ECCouncil

112-51

Network Defense Essentials (NDE) Exam

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

George, a certified security professional, was hired by an organization to ensure that the server accurately responds to customer requests. In this process, George employed a security solution to monitor the network traffic toward the server. While monitoring the traffic, he identified attack signatures such as SYN flood and ping of death attempts on the server.
Which of the following categories of suspicious traffic signature has George identified in the above scenario?

A. Informational
B. Reconnaissance
C. Unauthorized access
D. Denial-of-service (DoS)

Answer: D

Explanation:
Denial-of-service (DoS) is the category of suspicious traffic signature that George identified in the above scenario. DoS signatures are designed to detect attempts to disrupt or degrade the availability or performance of a system or network by overwhelming it with excessive or malformed traffic. SYN flood and ping of death are examples of DoS attacks that exploit the TCP/IP protocol to consume the resources or crash the target server. A SYN flood attack sends a large number of TCP SYN packets to the target server, without completing the three-way handshake, thus creating a backlog of half-open connections that exhaust the server's memory or bandwidth. A ping of death attack sends a malformed ICMP echo request packet that exceeds the maximum size allowed by the IP protocol, thus causing the target server to crash or reboot. DoS attacks can cause serious damage to the organization's reputation, productivity, and revenue, and should be detected and mitigated as soon as possible123. Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-33 to 3-34
What is a denial-of-service attack?, Cloudflare, 2020
Denial-of-service attack - Wikipedia, Wikipedia, March 16, 2021

Question: 2

Identify the loT communication model that serves as an analyzer for a company to track monthly or yearly energy consumption. Using this analysis, companies can reduce the expenditure on energy.

A. Device-to-device model
B. Cloud-to-cloud model

C. Device-to-cloud model
D. Device-to-gateway model

Answer: C

Explanation:
The IoT communication model that serves as an analyzer for a company to track monthly or yearly energy consumption is the device-to-cloud model. The device-to-cloud model is a IoT communication model where the IoT devices, such as smart meters, sensors, or thermostats, send data directly to the cloud platform, such as AWS, Azure, or Google Cloud, over the internet. The cloud platform then processes, analyzes, and stores the data, and provides feedback, control, or visualization to the users or applications. The device-to-cloud model enables the company to monitor and optimize the energy consumption of the IoT devices in real time, and to leverage the cloud services, such as machine learning, big data analytics, or artificial intelligence, to perform advanced energy management and demand response. The device-to-cloud model also reduces the complexity and cost of the IoT infrastructure, as it does not require intermediate gateways or servers to connect the IoT devices to the cloud123. Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-38 to 3-39
IoT Communication Models: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing, DZone, July 9, 2018
IoT Communication Models: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing, Medium, March 26, 2019

Question: 3

Finch, a security professional, was instructed to strengthen the security at the entrance. At the doorway, he implemented a security mechanism that allows employees to register their retina scan and a unique six- digit code, using which they can enter the office at any time.
Which of the following combinations of authentication mechanisms is implemented in the above scenario?

A. Biornetric and password authentication
B. Password and two-factor authentication
C. Two-factor and smart card authentication
D. Smart card and password authentication

Answer: A

Explanation:
The combination of authentication mechanisms that is implemented in the above scenario is biometric and password authentication. Biometric authentication is a type of authentication that uses an inherent factor, such as a retina scan, to verify the identity of the user. Password authentication is a type of authentication that uses a knowledge factor, such as a six-digit code, to verify the identity of the user. By combining biometric and password authentication, Finch

has implemented a two-factor authentication (2FA) system that requires the user to provide two different types of authentication factors to gain access to the office. 2FA is a more secure way of authentication than using a single factor, as it reduces the risk of unauthorized access due to stolen or compromised credentials. Biometric and password authentication is a common 2FA method that is used in many applications, such as banking, e-commerce, or health care123.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-28 to 3-29
What is Biometric Authentication?, Norton, July 29, 2020
What is Two-Factor Authentication (2FA)?, Authy, 2020

Question: 4

Identify the UBA tool that collects user activity details from multiple sources and uses artificial intelligence and machine learning algorithms to perform user behavior analysis to prevent and detect various threats before the fraud is perpetrated.

A. Nmap
B. ClamWin
C. Dtex systems
D. Wireshark

Answer: C

Explanation:
Dtex Systems is the UBA tool that collects user activity details from multiple sources and uses artificial intelligence and machine learning algorithms to perform user behavior analysis to prevent and detect various threats before the fraud is perpetrated. Dtex Systems is a user and entity behavior analytics (UEBA) platform that provides visibility, detection, and response capabilities for insider threats, compromised accounts, data loss, and fraud. Dtex Systems collects user activity data from endpoints, servers, cloud applications, and network traffic, and applies advanced analytics and machine learning to establish baselines of normal user behavior, identify anomalies, and assign risk scores. Dtex Systems also provides contextual information, such as user intent, motivation, and sentiment, to help security teams understand and respond to the threats. Dtex Systems can integrate with other security tools, such as SIEM, DLP, or IAM, to enhance the security posture of the organization123. Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-35 to 3-36
Dtex Systems - Wikipedia, Wikipedia, March 16, 2021
Dtex Systems - User and Entity Behavior Analytics (UEBA), Dtex Systems, 2020

Question: 5

Below is the list of encryption modes used in a wireless network.

