BRAINWARE UNIVERSITY

Term End Examination 2021 - 22

Programme – Bachelor of Science (Honours) in Advanced Networking & Cyber Security

Course Name – Vulnerability Analysis / Penetration Testing

Course Code - BNCSD601B

(Semester VI)

Time : 1 Hr.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) Is penetration testing used for helping or for damaging a system?

a) Damaging b) Helping

c) I don't know d) none of these

(2) What is a risk involved in doing penetration testing?

a) You have to pay for the testing b) Some operations of the company might slow down.

c) Skynet takes over the world d) none of these

(3) On which is the National Vulnerability Database primarily built upon?

a) Vulnerabilities b) NVD

c) Patch d) CVE identifiers

(4) What are the gateways by which threats are manifested?

a) Ports b) Computer Networks

c) Patches d) Vulnerabilities

(5) Find the wrong statement about penetration testing

a) It is an unintentional attack b) Pen-testing is used for security assessment

c) Pen testing improves the security of the system d) Pen testing does discovers security weaknesses

(6) Which stage does not verify or try to exploit the vulnerability, just lists and ranks the identified weaknesses

a) Vulnerability assessment b) Vulnerability scan

c) none of these

(7) What remains the same in both internal and external testing?

a) The target b) The attacker

c) the hacker
d) none of these

(8) _____ saves time and resources, but is not accurate or professional
a) Automated pentesting
b) Manual testing
c) Hybrid testing
d) none of these

(9) Which of the following files in Linux is used to store account passwords?
a) /etc/passwd
b) /etc/password
c) /etc/login
d) /etc/shadow

(10) Which of the following TCP flags is used for closing a connection?
a) ACK
b) RST
c) PSH
d) FIN

(11) A _____ is a software bug that attackers can take advantage to gain unauthorized access in a system.
a) a) System error
b) b) Bugged system
c) c) Security bug
d) d) System virus

(12) What is the command to find MAC address in windows ?
a) ipconfig
b) get mac
c) getmac /v
d) none

(13) What translates IP address into MAC address?
a) a) Organizationally Unique Identifier
b) b) Address Resolution Protocol
c) c) Network Interface Card
d) d) Burned In Address

(14) For discovering the OS running on the target system, the scanning has a specific term. What is it?
a) A : Footprinting
b) B : Fingerprinting
c) C : 3D Printing
d) D : screen-printing

(15) _____ scanning is an automatic process for identifying vulnerabilities of the system within a network.
a) A : Network
b) B : Port
c) C : Vulnerability
d) D : System

(16) Command to scan port 80, 443,8080
a) nmap -p 80,443,8080
b) nmap -p 80-8080
c) nmap -p [80,443,8080]
d) nmap -p 80:443:8080

(17) Save scan result in plain text file
a) nmap -oN result.txt
b) nmap -oX result.txt
c) nmap -oG result.txt
d) It can't save in plain text format

(18) Which of the following tech-concepts cannot be sniffed?
a) a) Cloud sessions
b) b) FTP passwords
c) c) Telnet passwords
d) d) Chat sessions

(19) Active sniffing is difficult to detect.
a) a) True
b) b) False

(20) Which of them is not an objective of sniffing for hackers?
a) a) Fetching passwords
b) b) Email texts
c) c) Types of files transferred
d) d) Geographic location of a user

(21) Which tool can be used to perform a DNS zone transfer on Windows?
a) DNSlookup
b) nslookup

c) whois
d) ipconfig

(22) Which command is used to display the ARP table

a) arp
b) arp -a
c) arp -d
d) arp -all

(23) DNS stands for _____

a) a) Data Name System
b) b) Domain Name Server
c) c) Domain Name System
d) d) Domain's Naming System

(24) Which of the following is not an example of DNS hijacking?

a) a) ISP DNS hijacking
b) b) DNS hijacking for phishing
c) c) DNS hijacking for pharming
d) d) HTTP-based DNS hacking

(25) DNS poisoning is very dangerous because it can extend its reach from one _____ _ to another.

a) a) ISP server
b) b) DNS server
c) c) Linux server
d) d) Domain user

(26) The user could be influenced by DNS hijacking if the government of that country uses DNS redirecting as a mechanism to mask censorship

a) DNS lookup
b) DNS Hijacking
c) DNS Spoofing
d) None

(27) Some security issues might exist owing to misconfigured _____ which can direct to disclosure of information regarding the domain.

a) A : DNS names
b) B : HTTP setup
c) C : ISP setup
d) D : FTP-unsecured

(28) Which one of the following allows client to update their DNS entry as their IP address change?

a) Dynamic DNS
b) authoritative name server
c) mail transfer agent
d) None of the above

(29) What does HTTP do?

a) a) Enables network resources and reduces pe rception of latency
b) b) Reduces perception of latency and allows multiple concurrency exchange
c) c) Allows multiple concurrent exchange and enables network resources
d) d) Enables network resources and reduces pe rception of latency and Allows multiple conc urrent exchange

