



A brief overview of types of actors and their motives

TOTAL POINTS 25

1. Which hacker organization hacked into the Democratic National Convention and released Hillary Clinton's emails?

1 point

- ☒ Fancy Bears
- ☐ Anonymous
- ☐ Syrian Electronic Army
- ☐ Guardians of the Peace
- ☐ All of the above

2. What challenges are expected in the future?

1 point

- ☐ Enhanced espionage from more countries
- ☐ Far more advanced malware
- ☐ New consumer technology to exploit
- ☒ All of the above

3. Why are cyber attacks using SWIFT so dangerous?

1 point

- ☐ SWIFT is the flight plan and routing system used by all cooperating nations for international commercial flights
- ☒ SWIFT is the protocol used by all banks to transfer money
- ☐ SWIFT is the protocol used by all US healthcare providers to encrypt medical records
- ☐ SWIFT is the protocol used to transmit all diplomatic telegrams between governments around the world

4. Which statement best describes Authentication?

1 point

- ☐ Prevention of unauthorized use of a resource
- ☒ Assurance that the communicating entity is the one claimed
- ☐ Assurance that a resource can be accessed and used
- ☐ Protection against denial by one of the parties in communication

5. Trusted functionality, security labels, event detection, security audit trails and security recovery are all examples of which type of security mechanism?

1 point

- ☐ Contingent security mechanism
- ☐ Active security mechanism
- ☒ Passive security mechanism
- ☐ External security mechanism

6. If an organization responds to an intentional threat, that threat is now classified as what?

1 point

- ☐ An open case
- ☒ An attack
- ☐ A malicious threat
- ☐ An active threat

7. An attack that is developed particularly for a specific customer and occurs over a long period of time is a form of what type of attack?

1 point

- ☐ Water Hole
- ☐ Spectra
- ☐ Denial of Service (DOS)
- ☒ Advanced Persistent Threat

8. Which of three (3) these approaches could be used by hackers as part of a Business Email Compromise attack?

1 point

- ☒ Account compromise
- ☐ Request to make a payment
- ☒ Attorney impersonation
- ☒ CEO Fraud, where CEO sends email to an employee

9. Which type of actor was **not** one of the four types of actors mentioned in the video *A brief overview of types of actors and their motives*?

1 point

- ☒ Black Hats
- ☐ Hackers
- ☐ Hactivists
- ☐ Internal
- ☐ Governments

10. A political motivation is often attributed to which type of actor?

1 point

- ☐ Hackers
- ☐ Security Analysts

- ☒ Hactivist
- ☐ Internal

11. The video *Hacking organizations* called out several countries with active government sponsored hacking operations in effect. Which one of these was among those named?

1 point

- ☒ Israel
- ☐ Canada
- ☐ Egypt
- ☐ South Africa

12. Which of these is **not** a known hacking organization?

1 point

- ☒ The Ponemon Institute
- ☐ Fancy Bears
- ☐ Syrian Electronic Army
- ☐ Anonymous
- ☐ Guardians of the Peace

13. Which type of actor hacked the 2016 US Presidential Elections?

1 point

- ☒ Government
- ☐ Hackers
- ☐ Internal
- ☐ Hactivists

14. True or False: Passive attacks are easy to detect because the original messages are usually altered or undelivered.

1 point

- ☒ False
- ☐ True

15. True or False: Authentication, Access Control and Data Confidentiality are all addressed by the ITU X.800 standard.

1 point

- ☒ True
- ☐ False

16. Cryptography, digital signatures, access controls and routing controls considered which?

1 point

- ☐ Pervasive security mechanisms
- ☐ Security Policy
- ☐ Business Policy
- ☒ Specific security mechanisms

17. True or False: Only acts performed with intention to do harm can be classified as Organizational Threats

1 point

- ☒ False
- ☐ True

18. Traffic flow analysis is classified as which?

1 point

- ☐ An origin attack
- ☐ A masquerade attack
- ☐ An active attack
- ☒ A passive attack

19. How would you classify a piece of malicious code designed to cause damage, can self-replicate and spreads from one computer to another by attaching itself to files?

1 point

- ☐ Adware
- ☐ Virus
- ☐ Trojan Horse

- ☐ Spyware
- ☒ Worm
- ☐ Ransomware

20. Botnets can be used to orchestrate which form of attack?

1 point

- ☐ Distribution of Spam
- ☐ DDoS attacks
- ☐ Phishing attacks
- ☐ Distribution of Spyware
- ☐ As a Malware launchpad
- ☒ All of the above

21. Policies and training can be classified as which form of threat control?

1 point

- ☐ Technical controls
- ☐ Passive controls
- ☐ Active controls
- ☒ Administrative controls

22. Which type of attack can be addressed using a switched Ethernet gateway and software on every host on your network that makes sure their NICs is not running in promiscuous mode.

1 point

- ☒ Packet Sniffing
- ☐ Host Insertion
- ☐ Trojan Horse
- ☐ Ransomware
- ☐ All of the above

23. A flood of maliciously generated packets swamp a receiver's network interface preventing it from responding to legitimate traffic. This is characteristic of which form of attack?

1 point

- ☒ A Denial of Service (DOS) attack
- ☐ A Trojan Horse
- ☐ A Masquerade attack
- ☐ A Ransomware attack

24. A person calls you at work and tells you he is a lawyer for your company and that you need to send him specific confidential company documents right away, or else! Assuming the caller is not really a lawyer for your company but a bad actor, what kind of attack is this?

1 point

- ☒ A Social Engineering attack
- ☐ A Trojan Horse
- ☐ A Denial of Service attack
- ☐ A Worm attack

25. True or False: An individual hacks into a military computer and uses it to launch an attack on a target he personally dislikes. This is considered an act of cyberwarfare.

1 point

- ☒ False
- ☐ True

☒ I, **Thomas John James**, understand that submitting another's work as my own can result in zero credit for this assignment. Repeated violations of the Coursera Honor Code may result in removal from this course or deactivation of my Coursera account.

[Learn more about Coursera's Honor Code](#)



Save

Submit