BRAINWARE UNIVERSITY

Term End Examination 2020 - 21

Programme – Master of Science in Advanced Networking & Cyber Security

Course Name – Ethical hacking and Digital Forensic Tools

Course Code - MNCS304

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) In which year the term hacking was coined?

a) 1965-67 b) 1955-60

c) 1970-80 d) 1980-82

(ii) From where the term 'hacker' first came to existence?

a) MIT b) Stanford University

c) California d) Bell's Lab

(iii) The full form of Malware is _____

a) Malfunctioned Software b) Multipurpose Software

c) Malicious Software d) Malfunctioning of Security

(iv) 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

(v) _____ 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

(vi) 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) Hactivism

(vii) 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

(viii) 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

(ix) 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

(x) Which of them is not a wireless attack?

a) Eavesdropping
b) MAC Spoofing
c) Wireless Hijacking
d) Phishing

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

a) Keyhijacking
b) Keyjacking
c) Keylogging
d) Keyboard monitoring

(xii) _____ are the special type of programs used for recording and tracking user's keystroke

a) Keylogger
b) Trojans
c) Virus
d) Worms

(xiii) _____ is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish political gain.

a) Cyber-warfare
b) Cyber campaign
c) Cyber-terrorism
d) Cyber attack

(xiv) _____ 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

(xv) From the options below, which of them is not a threat to information security?

a) Disaster
b) Eavesdropping
c) Information leakage
d) Unchanged default password

(xvi) 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

(xvii) Compromising confidential information comes under _____

a) Bug
b) Threat
c) Vulnerability
d) Attack

(xviii) How many basic processes or steps are there in ethical hacking?

a) 4
b) 5
c) 6
d) 7

(xix) Which of the following is not a reconnaissance tool or technique for information gathering?

a) Hping
b) NMAP
c) Google Dorks
d) Nexpose

(xx) _____ phase in ethical hacking is known as the pre-attack phase.

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

(xxi) While looking for a single entry point where penetration testers can test the vulnerability, they use _____ phase of ethical hacking.

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

(xxii) Which of them does not comes under scanning methodologies?

a) Vulnerability scanning
b) Sweeping
c) Port Scanning
d) Google Dorks

(xxiii) Which of them is not a scanning tool?

a) NMAP
b) Nexpose
c) Maltego
d) Nessus

(xxiv) _____ ensures the integrity and security of data that are passing over a network.

a) Firewall
b) Antivirus
c) Pentesting Tools
d) Network-security protocols

(xxv) Which of the following is not a strong security protocol?

a) HTTPS
b) SSL
c) SMTP
d) SFTP

(xxvi) Which of the following is not a secured mail transferring methodology?

a) POP3
b) SSMTP
c) Mail using PGP
d) S/MIME

(xxvii) _____ is a set of conventions & rules set for communicating two or more devices residing in the same network?

a) Security policies
b) Protocols
c) Wireless network
d) Network algorithms

(xxviii) HTTPS is abbreviated as _____

a) Hypertexts Transfer Protocol Secured
b) Secured Hyper Text Transfer Protocol
c) Hyperlinked Text Transfer Protocol Secured
d) Hyper Text Transfer Protocol Secure

(xxix) _____ is any action that might compromise cyber-security.

a) Threat
b) Vulnerability
c) Exploit
d) Attack

(xxx) _____ is the method of developing or creating a structurally similar yet unauthentic and illegitimate data of any firm or company.

a) Data copying
b) Data masking
c) Data breaching
d) Data duplicating

(xxxi) Data masking is also known as _____

a) Data obfuscation
b) Data copying
c) Data breaching
d) Data duplicating

(xxxii) Backdoors are also known as _____

a) Trap doors
b) Front doors
c) Cover doors
d) Back entry

(xxxiii) Adware are pre-chosen _____ developed to display ads.

a) banner
b) software
c) malware
d) shareware

(xxxiv) _____ 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

(xxxv) Finding & publishing any user's identity with the help of different personal details is called _____

a) Doxing
b) Data breaching
c) Personal data copying
d) Secure File Transferring Protocol

(xxxvi) Whaling is the technique used to take deep and _____ information about any individual.

a) sensitive
b) powerful
c) useless
d) casual

(xxxvii) _____ is an attempt to steal, spy, damage or destroy computer systems, networks or their associated information.

a) Cyber-security
b) Cyber attack
c) Digital hacking
d) Computer security

(xxxviii) _____ is a device which secretly collects data from credit / debit cards.

a) Card Skimmer
b) Data Stealer
c) Card Copier
d) Card cloner

(xxxix) _____ is the practice implemented to spy someone using technology for gathering sensitive information.

a) Cyber espionage
b) Cyber-spy
c) Digital Spying
d) Spyware

(xl) Zero-day exploits are also called _____

a) Zero-day attacks
b) Hidden attacks
c) Un-patched attacks
d) Un-fixed exploits

(xli) Physical ports are usually referred to as _____

a) Jacks
b) Cables
c) Interfaces
d) Hardware plugs

(xlii) Number of logical ports ranges from _____ to _____

a) 0, 255
b) 1, 65535
c) 1, 65536
d) 0, 65536

(xliii) _____ needs some control for data flow on each and every logical port.

a) Antivirus
b) Network firewall
c) Intrusion Detection Systems (IDS)
d) Anti-malware

(xliv) Which of the following is the port number for Telnet?

a) 20
b) 21
c) 22
d) 23

(xlv) Firewalls can be of _____ kinds.

a) 1 b) 2

c) 3 d) 4

(xlvi) Firewall examines each _____ that are entering or leaving the internal network.

a) Emails users b) Updates

c) Connections d) Data packets

(xlvii) A firewall protects which of the following attacks?

a) Phishing b) Dumpster diving

c) Denial of Service (DoS) d) Shoulder surfing

(xlviii) There are _____ types of firewall.

a) 5 b) 4

c) 3 d) 2

(xlix) Packet filtering firewalls are deployed on _____

a) Routers b) Switches

c) Hubs d) Repeaters

(l) In the _____ layer of OSI model, packet filtering firewalls are implemented

a) Application layer b) Session layer

c) Presentation layer d) Network layer

(li) One advantage of Packet Filtering firewall is _____

a) More efficient b) Less complex

c) Less costly d) Very fast

(lii) Packet filtering firewalls work effectively in _____ networks.

a) Very simple
b) Smaller
c) Large
d) Very large complex

(liii) Which of these comes under the advantage of Circuit-level gateway firewalls?

a) They maintain anonymity and also inexpensive
b) They are light-weight
c) They're expensive yet efficient
d) They preserve IP address privacy yet expensive

(liv) _____ 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

(lv) Packet filtering firewalls are also called _____

a) First generation firewalls
b) Second generation firewalls
c) Third generation firewalls
d) Fourth generation firewalls

(lvi) Stateful Multilayer firewalls are also called _____

a) First generation firewalls
b) Second generation firewalls
c) Third generation firewalls
d) Fourth generation firewalls

(lvii) 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

(lviii) _____ is a widespread app's coding mistake made by developers which could be exploited by an attacker for gaining access or malfunctioning your system.

a) Memory leakage
b) Buffer-overrun
c) Less processing power
d) Inefficient programming

(lix) Buffer-overflow may remain as a bug in apps if _____ are not done fully.

a) Boundary hacks
b) Memory checks
c) Boundary checks
d) Buffer checks

(lx) Old operating systems like _____ and NT-based systems have buffer-overflow attack a common vulnerability.

a) Windows 7
b) Chrome
c) IOS12
d) UNIX