
b) False

ANSWAR: a

….. is unlawful intrusion into a computer or a network.

a) Hacking
b) Malware
c) Data Protection
d) Anonymity

ANSWAR: a

A Hacker can intrude through the security levels of a computer system or network and can acquire unauthorised access to other computers.

a) True
b) false

ANSWAR: a

…. means malicious software which is created to impair a computer system

a) Hacking
b) Malware
c) Data Protection
d) Anonymity

ANSWAR: b

Common malware are ….

a) viruses
b) spyware
c) worms
d) trojan horses
e) All of them

ANSWAR: e

A spyware can delete files from a hard drive while a virus can collect data from a computer

a) true
b) false

ANSWAR: b

Explanation : A virus can delete files from a hard drive while a spyware can collect data from a computer

……. can delete files from a hard drive.

f) viruses
g) spyware
h) worms
i) trojan horses
j) All of them

ANSWAR: a

……. can collect data from a computer.

a) viruses
b) spyware
c) worms
d) trojan horses
e) All of them

ANSWAR: b

……. also known as information privacy or data privacy is the process of safeguarding data which intends to influence a balance between individual privacy rights while still authorising data to be used for business purposes.

a) Hacking
b) Malware
c) Data Protection
d) Anonymity

ANSWAR: c

……. is a way of keeping a user's identity masked through various applications.

a) Hacking
b) Malware
c) Data Protection
d) Anonymity

ANSWAR: d

From example of Privacy Concerns of issues of computer ethics is…

a) Hacking
b) Malware
c) Data Protection
d) Anonymity
e) All of them

ANSWAR: e

From example of Intellectual Property Rights of issues computer ethics is….

a) Copyright
b) Plagiarism
c) Cracking
d) Software License
e) All of them

ANSWAR:e

…. is a form of intellectual property that gives proprietary publication, distribution and usage rights for the author. This means that whatever idea the author created cannot be employed or disseminated by anyone else without the permission of the author.

a) Copyright
b) Plagiarism
c) Cracking
d) Software License

ANSWAR: a

… is an act of copying and publishing another person's work without proper citation. It's like stealing someone else's work and releasing it as your own work.

a) **Copyright**
b) **Plagiarism**
c) **Cracking**
d) **Software License**

ANSWAR: b

…. is a way of breaking into a system by getting past the security features of the system. It's a way of skipping the registration and authentication steps when installing a software.

a) **Copyright**
b) **Plagiarism**
c) **Cracking**
d) **Software License**

ANSWAR: c

…..allows the use of digital material by following the license agreement. Ownership remains with the original copyright owner, users are just granted licenses to use the material based on the agreement

a) **Copyright**
b) **Plagiarism**
c) **Cracking**
d) **Software License**

ANSWAR: d

From example of Effects on Society of issues computer ethics is….

a) **Jobs**
b) **Environmental Impact**
c) **Social Impact**
d) **All of them**

ANSWAR: d

……Some jobs have been abolished while some jobs have become simpler as computers have taken over companies and businesses. Things can now be done in just one click whereas before it takes multiple steps to perform a task. This change may be considered unethical as it limits the skills of the employees.

e) **Jobs**

f) Environmental Impact
g) Social Impact
h) All of them

ANSWAR: a

…….Environment has been affected by computers and the internet since so much time spent using computers increases energy usage which in turn increases the emission of greenhouse gases.

i) Jobs
j) Environmental Impact
k) Social Impact
l) All of them

ANSWAR: j

…..Computers and the internet help people stay in touch with family and friends. Social media has been very popular nowadays.

m)Jobs
n) Environmental Impact
o) Social Impact
p) All of them

ANSWAR: o

Which of the following is a common privacy concern related to computer ethics?

a) Properly citing sources in academic writing

b) Ensuring the safety of physical documents

c) Protecting data from hacking and malware

d) Energy-efficient computer usage

ANSWAR: c

What does copyright grant to the author of a work?

a) Exclusive ownership and distribution rights

b) A license to use the work without restrictions

c) Permission to use others' work without citation

d) The right to modify and republish the work freely

ANSWAR: a

What is plagiarism in the context of intellectual property rights?

a) Properly crediting the original author of a work

b) Selling copyrighted material without permission

c) Copying and using someone else's work without citation

d) Offering free access to one's copyrighted work

ANSWAR: c

What does "cracking" refer to concerning intellectual property rights?

a) Properly securing computer systems against unauthorized access

b) A method of breaking into a system by bypassing security features

c) The process of legally obtaining software licenses

d) The act of cracking open a computer to repair it

ANSWAR: b

How have computers impacted the job market?

a) They have created new job opportunities and increased employee skills.

b) They have led to the elimination of jobs and made tasks more complex.

c) They have no impact on the job market.

d) They have led to job automation, but only in specific industries.

ANSWAR: b

What is a potential ethical concern related to the use of computers for work?

a) Increased employee skills and job satisfaction

b) Negative effects on health and safety of employees

c) Improved environmental impact due to energy-efficient computers

d) Positive social impacts on communication and relationships

ANSWAR: b

How has computer technology affected the environment?

a) Reduced energy usage and greenhouse gas emissions

b) Increased energy consumption and pollution

c) Had no impact on the environment

d) Eliminated the need for energy consumption

ANSWAR: b

What are some of the social impacts of computer technology?

a) Improved hand-eye coordination and reduced stress

b) Increased addiction, isolation, and exposure to violence

c) Reduced access to government services

d) Enhanced business automation and data analysis

ANSWAR: b

What is the purpose of ethics?

a) To legally mandate behavior

b) To influence how people lead their lives

c) To benefit a select few

d) To replace laws in society

ANSWAR: b

How do ethics differ from laws?

a) Ethics legally mandate what is right or wrong.

b) Ethics govern personal conduct, while laws mandate legal behavior.

c) Ethics are strictly implemented, while laws are flexible.

d) Ethics and laws have the same principles.