(30) Response is made up of a _____ status code.

a) a) two-digit
b) b) three-digit
c) c) five-digit
d) d) six-digit

(31) HTTP expands?

a) a) HyperText Transfer Protocol
b) b) HyperTerminal Transfer Protocol
c) c) HyperText Terminal Protocol
d) d) HyperTerminal Text Protocol

(32) BeEF is short for

a) Browser Exploitation Framework
b) Browser Framework
c) Browser Exploitation
d) None

(33) Where are Windows 10 passwords stored?

a) C:\Windows\System32\drivers\etc\hosts
b) C:\windows\system32\config\SAM
c) C:\Windows\security\database\secedit.sdb
d) None

(34) Which one of them is not a network scanner?

a) 1. NMAP
b) 2. Qualys
c) 3. SoftPerfect
d) 4. Netcat

(35) Key loggers are form of

a) A. Spyware
b) B. Shoulder surfing
c) C. Trojan
d) D. Social engineering

(36) What is purpose of Denial of Service attacks?

a) A. Exploit weakness in TCP/IP attack.
b) B. To execute a trojan horse on a system.
c) C. To overload a system so it is no longer operational.
d) D. To shutdown services by turning them of f.

(37) What port does http use?

a) A. 22
b) B. 80
c) C. 20
d) D. 23

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

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

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

a) A. Reconnaissance
b) B. Maintaining Access
c) C. Scanning
d) D. Gaining Access

(40) _____ is a popular IP address and port scanner.

a) A. Cain and Abel
b) B. Snort
c) C. Angry IP Scanner
d) D. Ettercap

(41) _____ framework made cracking of vulnerabilities easy like point and click.

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

(42) Aircrack-ng is used for _____

a) A. Firewall bypassing
b) B. Wi-Fi attacks
c) C. Packet filtering
d) D. System password cracking

(43) DOS stands for

a) A. Detection of system
b) B. Denial of Service
c) C. Detection of service
d) D. None of above

(44) In MetaSploit, Which command attacks the target machine?

a) a) attack
b) b) exploit
c) c) offense
d) d) hack

(45) Which programming language can be used to write Metasploit scripts for Metasploit 4. x Framework?

a) a) C
b) b) Python
c) c) C#
d) d) Ruby

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

a) Information gathering
b) Covering tracks
c) Cracking passwords
d) None of the above

(47) Which of the following can be considered as the elements of cyber security?

a) Application Security
b) Operational Security
c) Network Security
d) All of the above

(48) In Wi-Fi Security, which of the following protocol is more used?

a) WPA
b) WPA2
c) WPS
d) Both A and C

(49) The term "TCP/IP" stands for_____

a) Transmission Contribution protocol/ internet protocol
b) Transaction Control protocol/ internet protoc ol
c) Transmission Control Protocol/ internet prot ocol
d) Transmission Control Protocol/ intranet prot ocol

(50) which protocol is used for sending and receiving e-mail between e-mail clients and ser vers

a) SMTP
b) FTP
c) HTTPS
d) HTTP

(51) Which of them is not a proper method for email security?

a) a) Use Strong password
b) b) Use email Encryption
c) c) Spam filters and malware scanners
d) d) Click on unknown links to explore

(52) In order to infect a system, clicking an email attachment must cause which of the follo wing conditions to occur?

a) the attachment is saved to the disk
b) the attachment is decompressed
c) the attachment opens in a preview editor
d) the attachment executes

(53) What is a keylogger?

a) Software that that records keys you set when encrypting files
b) Software that records keystrokes made on a keyboard
c) Software used to log all attempts to access a certain file
d) Software that steals passwords or "keys" that you have saved on your computer

(54) Example of a good password is

a) a.name of a partner or spouse
b) b.name of a child or pet
c) c.word related to a job or hobby
d) d. words contains multiple random digits

(55) Which of the following is used for monitoring traffic and analyzing network flow?

a) Managed detection and response
b) Cloud access security broker
c) Network traffic analysis
d) Network Security Firewall

(56) Which of the following is not a cybercrime?

a) a) Denial of Service
b) b) Man in the Middle
c) c) Malware
d) d) AES

(57) Which of the following is the least strong securlty encryption standard?

a) a) WPA3
b) b) WPA2
c) c) WPA
d) d) WEP

(58) Which of the following DDoS in mobile systems wait for the owner to trigger the cybe r attack?

a) a) botnets
b) b) programs
c) c) virus
d) d) worms

(59) Which of the following is not an email-related hacking tool?

a) a) Mail Password
b) b) Email Finder Pro
c) c) Mail PassView
d) d) Sendinc

(60) When you use the $_GET variable to collect data, the data is visible to _____

a) only you
b) everyone

c) selected few

d) none