BRAINWARE UNIVERSITY

Term End Examination 2020 - 21

Programme – Master of Science in Advanced Networking & Cyber Security

Course Name – Cyber Security-I

Course Code - MNCS303

Semester / Year - Semester III

Time allotted : 75 Minutes | Full Marks : 60

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 60=60

1. *(Answer any Sixty)*

(i) Why would a hacker use a proxy server?

a) To create a stronger connection with the target.
b) To hide malicious activity on the network.
c) To create a ghost server on the network.
d) To obtain a remote access connection.

(ii) What type of symmetric key algorithm using a streaming cipher to encrypt information?

a) RC4
b) Blowfish
c) SHA
d) MD5

(iii) Which of the following is not a factor in securing the environment against an attack on security?

a) The education of the attacker
b) The system configuration
c) The business strategy of the company
d) The network architecture

(iv) To hide information inside a picture, what technology is used?

a) Rootkits
b) Bitmapping
c) Image Rendering
d) Steganography

(v) Which phase of hacking performs actual attack on a network or system?

a) Gaining Access
b) Reconnaissance

c) Maintaining Access

d) Scanning

(vi) Which of the following is not a typical characteristic of an ethical hacker?

a) Excellent knowledge of Windows.

b) Understands the process of exploiting network vulnerabilities.

c) Patience, persistence and perseverance.

d) Has the highest level of security for the organization.

(vii) The first phase of hacking an IT system is compromise of which foundation of security?

a) Availability

b) Integrity

c) Authentication

d) Confidentiality

(viii) Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?

a) Web-based

b) Computer-based

c) Human-based

d) User-based

(ix) What does confidentiality of data refer to?

a) Rules which allow access only to all parties

b) Rules which hide data

c) Rules which restrict access only to those who need to know

d) Rules which prevent data from being changed

(x) What does integrity of data refer to?

a) The level of assurance which can be given as to how structured data is

b) The level of assurance which can be given as to how strong data is

c) The level of assurance which can be given as to how relevant the data is

d) The level of assurance which can be given as to how accurate and trustworthy data is

(xi) What does availability of data refer to?

a) The level of assurance that data exists

b) The level of assurance that data will be available to people who need it, when they need it

c) The level of assurance that data will be restricted to people who need it, when they need it

d) The level of assurance that data will be accurate and trustworthy

(xii) Alice is buying books from an online retail site, and she finds that she is able to change the price of a book from £19.99 to £1.99. Which part of the CIA triad has been broken?

a) C

b) I

c) A

d) None of these

(xiii) Cynthia is working on her university applications online, when the admissions website crashes. She is unable to turn in her application on time.

a) C

b) I

c) A

d) None of these

(xiv) Tony gets his phone bill in the mail. The bill was supposed to be for £80, but the mail person spilled water on the bill, smearing the ink. The bill now asks for £8.

a) I

b) A

c) C

d) None of these

(xv) Kim has taken her A-Level exam and is waiting to get her results by email. By accident, Kim's results are sent to Karen.

a) C

b) I

c) A

d) None of these

(xvi) Rob opens his fitness tracking app to start logging a workout. The app crashes, and he is unable to log his workout.

a) C

b) I

c) A

d) None of these

(xvii) What are the characteristics of Host based IDS?

a) The host operating system logs in the audit information

b) Logs includes logins, file opens and program executions

c) Logs are analysed to detect tails of intrusion

d) All of the mentioned

(xviii) What are the drawbacks of the host based IDS?

a) Selective logging runs the risk of missed attacks

b) They are very fast to detect

c) Unselective logging of messages may increase the audit burdens

d) They have to be programmed for new patterns

(xix) What are the strengths of the host based IDS?

a) Attack verification

b) System specific activity

c) No additional hardware required

d) All of the mentioned

(xx) What are characteristics of Network based IDS?

a) They look for attack signatures in network traffic

b) Filter decides which traffic will not be discarded or passed

c) It is programmed to interpret a certain series of packet

d) It models the normal usage of network as a noise characterization

(xxi) What are strengths of Network based IDS?

a) Cost of ownership reduced

b) Malicious intent detection

c) Real time detection and response

d) All of the mentioned

(xxii) When discussing IDS/IPS, what is a signature?

a) Patterns of activity or code corresponding to attacks

b) An electronic signature used to authenticate the identity of a user on the network

c) "Normal," baseline network behaviour
d) None of these

(xxiii) Which technologies are increasingly used today instead of IDS?

a) IPS
b) SIEM
c) Data loss prevention
d) All of these

(xxiv) A false positive can be defined as:

a) An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behaviour
b) An alert that indicates nefarious activity on a system that, upon further inspection, turns out to truly be nefarious activity
c) The lack of an alert for nefarious activity
d) All of these

(xxv) DES (i) is a symmetric key encryption method (ii) guarantees absolute security (iii) is implementable as hardware VLSI chip (iv) is a public key encryption method

a) i and ii
b) ii and iii
c) i and iii
d) iii and iv

(xxvi)

DES using 56 bit keys_____

a) Can Be Broken With Presently Available High Performance Computers
b) Cannot be broken in reasonable time using presently available computers
c) Can be broken only if the algorithm is known using even slow computers.
d) It is impossible to break ever

(xxvii) Triple DES uses_____

a) 168 bit keys on 64-bit blocks of plain text
b) Works with 144 bit blocks of plain text and applies DES algorithm once.

c) Working On 64-Bit Blocks of Plain Text and 56 Bit Keys By Applying DES Algorithm For Three Rounds.

d) Uses 128 bit blocks of plain text and 112 bit keys and apply DES algorithm thrice.