ANSWAR: b

What does computer ethics primarily involve?

a) Dictating how computers are manufactured

b) Society's views on the use of computers, both hardware and software

c) Establishing technical specifications for computer hardware

d) Regulating the price of computer software

ANSWAR: b

Which of t he following is a form of hacking?

a) Legally accessing a computer system with permission

b) Unlawfully intruding into a computer or network

c) Encrypting personal data for protection

d) Updating computer software

ANSWAR: b

What is the primary goal of malware like viruses and spyware?

a) Improve computer system performance

b) Collect data from a computer

c) Enhance data protection

d) Eliminate the need for software updates

ANSWAR: b

What is data protection in the context of computer ethics?

a) Safeguarding data to promote data breaches

b) Stripping away individual privacy rights

c) Balancing individual privacy rights with business data usage

d) Eliminating the need for data storage

ANSWAR: c

What does copyright grant to the author of a work?

a) Exclusive ownership and distribution rights

b) Permission to use the work without restrictions

c) The right to modify and republish the work freely

d) The ability to use others' work without citation

ANSWAR: a

What is plagiarism?

a) Properly crediting the original author of a work

b) A legal method of using others' work without permission

c) Copying and publishing another person's work without proper citation

d) The act of creating new works inspired by others

ANSWAR: c

How have computers affected job roles?

a) All jobs have become more complicated due to computers.

b) Some jobs have become simpler, and tasks can be done more efficiently.

c) Computers have no impact on the job market.

d) Computers have eliminated all job roles.

ANSWAR: b

What is an ethical concern related to the health and safety of employees using computers?

a) Increased stress relief for employees

b) Potential health issues from constant computer usage

c) Enhanced job satisfaction for computer users

d) Reduced environmental impact from computer use

ANSWAR: b

LECTURE 2:

1) Ethical hackers are employed either through contracts or direct employment to test the security of an organization.

a. True

b. False

ANSWAR: a

2) They use the same skills and tactics as a hacker but with permission from the system owner to carry out their attack against the system.

a. True

b. False

ANSWAR: a

3) Ethical hackers work under contract for a company or client, and their contracts specify what is off-limits and what they are expected to do.

a. True

b. False

ANSWAR: a

4) Their role does not depend on the specific needs of a particular organization

a. True

b. False

ANSWAR: b

5) These hackers have limited or no training and know how to use only basic techniques or tools

a. White-hat hackers

b. Black-hat hackers

c. Script kiddies

d. Gray-hat hackers

ANSWAR: c

6) script kiddies Even then they may not understand any or all of what they are doing.

a. True

b. False

ANSWAR: a

7)…….. These hackers think like the attacking party but work for the good guys

a. White-hat hackers

b. Black-hat hackers

c. Script kiddies

d. Gray-hat hackers

ANSWAR: a

8)…….. are typically characterized by having a code of ethics that saysessentially they will cause no harm.

a. White-hat hackers

b. Black-hat hackers

c. Script kiddies

d. Gray-hat hackers

ANSWAR: a

9) White-hat hacker is also known as ethical hackers or Pen testers (penetration testing)

a. True

b. False

ANSWAR: a

10)…….. These hackers straddle the line between good and bad and have decided to reform and become the good side

a. White-hat hackers

b. Black-hat hackers

c. Script kiddies

d. Gray-hat hackers

ANSWAR: d

11) Once the gray-hat hackers are reformed, they still might not be fully trusted.

a. True

b. False

ANSWAR: a

12)…… These hackers are the bad guys who operate on the opposite side of the law.

a. White-hat hackers

b. Black-hat hackers

c. Script kiddies

d. Gray-hat hackers

ANSWAR: b

13) Black-Hat Hackers may or may not have an agenda.

a. True

b. False

ANSWAR: a

14) In most cases, black-hat hacking and outright criminal activity are far removed from each other.

a. True

b. False

ANSWAR: b

15)……. These hackers try to knock out a target to prove a point.

a. White-hat hackers

b. Black-hat hackers

c. Suicide hackers

d. Gray-hat hackers

ANSWAR: c

16) They are not stealthy, because they are not worried about getting caught or doing prison time.

a. White-hat hackers

b. Black-hat hackers

c. Suicide hackers

d. Gray-hat hackers

ANSWAR: c

17)Which of the following belongs to Code of Conduct and Ethics

a. Keep private and confidential information gained in your professional work.

b. Protect the intellectual property of others by relying on your own innovation and efforts.

c. Disclose to appropriate persons or authorities potential dangers to any e-commerce clients, the Internet community, or the public.

d. Never knowingly use software or a process that is obtained or retained either illegally or unethically.

e. All of the above

ANSWAR: e

18) Which of the following belongs to Code of Conduct and Ethics

a. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices

b. Not associate with malicious hackers nor engage in any malicious activities and Ensure all penetration testing activities are authorized and within legal limits.

c. Not take part in any black-hat activity or be associated with

any black-hat community

d. Not make inappropriate reference to the certification or

misleading use of certificates, marks,or logos in

publications, catalogues, documents, or speeches.

