Topic- Cyber Security

MTDT009

1. **The CIA triad stands for?**
    a. Confidentiality, Integrity, and Availability
    b. Criticality, Integrity, and Availability
    c. Confidentiality, Integrity, and Accesibility
    d. Confidentiality, Inseperability, and Availability
    e. Confidentiality, Interpretability, and Availability

    Answer:- Confidentiality, Integrity, and Availability
2. **Which type of software does malicious tasks on a device or network such as corrupting data or taking control of a system?**
    a. Malware
    b. Adware
    c. Spyware
    d. Ransomware
    e. Trojan

    Answer:- Malware
3. **Which form of malware hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords?**
    a. Malware
    b. Adware
    c. Spyware
    d. Ransomware
    e. Trojan

    Answer:- Spyware
4. **Which is a type of malware that denies access to a computer system or data until a ransom is paid?**
    a. Malware
    b. Adware
    c. Spyware
    d. Ransomware
    e. Trojan

    Answer:- Ransomware
5. **What is name of threat when an unauthorized user gains access to a system or network and remains there without being detected for an extended period of time?**
    a. Advance Persistent Threat
    b. Malware
    c. Phishing

d. Baiting
e. Spyware

Answer:- Advance Persistent Threat

6. **Which of the following officials is not mandatory member of Cyber Crisis Management team?**
   a. CISO
   b. CTO
   c. CRO
   d. CLO
   e. ALL

   Answer:- CLO

7. **Cyber Security Policy is a set of directives that shall enable bank to ----,----- & ----- Cyber-attacks in a timely manner to protect the Confidentiality, Integrity and Availability of data at bank**
   a. Respond,Recover,Learn
   b. Identify,Detect ,Mitigate
   c. Identify,Protect,Detect
   d. Confidentiality, Inseperability, and Availability
   e. Confidentiality, Integrity, and Availability

   Answer:- Identify,Detect ,Mitigate

8. **Threat for which "The possible reason is a current or former employee seeking financial gain from stealing and selling the intellectual property of the bank"?**
   a. Corporate espionage
   b. Cyber Espionage
   c. Employee-Threat
   d. Whaling
   e. ClickJacking

   Answer:- Corporate espionage

9. **Name a hacker who doesn't possess technical expertise and relies on pre-developed scripts and programs to perform attacks?**
   a. Thrill Seeker
   b. Script Kiddies
   c. Insider Hacker
   d. Corporate espionage
   e. Sophisticated attackers

   Answer:- Script Kiddies

10. **Identify the Threat "The possible reason is due to the existence of bank over the internet and having information of value"?**
    a. Sophisticated attackers
    b. Unsophisticated attackers
    c. Script Kiddies
    d. Insider Hacker
    e. Thrill Seeker

    Answer:- Sophisticated attackers
11. **A Socially or politically motivated hacker with the intention of fulfilling a social or political agenda is known as?**
    a. Thrill Seeker
    b. Script Kiddies
    c. Hacktivists
    d. Insider Hacker
    e. Sophisticated attackers

    Answer:- Hacktivists
12. **A hacker with threatening objectives such as harming people or destroying critical systems and information is known as ----------.**
    a. Cyber Terrorist
    b. Thrill Seeker
    c. Script Kiddies
    d. Hacktivists
    e. Insider Hacker

    Answer:- Cyber Terrorist
13. **Individuals that are hired by a company to break into their system / network to discover potential Security lapses / weaknesses / vulnerabilities are known as ---------.**
    a. Script Kiddies
    b. Black Hat Hacker
    c. Grey Hat Hacker
    d. White Hat / Ethical Hacker
    e. Grey Hacker

    Answer:- White Hat / Ethical Hacker
14. **Malicious hackers that exploit Security vulnerabilities for personal gain. They may also destroy information they find, steal passwords, and steal sensitive data, negatively impact operations technology are known as?**
    a. Script Kiddies

b. Black Hat Hacker
c. Grey Hat Hacker
d. White Hat / Ethical Hacker
e. Grey Hacker

Answer:- Black Hat Hacker

15. **Which type of hacker will break into a system/ network without the owner' s consent/ knowledge and will publically disclose any Security vulnerabilities/ flaws? However, they do not take advantage of the flaw for their own personal gain. Their goal is to**
    a. Script Kiddies
    b. Black Hat Hacker
    c. Grey Hat Hacker
    d. White Hat / Ethical Hacker
    e. Grey Hacker

