Free Questions for 200-201 by go4braindumps

Shared by Barber on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the communication channel established from a compromised machine back to the attacker?

Options:

A- man-in-the-middle

B- IDS evasion

C- command and control

D- port scanning

Answer:

C

Question 2

Question Type: MultipleChoice

A cyberattacker notices a security flaw in a software that a company is using They decide to tailor a specific worm to exploit this flaw and extract saved passwords from the software To which category of the Cyber Kill Cham model does this event belong?

Options:

A- reconnaissance

B- delivery

C- weaponization

D- exploitation

Answer:

C

Question 3

Question Type: **MultipleChoice**

What is a difference between SI EM and SOAR security systems?

Options:

A- SOAR ingests numerous types of logs and event data infrastructure components and SIEM can fetch data from endpoint security software and external threat intelligence feeds

B- SOAR collects and stores security data at a central point and then converts it into actionable intelligence, and SIEM enables SOC teams to automate and orchestrate manual tasks

C- SIEM raises alerts in the event of detecting any suspicious activity, and SOAR automates investigation path workflows and reduces time spent on alerts

D- SIEM combines data collecting, standardization, case management, and analytics for a defense-in-depth concept, and SOAR collects security data antivirus logs, firewall logs, and hashes of downloaded files

Answer:

C

Question 4

Question Type: MultipleChoice

Endpoint logs indicate that a machine has obtained an unusual gateway address and unusual DNS servers via DHCP Which type of attack is occurring?

Options:

A- command injection

B- man in the middle attack

C- evasion methods

D- phishing

Answer:

B

Question 5

Question Type: MultipleChoice

After a large influx of network traffic to externally facing devices, a security engineer begins investigating what appears to be a denial of service attack When the packet capture data is reviewed, the engineer notices that the traffic is a single SYN packet to each port Which type of attack is occurring?

Options:

A- traffic fragmentation

B- port scanning

C- host profiling

D- SYN flood

Answer:

D

Question 6

Question Type: **MultipleChoice**

What is sliding window anomaly detection?

Options:

A- Detect changes in operations and management processes.

B- Identify uncommon patterns that do not fit usual behavior.

C- Define response times for requests for owned applications.

D- Apply lowest privilege/permission level to software

Answer:

B

Question 7

Question Type: MultipleChoice

An organization that develops high-end technology is going through an internal audit The organization uses two databases The main database stores patent information and a secondary database stores employee names and contact information A compliance team is asked to analyze the infrastructure and identify protected data Which two types of protected data should be identified? (Choose two)

Options:

A- Personally Identifiable Information (Pll)

B- Payment Card Industry (PCI)

C- Protected Hearth Information (PHI)

D- Intellectual Property (IP)

E- Sarbanes-Oxley (SOX)

Answer:

A, D

Question 8

Question Type: MultipleChoice

An engineer is working on a ticket for an incident from the incident management team A week ago. an external web application was targeted by a DDoS attack Server resources were exhausted and after two hours it crashed. An engineer was able to identify the attacker and technique used Three hours after the attack, the server was restored and the engineer recommended implementing mitigation by Blackhole filtering and transferred the incident ticket back to the IR team According to NIST SP800-61, at which phase of the incident response did the engineer finish work?

Options:

A- preparation

B- post-incident activity

C- containment eradication and recovery

D- detection and analysis

Answer:

C

Question 9

Question Type: MultipleChoice

How can TOR impact data visibility inside an organization?

Options:

A- increases data integrity

B- increases security

C- decreases visibility

D- no impact

Answer:

C

Question 10

Question Type: MultipleChoice

What is a difference between a threat and a risk?

Options:

A- A threat is a sum of risks and a risk itself represents a specific danger toward the asset

B- A threat can be people property, or information, and risk is a probability by which these threats may bring harm to the business

C- A risk is a flaw or hole in security, and a threat is what is being used against that flaw

D- A risk is an intersection between threat and vulnerabilities, and a threat is what a security engineer is trying to protect against

Answer:

D

Question 11

Question Type: MultipleChoice

Which evasion method involves performing actions slower than normal to prevent detection?

Options:

A- timing attack

B- traffic fragmentation

C- resource exhaustion

D- tunneling

Answer:

C