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

QUESTION 1

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

A. Eve is trying to connect as a user with Administrator privileges

B. Eve is trying to enumerate all users with Administrative privileges

C. Eve is trying to carry out a password crack for user Administrator

D. Eve is trying to escalate privilege of the null user to that of Administrator

Correct Answer: C

QUESTION 2

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?

A. vendor risk management

B. Security awareness training

C. Secure deployment lifecycle

D. Patch management

Correct Answer: D

Patch management is that the method that helps acquire, test and install multiple patches (code changes)

on existing applications and software tools on a pc, enabling systems to remain updated on existing

patches and determining that patches are the suitable ones.

Managing patches so becomes simple and simple.

Patch Management is usually done by software system firms as a part of their internal efforts to mend

problems with the various versions of software system programs and also to assist analyze existing

software system programs and discover any potential lack of security features or different upgrades.

https://www.leads4pass.com/312-50v11.html
2024 Latest leads4pass 312-50V11 PDF and VCE dumps Download

Software patches help fix those problems that exist and are detected solely once the software\\'s initial

unharness. Patches mostly concern security while there are some patches that concern the particular

practicality of programs as well.

QUESTION 3

Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes.
He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its
firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or
businesses that use it as an IaaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

A. Man-in-the-cloud (MITC) attack

B. Cloud cryptojacking

C. Cloudborne attack

D. Metadata spoofing attack

Correct Answer: C

QUESTION 4

An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

A. Machine A: netcat -l -p -s password 1234

B. Machine A: netcat -l -e magickey -p 1234

C. Machine A: netcat -l -p 1234

D. Use cryptcat instead of netcat

Correct Answer: D

QUESTION 5

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to
secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard

that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

A. PGP

B. S/MIME

C. SMTP

D. GPG

Correct Answer: A