e. Not be in violation of any law of the land or have any

previous conviction

f. All of the above

ANSWAR: f

19)…….. This term describes a target that mayattract an above-average level of attention from an attacker

a. target

b. hack value

c. attack

d. target of evaluation

ANSWAR: b

20)……. is a system or resource that is being evaluated for vulnerabilities.

a. target

b. hack value

c. attack

d. target of evaluation(TOE)

ANSWAR: d

21) This is the act of targeting and actively engaging a TOE.

a. target

b. hack value

c. attack

d. target of evaluation(TOE)

ANSWAR: c

22) This is a clearly defined way to breach the security of a system.

a. target

b. hack value

c. exploit

d. target of evaluation(TOE)

ANSWAR: c

23) This describes a threat or vulnerability that is unknown to developers and has not been addressed.

a. target

b. zero day

c. exploit

d. target of evaluation(TOE)

ANSWAR: b

24) zero day isn`t considered a serious problem in many cases.

a. true

b. false

ANSWAR: b

25)This is a state of well-being in an environment where only actions that are defined are allowed

a. target

b.security

c. Exploit

d. target of evaluation(TOE)

ANSWAR: b

26)……. is considered to be a potential violation of security

a. threat

b. vulnerability

c. Exploit

d. target of evaluation(TOE)

ANSWAR: a

27) ……. is a weakness in a system that can be attacked and used as an entry point into an environment.

a. threat

b. vulnerability

c. Exploit

d. Daisy chaining

ANSWAR: b

28)…… is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action.

a. threat

b. vulnerability

c. Exploit

d. Daisy chaining

ANSWAR: d

29)…… means that you are using primarily passive methods of gaining information from a target prior to performing the later active methods.

a. scanning

b. footprinting

c. enumeration

d.system hacking

ANSWAR: b

30) ……is the phase in which you take the information gleaned from the footprinting phase

a. scanning

b. footprinting

c. enumeration

d.system hacking

ANSWAR: a

31) The idea in…….. is to act on the information from the prior phase, not to blunder around without purpose and set off alarms

a. scanning

b. footprinting

c. enumeration

d.system hacking

ANSWAR: a

32) is the next phase where you extract much more detailed information about what you uncovered in the scanning phase to determine its usefulness

a. scanning

b. footprinting

c. enumeration

d.system hacking

ANSWAR: c

33) in enumeration Results of this step can include a list of usernames, groups, applications, banner settings, and auditing information.

a. true

b. false

ANSWAR: a

34) in ……. You can now plan and execute an attack based on the information you uncovered.

a. scanning

b. footprinting

c. enumeration

d.system hacking

ANSWAR: d

35) in ……. You could, for example, start choosing user accounts to attack based on the ones uncovered in the enumeration phase

a. scanning

b. footprinting

c. enumeration

d.system hacking

ANSWAR: d

36) in system hacking You could also start crafting an attack based on service information uncovered by retrieving banners from applications or services.

a. true

b. false

ANSWAR: a

37)……. is the hacking phase, where you can start to obtain privileges that are granted to higher privileged accounts than you broke into originally. Depending on your skills

a. escalation of privilege

b. covering tracks

c. planting of backdoors

d. non of them

ANSWAR: a

38) in escalation of privilege might be possible to move from a low-level account such as a guest account all the way up to administrator or system-level access.

a. true

b. false

ANSWAR: a

39)…….. is the phase when you attempt to remove evidence of your presence in a system

a. escalation of privilege

b. covering tracks

c. planting of backdoors

d. non of them

ANSWAR: b

40) in …….. You purge log files and destroy other evidence that might give away the valuable clues needed for the system owner to determine an attack occurred.

a. escalation of privilege

b. covering tracks

c. planting of backdoors

d. non of them

ANSWAR: b

41) means to leave something behind that would enable you to come back later if you wanted. Items such as special accounts or Trojan horses

come to mind.

a. escalation of privilege

b. covering tracks

c. planting of backdoors

d. non of them

ANSWAR: c

42) what of the following belongs to Types of Hackers.

a. White-hat hackers

b. Black-hat hackers

c. Script kiddies

d. Gray-hat hackers

e. Suicide hackers

f. All of them

ANSWAR: f

43) what of the following belongs to hacking steps.

a. scanning

b. footprinting

c. enumeration

d.system hacking

e. all of them

ANSWAR: e

44) what of the following belongs to hacking methodologies.

a. escalation of privilege

b. covering tracks

c. planting of backdoors

d. all of them

ANSWAR: d

LECTURE 3:

1) …….. is the first phase of the ethical hacking process.

a. footprinting

b.scanning

c. enumeration

d. non of them

ANSWAR: a

2) ……The goal is to gather as much information as is reasonable and useful about a potential Target.

a. footprinting

b.scanning

c. enumeration

d. non of them

ANSWAR: a

3) ……It focuses on an active engagement of the target with the intention of obtaining more information.

a. footprinting

b.scanning

c. enumeration

d. non of them

ANSWAR: b

4) During scanning phase tools such as these are used: Pings, Ping sweeps , Port scans or Tracert

a. True

b. False

ANSWAR: a

5) (Trace Route), a command-line utility that you can use to trace the path that an Internet Protocol (IP) packet takes to its destination.

a. True

b. False

ANSWAR: a

6) It is the initial transition from being on the outside looking in to moving to the inside of the system to gather data. This information is carried forward into the attack phase.

a. footprinting

b.scanning

c. enumeration

d. non of them

ANSWAR: c

7)……. is the systematic investigating a target with the goal of obtaining user lists, routing tables, and protocols from the system.

