CS0-002$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

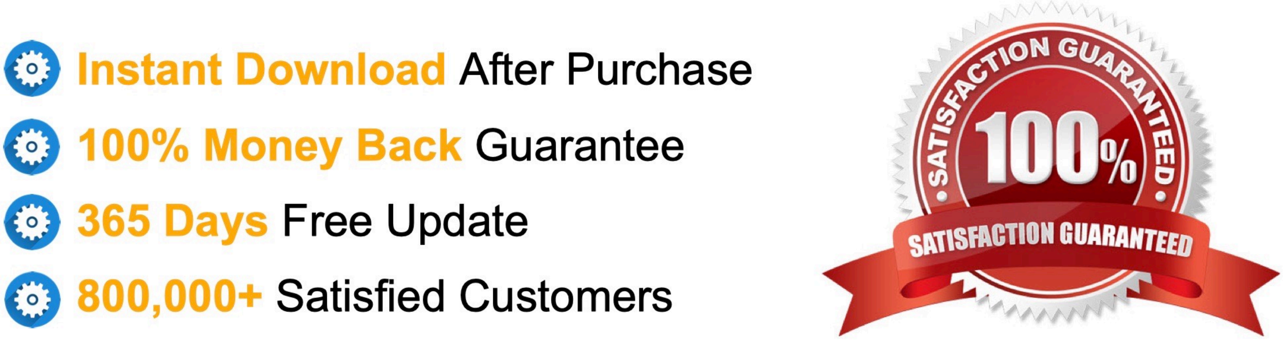
Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.pass2lead.com/cs0-002.html

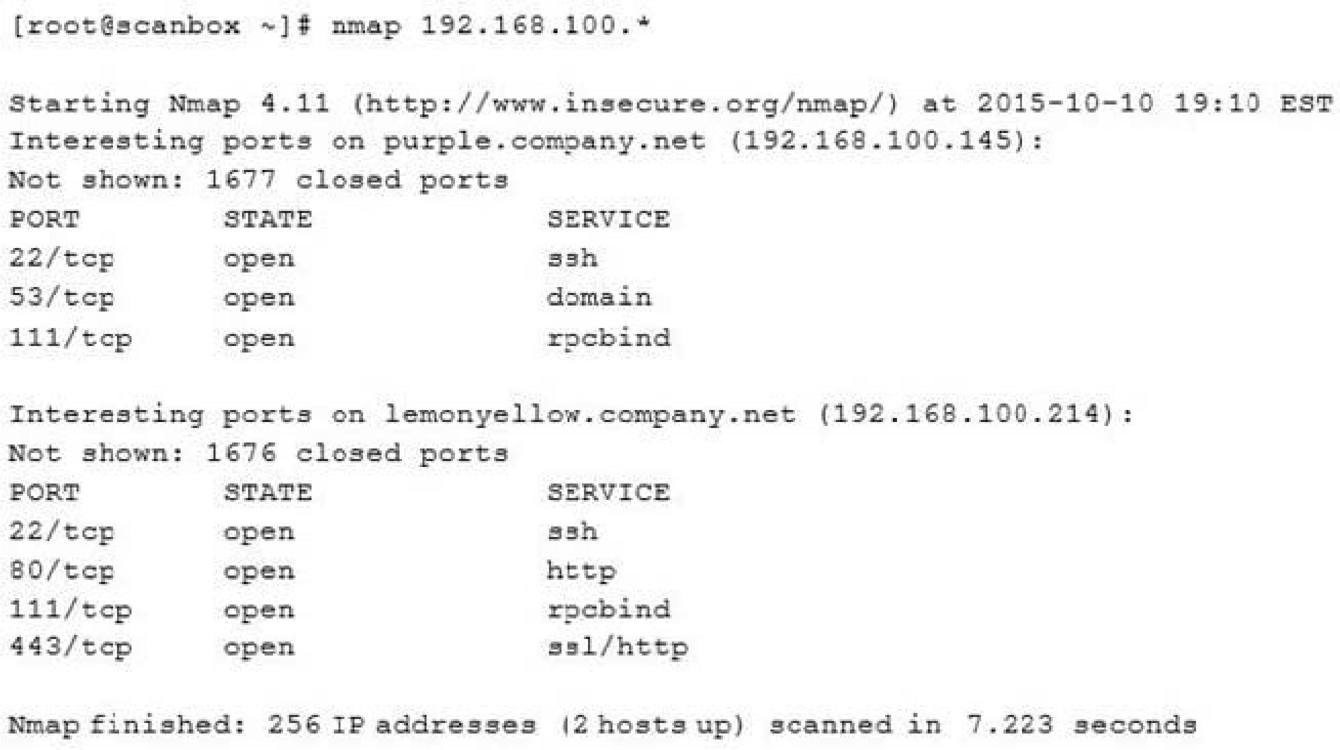
100% Passing Guarantee
100% Money Back Assurance

