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

Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.

What type of attack is outlined in the scenario?

A. Watering Hole Attack

B. Heartbleed Attack

C. Shellshock Attack

D. Spear Phising Attack

Correct Answer: A Section: (none)

Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

Incorrect Answers:

B: Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or a client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug\'s name derives from "heartbeat".

C: Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

D: Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business.

References: https://en.wikipedia.org/wiki/Watering_Hole

QUESTION 2

You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.

Which command-line utility are you most likely to use?

A. Grep

B. Notepad

C. MS Excel

D. Relational Database

Correct Answer: A Section: (none)

grep is a command-line utility for searching plain-text data sets for lines matching a regular expression.

References: https://en.wikipedia.org/wiki/Grep

QUESTION 3

Which type of scan measures a person\\\'s external features through a digital video camera?

A. Iris scan

B. Retinal scan

C. Facial recognition scan

D. Signature kinetics scan

Correct Answer: C Section: (none)

QUESTION 4

At a Windows Server command prompt, which command could be used to list the running services?

A. Sc query type= running

B. Sc query \\servername

C. Sc query

D. Sc config

Correct Answer: C Section: (none)

QUESTION 5

Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.

B. given root or administrative privileges.

C. trusted to keep all data and access to that data under their sole control.

D. given privileges equal to everyone else in the department.

Correct Answer: A Section: (none)

312-50V9 PDF Dumps   **312-50V9 VCE Dumps**   **312-50V9 Practice Test**