a. footprinting

b. scanning

c. enumeration

d. non of them

ANSWAR: c

8)Simple Information Gathering using Google

a. Reading the news

b. Key-persons with contact details

c. social Media info

d. All of the mention

ANSWAR: d

9) Every information can be important, hackers collect all available information and systemize them before planning the attack!

a. True

b. false

ANSWAR: a

10)Collecting information from webpages

a. All static information can be downloaded at once (noisy, but useful)

b. Several tools exist like wget or Httrack

c. We can look for specific info such as email addresses, phone numbers, meta data, etc. using web data extractor. Sponsor

d. All of them

ANSWAR: d

11) Foca is able to find documents by extensions: it is a tool used mainly to find metadata and hidden information in the documents its scans. These documents may be on web pages and can be downloaded and analyzed with FOCA.

a. True

b. false

ANSWAR: a

12) foca also shows several technical information

a. True

b. false

ANSWAR: a

13) Displays the version of a web page that Google contains in its cache instead of displaying the current version. Syntax: cache:<website name>

a. info

b. link

c. site

d. cache

e. allintitle

f. All of them

ANSWAR: d

14) Lists any web pages that contain links to the page or site specified in the query. Syntax: link:<website name>

a. info

b. link

c. site

d. cache

e. allintitle

f. All of them

ANSWAR: b

15) resents information about the listed page. Syntax: info:<website name>

a. info

b. link

c. site

d. cache

e. allintitle

f. All of them

ANSWAR: a

16) Restricts the search to the location specified. Syntax: <keyword> site:<website name>

a. info

b. link

c. site

d. cache

e. allintitle

f. allinurl

ANSWAR: c

17)Returns pages with specified keywords in their title. Syntax: allintitle: <keywords>

a. info

b. link

c. site

d. cache

e. allintitle

f. allinurl

ANSWAR: e

18)Returns only results with the specific query in the URL. Syntax: allinurl: <keywords>

a. info

b. link

c. site

d. cache

e. allintitle

f. allinurl

ANSWAR: f

19) Filter to domain: use the site keyword

a. true

b. false

ANSWAR: a

20)Filter to file type with extension: use the …… keyword

a. type

b.site

c. non of them

ANSWAR: a

LECTURE 4:

1) …….deals with protection and preservation of information in all its forms

a. Cryptography

b. Save

c. Authentication

d. Nonrepudation

ANSWAR: a

2) the underlying goal of cryptography has never changed, even though the tools have.

a. True

b. False

ANSWAR: a

3) cryptanalysis, which no deals with unlocking or uncovering the secrets that others try so hard to hide or obscure

a. True

b. False

ANSWAR: b

4) One of the most widely used applications of cryptography is in the safeguarding of communications between two parties wanting to share information.

a. True

b.false

ANSWAR: a

5) In today's world only the information be kept secret

a. True

b. False

ANSWAR: b

6) In today's world, not only must information be kept secret, but provisions to detect unwelcome or unwanted modifications are just as important.

a. True

b. False

ANSWAR: a

7) Is the body of knowledge relating to cryptography concerned only with protecting information?

a. Yes

b. No

c. Sometimes no and sometimes yes

d. Yes but that has changed

ANSWAR: d

8)……. is the primary goal that encryption seeks to achieve

a. Integrity

b. Authentication

c. Confidentiality

d. Key distribution

ANSWAR: c

9) …….is done to keep secret information from disclosure, away from prying eyes.

a. Decryption

b.Encryption

c. Nonrepudiation

d. cryptography

ANSWAR: b

10) Cryptography can detect changes in information and thus prove its integrity or original unmodified state.

a. True

b. False

ANSWAR: a

11) Cryptography can detect changes in information and thus prove its integrity or original unmodified state. The previous part is the definition of:

a. Authentication

b.Confidentiality

c. Integrity

d. Nonrepudiation

ANSWAR: c

12) Cryptography allows a person, object, or party to be identified with a high degree of confidence.

a. True

b. False

ANSWAR: a

13) Cryptography allows a person, object, or party to be identified with a high degree of confidence. The previous part is the definition of:

a. Authentication

b.Integrity

c. Confidentiality

d. Key distribution

ANSWAR: a

14) …….is an essential component of a secure system because it allows software and other things to be positively identified.

a. Authentication

b.Integrity

c. Confidentiality

d. nonrepudiation

ANSWAR: a

15) …….The ability to provide positive identification of the source or originator of an event is an important part of security

a. Authentication

b.Integrity

c. Confidentiality

d. nonrepudiation

ANSWAR: d

16)in nonrepudiation a person engaged in an agreement can not claim later on he is not the issuer of this agreement

a. true

b.false

ANSWAR: a

17) ……..One of the most valuable components of a cryptosystem is the key, which is the specific secret combination or code used in a cryptographic function.

a. Authentication

b.Integrity

c. Confidentiality

d. Key distribution

ANSWAR: d

18) Key Distribution isn`t important to the cryptosystem

a. True

b. False

ANSWAR: b

19) ……is the original message. It has not been altered; it is the usable information.

