CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org - d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT (0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(C.0179s) ICMP SCANNABLE > SCANNER echo reply(type-0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seg=713 checksum=16000
massping done: num_host:1 num response:1
Initiating SYN STEALTH Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER: 63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER: 63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER: 63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCB SCANNER:60517 > SCANNADLE:139 iplen=40 seq=1040604
The SYN STEALTH Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT          STATE       SERVICE
22/tcp        open        ssh
113/tcp       closed      auth
139/tcp       filtered    netbios-ssh
1433/tcp      closed      ms-sql

Nmap done:1 10.155.187.1 (1 host)
```

Which of the following actions will an attacker be able to initiate directly against this host?

A. Password sniffing

B. ARP spoofing

C. A brute-force attack

D. An SQL injection

Correct Answer: C

The Nmap command given in the question performs a TCP SYN scan (-sS), a service version detection scan (-sV), an OS detection scan (-O), and a port scan for ports 1-1024 (-p 1-1024) on the host 192.168.1.1. This command will reveal information about the hos" and running services, which can be used by an attacker to launch a brute-force attack against the host. A brute-force attack is a method of guessing passwords or encryption keys by trying many possible combinations until finding the correct one. An attacker can use the information from the Nmap scan to target specific services or protocols that may have weak or default credentials, such as FTP, SSH, Telnet, or HTTP.

QUESTION 2

Which of the following ICS network protocols has no inherent security functions on TCP port 502?

A. CIP

B. DHCP

C. SSH

D. Modbus

Correct Answer: D

Modbus is an industrial control system (ICS) network protocol that is used for communication between devices such as sensors, controllers, actuators, and monitors. Modbus has no inherent security functions on TCP port 502, which is the default port for Modbus TCP/IP communication. Modbus does not provide any encryption, authentication, or integrity protection for the data transmitted over the network, making it vulnerable to various attacks such as replay, modification, spoofing, or denial-of-service.

QUESTION 3

A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

A. External

B. Agent-based

C. Non-credentialed

D. Credentialed

Correct Answer: B

Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to-date results, as the agents can scan continuously or ondemand, regardless of the system or network status or location.

QUESTION 4

Which of the following describes the difference between intentional and unintentional insider threats\\'?

A. Their access levels will be different

B. The risk factor will be the same

C. Their behavior will be different

D. The rate of occurrence will be the same

Correct Answer: C

The difference between intentional and unintentional insider threats is their behavior. Intentional insider threats are malicious actors who deliberately misuse their access to harm the organization or its assets. Unintentional insider threats are

careless or negligent users who accidentally compromise the security of the organization or its assets. Their access levels, risk factors, and rates of occurrence may vary depending on various factors, but their behavior is the main distinction.

Reference:

CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 12;

https://www.cisa.gov/sites/default/files/publications/Insider_Threat_Mitigation_Guide_508.pdf

QUESTION 5

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)

{

Get-ADUser $user -Properties primaryGroupID |select-object pr:

Add-ADGroupMember "Domain Users" -Members $user

Set-ADUser $user -Replace 0(primaryGroupID=513)

}
```

Which of the following scripting languages was used in the script?

A. PowerShel

B. Ruby

C. Python

D. Shell script

Correct Answer: A

The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

CS0-003 PDF Dumps CS0-003 VCE Dumps CS0-003 Practice Test