    Answer:- Grey Hat Hacker

16. **What do we call to Hackers that are for profit and hired to engage in electronic corporate espionage. They will commonly use dumpster diving and social engineering to accomplish their objectives?**
    a. Crackers
    b. Thrill Seeker
    c. Black Hat Hacker
    d. Hacktivists
    e. Thrill Seeker

    Answer:- Crackers

17. **Crisis Identification Criterian for Revenue Loss is ?**
    a. More than 1 Crore
    b. More than 3 Crore
    c. More than 2 Crore
    d. More than 5 Crore
    e. More than 10 Crore

    Answer:- More than 1 Crore

18. **Crisis Identification Criterian for Data Loss is ?**
    a. of at least 500 customer data records of confidential bank data
    b. of at least 100 customer data records of confidential bank data
    c. of at least 1000 customer data records of confidential bank data
    d. of at least 10000 customer data records of confidential bank data
    e. of at least 100000 customer data records of confidential bank data

Answer:- of at least 500 customer data records of confidential bank data

19. **Availability impact of more than --- minutes for a critical customer facing application is Crisis.**

    a. 60
    b. 30
    c. 90
    d. 45
    e. 180

Answer:- 30

20. **User IDs that have not been used for a period of ---- weeks can be considered stale**

    a. 1
    b. 2
    c. 3
    d. 4
    e. 5

Answer:- 3

21. **A ---------- is a group of trained professionals authorized and organized to emulate a potential adversary‘s attack or exploitation capabilities against an enterprise‘s security posture**

    a. Red team
    b. Blue Team
    c. Green Team
    d. Yellow Team
    e. Cyber-SOC

Answer:- Red team

22. **Incident of phishing e-mail should be reported to?**

    a. antiphishing.ciso@unionbankofindia.bank
    b. phishing.ciso@unionbankofindia.com
    c. ciso@unionbankofindia.com
    d. incidentreporting@unionbankofindia.bank
    e. phishing@unionbankofindia.bank

Answer:- antiphishing.ciso@unionbankofindia.bank

23. **Phishing technique targeting Top executives like CEO, CFO and COO is called?**

    a. Corporate espionage
    b. Cyber Espionage

c. Employee-Threat
d. Whaling
e. ClickJacking

Answer:- Whaling

24. An intruder searches your PC's recycle bin. Identify the social engineering mechanism?

a. Corporate espionage
b. Cyber Espionage
c. Dumpster Diving
d. Whaling
e. ClickJacking

Answer:- Dumpster Diving

25. Who is ultimately responsible of cyber security?

a. Board Of Directors
b. CISO
c. CTO
d. ED Overseeing IT
e. CRO

Answer:- Board Of Directors

26. CISO should report to ----------

a. ED overseeing RMD
b. MD
c. CTO
d. ED Overseeing IT
e. CRO

Answer:- ED overseeing RMD

27. --------- is an attack aimed at stealing the 'sensitive personal data',that can lead to committing online economic frauds.

a. Phishing
b. Whaling
c. Denial of Service attack
d. Baiting
e. Vishing

Answer:- Phishing

28. **A hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fixit. This exploit is called a ----------.**
    a. Phishing
    b. Adware
    c. Zero Day Attack
    d. Denial of Service attack
    e. Baiting

    Answer:- Zero Day Attack

29. **What is CCMP?**
    a. Cyber Crisis Management Plan
    b. Cyber Crisis Mitigation Plan
    c. Cyber Control Management Plan
    d. Cyber Crime Management Plan
    e. Cyber Crime Mitigation Plan

    Answer:- Cyber Crisis Management Plan

30. **What is Cyber Security Governance Management Strategy?**
    a. Identify,Protect,Detect,Respond,Recover,Learn
    b. Identify,Protest,Detect,Respond,Recover,Learn
    c. Identify,Protest,Detect,Remediate,Recover,Learn
    d. Initiate,Protest,Detect,Remediate,Recover,Learn
    e. None

    Answer:- Identify,Protect,Detect,Respond,Recover,Learn