iNeuron

CSM – Cyber Security Questions

1. What is correct about digital signatures?
   a. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
   b. Digital signatures may be used in different documents of the same type.
   c. Digital signatures are issued once for each user and can be used everywhere until they expire.
   d. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.

2. A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?
   a. Black Hat
   b. White Hat
   c. Gray Hat
   d. Suicide Hacker

3. Which of the following steps for risk assessment methodology refers to vulnerability identification?

a. Identifies sources of harm to an IT system. (Natural, Human, Environmental)
b. Determines risk probability that vulnerability will be exploited (High, Medium, Low)
c. Assigns values to risk probabilities; Impact values.
d. Determines if any flaws exist in systems, policies, or procedures

4. By using a smart card and pin, you are using a two-factor authentication that satisfies

a. Something you know and something you are
b. Something you are and something you remember
c. Something you have and something you are
d. Something you have and something you know

5. A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway, they are both on the 192.168.1.0/24. Which of the following has occurred?

a. The computer is not using a private IP address
b. The gateway is not routing to a public IP address
c. The computer is using an invalid IP address
d. The gateway and the computer are not on the same network

6. PGP, SSL, and IKE are all examples of which type of cryptography?

a. Public Key
b. Digest
c. Hash Algorithm
d. Secret Key

7. Which of the following Linux commands will resolve a domain name into IP address?

a. host -t soa hackeddomain.com
b. host -t a hackeddomain.com
c. host -t AXFR hackeddomain.com
d. host -t ns hackeddomain.com

8. Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users

a. LDAP Injection attack
b. SQL injection attack
c. Cross-Site Scripting (XSS)
d. Cross-Site Request Forgery (CSRF)

9. env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd' What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?

a. Changes all passwords in passwd
b. Removes the passwd file
c. Add new user to the passwd file
d. Display passwd content to prompt

10. ___________is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

a. Resource transfer
b. Resource records
c. Zone transfer
d. DNSSEC

11. To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program. What term is commonly used when referring to this type of testing?

a. Mutating
b. Randomizing
c. Bounding
d. Fuzzing

12. While using your bank's online servicing you notice the following string in the URL bar: http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21 You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes. Which type of vulnerability is present on this site?

a. Web Parameter Tampering
b. SQL injection
c. XSS Reflection
d. Cookie Tampering

13. You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

a. Piggybacking
b. Tailgating
c. Social engineering
d. Eavesdropping

14. Hackers often raise the trust level of a phishing message by modelling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

a. Enumeration
b. Exploration
c. Reconnaissance
d. Investigation

15. Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

a. 113
b. 161
c. 96
d. 123

16. Which method of password cracking takes the most time and effort?

a. Dictionary attack
b. Rainbow tables
c. Brute force
d. Shoulder surfing

17. User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

a. Presentation
b. Transport
c. Session
d. Application

18. Scenario:1. Victim opens the attacker's web site. 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'. 3. Victim clicks to the interesting and attractive content URL. 4. Attacker creates a transparent 'iframe' in front of the URL which the victim attempts to click, so the victim thinks that

he/she clicks on the 'Do you want to make $1000 in a day?' URL but actually he/she clicks on the content or URL that exists in the transparent 'iframe' which is setup by the attacker. What is the name of the attack which is mentioned in the scenario?

a. Clickjacking Attack
b. Session Fixation
c. HTML Injection
d. HTTP Parameter Pollution

19. Which of the following is assured by the use of a hash?

a. Confidentiality
b. Authentication
c. Availability
d. Integrity

20. While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

a. Cross-Site Scripting
b. Cross-Site Request Forgery
c. Clickjacking
d. Web form input validation

21. Which system consists of a publicly available set of databases that contain domain name registration contact information?
a. CAPTCHA
b. WHOIS
c. IETF
d. IANA

22. Which of the category is old in OWASP Top 10 2017 to compare new OWASP Top 10 2021?
a. Broken Access Control
b. Insecure Design
c. Software and Data Integrity Failure
d. Server-Side Request Forgery (SSRF)

23. Which category includes XSS in OWASP Top 10 2021?
a. Broken Access Control
b. Insecure Design
c. Software and Data Integrity Failure
d. Injection

