



**BRAINWARE UNIVERSITY**  
**ODD Semester Examinations 2021- 22**

Programme – Master of Science in Advanced Networking & Cyber Security - 2020 [M.Sc.(ANCS)]

Course Name – Ethical hacking and Digital Forensic Tools

Course Code – MNCS304

(Semester III)

Time allotted : 1 Hour 15 Minutes

Full Marks : 60

(Multiple choice type question)

60 x 1 = 60

*Choose the correct alternative from the following*

- (I) \_\_\_\_\_ is any action that might compromise cyber-security.
- A) Threat  
B) Vulnerability  
C) Exploit  
D) Attack
- (II) Network administrators can create their own ACL rules based on \_\_\_\_\_ and \_\_\_\_\_
- A) Address, Protocols and Packet attributes  
B) Address, Protocols and security policies  
C) Address, policies and Packet attributes  
D) Network topology, Protocols and data packets
- (III) \_\_\_\_\_ is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.
- A) Network Security  
B) Database Security  
C) Information Security  
D) Physical Security
- (IV) For hacking a database or accessing and manipulating data which of the following language the hacker must know?
- A) SQL  
B) HTML  
C) Tcl  
D) F#
- (V) The \_\_\_\_\_ command is used on Linux for getting the DNS and host-related information.
- A) Dnslookup  
B) Lookup  
C) Nslookup  
D) Inflookup
- (VI) RBAC is abbreviated as \_\_\_\_\_
- A) Rule-Based Accessing Control  
B) Role-Based Access Control  
C) Rule-Based Access Control  
D) Role-Based Accessing Control
- (VII) \_\_\_\_\_ ensures the integrity and security of data that are passing over a network.
- A) Firewall  
B) Antivirus  
C) Pentesting Tools  
D) Network-security protocols
- (VIII) Existence of weakness in a system or network is called \_\_\_\_\_
- A) Threat  
B) Vulnerability  
C) Exploit  
D) Attack
- (IX) \_\_\_\_\_ is a code injecting method used for attacking the database of a system / website.
- A) HTML injection  
B) SQL Injection  
C) Malicious code injection  
D) XML Injection
- (X) Firewall examines each \_\_\_\_\_ that are entering or leaving the internal network.
- A) Emails users  
B) Updates  
C) Connections  
D) Data packets
- (XI) \_\_\_\_\_ is based on sniffer traces from the remote system.
- A) Active fingerprinting  
B) Passive fingerprinting  
C) OS fingerprinting  
D) Network fingerprinting

- (XII) \_\_\_\_\_ buffer overflows, which are more common among attackers.
- A) Memory-based  
B) Queue-based  
C) Stack-based  
D) Heap-based
- (XIII) 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
- (XIV) Which of them does not comes under scanning methodologies?
- A) Vulnerability scanning  
B) Sweeping  
C) Port Scanning  
D) Google Dorks
- (XV) \_\_\_\_\_ are deadly exploits where the vulnerability is known and found by cyber-criminals but not known and fixed by the owner of that application or company.
- A) Unknown attacks  
B) Secret attacks  
C) Elite exploits  
D) Zero-day exploits
- (XVI) \_\_\_\_\_ is gained if you send especially skilled packets to a target machine.
- A) Active fingerprinting  
B) Passive fingerprinting  
C) OS fingerprinting  
D) Network fingerprinting
- (XVII) In an application that uses heap, the memory for data is allocated \_\_\_\_\_
- A) Logical  
B) Dynamically  
C) Statically  
D) At the beginning of the program
- (XVIII) The full form of Malware is \_\_\_\_\_
- A) Malfunctioned Software  
B) Multipurpose Software  
C) Malicious Software  
D) Malfunctioning of Security
- (XIX) There are \_\_\_\_\_ types of firewall.
- A) 5  
B) 4  
C) 3  
D) 2
- (XX) Lack of access control policy is a \_\_\_\_\_
- A) Bug  
B) Threat  
C) Vulnerability  
D) Attack
- (XXI) \_\_\_\_\_ is the first phase of ethical hacking.
- A) DNS poisoning  
B) Footprinting  
C) ARP-poisoning  
D) Enumeration
- (XXII) 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
- (XXIII) \_\_\_\_\_ is an attack technique occurs when excess data gets written to a memory block.
- A) Over buffering  
B) Buffering  
C) Buffer overflow  
D) Memory full
- (XXIV) Attackers commonly target \_\_\_\_\_ for fetching IP address of a target or victim user.
- A) Websites  
B) Web pages  
C) Ip tracker  
D) Emails
- (XXV) Which of the following is the port number for FTP data?
- A) 20  
B) 21  
C) 22  
D) 23
- (XXVI) Which of the following operations DNSenum cannot perform?
- A) Perform reverse lookups  
B) Get the host's addresses  
C) Get extra names and sub-domains through Google scraping  
D) Get the admin password
- (XXVII) \_\_\_\_\_ is the way or technique through which majority of the malware gets installed in our system.

- A) Drive-by click  
C) Drive-by download
- B) Drive-by redirection  
D) Drive-by injecting USB devices

(XXVIII) Which method of hacking will record all your keystrokes?

- A) Keyhijacking  
C) Keylogging
- B) Keyjacking  
D) Keyboard monitoring

(XXIX) Circuit-level gateway firewalls are installed in \_\_\_\_\_ layer of OSI model.

- A) Application layer  
C) Presentation layer
- B) Session layer  
D) Network layer

(XXX) In which year the term hacking was coined?