a. Cipher text

b. Plain text

c. Key

d. algorithms

ANSWAR: b

20) Text Cipher text is the identical of plain text

a. true

b.false

ANSWAR: b

21) Text Cipher text is the opposite of plain text

a. true

b.false

ANSWAR: a

22) ……it is a message or other data that has been transformed into a different format using a mechanism known as an algorithm

a. Cipher text

b. Plain text

c. Key

d. algorithms

ANSWAR: a

23) …….It is also something that can be reversed using an algorithm and a key

a. Cipher text

b. Plain text

c. Key

d. algorithms

ANSWAR: a

24) …….transform clear text into cipher text

a. Cipher text

b. Plain text

c. Key

d. algorithms

ANSWAR: d

25) ……..a formula that includes discrete steps that describe how the encryption and decryption process is to be performed in a given instance.

a. Cipher text

b. Plain text

c. Key

d. algorithms

ANSWAR: d

26) A ……. is a discrete piece of information, usually random in nature, that determines the result or output of a given cryptographic operation.

a. Cipher text

b. Plain text

c. Key

d. algorithms

ANSWAR: c

27) Keys: It can be thought of in the same way a key in the physical world is, as a special item used to open or unlock something—in this case, a piece of information?

a. Cipher text

b. Plain text

c. Keys

d. algorithms

ANSWAR: c

28) symmetric and asymmetric is the type of cryptography ?

a. True

b. False

ANSWAR: a

29) in …….The Same key is used for both encryption and decryption and must be kept secret

a. Symmetric Cryptography

b. Asymmetric Cryptography

c. Symmetric Cryptography and Asymmetric Cryptography

d. Non of them

ANSWAR: a

30) The Features of symmetric cryptography:

a. Preserving confidentiality

b.Increased speed over many non-symmetric systems

c. Ensuring simplicity

d. Providing authenticity

e. All of the above

ANSWAR: e

31) The concept of public key cryptography was intended to overcome the key management problems inherent in previous systems.

a. True

b. False

ANSWAR: a

32) In asymmetric cryptography system, each user who is enrolled receives key called

a. Public key only

b. Private key only

c. Public key and private key

d. Non of the above

ANSWAR: c

33) the public key and the private key. Each person's private key is published, whereas the public key is kept secret.

a. True

b. False

ANSWAR: b

34) in…….. system of generating keys provides a means of nonrepudiation that is not possible with symmetric Systems.

a. Symmetric Cryptography/ Asymmetric Cryptography

b. Authentication system

c. Asymmetric Cryptography

d. Non of them

ANSWAR: c

35) Since anything encrypted with the public key can be reversed only with the corresponding private key

a. True

b. False

ANSWAR: b

36) Since anything encrypted with the private key can be reversed only with the corresponding public key

a. True

b. False

ANSWAR: a

37) Since anything encrypted with the private key can be reversed only with the corresponding public key and only one person holds the private key, then the identity of the encrypting party can be assured. The previous part is the

definition of:

a. Cryptography

b. Digital signature

c. Symmetric cryptography

d. Non of the above

ANSWAR: b

38) can be considered a type of one-way encryption. More accurately, it is a process that creates a scrambled output that cannot be reversed

a. Cryptography

b. Digital signature

c. Symmetric cryptography

d. Hashing

ANSWAR: d

39) The process outputs what is known as a hash, hash value, or message digest

a. True

b. False

ANSWAR: a

40) hashing is commonly used to validate the integrity of information.

a. True

b. False

ANSWAR: a

41) ……. is commonly used to validate the integrity of information.

a. Cryptography

b. Digital signature

c. Symmetric cryptography

d. Hashing

ANSWAR: d

42) A hash function generates a …… that is always the same length no matter how large or small the data entering the process or algorithm is.

a. a variable-length

b. a fixed-length

c. a changeable-length

d. non of them

ANSWAR: b

43) The fixed-length value is unique for every different input that enters the process

a. True

b. False

ANSWAR: a

44) Cryptographic systems are all vulnerable to what is known as a brute-force attack.

a. True

b. False

ANSWAR: a

45) In ……. attack, every possible combination of characters is tried in an attempt to uncover a valid key

a. Man-in-the-Middle

b. Phishing

c. Internet of Things (IoT)

d.Brute-force

ANSWAR: d

LECTURE 5:

Which of the following is an example of malware?

a. Antivirus software

b. Video editing software

c. Malicious software

d. System optimization tool

ANSWAR: c

Malware is short for malicious software.

a) True
b) False

ANSWAR: a

Categories of malware….

a) viruses, worms, Trojans
b) Logic bombs
c) adware and spyware

d) all of them

ANSWAR: d

…… are a modern form of malware that can hide within the core components of a system and stay undetected by modern scanners.

a) Viruses
b) Logic bombs
c) Rootkits
d) None

ANSWAR: c

……..Techniques include renaming a package to the name of a legitimate program and altering other files on a system to prevent them from being detected and running

a) Viruses
b) Logic bombs
c) Rootkits
d) Adware

ANSWAR: c

…are by far the best-known form of malicious software. This type of malware is designed to replicate and attach itself to other files resident on the system.

a) Viruses
b) Logic bombs
c) Rootkits
d) Adware

ANSWAR: a

viruses require some sort of user action to initiate their infectious activities.

a) True
b) False

ANSWAR: a

What does the virus do then?

a) Altering data , Infecting other programs ,Replicating
b) Encrypting itself, Transforming itself into another form
c) Altering configuration settings

d) Destroying data
e) Corrupting or destroying hardware
f) All of them

ANSWAR: d

The author may choose to create the virus completely from scratch or use one of the many construction kits that are available to create the virus of their choice.

a) True
b) False

ANSWAR: a

……are an advanced form of malware, compared to viruses, and have different goals in many cases.

a) Viruses
b) Logic bombs
c) Rootkits
d) Worms
e) Spyware

ANSWAR: d

One of the main characteristics of worms is their inherent ability to replicate and spread across networks extremely quickly.

