

- 1) Non -experts who breaks into computer system by using pre-packaged tools written by others is known as
- a) Black hat
  - b) white hat
  - c) script kiddies
  - d) none of these
- 2) Pre attack phase which gathers information about a computer system and the companies it belongs to is known as
- a)foot printing
  - b)flood
  - c)DoS
  - d) None of the above
- 3) scan which uses FIN,PSH and URG flag is known as
- a) XMAS
  - b) ACK scan
  - c) SYN Scan
  - d) Null scan
- 4) search engine which is used for banner grabbing is
- a) Google hack database
  - b) SHODAN
  - c) yahoo
  - d) None of the above
- 5) The following commands is used for  
'nc -n 192.168.1.2 80 HEAD / HTTP/1.0'
- a) scanning
  - b) reconnassaince
  - c) banner grabing
  - d) none of the above
- 6) tool which shows the path taken by the packet to reach its destination
- a )who is
  - b) nmap
  - c) wireshark
  - d) trace route
- 7) The following search in google is used for ' intitle:index.of'
- a) Domain search
  - b) Directory listing
  - c) data base identification
  - d) none of the above
- 8) What does the following command trying to accomplish?  
nmap -sU -p445 192.168.0.0/24
- A. Verify that UDP port 445 is closed on 192.168.0.0 network
  - B. Verify that TCP port 445 is open on 192.168.0.0 network
  - C. Verify that NETBIOS is running on 192.168.0.0 network
  - D. Verify that UDP port 445 is open on 192.168.0.0 network

9) What does ICMP Type and code for 'Destination network unreachable' message

- A. Type 0, code 0
- B. Type 3, Code 0
- C. Type 8, Code 0
- D. None of the Above

10) Which of the following security solutions uses the same key for both encryption and authentication?

- A. WPA
- B. WPA2
- C. WEP
- D. 802.11i

11) Which form of authentication does WPA2 use?

- A. Passphrase only
- B. 802.1x/EAP/RADIUS
- C. Passphrase or 802.1x/EAP/RADIUS
- D. AES

12). 802.11i is most similar to which wireless security standard?

- A. WPA2
- B. WPA
- C. TKIP
- D. AES

13) Which of the following is a Layer 3 security solution for WLANs?

- A. MAC filter
- B. WEP
- C. WPA
- D. VPN

14) Which of the following are Layer 7 application-secure protocols used to secure data on WLAN hotspots?

- A. HTTPS
- B. HTTP
- C. FTP
- D. VPN

15) Which group of malware record every movement on a computer ?

- a) Trapper
- b) Trojan Horse
- c) Key logger
- d) Worm

16) "Stuxnet" is a

- a) Virus
- b) Worm
- c) Trojan Horse
- d) Rootkit

17) Which one is not a countermeasure against Malware ?

- a) Updating System with latest patches
- b) Taking backup regularly
- c) End User security training
- d) Installing MS Office

18) What is “wrapper” related to Malware?

- a) A tool to create virus
- b) Any legitimate software used to hide Trojan
- c) Attack module of Malware
- d) None of the above

19) What type of password attack would be more successful against the password T68k\$Sp24K9

- |                      |                |
|----------------------|----------------|
| A. Dictionary        | B. Brute force |
| C. Password Guessing | D. Hybrid      |

20) This kind of password cracking method uses word lists in combination with numbers and special characters:

- A. Linear
- B. Symmetric
- C. Hybrid
- D. Brute Force

21) Eavesdropping means

- A. art of interacting with people either face to face or over the telephone and getting them to give out valuable information such as passwords
- B. the process of listening, monitoring, or examining someone without their permission or knowledge.
- C. a term used in civil litigation that describes the discovery of information in electronic format, typically recovered through digital forensics analysis.
- D. a program that reads data in and manipulates the data to fit another output pattern or removes data that may not be needed.

22) Hydra is a popular tool for-

- |                              |                              |
|------------------------------|------------------------------|
| A. online password-cracking  | C. Generating Rainbow tables |
| B. offline password-cracking | D. non electronic attack     |

23) Which is a non-technical attack?

- |                    |                      |
|--------------------|----------------------|
| A. Dumpster Diving | C. Rule Based Attack |
| B. Rainbow tables  | D. Password Guessing |

24) Which of the following is essential information to a hacker performing a session-hijacking attack?

- A. Session ID

- B. Session number
- C. Sequence number
- D. Source IP address

25) Which of the following is the best countermeasure to session hijacking?

- A. Port filtering firewall
- B. Encryption
- C. Session monitoring
- D. Strong passwords

26) What is an ISN?

- A. Initiation session number
- B. Initial sequence number
- C. Initial session number
- D. Indication sequence number

27) which of the following is not the part of OS hardening

- a) removal of all non-essential services
- b) Updating the kernel
- c) applying patches
- d) restoring the system to their default configuration

28) Cyber Crime is defined under Indian Cyber Law

- A. True
- B. False

29) Copyright law does not protect

- A. Musical Works
- B. Literary Works
- C. Ideas or Concepts
- D. Sound Recordings

30) Whether Intellectual Property can be sold

- A. No
- B. Sale is possible
- C. Yes
- D. None

31) To be considered a computer crimes, what needs to be involved in the crime

- A. Technology
- B. Computers
- C. Data
- D. Networks

32) Public key encryption method is a system

- A. Which uses a set of public keys one for each participant in e-Commerce
- B. Which uses the RSA coding system
- C. In which each person who wants to communicate has two keys; a private key known to him only and a public key which is publicized to enable others to send message to him
- D. Which is a standard for use in e-Commerce.

33) The Information Technology Act, 2000 is concerned with :

- A. Legal recognition of digital signatures
- B. Definition of various types of computer crimes and penalties for the same
- C. Appointment of certifying authorities for issuing digital signatures
- D. All of the above

34) Patents are generally granted to

- A. Inventions that are new
- B. Non obvious subject matter
- C. Processes and Methods
- D. A and B
- E. B and C