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.leads4pass.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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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 2

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

A. Heuristic Analysis

B. Code Emulation

C. Scanning

D. Integrity checking

Correct Answer: B

QUESTION 3

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?

A. WEP

B. RADIUS

C. WPA

D. WPA3

Correct Answer: A

Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that\\'s designed to supply a wireless local area network (WLAN) with A level of security and privacy

like what\'s usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren\'t necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network\'s physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy.A research group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks). within the course of the group\'s examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP ?which is included in many networking products ?was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it\'s very effective.

QUESTION 4

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

A. Produces less false positives

B. Can identify unknown attacks

C. Requires vendor updates for a new threat

D. Cannot deal with encrypted network traffic

Correct Answer: B

QUESTION 5

Fred is the network administrator for his company. Fred is testing an internal switch.

From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.

B. He can send an IP packet with the SYN bit and the source address of his computer.

C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.

D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Correct Answer: D

312-50V11 Practice Test   312-50V11 Study Guide   312-50V11 Braindumps