a) True
b) False

ANSWAR: a

……type of malware that is designed to collect and forward information regarding a victim's activities to an interested party

a) Viruses
b) Adware
c) Trojan
d) Worms
e) Spyware

ANSWAR: e

….. is a well-known type of malware. Many systems are actively infected with this type of malware from the various installations and other activities they perform.

a) Viruses
b) Adware
c) Trojan
d) Worms
e) Spyware

ANSWAR: b

…..is a software application that is designed to provide covert access to a victim's system.

a) Logic bombs
b) Adware
c) Worms
d) Spyware
e) Trojan

ANSWAR: e

…….a special type of malware that infects a system and causing harm while appearing to look like a legitimate program

a) Viruses
b) Adware
c) Spyware
d) Trojan

ANSWAR: d

Types of Trojans is….

a) Remote Access Trojans (RATs)
b) Data Sending
c) Destructive
d) All of them

ANSWAR: d

……To fit into this category, a Trojan must capture some sort of data from the victim's system, including files and keystrokes. Once captured, this data can be transmitted via email or other means if the Trojan is so enabled. Keyloggers are common Trojans of this type.

a) Remote Access Trojans (RATs)
b) Data Sending
c) Destructive

d) None

ANSWAR: b

…..This type of Trojan seeks to corrupt, erase, or destroy data outright on a system. In more extreme cases, the Trojan may affect the hardware in such a way that it becomes unusable.

a) Remote Access Trojans (RATs)
b) Data Sending
c) Destructive
d) None

ANSWAR: c

…..Designed to give an attacker remote control over avictim's system. Two well-known members of this class are the SubSeven program and its cousin, Back Orifice, although both are older examples.

a) Remote Access Trojans (RATs)
b) Data Sending
c) Destructive
d) None

ANSWAR: a

Spyware It may replace home pages in browsers, place pop-up ads on a user's desktop, or install items on a victim's system that are designed to advertise products or services.

a) True
b) False

ANSWAR: b

Explanation : Adware

Methods of Spyware Infection….

a) Instant Messaging (IM)
b) Internet Relay Chat (IRC)
c) Email Attachments
d) All of them
e) None

ANSWAR: d

….is a commonly used mechanism to deliver messages and software because of its widespread use and the ability to entice new users to download software.

a) Instant Messaging (IM)
b) Internet Relay Chat (IRC)
c) Email Attachments
d) None

ANSWAR: b

….. With the rise of email as a communication medium, the practice of using it to distribute malware has also risen.

a) Instant Messaging (IM)
b) Internet Relay Chat (IRC)
c) Email Attachments
d) None

ANSWAR: c

….Delivering malicious software via IM is easy. Plus, IM software has never had much in the way of security controls.

a) Instant Messaging (IM)
b) Internet Relay Chat (IRC)
c) Email Attachments
d) None

ANSWAR: a

….Downloading software for free from unknown or untrusted sources can mean that you also download something nastier, such as spyware.

a) Physical Access
b) Browser Defects
c) Freeware
d) Websites

ANSWAR: c

…..Software is sometimes installed on a system via web browsing. When a user visits a given website, spyware may be downloaded and installed using scripting or some other means

a) Physical Access
b) Browser Defects
c) Freeware

d) Websites

ANSWAR: d

….Many users forget or do not choose to update their browsers as soon as updates are released, so distribution of spyware becomes easier.

a) Physical Access
b) Browser Defects
c) Freeware
d) Websites

ANSWAR: b

…..Once an attacker gains physical access, it becomes relatively easy to install spyware and compromise the system.

a) Physical Access
b) Browser Defects
c) Freeware
d) Websites

ANSWAR: a

What does the term "malware" refer to?

a. Software that enhances computer performance

b. Software that protects against viruses

c. Software that carries out malicious activities

d. Software used for data encryption

ANSWAR: c

Which of the following is a category of malware?

a. Firewalls

b. Rootkits

c. Data backups

d. Network routers

ANSWAR: b

What is the main purpose of a virus?

a. To steal personal information

b. To replicate and attach to other files

c. To enhance computer performance

d. To encrypt data

ANSWAR: b

How do viruses spread to different systems?

a. Through email attachments

b. By altering configuration settings

c. Through network routers

d. By infecting antivirus software

ANSWAR: a

What is the typical process of developing a virus?

a. Design, replication, launch, detection, elimination

b. Replication, launch, detection, design, elimination

c. Design, launch, replication, detection, elimination

d. Launch, detection, replication, design, elimination

ANSWAR: c

What is the purpose of antivirus software?

a. To create viruses for testing purposes

b. To identify and eliminate viruses

c. To replicate and spread viruses

d. To encrypt data on a system

ANSWAR: b

What is the recommended precaution before executing a virus code?

a. Make sure to have multiple antivirus programs installed

b. Execute the code on a secure network

c. Back up all important data

d. Avoid executing the code to prevent system damage

ANSWAR: d

Which utility can be used to convert a batch file into an executable virus?

a. Notepad

b. Antivirus software

c. JPS Virus Maker

d. bat2com

ANSWAR: d

What is the purpose of a rootkit?

a. To protect against viruses

b. To hide within a system and evade detection

c. To encrypt data on a system

d. To replicate and spread to different systems

ANSWAR: b

What is the difference between a virus and a worm?

a. A virus requires user action to spread, while a worm can spread automatically.

b. A virus can alter data, while a worm can only replicate itself.

c. A virus affects hardware, while a worm affects software.

d. There is no difference; the terms are interchangeable.

