ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Eccouncil

Code: 112-51

Exam: Network Defense Essentials Exam (NDE)

https://www.examsnest.com/exam/112-51/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

Amber is working as a team lead in an organization. She was instructed to share a policy document with all the employees working from remote locations and collect them after filling. She shared the files from her mobile device to the concerned employees through the public Internet. An unauthorized user accessed the file in transit, modified the file, and forwarded it to the remote employees.
Based on the above scenario, identify the security risk associated with mobile usage policies.

A. Lost or stolen devices
B. Infrastructure issues
C. Improperly disposing of devices
D. Sharing confidential data on an unsecured network

Answer: D

Explanation:

Sharing confidential data on an unsecured network is a security risk associated with mobile usage policies. Mobile devices are often used to access and transmit sensitive information over public or untrusted networks, such as WiFi hotspots, cellular networks, or Bluetooth connections. This exposes the data to interception, modification, or redirection by malicious actors who may exploit mobile security vulnerabilities or use network-based attacks, such as man-in-the-middle, spoofing, or sniffing. To prevent this risk, mobile users should follow best practices such as using encryption, VPN, certificate pinning, and secure protocols to protect the data in transit. They should also avoid sending or receiving sensitive data over unsecured networks or applications, and verify the identity and integrity of the endpoint servers before establishing a connection. Reference:
The 9 Most Common Security Threats to Mobile Devices in 2021, Auth0, June 25, 2021
7 Mobile App Security Risks and How to Mitigate Them, Cypress Data Defense, July 10, 2020
The Latest Mobile Security Threats and How to Prevent Them, Security Intelligence, February 19, 2019

Question: 2

Barbara, a security professional, was monitoring the IoT traffic through a security solution. She identified that one of the infected devices is trying to connect with other IoT devices and spread malware onto the network. Identify the port number used by the malware to spread the infection to other IoT devices.

A. Port 25
B. Port 443

C. Port 110
D. Port 48101

Answer: D

Explanation:

Port 48101 is the port number used by the malware to spread the infection to other IoT devices. This port is associated with the Mirai botnet, which is one of the most notorious IoT malware that targets vulnerable IoT devices and turns them into a network of bots that can launch distributed denial-of-service (DDoS) attacks. Mirai scans the internet for IoT devices that use default or weak credentials and infects them by logging in via Telnet or SSH. Once infected, the device connects to a command and control (C&C) server on port 48101 and waits for instructions. The C&C server can then direct the botnet to attack a target by sending TCP, UDP, or HTTP requests. Mirai has been responsible for some of the largest DDoS attacks in history, such as the one that disrupted Dyn DNS in 2016 and affected major websites like Twitter, Netflix, and Reddit. Reference:
Mirai (malware), Wikipedia, March 16, 2021
Mirai Botnet: A History of the Largest IoT Botnet Attacks, Imperva, December 10, 2020
Mirai Botnet: How IoT Devices Almost Brought Down the Internet, Cloudflare, March 17, 2021

Question: 3

Below are the various steps involved in establishing a network connection using the shared key authentication process.
1.The AP sends a challenge text to the station.
2.The station connects to the network.
3.The station encrypts the challenge text using its configured 128-bit key and sends the encrypted text to the AP.
4.The station sends an authentication frame to the AP.
5.The AP uses its configured WEP key to decrypt the encrypted text and compares it with the original challenge text.
What is the correct sequence of steps involved in establishing a network connection using the shared key authentication process?

A. 4 -- >2 -- >1 -- >3 -- >5
B. 4 -- >1 -- >3 -- >5 -- >2
C. 2 -- >4 -- >5 -- >1 -- >3
D. 4 -- >5 -- >3 -- >2 -- >1

Answer: B

Explanation:

The correct sequence of steps involved in establishing a network connection using the shared key authentication process is 4 -> 1 -> 3 -> 5 -> 2. This is based on the following description of the shared key authentication process from the Network Defense Essentials courseware:
The station sends an authentication frame to the AP, indicating that it wants to use shared key authentication.
The AP responds with an authentication frame containing a challenge text, which is a random string

of bits.
The station encrypts the challenge text using its configured WEP key, which is derived from the shared secret key (password) that is also known by the AP. The station sends the encrypted text back to the AP in another authentication frame.
The AP decrypts the encrypted text using its configured WEP key and compares it with the original challenge text. If they match, the AP sends a positive authentication response to the station. If they do not match, the AP sends a negative authentication response to the station.
The station connects to the network if the authentication is successful.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-18 to 3-19
Shared Key Authentication - Techopedia, Techopedia, June 15, 2017

Question: 4

Identify the backup mechanism that is performed within the organization using external devices such as hard disks and requires human interaction to perform the backup operations, thus, making it suspectable to theft or natural disasters.

A. Cloud data backup
B. Onsite data backup
C. Offsite data backup
D. Online data backup

Answer: B

Explanation:

Onsite data backup is the backup mechanism that is performed within the organization using external devices such as hard disks and requires human interaction to perform the backup operations, thus, making it susceptible to theft or natural disasters. Onsite data backup means storing the backup data on a local storage device, such as an external hard drive, a USB flash drive, a CD/DVD, or a tape drive, that is physically located in the same premises as the original data source. Onsite data backup has some advantages, such as fast backup and restore speed, easy access, and low cost. However, it also has some disadvantages, such as requiring manual intervention, occupying physical space, and being vulnerable to damage, loss, or theft. If a disaster, such as a fire, flood, earthquake, or power outage, occurs in the organization, both the original data and the backup data may be destroyed or inaccessible. Therefore, onsite data backup is not a reliable or secure way to protect the data from unforeseen events. Reference:
Should I Use an External Hard Drive for Backup in 2024?, Cloudwards, February 8, 2024
How to Back Up a Computer to an External Hard Drive, Lifewire, April 1, 2022
Best Way to Backup Multiple Computers to One External Drive, AOMEI, December 29, 2020

Question: 5

Which of the following types of network traffic flow does not provide encryption in the data transfer process, and the data transfer between the sender and receiver is in plain text?

A. SSL traffic

B. HTTPS traffic
C. SSH traffic
D. FTP traffic

Answer: D

Explanation:

FTP traffic does not provide encryption in the data transfer process, and the data transfer between the sender and receiver is in plain text. FTP stands for File Transfer Protocol, and it is a standard network protocol for transferring files between a client and a server over a TCP/IP network. FTP uses two separate channels for communication: a control channel for sending commands and receiving responses, and a data channel for transferring files. However, FTP does not encrypt any of the data that is sent or received over these channels, which means that anyone who can intercept the network traffic can read or modify the contents of the files, as well as the usernames and passwords used for authentication. This poses a serious security risk for the confidentiality, integrity, and availability of the data and the systems involved in the file transfer. Therefore, FTP is not a secure way to transfer sensitive or confidential data over the network. Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-31 to 3-32
What is FTP, and Why Does It Matter in 2021?, Kinsta, January 4, 2021
FTP Security, Wikipedia, February 9, 2021

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Eccouncil

Code: 112-51

Exam: Network Defense Essentials Exam (NDE)

https://www.examsnest.com/exam/112-51/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation