EC-Council

Exam Questions 312-85

Certified Threat Intelligence Analyst

NEW QUESTION 1
Lizzy, an analyst, wants to recognize the level of risks to the organization so as to plan countermeasures against cyber attacks. She used a threat modelling methodology where she performed the following stages:
Stage 1: Build asset-based threat profiles
Stage 2: Identify infrastructure vulnerabilities
Stage 3: Develop security strategy and plans
Which of the following threat modelling methodologies was used by Lizzy in the aforementioned scenario?

A. TRIKE
B. VAST
C. OCTAVE
D. DREAD

Answer: C

NEW QUESTION 2
An XYZ organization hired Mr. Andrews, a threat analyst. In order to identify the threats and mitigate the effect of such threats, Mr. Andrews was asked to perform threat modeling. During the process of threat modeling, he collected important information about the treat actor and characterized the analytic behavior of the adversary that includes technological details, goals, and motives that can be useful in building a strong countermeasure.
What stage of the threat modeling is Mr. Andrews currently in?

A. System modeling
B. Threat determination and identification
C. Threat profiling and attribution
D. Threat ranking

Answer: C

NEW QUESTION 3
Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

A. Risk tolerance
B. Timeliness
C. Attack origination points
D. Multiphased

Answer: C

NEW QUESTION 4
In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

A. Distributed storage
B. Object-based storage
C. Centralized storage
D. Cloud storage

Answer: B

NEW QUESTION 5
A team of threat intelligence analysts is performing threat analysis on malware, and each of them has come up with their own theory and evidence to support their theory on a given malware.
Now, to identify the most consistent theory out of all the theories, which of the following analytic processes must threat intelligence manager use?

A. Threat modelling
B. Application decomposition and analysis (ADA)
C. Analysis of competing hypotheses (ACH)
D. Automated technical analysis

Answer: C

NEW QUESTION 6
Steve works as an analyst in a UK-based firm. He was asked to perform network monitoring to find any evidence of compromise. During the network monitoring, he came to know that there are multiple logins from different locations in a short time span. Moreover, he also observed certain irregular log in patterns from locations where the organization does not have business relations. This resembles that somebody is trying to steal confidential information.
Which of the following key indicators of compromise does this scenario present?

A. Unusual outbound network traffic
B. Unexpected patching of systems
C. Unusual activity through privileged user account
D. Geographical anomalies

Answer: C

NEW QUESTION 7

Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information. After obtaining confidential data, he further sells the information on the black market to make money.
Daniel comes under which of the following types of threat actor.

A. Industrial spies
B. State-sponsored hackers
C. Insider threat
D. Organized hackers

Answer: D

NEW QUESTION 8
Miley, an analyst, wants to reduce the amount of collected data and make the storing and sharing process easy. She uses filtering, tagging, and queuing technique to sort out the relevant and structured data from the large amounts of unstructured data.
Which of the following techniques was employed by Miley?

A. Sandboxing
B. Normalization
C. Data visualization
D. Convenience sampling

Answer: B

NEW QUESTION 9
Kathy wants to ensure that she shares threat intelligence containing sensitive information with the appropriate audience. Hence, she used traffic light protocol (TLP).
Which TLP color would you signify that information should be shared only within a particular community?

A. Red
B. White
C. Green
D. Amber

Answer: D

NEW QUESTION 10
In which of the following forms of bulk data collection are large amounts of data first collected from multiple sources in multiple formats and then processed to achieve threat intelligence?

A. Structured form
B. Hybrid form
C. Production form
D. Unstructured form

Answer: D

NEW QUESTION 10
Tyrion, a professional hacker, is targeting an organization to steal confidential information. He wants to perform website footprinting to obtain the following information, which is hidden in the web page header.
Connection status and content type
Accept-ranges and last-modified information
X-powered-by information
Web server in use and its version
Which of the following tools should the Tyrion use to view header content?

A. Hydra
B. AutoShun
C. Vanguard enforcer
D. Burp suite

Answer: D

NEW QUESTION 11
Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.
Which of the following phases of cyber kill chain methodology is Jame executing?

A. Reconnaissance
B. Installation
C. Weaponization
D. Exploitation

Answer: C

NEW QUESTION 12
Walter and Sons Company has faced major cyber attacks and lost confidential data. The company has decided to concentrate more on the security rather than

other resources. Therefore, they hired Alice, a threat analyst, to perform data analysis. Alice was asked to perform qualitative data analysis to extract useful information from collected bulk data.
Which of the following techniques will help Alice to perform qualitative data analysis?

A. Regression analysis, variance analysis, and so on
B. Numerical calculations, statistical modeling, measurement, research, and so on.
C. Brainstorming, interviewing, SWOT analysis, Delphi technique, and so on
D. Finding links between data and discover threat-related information

Answer: C

NEW QUESTION 17
An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.
Which of the following technique is used by the attacker?

A. DNS zone transfer
B. Dynamic DNS
C. DNS interrogation
D. Fast-Flux DNS

Answer: D

NEW QUESTION 20
......