Marks: 20

1) An attacker observes the common websites visited by the victim, and then uses one of the websites to attack the victim's machine. This attack is called as a _____. **[01]**
A) Clicker Trojan attack
B) Waterhole attack
C) Social Engineering attack
D) Sinkhole attack

2) When a malicious website pretends to be a legitimate website, the attack is called as _____. **[01]**
A) Clickjacking
B) Hijacking
C) Waterholing
D) Phishing

3) The malware WannaCry is a _____. **[01]**
A) Trojan
B) Spyware
C) Adware
D) Ransomware

4) DDoS attacks affect the _____ of a system. **[01]**
A) Confidentiality
B) Integrity
C) Availability
D) Deniability

5) Man-in-the-middle attacks affect the _____ of a system. **[01]**
A) Confidentiality
B) Integrity
C) Availability
D) Deniability

6) Eavesdropping attacks affect the _____ of a system. **[01]**
A) Confidentiality
B) Integrity
C) Availability
D) Deniability

7) Which tool can be used to perform a DNS zone transfer on Windows?   **[01]**
A) nslookup
B) DNSlookup
C) whois
D) ipconfig

8) Dumpster diving can be considered as a _____ type of social engineering attack.   **[01]**
A) Human-based
B) Computer-based
C) Physical access
D) Paper-based

9) Hacking for a cause is called _____.   **[01]**
A) Hacktivism
B) Black-hat hacking
C) Active hacking
D) Activism

10) _____ hackers are bad guys that operate on the opposite side of the law.   **[01]**
A) Black hat
B) White hat
C) Green hat
D) Red hat

11) _____ hackers straddle the line between the good and the bad side.   **[01]**
A) Green hat
B) White hat
C) Grey hat
D) Black hat

12) When a hacker pretends to be a legitimate user on the system, it is called _____.   **[01]**
A) Account Elevation
B) Impersonation
C) Authentication
D) Help desk

13) The hackers who always take permission of the authorities to find security vulnerabilities are called
_____.   **[01]**
A) Green hat
B) White hat
C) Grey hat
D) Black hat

14) The process of gathering information about your target is known as_____.   **[01]**
A) Enumeration
B) Hacking
C) Data gathering
D) Hijacking

15) The maximum length of an SSID is _____ characters. **[01]**
A) 8
B) 16
C) 32
D) 64

16) In VoIP, data needs to be protected from _____ attack. **[01]**
A) Man-in-the-middle
B) Eavesdropping
C) Masquerade
D) Server

17) Internet is a _____ switched network. **[01]**
A) Circuit
B) Packet
C) IP
D) MAC

18) A _____ is a decoy computer system for luring and trapping hackers. **[01]**
A) Jackpot
B) LurePot
C) Honeypot
D) TrappingPot

19) The underlying encryption engine used by WEP is _____. **[01]**
A) RC4
B) RC8
C) RC16
D) RC32

20) The preferred communications method used with respect to bot-nets are _____. **[01]**
A) IRC
B) TFTP
C) SMTP
D) POP3

x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x