Containment of Web Application Security Incidents

Objectives:

At the end of this episode, I will be able to:

Understand what containment of Web Application security incidents is.

Explain what the containment practices for web application security incidents that IH&R team members should be familiar with are.

Identify what the methods used by the incident handlers during containment are.

External Resources:

Containment of Web Application Security Incidents

Some of the containment practices for web application security incidents include:

```
▪ Enable the Blackhole feature on the web application, so that it drops all
the requests from same source after a limit.

▪ The organization must increase the capacity of their servers in terms of
handling connections. By upgrading server availability, it becomes difficult
for the attackers to perform a low-and-slow attack.

▪ Anti DDoS service providers such as CloudFlare offer DDoS protection and
other features such as maintaining web application “always online”, even if
the administrators take it offline for maintenance purposes. Organizations
may choose such services to fight back effectively against web attacks.

▪ Use routers that can consume all incoming traffic and filter out the
legitimate ones by identifying their protocols, patterns, and standard samples
of incoming packets to mitigate DDoS.

▪ Use a Web Application Firewall (WAF) to monitor and block potential threats.

▪ Deny unnecessary access to any resources for unauthorized users. To reduce
burden on servers, cache the content that unauthorized users send, instead of
using main databases for it.

▪ Isolate the attacker’s operation on the network by removing suspicious user
credentials from the network and web application.

▪ Enable ingress/egress filtering to restrict the flow of traffic from one
network to another, typically from a compromised system.

▪ Install dedicated hardware or software firewall to block UDP or TCP flood
attacks.

▪ Implement CAPTCHA to ensure that only humans are able to submit any requests
or forms in the web application.

▪ Make sure that the web application does not display debugging information
to the users.

▪ Harden Apache by installing the mod_reqtimeout module, which will help the
server to block malicious connections.

▪ Maintain a backup internet connection with a pool of IP addresses for
crucial users.

▪ Perform malware and virus scans, and delete the cookies from the browser
regularly.
```

What are the methods used by the incident handlers during containment? -

```
▪ Whitelisting/Blacklisting
▪ Web Content Filtering
▪ Proxy Servers
```