ANSWAR: a

What is the main characteristic of spyware?

a. It replicates and spreads to other systems.

b. It encrypts data on the infected system.

c. It steals personal information without the user's knowledge.

d. It alters configuration settings of the operating system.

ANSWAR: c

How can rootkits remain undetected by antivirus scanners?

a. They encrypt their code to avoid detection.

b. They hide within the core components of the system.

c. They actively disable antivirus software upon detection.

d. They only infect hardware and not software.

ANSWAR: b

What are logic bombs?

a. Malware that displays annoying pop-up advertisements.

b. Malware that encrypts data and demands a ransom for decryption.

c. Malware that is triggered by a specific event or condition.

d. Malware that replicates itself rapidly and consumes system resources.

ANSWAR: c

How do adware programs typically generate revenue?

a. By stealing sensitive information and selling it to third parties.

b. By encrypting data and demanding a ransom for its release.

c. By displaying targeted advertisements to users.

d. By spreading to other systems and infecting them.

ANSWAR: c

What is the primary purpose of antivirus software?

a. To create and distribute viruses for research purposes.

b. To detect and eliminate malware infections on a system.

c. To encrypt sensitive data stored on a computer.

d. To optimize system performance and improve speed.

ANSWAR: b

What precautionary measures can help protect against malware infections?

a. Regularly update antivirus software and operating system.

b. Disable firewalls and remove all security software.

c. Download and execute files from unknown sources.

d. Share personal information freely on public websites.

ANSWAR: a

What is the recommended action if you suspect your computer is infected with malware?

a. Disconnect from the internet and perform a full system scan.

b. Share your suspicions with friends and colleagues.

c. Ignore the symptoms and continue using the computer normally.

d. Install more malware to counteract the existing malware.

ANSWAR: a

What is the purpose of signature files in antivirus software?

a. To encrypt malware code and render it harmless.

b. To identify and recognize specific patterns of known malware.

c. To create backup copies of important system files.

d. To monitor network traffic and detect potential threats.

ANSWAR: b

How can users protect their data from ransomware attacks?

a. Regularly update antivirus software and operating system.

b. Avoid clicking on suspicious links or opening unknown email attachments.

c. Share sensitive information with unknown websites and services.

d. Disable all security features to improve system performance.

ANSWAR: b

What is a keylogger and how does it work?

a. A type of malware that steals encryption keys from a system.

b. A hardware device used to log keystrokes on a keyboard.

c. A software program that records keystrokes on a computer.

d. A security feature that encrypts keystrokes for enhanced privacy.

ANSWAR: c

What is phishing and how can it be recognized?

a. A type of malware that infects email attachments.

b. A social engineering attack that tricks users into revealing sensitive information.

c. A technique used to encrypt computer files and demand ransom for decryption.

d. A form of network attack that targets routers and switches.

ANSWAR: b

What is two-factor authentication (2FA) and why is it important?

a. A method of using two different antivirus programs for enhanced protection.

b. A technique of encrypting data with two different algorithms simultaneously.

c. A security measure that requires users to provide two forms of authentication to access an account.

d. A process of scanning a computer with two different antivirus engines.

ANSWAR: c

What is a DDoS attack and how does it work?

a. A virus that spreads rapidly across multiple computers in a network.

b. A method of encrypting data to render it unreadable without a decryption key.

c. A cyber attack that floods a network or website with a massive volume of traffic to disrupt its services.

d. A technique of infiltrating a system by exploiting vulnerabilities in its firewall.

ANSWAR: c

What is social engineering and what are some common examples?

a. A technique of manipulating social media algorithms for personal gain.

b. A method of using social media platforms for targeted advertising.

c. A psychological manipulation tactic used to deceive people into revealing sensitive information.

d. A process of building a strong network of social connections for professional purposes.

ANSWAR: c

What is ransomware and how does it typically infect a system?

a. A type of malware that locks computer files and demands a ransom for their release.

b. A technique of exploiting vulnerabilities in network routers to gain unauthorized access.

c. A form of attack that manipulates search engine results to redirect users to malicious websites.

d. A method of encrypting email messages to protect them from unauthorized access.

ANSWAR: a

What is a firewall and what is its role in cybersecurity?

a. A software program that monitors network traffic for potential threats.

b. A hardware device used to improve network connectivity and speed.

c. A technique of encrypting data transmissions for secure communication.

d. A process of creating multiple virtual instances of an operating system for enhanced security.

ANSWAR: a

What is the difference between symmetric and asymmetric encryption?

a. Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption uses different keys.

b. Symmetric encryption is used for data at rest, while asymmetric encryption is used for data in transit.

c. Symmetric encryption is more secure than asymmetric encryption.

d. Asymmetric encryption is faster and more efficient than symmetric encryption.

ANSWAR: a

What is a zero-day vulnerability and why is it a concern?

a. A software bug that has zero impact on system security.

b. A vulnerability that is discovered and patched before it can be exploited.

c. A previously unknown software vulnerability that can be exploited by attackers before a patch is available.

d. A security feature that prevents unauthorized access to a system.

ANSWAR: c

What is the purpose of a virtual private network (VPN)?

a. To protect computer hardware from physical damage.

b. To create a secure and encrypted connection over a public network.

c. To scan and remove malware from a computer system.

d. To optimize network performance and improve internet speed.

ANSWAR: b

Which of the following is a characteristic of worms?

a. They require a host application to perform their activities.

b. They rely on user interaction to function.

c. They replicate and spread slowly across networks.

d. They consume bandwidth and resources.

