312-39 Q&As

Certified SOC Analyst (CSA)

Pass EC-COUNCIL 312-39 Exam with 100% Guarantee

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

https://www.pass4itsure.com/312-39.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

Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

A. DoS Attack

B. Man-In-Middle Attack

C. Ransomware Attack

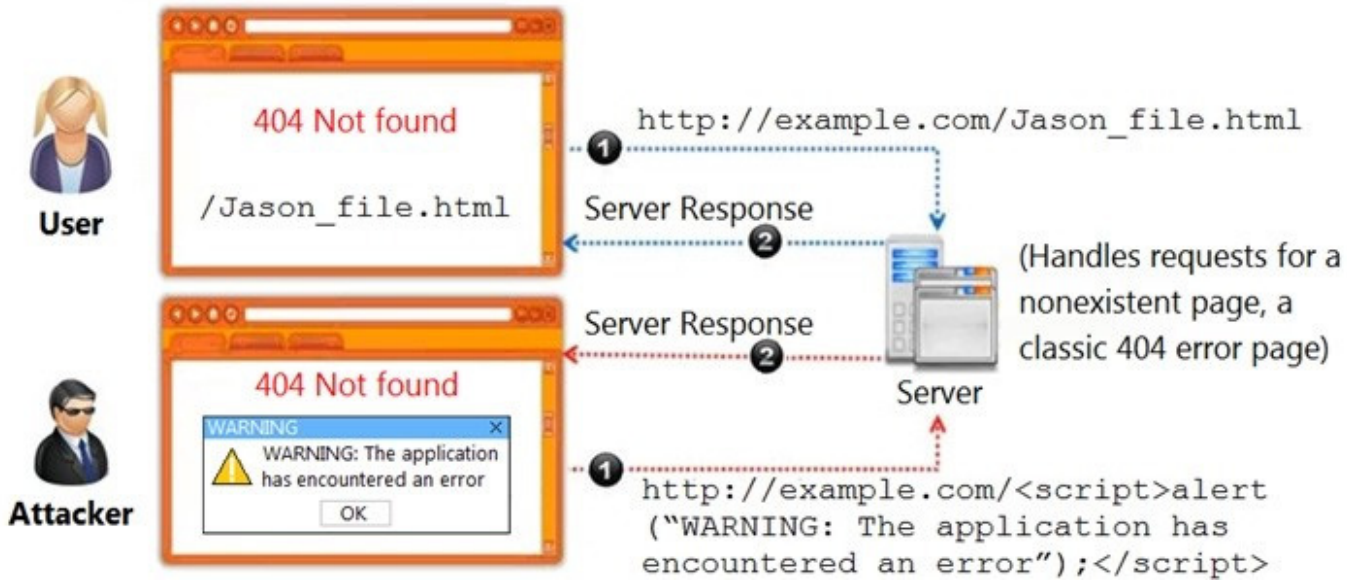
D. Reconnaissance Attack

Correct Answer: D

Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf

QUESTION 2

Identify the type of attack, an attacker is attempting on www.example.com website.



A. Cross-site Scripting Attack

B. Session Attack

C. Denial-of-Service Attack

D. SQL Injection Attack

Correct Answer: A

QUESTION 3

Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?

A. threat_note

B. MagicTree

C. IntelMQ

D. Malstrom

Correct Answer: C

QUESTION 4

A type of threat intelligent that find out the information about the attacker by misleading them is known as _____.

A. Threat trending Intelligence

B. Detection Threat Intelligence

C. Operational Intelligence

D. Counter Intelligence

Correct Answer: C

Reference: https://www.recordedfuture.com/threat-intelligence/

QUESTION 5

Which of the following is a default directory in a Mac OS X that stores security-related logs?

A. /private/var/log

B. /Library/Logs/Sync

C. /var/log/cups/access_log

D. ~/Library/Logs

Correct Answer: D