Chapter 5 Basics of Hacking (CO5)

1. Ethical Hacking is also known as \_\_\_\_\_ A. Black Hat

Hacking.

B. White Hat Hacking.

C. Encryption.

D. None of these.

Ans. B

2. Tool(s) used by ethical hacker\_\_\_\_\_.

A. Scanner

B. Decoder

C. Proxy

D. All of these.

Ans. D

3. Vulnerability scanning in Ethical hacking finds\_\_\_\_\_. A.

Strengths.

B. Weakness.

C. A &B

D. None of these.

Ans. B

4. Ethical hacking will allow to\_\_\_\_ all the massive security

breaches. A. Remove.

B. Measure.

C. Reject.

D. None of these.

Ans. B

5. Sequential step hackers use are: \_ \_ \_ \_.

A. Maintaining Access.

B. Reconnaissance

C. Scanning.

D. Gaining Access.

Ans. A

6. \_\_\_\_\_\_ is the art of exploiting the human elements to gain

access to the authorized user. A. Social Engineering. B.

IT Engineering.

C. Ethical Hacking.

D. None of the above.

Ans. A

7. Which hacker refers to ethical hacker?

A. Black hat hacker.

B. White hat hacker.

C. Grey hat hacker.

D. None of the above.

Ans. B

8. The term cracker refers to\_\_\_\_\_

A. Black hat hacker.

B. White hat hacker.

C. Grey hat hacker.

D. None of the above.

Ans. A

9. Who described a dissertation on fundamentals of hacker’s

attitude?

A. G. Palma.

B. Raymond.

C. Either.

D. Jhon Browman.

Ans. B

10.Computer Hackers have been in existence for more than a\_\_\_\_. A.

Decade.

B. Year.

C. Century

D. Era.

Ans. C

11.Hackers do hack for?

A.Fame.

B. Profit.

C. Revenge.

D. All the above

Ans. D

12.The intent of ethical hacker is to discover vulnerabilities from a\_\_\_\_\_ point of view to better secure system.

A. Victims.

B. Attackers.

C. Both A & B D. None of these.

Ans. B

13.Security audits are usually based on\_\_\_

A. Entries.

B. Checklists.

C. Both A & B

D. None of the above

Ans. B

14.Ethical hacking consist of \_\_\_\_\_\_\_

A.Penetration testing.

B. Intrusion testing.

C. Red teaming.

D. All of the above.

Ans. D

15.\_\_\_\_\_\_\_ is a person who find and exploits the weakness in computer system.

A. Victim

B. Hacker

C. Developer

D. None of the above.

Ans. B

16. A white hat hacker is the one who \_\_\_\_\_

A. Fix identifies weakness

B. Steal the data

C. Identifies the weakness and leave message to owner

D. None of the above

Ans. A

17.A black hat hacker is the one who \_\_\_\_\_\_\_

A. Fix identifies weakness

B. Steal the data

C. Identifies the weakness and leave message to owner

D. None of the above.

Ans. B

18. A grey hat hacker is the one who\_\_\_\_\_\_\_

A. Fix identifies weakness

B. Steal the data

C. Identifies the weakness and leave message to owner

D. None of the above

Ans. C

19. Keeping information secured can protect an organization image and save and organization lot

of money

A. True

B. False

Ans. A

20.Information is a one of the most valuable assets of organization

A. True

B. False

Ans. A

21. To catch a thief, think like \_\_\_\_\_

A. Police

B. Forensics

C. Thief

D. Hacker

Ans. C

22.\_\_\_\_\_\_\_can create false feeling of safety

A. Firewall

B. Encryption

C. VNPs

D. All the above

Ans. D

23.\_\_\_\_\_\_ exploits that involves manipulating people and user even your self are the greatest

vulnerability within any computer

A. Nontechnical attacks

B. Network infrastructure attack

C. Operating system attack

D. Application and other specialized attack

Ans. A

24.Connecting into network through a rogue modem attached to computer behind a firewall is an

example of \_\_\_\_-

A. Nontechnical attacks

B. Network infrastructure attack

C. Operating system attack

D. Application and other specialized attack

Ans. B

25.\_\_\_\_\_\_ comprise of large portion of hacker attacks simply because every computer has one

and so well know exploits can be used against them

A. Nontechnical attacks

B. Network infrastructure attack

C. Operating system attack

D. Application and other specialized attack

Ans. C

26.\_\_\_\_\_\_ should be done before ethical hacking process.

A.Data gathering.

B. Attacking C.

Planning

D. Research

Ans. C

27.Which permission is necessary before ethical hacking?

A.Written permission.

B. Decision maker permission

C.Privacy permission

D. Risk permission.

Ans. A

28. Which tool is used to crack the password?

A. Nmap

B. LC4

C. ToneLOC

D. Nessus

Ans. B

29. Which tool is used for depth analysis of a web application?

A. Whisker

B. Super scan

C. Nikto

D. Kismet

Ans. A

30. Which tool is used to encrypt Email?

A. WebInspect

B. QualyGuard

C. PGP (pretty good privacy)

D. None of the above.

Ans. C

31.Malicious attacker often think like?

A. Thieves

B. Kidnapper

C. Both A & B

D. None of the above

Ans. C

32.Which hacker try to distribute political or social message through their work?

A. Black hat hacker

B. Hactivist

C. Script kiddes

D. White hat hacker

Ans. B

33.\_\_\_\_\_\_\_ are part of organized crime on internet.

A. Criminal

B. Antinationalist

C. Hacker for hire

D. None of the above

Ans. C

34. Which magazines releases the latest hacking methods?

A. 2600

B. Hackin9

C. PHRACK

D. All the above

Ans. D

35. Performing a shoulder surfing in order to check other’s password is \_\_\_\_\_\_\_\_\_\_\_\_ ethical

practice.

A. a good

B. not so good

C. very good social engineering practice

D. a bad

Ans. D

36. \_\_\_\_\_\_\_\_\_\_\_ has now evolved to be one of the most popular automated tools for unethical

hacking.

A. Automated apps

B. Database software

C. Malware

D. Worms

Ans. C

37. Leaking your company data to the outside network without prior permission of senior authority

is a crime.

A. True

B. False

Ans. A

38. A penetration tester must identify and keep in mind the \_\_\_\_\_\_\_\_\_\_\_ & \_\_\_\_\_\_\_\_\_\_\_

requirements of a firm while evaluating the security postures.

A. privacy and security

B. rules and regulations

C. hacking techniques

D. ethics to talk to seniors

Ans. A

39. The legal risks of ethical hacking include lawsuits due to \_\_\_\_\_\_\_\_\_\_ of personal data.

A. stealing

B. disclosure

C. deleting

D. hacking

Ans. B

40. Before performing any penetration test, through legal procedure, which key points listed below

is not mandatory?

A. Know the nature of the organization

B. Characteristics of work done in the firm

C. System and network

D. Type of broadband company used by the firm

Ans. D