ANSWAR: d

What is one of the main differences between viruses and worms?

a. Viruses require user interaction to spread, while worms do not.

b. Viruses consume bandwidth and resources, while worms do not.

c. Viruses replicate and spread rapidly across networks, while worms do not.

d. Viruses rely on host applications to perform their activities, while worms do not.

ANSWAR: a

What is the primary characteristic of spyware?

a) It asks for the user's permission before collecting information.

b) It operates behind the scenes to collect information without user consent.

c) It only targets ads and generates revenue.

d) It alters system settings openly.

ANSWAR: b

Which of t he following methods is NOT commonly used for spyware infection?

a) Instant Messaging (IM)

b) Physical Access

c) Software Updates

d) Email Attachments

ANSWAR: c

Why is Instant Messaging (IM) a common method for delivering spyware?

a) IM software has robust security controls.

b) It always requires user consent for software downloads.

c) IM software is easy to compromise.

d) IM users are not susceptible to spyware.

ANSWAR: c

Which method of spyware infection involves users downloading software for free from untrusted sources?

a) Physical Access

b) Freeware Download

c) Browser Defects

d) Email Attachments

ANSWAR: b

How can spyware be installed on a system through web browsing?

a) By asking the user for permission explicitly.

b) By exploiting known browser vulnerabilities.

c) By sending an email attachment.

d) By using Internet Relay Chat (IRC).

ANSWAR: b

What is the primary motive for spyware authors to collect information from victims' systems?

a) To enhance system security

b) For research and analysis purposes

c) To generate revenue or steal sensitive information

d) To provide a better user experience

ANSWAR: c

Which of the following is a legitimate way to protect your system from spyware?

a) Never update your software or browsers

b) Download software from untrusted sources

c) Regularly update your software and use reputable security software

d) Disable your firewall and antivirus programs

ANSWAR: c

What is the most common method of spyware distribution through email attachments?

a) Encrypted ZIP files

b) Executable files with suspicious names

c) PDF documents with embedded scripts

d) Text files containing harmless information

ANSWAR: b

Which of the following scenarios is NOT a common use of spyware?

a) Tracking user browsing habits for marketing purposes

b) Stealing sensitive financial information for identity theft

c) Providing software updates to improve system performance

d) Altering system settings to disrupt normal operation

ANSWAR: c

What is one potential consequence of spyware infections on a system?

a) Improved system performance

b) Increased online privacy and security

c) Slower computer performance and privacy breaches

d) Automatic removal of malicious software

ANSWAR: c

What is the primary purpose of adware?

a) To improve system security

b) To steal sensitive information

c) To display advertisements and pop-up ads

d) To replace the operating system

ANSWAR: c

How is adware typically distributed to a victim's system?

a) Through email attachments

b) As standalone software installations

c) Through legitimate software downloads

d) Stealthily from websites or bundled with other software

ANSWAR: d

What are some common behaviors exhibited by adware-infected systems?

a) The CD drawer opens and closes continuously

b) The screen inverts colors

c) Documents print without explanation

d) All of the above

ANSWAR: d

What is the primary characteristic of a Trojan?

a) It appears as a legitimate program but causes harm to a system

b) It openly displays malicious intent to the user

c) It primarily spreads through email attachments

d) It targets only data capture and storage space consumption

ANSWAR: a

Which of the following operations can be performed by a hacker using a Trojan?

a) Changing screen saver settings

b) Consuming computer storage space

c) Printing documents without explanation

d) Installing keyloggers and stealing data

ANSWAR: d

What is the purpose of Remote Access Trojans (RATs)?

a) To capture and send data from a victim's system

b) To destroy data on the victim's system

c) To provide attackers with remote control over a victim's system

d) To alter screen settings on the victim's computer

ANSWAR: c

Which type of Trojan aims to corrupt, erase, or destroy data on a system?

a) Data Sending Trojans

b) Destructive Trojans

c) Remote Access Trojans (RATs)

d) Keyloggers

ANSWAR: b

What is the primary purpose of adware?

a) To protect your system from malware

b) To replace home pages in browsers

c) To provide covert access to a victim's system

d) To encrypt sensitive data

ANSWAR: b

How is adware typically distributed to a victim's system?

a) Through email attachments

b) As part of legitimate software installations

c) By exploiting browser vulnerabilities

d) Through instant messaging (IM)

ANSWAR:b

What are some common actions of adware on a victim's system?

a) Stealing sensitive data

b) Displaying ads, pop-ups, and nag screens

c) Changing screen settings

d) Printing documents without explanation

ANSWAR: b

Which of the following behaviors is NOT an indication of a Trojan infection?

a) The CD drawer of the computer opens and closes

b) Screen settings change by themselves

c) The browser is redirected to a strange web page

d) The mouse cursor moves unusually fast

ANSWAR: d

What operations can be performed by a hacker using a Trojan on a target computer system?

a) Installing security updates

b) Consuming computer storage space

c) Enhancing system performance

d) Stealing data and modifying files

ANSWAR: d

Which type of Trojan is designed to provide an attacker with remote control over a victim's system?

a) Data Sending Trojan

b) Destructive Trojan

c) Adware Trojan

d) Remote Access Trojan (RAT)

ANSWAR: d

What is the primary purpose of Data Sending Trojans?

a) To corrupt and destroy data

b) To change screen settings

c) To capture and transmit data from the victim's system

d) To display pop-up ads

ANSWAR: c