312-50V11 Q&As

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

https://www.pass4itsure.com/312-50v11.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

A. Data items and vulnerability scanning

B. Interviewing employees and network engineers

C. Reviewing the firewalls configuration

D. Source code review

Correct Answer: A

QUESTION 2

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SVN ping scan?

A. nmap -sn -pp

B. nmap -sn -PO

C. Anmap -sn -PS

D. nmap -sn -PA

Correct Answer: C

QUESTION 3

which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. SSO

B. RADIUS

C. WPA

D. NTLM

Correct Answer: B

Remote Authentication Dial-In User Service (RADIUS) could be a networking protocols, in operation on ports 1812 and 1813, that gives centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS was developed by American Revolutionary leader Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the net Engineering Task Force

(IETF) standards. RADIUS could be a client/server protocol that runs within the application layer, and might use either protocol or UDP as transport. Network access servers, the gateways that management access to a network, sometimes contain a RADIUS consumer element that communicates with the RADIUS server . RADIUS is commonly the back-end of alternative for 802.1X authentication moreover. The RADIUS server is sometimes a background method running on a UNIX system or Microsoft Windows server.

QUESTION 4

Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64

B. 128

C. 255

D. 138

Correct Answer: B

QUESTION 5

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

TCP port 21 no response

TCP port 22 no response

TCP port 23 Time-to-live exceeded

A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server

B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error

C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall

D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host

Correct Answer: C