24. Which of the following files in Linux is used to store account passwords?

a. /etc/passwd
b. /etc/passwords
c. /etc/login
d**. /etc/shadow**

25. Which of the following value denotes full access (read/write/execute) to all users and groups?

a. 555
b. 666
c**. 777**
d. 077

26. You can add a row using SQL in a database with which of the following?
a. ADD
b. CREATE
c. INSERT
d. MAKE

27. A SQL query is terminated by which of the following symbols?
a. Single quote
b. Double quote
c. Exclamation mark
d. **Semicolon**

28. Which of the following is not a layer of the TCP/IP protocol?
a. Application Layer
b. **Session Layer**
c. Transport Layer
d. Internetwork layer

29. Port number 443 is used by which of the following?
a. FTP
b. SMTP
c. HTTPS
d. DHCP

30. Which of the following is not a benefit of virtualization?
a. Virtualization technology is eco-friendly.
b. Virtualization facilitates faster deployments.
c. **Virtualization increases overall cost.**
d. None of the above.

31. In computer security, which of the following means that computer system assets can be modified only by authorized parties?
a. Confidentiality
b**. Integrity**
c. Availability
d. Authenticity

32. A weakness in a system is known as a:

a. Risk
b. Threat
c. Exploit
d. **Vulnerability**

33. Which of the following is a small piece of information that is sent from a website to the client system and is retained for further tracking?

a. HTTP
b**. Cookie**
c. XML
d. None of the above

34. Which of the following would help prevent SQL injection?
a. Using HTTPS
b. Installing anti-virus software
c. **Using a parameterized query**
d. All of the above

35. ________________ hacking refers to mistreatment of applications through HTTP or HTTPS that can be done by manipulating the web application through its graphical web interface or by tampering the Uniform Resource Identifier (URI).
a. Android application
b. Web application
c. PC application
d. Cloud application

36. Which of the following is not an appropriate method of web application hacking?
a. XSS
b. CSRF
c. SQLi
d. Brute-force

37. Use of ________________ can bring external files and worms and virus along with it to the internal systems.
a. smart-watch
b. **pen drive**
c. laptop
d. iPod

38. Which of the following OSI layers is responsible for node-to-node routing of packets?
a. Physical layer
b. Transport layer
c**. Network layer**
d. Datalink layer

39. Mary has added an apostrophe after an? id= parameter within the URL of a webpage. She now sees an error, saying there was a syntax error. What did Mary find?

a. Cross-Site Scripting vulnerability

b. PostgreSQL database exploit

c. SQL Injection

d. XSS attack

40. A hacker managed to find an XSS vulnerability. Now she wants to take over sessions. Where does she need the data retrievable from?

a. document.session

b. session.cookie

c. **document.cookie**

d. document.write

41. A website's URL contains 'index.php?page=home.php'. The page=parameter allows remote URLs to be passed and it loads them.
What is this an example of?

a. **Remote File Inclusion**

b. Remote File Injection

c. Remote File Impersonation

d. Local File Inclusion

42. A client has said that he created a case-insensitive filter for 'script' from being inserted in any forms to prevent an XSS PoC. How can you bypass this?

a. <sCrIPt>alert(1);</ScRiPT>

b. <javascript>alert(1);</script>

c. **<img src=x onerror=alert(1)>**

d. <jAvaScript>alert(10);</alErt>

43. Web server will log which part of a GET request?

a. Hidden tags

b. Query Strings

c. Header

d. Cookies

44. Cross Site Scripting is an attack against

a. Client (Browser)

b. Database

c. Web Application

d. Web Server

45. "|/bin/ls -al" is a payload for which injection attack?

a. SQL Injection

b. HTML Injection

c. **OS Command Injection**

d. All the Above

46. Which of the following is most common intercepting tool?

a. Commix

b. BeEF

c. SQL Map

d. **Burpsuite**

47. Which of the following automated tools are used for SQLi attack?

a. **Sqlmap**

b. Commix

c. BeEF

d. Wireshark

48. Web application firewalls (WAFs) help prevent which application layer attack?

a. XSS

b. SQL injection

c. DDoS

d. All of the above

49. _______ is commonly known for providing backdoor access to the system for malicious users.

a. Trojans

b. Worms

c. Rootkits

d. Botnets

50. Threats can exploit assets if assets are not vulnerable.

a. False

b. True