1. When you collected important information on the target system, the type of that environment can be changed from \_\_\_\_\_\_ to \_\_\_\_\_\_\_?

a) secure, vulnerable

b) unknown, known

c) unknown, partially known

d) closed, open

2. An organization has both file server and backup server crashed at exactly the same time. By examining the servers, they find that critical operating system files were deleted. What kind of malware the servers were infected?

a.Worm

b.Crypto-malware

c.Trojan

d.Logic bomb

3. Each time you open a web browser, you see different pop-up ads every few minutes. It doesn't matter which websites are being visited, the pop-ups still appear. What type of attack does this sound like?

a.Ransomware

b.A potentially unwanted program

c.Worm

d.Virus

4. Weak configurations can include which of the following?

a. Firmware

b. Open ports

c. Lack of vendor support

d. Use of secure protocols

5. What is the purpose of HTTPS?

a. To enhance communication protocols

b. To implement Single Sign-On

c. To allow enumeration and monitoring of network resources

d. To use SSL or TLS to encrypt a channel over which HTTP traffic is transmitted

6. Your scan your network and notice that a large number of address changes to the MAC tables and lots of ARP and RARP messages. What kind of attack are you facing?

a. DNS poisoning

b. Disassociation attack

c. MAC flooding attack

d. Jamming attack

7. Whenever you visit Google, you see a certificate warning. Observating the network traffic, you notice that all HTTP and HTTPS requests are being routed to the same IP regardless of destination. What kind of attack are you facing?

a. Evil twin

b. Disassociation

c. Man in the middle

d. MAC cloning

8. You notice your PC injected with a malware loaded on startup and also loads a file called netutilities.dll each time Microsoft Word is opened. What kind of attack are you facing?

a. System infection

b. DLL injection

c. Race condition

d. Memory overflow

9. Your PC is much slower than usual. You see CPU utilization is extremely high and a running process called "btmine" affected the system. You also find that your systems is communicating with an IP address outside your country on UDP port 43232. When you disconnect the network connection, the CPU utilization drops significantly. What type of malware the system infected?

a. Dictionary

b. Hybrid attack

c. Rainbow tables

d. Crypto-malware

10. Which of the following are most vulnerable to injection attacks?

a. SQL queries based on user input

b. Session ID

c. Network Transport

d. Registry Keys

11. What is a weakness of the DNS protocol?

a. TCP can be used for large transfers such as zone transfers

b. Its encryption capabilities are slow

c. It is not scalable

d. Requests and replies are sent in plaintext

12. Understanding how a hacker attacks will help you can develop a defensive framwork by using which of the following?

a. Automated Indicator Sharing

b. Predictive analysis

c. Adversary Tactics, Techniques, and Procedures

d. Threat maps

13. What is the most important first step in a penetration test?

a. Collect important information

b. Persistence

c. Reconnaissance

d. Privilege escalation

14. Which of the following techniques can not be used to prevent SQL injection?

a. Least privilege of database account

b. Parameterized queries

c. All of the above

d. Stored procedures

15. What should you do to address weak configurations?

a. Remove unnecessary apps

b. All of above

c. Change default usernames and passwords

d. Disable unnecessary services

16. Which below version is the most secure protocol?

a. TLSv 1.1

b. HTTP

c. SSL

d. TLSv 1.3

17. How can proxy servers improve security?

a. They use TLS-based encryption to access all sites

b. They can control which sites and content employees access

c. They enforce appropriate use of company resources

d. They prevent access to phishing sites

18. Your website is crashing under an extremely high traffic volume. Examining at the traffic logs, you notice tens of thousands of requests for the same URL coming from hundreds of different IP addresses. What kind of attack are you facing?

a. URL redirection

b. Domain hijacking

c. DNS poisoning

d. DDoS

19. What is the Secure Shell (SSH) protocol?

a. It is an encrypted remote terminal connection program used for remote connections to a server

b. It provides Software as a Service (SaaS)

c. It provides snapshots of physical machines at a point in time

d. It provides dynamic network address translation

20. Which of the attacks take advantage of unsanitized file inclusion vulnerability?

a. Remote File Inclusion

b. All the above

c. Local File Inclusion

21. You are unable to connect to anything. You find that the MAC address for the default gateway setting doesn’t match the MAC address of the router. What kind of attack are you facing?

