BRAINWARE UNIVERSITY

Term End Examination 2021 - 22
Programme – Bachelor of Science (Honours) in Advanced Networking & Cyber Security
Course Name – Hacking Techniques, Tools and Incident Handling
Course Code - BNCSC601
(Semester VI)

Time allotted : 1 Hrs.15 Min. **Full Marks : 60**

[The figure in the margin indicates full marks.]

Group-A

(Multiple Choice Type Question) 1 x 60=60

Choose the correct alternative from the following :

(1) In which of the following, a person is constantly followed/chased by another person or gro up of several peoples?

a) A. Phishing b) B. Bulling
c) C. Stalking d) D .Identity theft

(2) Which one of the following can be considered as the class of computer threats?

a) A. Dos Attack b) B. Phishing
c) C. Soliciting d) D. Both A and C

(3) Which of the following refers to the violation of the principle if a computer is no more acc essible?

a) A. Access control b) B. Confidentiality
c) C. Availability d) D. All of the above

(4) Which one of the following usually used in the process of Wi-Fi-hacking?

a) A. Aircrack-ng b) B. Wireshark
c) C. Norton d) D. All of the above

(5) In ethical hacking and cyber security, there are _______ types of scanning:

a) A. 1 b) B. 2
c) C. 3 d) D. 4

(6) Which one of the following is actually considered as the first computer virus?

a) A. Sasser b) B. Blaster
c) C. Creeper d) D. Both A and C

(7) A hacker who plants a rogue wireless access point on a network in order to sniff the traffic on the wired network from outside the building is causing what type of security breach?

a) A. Physical b) B. Technical
c) C. Operational d) D. Remote access

(8) Which of the following is a reason to use Linux?

a) A. Linux has no security holes.
b) B. Linux is always up to date on security patc hes.
c) C. No rootkits can infect a Linux system.
d) D. Linux is flexible and can be modified.

(9) A system that performs attack recognition and alerting for a network is what?

a) A. HIDS
b) B. NIDS
c) C. Anomaly detection HIDS
d) D. Signature-based NIDS

(10) Which of the following is a honeypot-detection tool?

a) A. Honeyd
b) B. Specter
c) C. KFSensor
d) D. Sobek

(11) What is the command to install and run Snort?

a) A. snort –l c:\snort\log –c C:\snort\etc\snoft.co nf –A console
b) B. snort –c C:\snort\etc\snoft.conf –A console
c) C. snort –c C:\snort\etc\snoft.conf console
d) D. snort –l c:\snort\log –c –A

(12) What are the ways in which an IDS is able to detect intrusion attempts? (Choose all that a pply.)

a) A. Signature detection
b) B. Anomaly detection
c) C. Traffic identification
d) D. Protocol analysis

(13) How many keys exist is in a public/private key pair?

a) A. 1
b) B. 2
c) C. 3
d) D. 4

(14) What is the purpose of a pen test?

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

(15) Which of the following is an NMAP script that could help detect HTTP Methods such as GET,POST, HEAD, PUT, DELETE, TRACE?

a) A. http-git
b) B. http-headers
c) C. http enum
d) D. http-methods

(16) Which framework made cracking of vulnerabilities easy like point and click.

a) A. .NET
b) B. Metasploit
c) C. Zeus
d) D. Ettercap

(17) Nmap is abbreviated as

a) A. Network Mapper
b) B. New Mappping
c) C. Network Manager
d) D. Network Mac Address

(18) Which is a debugger and exploration tool.

a) A. Netdog
b) B. Netcat
c) C. Tcpdump
d) D. BackTrack

(19) Which is the popular command-line packet analyser.

a) A. Wireshark
b) B. Snort
c) C. Metasploit
d) D. Tcpdump

(20) Of the following, which is the best way for a person to find out what security holes exist o n the network?

a) A. Run a port scan
b) B. Use a network sniffer

c) C. Perform a vulnerability assessment
d) D. Use an IDS solution

(21) After using Nmap to do a port scan of your server, you find that several ports are open. W hich of the following should you do next?

a) A. Leave the ports open and monitor them for malicious attacks.
b) B. Run the port scan again.
c) C. Close all ports.
d) D. Examine the services and/or processes that use those ports.

(22) Which of the following tools uses ICMP as its main underlying protocol?

a) A. Ping scanner
b) B. Port scanner
c) C. Image scanner
d) D. Barcode scanner

(23) Which of the following is used when performing a quantitative risk analysis?

a) A. Asset value
b) B. Surveys
c) C. Focus groups
d) D. Best practices

(24) Which attack is a type of attack against an application that parses XML input.

a) A. Injection
b) B. HTML
c) C. XXE
d) D. XSS

(25) Which tool was made by OWASP Foundation

a) A. Metasploit
b) B. Nessus
c) C. ZAP
d) D.Nmap

(26) What is your digital footprint?

a) A. A scanned image of your foot
b) B. A photograph of your shoe
c) C.Having a blog, facebook or twitter page
d) D.All the information online about a person th at is stored online.

