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 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) 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) Which of the following are ways to conduct penetration testing?

a) Black Box testing, White Box testing, Grey Box Testing b) Black Box testing, Red Box Testing, Grey Box Testing

c) White Box testing, Brown Box Testing, Red Box Testing d) Black Box testing, Green Box Testing, White Box Testing

(3) 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

(4) Vulnerability analysis is also known as:

a) Penetration testing b) Penetration testing

c) Vulnerability assessment d) none of these

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

a) Vulnerabilities b) NVD

c) Patch d) CVE identifiers

(6) Which is a dictionary of common names for publicly known information security vulnerabilities?

a) Vulnerability b) Zero day

c) SANS Top 20 controls d) Common Vulnerabilities and Exposures

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

a) Ports b) Computer Networks

c) Patches
d) Vulnerabilities

(8) Which of the following can you use as a foundation when building a vulnerability assessment report?

a) Tools
b) Nmap
c) SQL Injection
d) none of these

(9) 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

(10) Which of the following servers works as a daemon at the back end when a client is used at the front end?

a) Nessus
b) IBM Security AppScan
c) MBSA
d) iScanOnline

(11) 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

(12) ______ testing aims to exploit identified vulnerabilities to check what information is exposed to the

a) Internal
b) External

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

a) The target
b) The attacker
c) the hacker
d) none of these

(14) Which attack can be much more devastating?

a) External attacks
b) Internal attacks

(15) __________ saves time and resources, but is not accurate or professional

a) Automated pentesting
b) Manual testing
c) Hybrid testing
d) none of these

(16) Pen testers will use _____ to protect the possibility of data leakage and add another layer of security

a) Code review
b) vulnerability scan
c) manual testing
d) none of these

(17) 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

(18) Which of the following protocols is used for translating IP addresses to MAC addresses?

a) DHCP
b) DNS
c) ARP
d) UDP

(19) Which of the following TCP flags is used for closing a connection?

a) ACK
b) RST
c) PSH
d) FIN

(20) Which of the following functions in Python is used to accept input from user?

a) a. raw-input()
b) b. read_raw()
c) c. raw_input()
d) d. get_inputs()

(21) A _________ is a software bug that attackers can take advantage to gain unauthorized acc

ess in a system.

a) a) System error
b) b) Bugged system
c) c) Security bug
d) d) System virus

(22) A zero-day vulnerability is a type of vulnerability unknown to the creator or vendor of the system or software

a) a) True
b) b) False

(23) What is the command to find MAC address in windows ?

a) ipconfig
b) get mac
c) getmac /v
d) none

(24) MAC stands for ________

a) a) Media Area Control
b) b) Memory Access Control
c) c) Memory Area Control
d) d) Media Access Control

(25) 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

(26) Which of them is not a scanning methodology?

a) A : Check for live systems
b) B : Check for open ports
c) C : Identifying the malware in the system
d) D : Identifying of services

(27) For discovering the OS running on the target system, the scanning has a specific term. Wh at is it?

a) A : Footprinting
b) B : Fingerprinting
c) C : 3D Printing
d) D : screen-printing

(28) Ping sweep is also known as ________________

a) A : ICMP Sweep
b) B : ICMP Call
c) C : IGMP Sweep
d) D : ICMP pinging

(29) _____________ scanning is an automatic process for identifying vulnerabilities of the syst em within a network.

a) A : Network
b) B : Port
c) C : Vulnerability
d) D : System

(30) Command to to detect if any packet filters or Firewall is used by host

a) nmap -sA
b) nmap -pA
c) nmap -PA
d) nmap -sN

(31) 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

(32) Perform a stealth scan

a) nmap -PS
b) nmap -sS
c) nmap –stealth
d) nmap -sT

(33) 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

(34) Nmap by default use _______ scan

a) SYN
b) TCP
c) SYN+ACK
d) FIN

(35) 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

(36) Which of the following is not a sniffing tool?

a) a) Wireshark
b) b) Maltego
c) c) Look@LAN
d) d) none

(37) Active sniffing is difficult to detect.

a) a) True
b) b) False

(38) Which of the below-mentioned protocol is not susceptible to sniffing?

a) a) HTTP
b) b) SMTP
c) c) POP
d) d) TCP

(39) 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

(40) What port number does HTTPS use?

a) 53
b) 443
c) 80
d) 21

(41) Which tool can be used to perform a DNS zone transfer on Windows?

a) DNSlookup
b) nslookup
c) whois
d) ipconfig

(42) arp spoofing is what type of attacks ?

a) Buffer overflow
b) Brute Force
c) MITM
d) None

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

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

(44) ARP only works with _____ IP addresses

a) 32-bit
b) 64-bit
c) none

(45) DNS stands for _____________

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

(46) ______________ is a form of nasty online attack in which a user gets redirects queries to a DNS because of override of system's TCP/IP settings.

a) a) DNS mal-functioning
b) b) DNS cracking
c) c) DNS redirecting
d) d) DNS hijacking

(47) 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

(48) A ______________ is essentially a text file residing on the server that hosts different dom ain containing entries for dissimilar resource records.

a) a) Zone file
b) b) Robot file
c) c) Bot file
d) d) DNS file

(49) DNS poisoning is very dangerous because it can extend its reach from one ___________ t

o another.

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

(50) The ____________ Domain Name Server data will get spread to the ISPs & will be cache d there.

a) a) working
b) b) compromised
c) c) corrupted
d) d) poisoned

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

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

(52) There are _________ main types of DNS hijacking

a) A : 4
b) B : 2
c) C : 3
d) D : 5

(53) Some security issues might exist owing to misconfigured __________________ which ca n direct to disclosure of information regarding the domain.

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

(54) Which one of the following allows client to update their DNS entry as their IP address cha nge?

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

(55) Response is made up of a ________ status code.

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

(56) BeEF is short for

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

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

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

(58) 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 oper ational.
d) D. To shutdown services by turning them off.

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

a) A. To create a stronger connection with the tar get
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

(60) __________ is a popular IP address and port scanner.

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