a. MAC cloning

b. ARP poisoning

c. Rogue access point

d. Disassociation

22. To secure communications during remote access of a system, which tool can be used?

a. SSH

b. Dd

c. OpenSSL

d. tcpdump

23. What is a step of Web Penetration?

a. Information gathering

b. Vulnerability scanning

c. All the above

d. Exploitation

24. What is the best way to ensure that JavaScript cannot be used to access a cookie?

a. Set the HttpOnly flag in the cookie

b. Use non-persistent cookies

c. Do not Set the secure flag in the cookie

d. Use the CAPTCHA system

25. To search through a Linux based system to find files containing a phrase, which tool can be used?

a. Curl

b. Logger

c. Chmod

d. grep

26. Which of the below extensions needs to be blacklisted in file upload areas?

a. .xml

b. .shtml

c. .php

d. All of above

27. When a hacker captures network traffic and retransmits it at another time, what type of attack is he using?

a.Man in the middle attack

b.Replay attack

c.Bluejacking attack

d.Denial-of-service attack

28. Output encoding and input validation can be considered as mitigation mechanisms for which vulnerability?

a.Cross-site scripting attack

b.All of the above

c.SQL injection

d.Clickjacking

29. Your database server is returning a large dataset to an online user. What kind of attack are you facing?

a.Memory leak

b.LDAP injection

c.Man in the middle

d.SQL injection

30. Your desktops is displaying a red screen with the message “Your files have been encrypted. Pay 1 bitcoin to recover them.” Your desktop has most likely been affected by what type of malware?

a.Spraying

b.Crypto-malware

c.Ransomware

d.Spyware

31. If a hacker has compromised a web application, he may be able to do which of following?

a.Carry out financial fraud

b.Hijack Session Cookies

c.All of the above

d.Steal personal information

32. You are testing your systems against weak passwords using the top 100 commonly used passwords. What is this test an example of?

a.Dictionary

b.Rainbow tables

c.Password spraying

d.All are correct

33. Common sources of vulnerability issues for any systems include which of the following?

a.Strong patch management

b.Identity theft

c.Data loss

d.Weak configurations

34. Which extension to be blacklist? shtml

35. In cross-site scripting, where does the malicious script execute?

user's browser

36. Which of these tools is used in penetration testing? Nmap

37. Examining the log file of a victim server, you find the cause "Reply from 192.0.0.1: bytes=45000 time<1ms TTL=128". What type of attack has been detected?

Buffer overflow

38. Which HTTP method can be used to discover all the allowed methods on the server? TRACE

39. Which is one of the key steps in pentesting and time-consuming? All of above

40. Which identifier can be used for session management? Session ID

41. A certificate authority consists of which of the following? All of above

42. not a packet capture analysis tool? Dd

43. what type of thread exploit system? A zero day attack

44. You are downloading and then installing a new animated screensaver. When you try to run the program, the cursor moves on its own and a command prompt window opens and quickly closes. What type of malware the animated screensaver is? A Trojan

45. Web Penetration can be done by which tool? Burp Suite

46. If you think a file is malware, what is the first tool you should use? Cuckoo

47. tool penetration testing? All

48. A certificate authority consists of which of the following? All above

49. You are scanning your PC and notice that it has TCP port 31337 open. When you use the security tool netcat to connect to the port a prompt pops up asking you "Enter password for access:". Your PC may be infected with what type of malware? Backdoor

50. You’re reviewing a web application and put a number in a text field. The application gives an error message containing variable names, filenames, and the full path of the application. This is an example of which of the following? Improper error handling

51. What is the purpose of the Secure Sockets Layer (SSL) protocol? provides encryption for transport-layer protocols across the web

52. Which of the following correctly describes Transport Layer Security (TLS)? it replaces ssl

53. What is the purpose of the DNS protocol? It translates name into IP addresses

54. Connections to third-party content associated with your business, such as a travel agency website for corporate travel, is an example of which of the following? Extranet

55. Industry-standard frameworks are useful for which of the following purposes? Aligning IT and security with the enterprise's business strategy

56. Which of the following represents the greatest risk if improperly configured?

Network infrastructure device

57. Which of the following is not a standard practice to support defense-in-depth?

User diversity

58. What is the primary purpose of a DMZ?

Prevent direct access to secure servers from the Internet.

59. Penetration test

an authorized attempt to break into the organization's information system

60. Security Test

In addition to break in attempt, it includes analyzing company's security policy and procedures

61. Network session hijacking

An attack on a network that requires guessing ISNs, being able to join a TCP session making both parties think he or she is the other party

62. Ransomware

Software that encrypts programs and data until a ransom is paid to remove it.

63. Malware

software that is intended to damage or disable computers and computer systems for money

64. virus

A piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data

65. Botnet

a group of compromised computers or mobile devices connected to a network

66. How does a mail gateway's control of spam improve security?

It can defeat many phishing attempts

67. Which of the following types of attacks is not normally considered a malicious code object?

Dos

68. Worm vs Virus

The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host; whereas worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system.