CyberRookie CSX Fundamentals - Mock Exam 6

Friday, September 13, 2019 3:01 PM

Section 6 - Security Implications and Adoption of Evolving Technologies

1. __________________________is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction."

A. Software as a Service (SaaS)

B. Cloud computing

C. Big data

D. Platform as a Service (PaaS)

2. Select all that apply. Which of the following statements about advanced persistent threats (APTs) are true?

A. APTs typically originate from sources such as organized crime groups, activists or governments.

B. APTs use obfuscation techniques that help them remain undiscovered for months or even years.

C. APTs are often long-term, multi-phase projects with a focus on reconnaissance.

D. The APT attack cycle begins with target penetration and collection of sensitive information.

E. Although they are often associated with APTs, intelligence agencies are rarely the perpetrators of APT attacks.

3. Which of the following are benefits to BYOD? (more than one)

A. Acceptable Use Policy is easier to implement.

B. Costs shift to the user.

C. Worker satisfaction increases.

D. Security risk is known to the user.

4. Choose three. Which types of risk are typically associated with mobile devices?

A. Organizational risk

B. Compliance risk

C. Technical risk

D. Physical risk

E. Transactional risk

5. Which three elements of the current threat landscape have provided increased levels of access and connectivity, and, therefore, increased opportunities for cybercrime?

A. Text messaging, Bluetooth technology and SIM cards

B. Web applications, botnets and primary malware

C. Financial gains, intellectual property and politics

D. Cloud computing, social media and mobile computing

6. A collection of threats is generally referred to as a(n):

Threat environment

Advanced persistent threat (APT)

Cyberwarfare

Hacktivism

7. An adversary which leverages sophisticated expertise, significant resources and multiple attack vectors is known as a(n):

Advanced persistent threat (APT)

Hacktivist

Cyberwarrior

Terrorist group

8. Most advanced persistent threat (APT) attacks are aimed at:

Stealing or manipulating data

Causing physical harm to employees

Causing damage to facilities

Disrupting organizational operations

9. When an attacker seeks to gain an initial entry to the enterprise infrastructure through a simple social engineering attack, it is called:

Spear phishing

Code injection

Target discovery

Data exfiltration

10. The key attributes of an advanced persistent threat (APT) include which of the following? Select all that apply.

Well-researched

Stealthy

Sophisticated

Persistent

11. At this stage of an attack, the adversary explores networked platforms within reach, maps out the network and harvests user credentials:

Command and control

Target discovery

Target penetration

Target research

12. Major physical risks of mobile devices include which of the following? Select all that apply.

Data breaches

Identity theft

Work disruptions

Data retrieval

13. The lack of formal training for employees on the use of mobile devices is considered a(n):

Organizational risk

Physical risk

Technical risk

Informational risk

14. Physical risk involving mobile devices can be mitigated through the use of which of the following? Select all that apply.

Cell-based tracking and locating the device

Remote shutdown/wipe capabilities

Remote SIM card lock capabilities

Employee training programs

15. Messaging, audio and Bluetooth are all examples of:

Physical risk

Technical risk

Informational risk

Organizational risk

16. Proxy level and presentation level are common attacks to:

Web view applications

Outdated hardware

Static data

History files

17. A fake web site presented through a mobile view is known as a(n):

Presentation level attack

Proxy level attack

Code injection

Script kiddie

18. Major benefits of cloud computing include which of the following? Select all that apply.

Scalability

Cost-effectiveness

Data protection

Timeliness of updates

19. Major risks of cloud computing include which of the following? Select all that apply.

Lack of scalability

Difficult to protect data

Provider non-compliance with requirements

Loss of governance

20. When vetting or auditing a cloud provider, organizations should assess the provider's:

Facilities, networks, hardware and operating systems

Facilities, networks, hardware and financial documents

Human resources, financial documents, hardware and operating systems

Networks, operating systems, human resources and references

Send me a copy of my responses.

Back

Submit

Page 7 of 7

Never submit passwords through Google Forms.