CYBER FORENSICS

MOCK QUESTIONS

1. CSIRT stands for?
A) Computer security incident response technology
B) Computer science incident response technology
C) Computer security incident response team
D) Computer security incident reading team

2. Which of the following is not a type of cybercrime?
A) Data theft
B) Forgery
C) Damage to data and systems
D) Installing antivirus for protection

3. Which one is windows-based tools to recover files?
A) Encase
B) TASK
C) Foremost
D) fatback

4. _____command is used to kill process by name or process ID.
A) PsList
B)RegMom
C) PsKill
D) PsService

5. While collecting the evidence related to network based on the volatility a proper order of collecting the evidence have to follow, is known as_____.
A) Order of investigation
B) Order of Evidence
C) Order of Volatility
D) Order of research

6. _____ means the header use spoofed addresses to con computers are fool them into thinking a message originated from different machine
A) IP Spoofing
B) Address Spoofing
C) ARP Spoofing
D) DNS Spoofing

7. Mail bombs means?
A) Flooding a mail server
B) Corrupting mailbox
C) Flooding a mail IP
D) Hacking Mail password

8. PsList_____.

A) Lists detailed information about process
B) Lists detailed information about Files
C) Lists detailed information about users
D) Lists detailed information about Admin

9. IDSs Stands for ?
A) Intrusion Detection Software
B) Intrusion Device Software
C) Intrusion Detection System
D) Incoming Device Security

10. _____command is used to determine the open ports
A) netstat
B) ipstat
C) openport
D) portscan

11. _____ is a suite of tools created by Sysinternals.
A) Browserhistory
B) Encase
C) FTK
D) pstools

12. SIM Stands for?
A) Subscriber Incoming Module
B) Subscriber Identity Module
C) Subscriber Insight Module
D) Subscriber Inshort Module

13. In case of _____ the evidence is collected from a system where the microprocessor is running.
A) live acquisition
B) static acquisition
C) sparse acquisition
D) Metasploit

14. _____ is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise.
A) Email security
B) Email hacking
C) Email protection
D) Email safeguarding

15. Which of the following will not help in preserving email security?
A)Create a strong password
B)Connect your email to a phone number
C)Use two-factor authentication for password verification and login
D)Click on unknown links and sites

16. "_____ is the process of making an archival or back up copy of the entire contents of a hard drive."
A)Investigation
B)Disk imaging
C)Formatting
D)S/w Installation

17. Which are the following are data compression techniques?
A)LZW
B)WZL
C)ZAW
D)ZLW

18. As a good forensic practice, why would it be a good idea to wipe a forensic drive before using it?
A)Different file and operating systems
B)Chain of Custody
C)No need to wipe
D)Cross-contamination

19. The ability to hide data in another file is called_____.
A)Encryption
B)Steganography
C)Data parsing
D)A and B

20. Which of the following is a proper search technique?
A)Manual Browsing
B)Keyword Search
C)Regular Expression Search
D)Search