(xxviii) Public key system is useful because

a) it uses two keys.

b) private key can be kept secret.

c) it is a symmetric key system.

d) there Is No Key Distribution Problem As Public Key Can Be Kept In A Commonly Accessible Database.

(xxix) In public key encryption if A wants to send an encrypted message

a) A encrypts message using his private key

b) A Encrypts Message Using B's Public Key

c) A encrypts message using B's private key

d) A encrypts message using his public key

(xxx) Triple DES_____

a) is a symmetric key encryption method

b) guarantees Excellent Security

c) is implementable as a hardware VLSI chip

d) is public key encryption method with three keys

(xxxi) Which of the following is valid difference between a Virus and a Spyware ?

a) Spyware damages data and also steals sensitive private information

b) Virus damages data, Spyware steals sensitive private information

c) Spyware damages data, Virus steals sensitive private information

d) Virus damages data and also steals sensitive private information

(xxxii) _____ is a process that helps you identify and manage potential problems that could undermine key business initiatives or projects.

a) Identification

b) Risk analysis

c) Monitoring

d) Planning

(xxxiii) _____ provides the quantum of information on a specific risk.

a) Risk Measurement
b) Risk Governance
c) Risk monitoring
d) Risk Mitigation

(xxxiv) _____ risks are those that the company must take in order to drive performance and long-term growth

a) Legal risk
b) Strategic risk
c) Core risk
d) Non-core risk

(xxxv) _____ risks are often not essential and can be minimized or eliminated completely.

a) Non-core risk
b) Legal risk
c) Strategic risk
d) Core risk

(xxxvi) What risks and challenges should be considered in the Internet of Everything?

a) Privacy and Security
b) Energy Consumption
c) Network Congestion
d) All of these

(xxxvii) This kind of crime involves altering raw data just before a computer processes it and then changes it back after the processing is completed

a) Data tampering
b) Salami attacks
c) Data diddling
d) None of these

(xxxviii) It is a medium for transporting Protocol Data units in a protected manner from source to destination is

a) End to End Measure
b) Link oriented measure
c) Association oriented Measure
d) None of these

(xxxix) A form of cybercrime in which attackers overload computing or network resources with so much of traffic to prevent access to resources is called _____

a) Denial of service
b) Distribution of service
c) Duplication of work
d) Cyber attack

(xl) DDOS attacks originate from _____

a) Intranet connected machines
b) Internet connected machines
c) Trojans
d) Spywares

(xli) Bots is a _____

a) Program to send mails automatically
b) Program to monitor logins
c) Program to specific tasks on a network
d) Program to check virus

(xlii) DDOS is _____

a) Distribution of service
b) Duplication of work
c) Cyber attack
d) Distributed Denial of service

(xliii) Systems in a botnet are also called as_____

a) Zombies
b) Zimson
c) FC
d) Gears

(xliv) A large amount of traffic to a victim network to congest the network is called _____

a) Amplification attack
b) Resource Depletion attack
c) Ransom attack
d) Flooding attack

(xlv) The process of analysts monitoring, responding and learning from adversaries internal to the network is _____

a) Passive defense
b) Intelligence
c) Active defense
d) Offense

(xlvi) _____ is a discipline that combines elements of law and computer science to collect and analyze information from various electronic gadgets that

are admissible in the court of law.

a) Cyber crime
b) Cyber forscience
c) Cyber forensics
d) Ethical hacking

(xlvii) _____ is a function of the organizational policies and processes as well as technologies.

a) Cyber-crime.
b) Cyber threat.
c) Threat intelligence.
d) Cyber security.

(xlviii) ____ are group of people habitually looking to steal identifies or information, such as social security information, credit card numbers, all for monetary objectives.

a) Spammers.
b) Spyware.
c) Spamware.
d) Phishers.

(xlix) _____ means preserving the authorized restriction on the access and disclosure, including means for protecting personal privacy and proprietary information.

a) Confidentiality.
b) Availability.
c) Integrity.
d) Threat intelligence.

(l) _____ is the act of sending multiple copies of unsolicited mails or mass emails such as chain letters to many users at a time.

a) Cyber theft.
b) Phishing.
c) Cyber laundering.
d) Spamming .

(li) Major areas covered in cyber security is/are _____.

a) application security.
b) information security
c) disaster security.
d) all of these

(lii) _____ is the planning process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a

disaster.

a) Disaster security.
b) Information security.
c) Application security.
d) Network security.

(liii) The altering of data so that it is not usable unless the changes are undone is _____.

a) ergonomics
b) compression
c) biometrics
d) encryption

(liv) Spammers are classified into _____

a) hucksters and warez
b) hucksters and piracy
c) hucksters and fraudsters
d) piracy and hucksters

(lv) Digital signature certificate is _____ requirement in various applications

a) Legislative
b) Statutory
c) Governmental
d) All of these

(lvi) The information technology act 2000 is the primary law in India dealing with _____

a) Cyber crime
b) Electronic commerce
c) both of these
d) None of these

(lvii) Accessing computer without prior authorization is a cyber-crimes that come under_____

a) Section 68
b) Section 65
c) Section 70
d) Section 66

(lviii) Technology no longer protected by copyright, available to everyone, is considered to be: _____

a) Proprietary
b) Open

c) Experimental
d) In the public domain

(lix) Cyber-crimes crossing International borders and involving the actions of atleast one nation state is sometimes referred to as

a) Cyber warfare
b) Warfare
c) Cyber battlespace
d) Espionage

(lx) Many cybercrimes come under the Indian Penal Code. Which one of the following is an example?

a) Sending threatening messages by email
b) Forgery of electronic records
c) Bogus websites
d) All of these