- A) 1965-67  
C) 1970-80
- B) 1955-60  
D) 1980-82

(XXXI) In the \_\_\_\_\_ layer of OSI model, packet filtering firewalls are implemented

- A) Application layer  
C) Presentation layer
- B) Session layer  
D) Network layer

(XXXII) When a packet does not fulfil the ACL criteria, the packet is \_\_\_\_\_

- A) Resend  
C) Destroyed
- B) Dropped  
D) Acknowledged as received

(XXXIII) \_\_\_\_\_ phase in ethical hacking is known as the pre-attack phase.

- A) Reconnaissance  
C) Gaining access
- B) Scanning  
D) Maintaining access

(XXXIV) In IP address, IP is abbreviated as \_\_\_\_\_

- A) Internet Program  
C) Intuition Programs
- B) Internet Protocol  
D) Internet Pathway

(XXXV) 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  
C) Hactivists
- B) White Hat Hackers  
D) Black Hat Hackers

(XXXVI) Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are \_\_\_\_\_

- A) State sponsored hackers  
C) Cyber Terrorists
- B) Blue Hat Hackers  
D) Red Hat Hackers

(XXXVII) Which of the following comes after scanning phase in ethical hacking?

- A) Scanning  
C) Reconnaissance
- B) Maintaining access  
D) Gaining access

(XXXVIII) Which of the following is the port number for FTP control?

- A) 20  
C) 22
- B) 21  
D) 23

(XXXIX) Why programming language is important for ethical hackers and security professionals?

- A) Only to write malware  
C) To teach programming
- B) For solving problems and building tool and programs  
D) To develop programs to harm others

(XL) \_\_\_\_\_ is a technique used when artificial clicks are made which increases revenue because of pay-per-click.

- A) Clickjacking  
C) Keylogging
- B) Clickfraud  
D) Click-hacking

(XLI) \_\_\_\_\_ is the hacking approach where cyber-criminals design fake websites or pages for tricking or gaining additional traffic

- A) Cyber-replication  
C) Website-Duplication
- B) Mimicking  
D) Pharming

(XLII) Firewalls can be of \_\_\_\_\_ kinds.

- A) 1  
C) 3
- B) 2  
D) 4

- (XLIII) Malicious code can be pushed into the \_\_\_\_\_ during \_\_\_\_\_ attack.
- A) stack, buffer-overflow
  - B) queue, buffer-overflow
  - C) memory-card, buffer-overflow
  - D) external drive, buffer-overflow
- (XLIV) Which of the following is not a software firewall?
- A) Windows Firewall
  - B) Outpost Firewall Pro
  - C) Endian Firewall
  - D) Linksys Firewall
- (XLV) Which of the following is not a secured mail transferring methodology?
- A) POP3
  - B) SSMTTP
  - C) Mail using PGP
  - D) S/MIME
- (XLVI) MAC is abbreviated as \_\_\_\_\_
- A) Machine Access Control
  - B) Mandatory Accounts Control
  - C) Mandatory Access Controlling
  - D) Mandatory Access Control
- (XLVII) Physical ports are usually referred to as \_\_\_\_\_
- A) Jacks
  - B) Cables
  - C) Interfaces
  - D) Hardware plugs
- (XLVIII) We can also implement \_\_\_\_\_ in Stateful Multilayer Inspection firewall
- A) External programs
  - B) Algorithms
  - C) Policies
  - D) Algorithms and external programs
- (XLIX) Number of logical ports ranges from \_\_\_\_\_ to \_\_\_\_\_
- A) 0, 255
  - B) 1, 65535
  - C) 1, 65536
  - D) 0, 65536
- (L) \_\_\_\_\_ is the information gathering phase in ethical hacking from the target user.
- A) Reconnaissance
  - B) Scanning
  - C) Gaining access
  - D) Maintaining access
- (LI) Which of the following information security technology is used for avoiding browser-based hacking?
- A) Anti-malware in browsers
  - B) Remote browser access
  - C) Adware remover in browsers
  - D) Incognito mode in a browser
- (LII) \_\_\_\_\_ persistence and up-to-date with the latest technological updates and their flaws are some of the major qualities; an ethical hacker must need to have.
- A) Lack of understanding
  - B) Weak programming skills
  - C) High patience
  - D) Low perseverance
- (LIII) \_\_\_\_\_ gateway firewalls are deployed in application-layer of OSI model.
- A) Packet Filtering Firewalls
  - B) Circuit Level Gateway Firewalls
  - C) Application-level Gateway Firewalls
  - D) Stateful Multilayer Inspection Firewalls
- (LIV) 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
- (LV) Backdoors are also known as \_\_\_\_\_
- A) Trap doors
  - B) Front doors
  - C) Cover doors
  - D) Back entry
- (LVI) \_\_\_\_\_ are a specific section of any virus or malware that performs illicit activities in a system.
- A) Malicious programs
  - B) Worms
  - C) Spyware
  - D) Payload
- (LVII) \_\_\_\_\_ suite is used for NTP enumeration.
- A) DNS
  - B) NTP
  - C) HTTP
  - D) SNMP
- (LVIII) Which of the following is the port number for SSH (Secure Shell)?

- A) 20
- C) 22

- B) 21
- D) 23

(LIX) Enumeration is done to gain information. Which of the following cannot be achieved using enumeration?

- A) Ip tables
- C) Private chats

- B) SNMP data, if not secured appropriately
- D) List of username and password policies

(LX) Packet filtering firewalls work effectively in \_\_\_\_\_ networks.

- A) Very simple
- C) Large

- B) Smaller
- D) Very large complex