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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

A security analyst has been asked to scan a subnet. During the scan, the following output was generated:



```
[root@scanbox ~]# nmap 192.168.100.*

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2015-10-10 19:10 EST
Interesting ports on purple.company.net (192.168.100.145):
Not shown: 1677 closed ports
PORT         STATE              SERVICE
22/tcp       open               ssh
53/tcp       open               domain
111/tcp      open               rpcbind

Interesting ports on lemonyellow.company.net (192.168.100.214):
Not shown: 1676 closed ports
PORT         STATE              SERVICE
22/tcp       open               ssh
80/tcp       open               http
111/tcp      open               rpcbind
443/tcp      open               ssl/http

Nmap finished: 256 IP addresses (2 hosts up) scanned in 7.223 seconds
```

Based on the output above, which of the following is MOST likely?

A. 192.168.100.214 is a secure FTP server

B. 192.168.100.214 is a web server

C. Both hosts are mail servers

D. 192.168.100.145 is a DNS server

Correct Answer: B

QUESTION 2

Given the output below:

#nmap 7.70 scan initiated Tues, Feb 8 12:34:56 2022 as: nmap -v -Pn -p 80,8000,443 -- script http-* -oA server.out 192.168.220.42

Which of the following is being performed?

A. Cross-site scripting

B. Local file inclusion attack

C. Log4] check

D. Web server enumeration

Correct Answer: D

Web server enumeration is the process of identifying information about a web server, such as its software version, operating system, configuration, services, and vulnerabilities. This can be done using tools like Nmap, which can scan ports and run scripts to gather information. In this question, the Nmap command is using the -p option to scan ports 80, 8000, and 443, which are commonly used for web services. It is also using the --script option to run scripts that start with http-*, which are related to web server enumeration. The output file name server.out also suggests that the purpose of the scan is to enumerate web servers. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://partners.comptia.org/docs/default- source/resources/comptia-cysa-cs0-002-exam-objectives

QUESTION 3

An analyst suspects a large database that contains customer information and credit card data was exfiltrated to a known hacker group in a foreign country. Which of the following incident response steps should the analyst take FIRST?

A. Immediately notify law enforcement, as they may be able to help track down the hacker group before customer information is disseminated.

B. Draft and publish a notice on the company\\'s website about the incident, as PCI regulations require immediate disclosure in the case of a breach of PII or card data.

C. Isolate the server, restore the database to a time before the vulnerability occurred, and ensure the database is encrypted.

D. Document and verify all evidence and immediately notify the company\\'s Chief Information Security Officer (CISO) to better understand the next steps.

Correct Answer: D

QUESTION 4

An organization wants to harden its web servers. As part of this goal, leadership has directed that vulnerability scans be performed, and the security team should remediate the servers according to industry best practices. The team has already chosen a vulnerability scanner and performed the necessary scans, and now the team needs to prioritize the fixes. Which of the following would help to prioritize the vulnerabilities for remediation in accordance with industry best practices?

A. CVSS

B. SLA

C. ITIL

D. OpenVAS

E. Qualys

Correct Answer: A

QUESTION 5

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

A. Continuous integration and deployment

B. Automation and orchestration

C. Static and dynamic analysis

D. Information sharing and analysis

Correct Answer: B