1.WPA2 Enterprise with RADIUS
2.WPA3
3.WPA2 PSK
4.WPA2 Enterprise
Identify the correct order of wireless encryption modes in terms of security from high to low.

A. 2 -- >1 -- >4 -- >3
B. 3 -- >1 -- >4 -- >2
C. 4 -- >2 -- >3 -- >1
D. 4 -- >3 -- >2 -- >1

Answer: A

Explanation:

Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both? - How-To Geek, How-To Geek, March 12, 2023
WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences - NetSpot, NetSpot, February 8, 2024
What is WPA3? And some gotchas to watch out for in this Wi-Fi security upgrade - CSO Online, CSO Online, November 18, 2020
[Types of Wireless Security Encryption - GeeksforGeeks], GeeksforGeeks, 2020
[Wireless Security Protocols: WEP, WPA, and WPA2 - Lifewire], Lifewire, February 17, 2021
[WPA vs. WPA2 vs. WPA3: Wi-Fi Security Explained - MakeUseOf], MakeUseOf, January 13, 2021

Question: 6

Which of the following IDS components analyzes the traffic and reports if any suspicious activity is
detected?

A. Command console
B. Network sensor
C. Database of attack signatures
D. Response system

Answer: B

Explanation:
The IDS component that analyzes the traffic and reports if any suspicious activity is detected is the network sensor. A network sensor is a device or software application that is deployed at a strategic point or points within the network to monitor and capture the network traffic to and from all devices on the network. A network sensor can operate in one of two modes: promiscuous or inline. In promiscuous mode, the network sensor passively listens to the network traffic and copies the packets for analysis. In inline mode, the network sensor actively intercepts and filters the network traffic and can block or modify the packets based on predefined rules. A network sensor analyzes the network traffic using various detection methods, such as signature-based, anomaly-based, or reputation-based, and compares the traffic patterns with a database of attack signatures or a model of normal behavior. If the network sensor detects any suspicious or malicious activity, such as a reconnaissance scan, an unauthorized access attempt, or a denial-of-service attack, it generates an alert and reports it to the IDS manager or the operator. A network sensor can also integrate with a response system to take appropriate actions, such as logging, notifying, or blocking, in response to the detected activity123. Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-33 to 3-34
Intrusion Detection System (IDS) - GeeksforGeeks, GeeksforGeeks, 2020
Intrusion detection system - Wikipedia, Wikipedia, March 16, 2021

Question: 7

Which of the following objects of the container network model (CNM) contains the configuration files of a container's network stack, such as routing table, container's interfaces, and DNS settings?

A. Endpoint
B. Sandbox
C. Network drivers
D. IPAM drivers

Answer: B

Explanation:
The object of the container network model (CNM) that contains the configuration files of a container's network stack, such as routing table, container's interfaces, and DNS settings, is the Sandbox. A Sandbox is a logical entity that encapsulates the network configuration and state of a container. A Sandbox can contain one or more endpoints from different networks, and provides isolation and security for the container's network stack. A Sandbox can be implemented using various technologies, such as Linux network namespaces, FreeBSD jails, or Windows compartments. A Sandbox allows the container to have its own view and control of the network resources, such as interfaces, addresses, routes, and DNS settings123. Reference:
The Container Networking Model | Training, Training, 2020
A Comprehensive Guide To Docker Networking - KnowledgeHut, KnowledgeHut, September 27, 2023
Design - GitHub: Let's build from here, GitHub, 2020

Question: 8

Mark, a network administrator in an organization, was assigned the task of preventing data from falling into the wrong hands. In this process, Mark implemented authentication techniques and performed full memory encryption for the data stored on RAM.
In which of the following states has Steve encrypted the data in the above scenario?

A. Data in use
B. Data in transit
C. Data inactive
D. Data in rest

Answer: A

Explanation:
The state in which Mark encrypted the data in the above scenario is data in use. Data in use refers to data that is being processed or manipulated by an application or a system, such as data stored on RAM or CPU registers. Data in use is the most vulnerable state of data, as it is exposed to various threats, such as memory scraping, buffer overflow, or side-channel attacks, that can compromise the confidentiality, integrity, or availability of the data. Data in use encryption is a technique that protects the data while it is being processed by encrypting it in memory using hardware or software solutions. Data in use encryption prevents unauthorized access or modification of the data, even if the system is compromised or the memory is dumped. Data in use encryption is one of the three types of data encryption, along with data at rest encryption and data in transit encryption123. Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-23 to 3-24
Encryption: Data at Rest, Data in Motion and Data in Use, Jatheon, 2020
Data in Use Encryption: What It Is and Why You Need It, Fortanix, 2020

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/