1) Nmaps shows the status of the port as ----- if the port is assessable but is unable to determine whether it is open or closed
a) open
b)unfiltered
c) closed
d) filtered

2) side-channel attack exploits predictable IP fragmentation ID sequence generation on the zombie host to glean information about the open ports on the target.
a) ACK scan
b) SYN Scan
c)NULL scan
d) Idle scan

3) Scan which will not determine the open port but used to map out firewall rulesets
a) XMAS
b)NULL
c) ACK
d) SYN

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) An "idle" system is also referred to as what?
a) Zombie
b) PC not connected to the Internet
c) PC not being used
d) Bot

7) If an attacker's computer sends an IPID of 31400 to a zombie computer on an closed port, what will be the response?
a) 31401
b) 31402
c) 31399
d) The zombie will not send a response

8) What organization maintains the details of vulnerabilities ?
a) CVE
b) IANA
c) APIPA

d) RIPE

9) What does WEP stands for?
a) Wireless Encryption Protocol
b) Wired Equivalent Privacy
c) Wireless Encryption Privacy
d) Wired Encryption Protocol

10) What makes WEP crackable?
a) Weakness of IV
b) Same key used for encryption and authentication
c) Length of the key
d) RC4

11) Which form of encryption does WPA use?
a) AES
b) TKIP
c) LEAP
d) Shared key

12) You just installed a new wireless access point for your home office. Which of the following steps should you take immediately to secure your WLAN?
a) Spoof your clients MAC address.
b) Change the Admin password on the AP.
c) Change the channel on the AP to Channel 11.
d) Set the SSID to SECURE.

13) What is an SSID used for on a WLAN?
a) To secure the WLAN
b) To manage the WLAN settings
c) To identify the WLAN
d) To configure the WLAN AP

14) What is a computer called when it is infected with a malware bot ?
a) Zombie
b) Android
c) Dirtybot
d) Botnet

15) Which malware is used to gain administrative rights to one's computer?
a) Virus
b) Rootkit
c) Worm
d) Torjan Horse

16) Which virus rewrite itself completely after each iteration ?
a) Polymorphic virus
b) Multipartite virus
c) Macro virus
d) Metamorphic virus

17) Which Trojan uses port 20 for covert channel ?
a) FTP Trojan
b) HTTP Trojan
c) ICMP Trojan
d) SMTP Trojan

18) What is RAT ?
a) Remote Action Test
b) Remote Access Trojan
c) Random Access Test
d) Remote Action Trojan

19) What is “Botnet” ?
a) Network of Zombies
b) Virus
c) A covert channel
d) Wrapper

20) You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords at are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack among these?

a) Online Attack
b) Dictionary Attack
c) Brute Force Attack
d) Hybrid Attack

21) Hydra is a popular tool for-

a) online password-cracking
b) offline password-cracking
c) Generating Rainbow tables
d) non electronic attack

22) Which of the following is a passive online attack?

a) Password Guessing
b) Network Sniffing
c) Brute Force Attack
d) Dumpster Diving

23) Shoulder surfing means

a) connection that encrypts the data transmitting over it to help protect it from being intercepted and read by a third-party.
b) Preventing a particular individual from accessing a service.
c) a software program that is intentionally installed on the computer by a user to monitor or spy on what other users of the same computer are doing.
d) a person that looks over another person's shoulder as they enter data into a computer or other device.

24) What is a sequence number?
a) A number that indicates where a packet falls in the data stream
b) A way of sending information from the sending to the receiving station
c) A number that the hacker randomly chooses in order to hijack a session
d) A number used in reconstructing a UDP session

25) What type of information can not be obtained during a session-hijacking attack? (Choose all that apply.)
a) Passwords
b) Credit card numbers
c) Confidential data
d) Authentication information

Ans. A B C

26) What is session hijacking?
a) Monitoring UDP sessions
b) Monitoring TCP sessions
c) Taking over UDP sessions
d) Taking over TCP sessions

27) What types of packets are sent to the victim of a session-hijacking attack to cause them to close their end of the connection?
a) FIN and ACK
b) SYN or ACK
c) SYN and ACK
d) FIN or RST

28) which of the following is not true regarding kernel modules
a) piece of code that can be loaded and unload into the kernel upon demand
b) used to extends the functionalities of the kernel without rebooting system
c) kernel modules begins with 'main'
d) none of the above

29) Identify the correct sequence
i) Identify active machines ii) OS fingerprinting
iii) Information gathering iv ) determining network range

a) iii , iv , i, ii
b) i, iii, iv, ii
c) iii, i, iv, ii
d) iv, i, iii, ii

30) The Information Technology Act 2000 is mainly

A. Intended to promote e-governance
B. Give legal recognition to e- transactions and EDI
C. Punish Cyber Criminals
D. A and B

E. A and C

31) Remedies available in case of Copyright Infringement

A. Civil Remedies
B. Criminal Remedies
C. All of the Above
D. Either A or B

32) Public Key System is useful because

A. It is a symmetric key system
B. It uses two keys
C. Private key can be a secret
D. There is no Key Distribution Problem as Public Key can be kept in a commonly accessible database

33) 'Fair use' is a term most relevant to

A. Intellectual Property Rights
B. Books borrowed for home reading
C. Copy right
D. Use of reference books

34) Cyber Criminals come in the category of

A. Intruders
B. Hackers
C. Employees
D. All

35) A computer can act as

A. Crime
B. Evidence
C. None
D. Both

36) Various kinds of e-contracts include

A. Click Contracts
B. Shrink Contracts
C. Web Contracts
D. All