(27) Maltego used for

a) A. OSI
b) B. Information gathering
c) C. Forensic
d) D. Traffic analyzer

(28) Using which tool you can intercept HTTP requests

a) A. Burpsuite
b) B.Nmap
c) C.Nikto
d) D.SQLmap

(29) What are the major components of the intrusion detection system?

a) A. Analysis Engine
b) B. Event provider
c) C. Alert Database
d) D. All of the mentioned

(30) What are the different ways to classify an IDS?

a) A. Zone based
b) B. Host & Network based
c) C. Network & Zone based
d) D. Level based

(31) Which is the tool used for IDS

a) A. Suricata
b) B. Nessus
c) C. Wazuh
d) D. Pfsense

(32) What is the primary goal of an Ethical Hacker?

a) A. Avoiding detection
b) B. Determining return on investment (ROI) fo r security measures
c) C. Resolving security vulnerabilities
d) D. Testing security controls

(33) Robert has added an apostrophe after an ?id= parameter within the URL of a webpage. Sh e now sees an error, saying there was a syntax error. What did Robert find?

a) A. Cross-Site Scripting vulnerability
b) B. PostgreSQL database exploit

c) C. SQL Injection
d) D. Broken Authtication

(34) What is ESSID?

a) A. MAC address of a connected client
b) B. MAC address of a target access point
c) C. Network name
d) D. Host name

(35) What is the preferred communications method used with systems on a bot-net?

a) A. IRC
b) B. E-mail
c) C. ICMP
d) D. TFTP

(36) What are the forms of password cracking techniques?

a) A. AttackBrute Forcing
b) B. AttacksHybrid
c) C. AttackSyllable
d) D. All of the above

(37) What is the attack called "evil twin_x009d_?

a) A. MAC spoofing
b) B. ARP poisoning
c) C. Rogue access point
d) D. Session hijacking

(38) An ethical hacker is trying to breach a website through SQL Injection. He also changed hi s User-Agent HTTP header, sent by his browser.What can he achieve with this action?

a) A. He acquires a matching SSL connection.
b) B. He obtains better performance of the websi te so that it responds faster to his requests.
c) C. He prevents forensics from revealing his re al browser that was used during the attack
d) D. He acquires a dublicate instance MAC addr ess so he can hide his identity

(39) What is the meaning of NOP?

a) A. Network Operation
b) B. No Operation
c) C. No one Point
d) D. None of the above

(40) What is the sequence of a TCP connection?

a) A. SYN-ACK
b) B. SYN-ACK-FIN
c) C. SYN-SYN-ACK
d) D. SYN-SYN ACK-ACK

(41) Which form of encryption does WPA use?

a) A. LEAP
b) B. TKIP
c) C. Shared key
d) D. None of the above

(42) What are the four Regional internet registries?

a) A. APNIC, PICNIC, NANIC, ARIN
b) B. APNIC, MOSTNIC, ARIN, RIPE NCC
c) C. APNIC, LACNIC, ARIN, RIPE NCC
d) D. APNIC, PICNIC, NANIC, RIPE NCC

(43) HTTPs uses which port number?

a) A. 21
b) B. 53
c) C. 80
d) D. 443

(44) Which of the following is a passive wireless discovery tool?

a) A. Kismet
b) B. Aircrack
c) C. Netsniff
d) D. NetStumbler

(45) Which type of hacker represents the highest risk to your network?

a) A. Script kiddies
b) B. Grey-hat hackers
c) C. Black-hat hackers
d) D. Disgruntled employees

(46) Banner grabbing is an example of what?

a) A. Footprinting
b) B. Application analysis
c) C. Active operating system fingerprinting
d) D. Passive operating system fingerprinting

(47) Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

a) A. Malware
b) B. Spyware
c) C. Adware
d) D. All of the above

(48) Which one of the following refers to the technique used for verifying the integrity of the message?

a) A. Digital signature
b) B. Decryption algorithm
c) C. Protocol
d) D. Message Digest

(49) In system hacking, which of the following is the most crucial activity?

a) A. Information gathering
b) B. Covering tracks
c) C. Cracking passwords
d) D. None of the above

(50) Which of the following statements is true about the VPN in Network security?

a) A. It is a type of device that helps to ensure th at communication between a device and a net work is secure.
b) B. It is usually based on the IPsec(IP Securit y) or SSL (Secure Sockets Layer)
c) C. It typically creates a secure, encrypted virtu al "tunnel" over the open internet
d) D. All of the above

(51) Which of the following type of text is transformed with the help of a cipher algorithm?

a) A. Transformed text
b) B. Complex text
c) C. Scalar text
d) D. Plain text

(52) In order to ensure the security of the data/ information, we need to ____________ the data

a) A. Encrypt
b) B. Decrypt
c) C. Delete
d) D. None of the above

(53) The full form of Malware is

a) A. Malfunctioned software
b) B. Multipurpose software
c) C. Malicious software
d) D. Malfunctioning software

(54) What are the types of scannings used in Ethical hacking?

a) Port scanning
b) Network scanning
c) Vulnerability scanning
d) All of the above

(55) Which are the port scanning tools?

a) Nmap
b) Metasploit
c) Burp Suite
d) Searchsploit

(56) Which one is social engineering attacks?

a) Brute force attack
b) Phishing attack
c) Man-in-the-middle attack
d) Side-channel attack

(57) Which one is the alternative CLI tools for ExploitDB

a) Powersploit
b) Searchsploit
c) Metasploit
d) Xerosploit

(58) Which one is not a primary choice as an OS for security professional?

a) Kali
b) Parrot
c) Windows
d) Black-Arch

(59) Wordlist generation tools for Brute-force attacks?

a) Cewl & Crunch
b) Nikto
c) Nmap
d) Nessus

(60) Metasploit is written in which programming language?

a) Python
b) Ruby
c) Perl
d) Golang