# 312-39$^{\text{Q\&As}}$

Certified SOC Analyst (CSA)

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

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

**QUESTION 1**

Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.

What is Ray and his team doing?

A. Blocking the Attacks

B. Diverting the Traffic

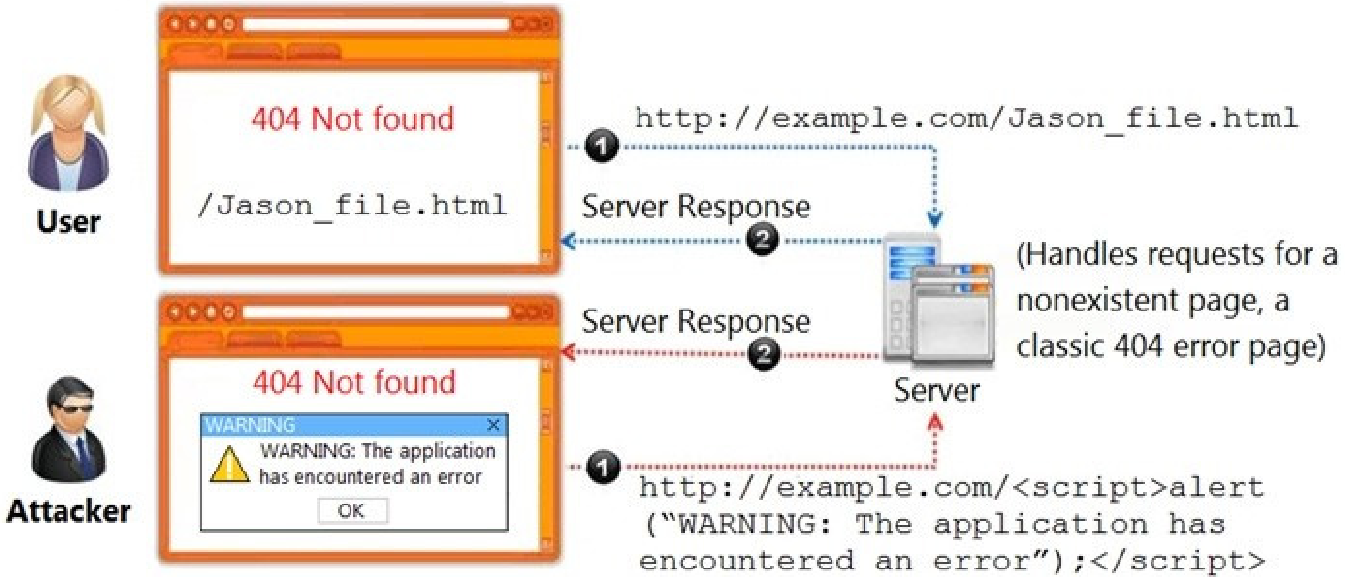
C. Degrading the services

D. Absorbing the Attack

Correct Answer: D

**QUESTION 2**

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


User
404 Not found
/Jason_file.html
1
http://example.com/Jason_file.html
Server Response
2
(Handles requests for a nonexistent page, a classic 404 error page)
Server
Server Response
2
Attacker
404 Not found
WARNING
WARNING: The application has encountered an error
OK
1
http://example.com/<script>alert ("WARNING: The application has encountered an error");</script>

A. Cross-site Scripting Attack

B. Session Attack

C. Denial-of-Service Attack

D. SQL Injection Attack

Correct Answer: A

**QUESTION 3**

Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.

A. Dictionary Attack

B. Rainbow Table Attack

C. Bruteforce Attack

D. Syllable Attack

Correct Answer: A

Reference:
https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic7-final/report.pdf

**QUESTION 4**

Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?

A. Command Injection Attacks

B. SQL Injection Attacks

C. File Injection Attacks

D. LDAP Injection Attacks

Correct Answer: B

Reference: https://www.kiuwan.com/owasp-top-10-a1-injection/

**QUESTION 5**

What does [-n] in the following checkpoint firewall log syntax represents?

```
fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file]
[-m unification_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]
```

A. Speed up the process by not performing IP addresses DNS resolution in the Log files

B. Display both the date and the time for each log record

C. Display account log records only

D. Display detailed log chains (all the log segments a log record consists of)

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk25532