312-50V9^{Q&As}

Certified Ethical Hacker Exam V9

Pass EC-COUNCIL 312-50V9 Exam with 100% Guarantee

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

https://www.pass2lead.com/312-50v9.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

When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host

B. Attacker floods TCP SYN packets with random source addresses towards a victim host

C. Attacker generates TCP ACK packets with random source addresses towards a victim host

D. Attacker generates TCP RST packets with random source addresses towards a victim host

Correct Answer: B Section: (none)

QUESTION 2

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use a scan tool like Nessus

B. Use the built-in Windows Update tool

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Correct Answer: A Section: (none)

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and

Exposures architecture for easy cross-linking between compliant security tools. The Nessus server is

currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based

operating systems.

Note: Significant capabilities of Nessus include:

Compatibility with computers and servers of all sizes.

Detection of security holes in local or remote hosts.

Detection of missing security updates and patches.

Simulated attacks to pinpoint vulnerabilities.

Execution of security tests in a contained environment.

Scheduled security audits.

References: http://searchnetworking.techtarget.com/definition/Nessus

---

QUESTION 3

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance

B. Peer review

C. Change management

D. Penetration testing

Correct Answer: C Section: (none)

QUESTION 4

What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

A. c:\compmgmt.msc

B. c:\gpedit

C. c:\ncpa.cpl

D. c:\services.msc

Correct Answer: A Section: (none)

QUESTION 5

Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning

B. Banner grabbing

C. Injecting arbitrary data

D. Analyzing service response

Correct Answer: D Section: (none)

312-50V9 PDF Dumps

312-50V9 VCE Dumps

312-50V9 Braindumps