Preparation for Handling Network Security Incidents

Objectives:

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

Understand why network Incident Handling is important for IH&R team members.

Explain what are the preparation steps or guidelines that should be followed by incident handlers for network incidents.

Identify common network security incidents that IH&R team members should be aware of.

External Resources:

Preparation for Handling Network Security Incidents

Why is Network Incident Handling important? -

Organizations require a proper network IH&R process in order to detect and contain network attacks as early as possible to minimize data losses and maintain business continuity.

In addition, the network IH&R process will help organizations to develop threat intelligence, and build an incident response team equipped with the proper tools to address ongoing threats.

Common network security incidents may include:

```
▪ Unauthorized Access
▪ Inappropriate Usage
▪ Denial of Service (DoS) / Distributed Denial of Service (DDoS)
▪ Wireless Networks
```

What are the preparation steps or guidelines that are followed by incident handlers for network incidents? -

```
▪ Communicate the goals of IH&R processes to ALL members of the organization.

▪ Configure network perimeter control devices such as firewalls, IDS, and IPS
systems to log all the access attempts and send notifications regarding the
attempts of intrusion to the administrator or incident response team.

▪ Implement Syslog or any other centralized logging mechanism to backup logs
from all the network security devices to a single location. This will help in
analysis and correlation of logs.

▪ Clearly define the roles and responsibility of all the users,
administrators, and IH&R team personnel during the incident response process
in maintaining secure access to network infrastructure.

▪ Implement standard network usage protocols

▪ Provide all the IH&R team members necessary training and conduct practice
sessions to verify the team’s efficiency.

▪ Backup all important servers and keep them accessible.

▪ Contact Internet service providers (ISPs) and their second-tier agents to
gather information about the incident handling and response processes for the
network incidents happening at their end.

▪ Gather the contact details of national and government security
organizations, such as CERT and Internet Crime Complaint Center (IC3) to seek
help in case of attacks that impact national security.

▪ Define proper data collection and accumulation strategies and define the
types of data to be collected while performing network forensic analysis.

▪ Define live analysis laboratory configurations and determine host hardening
and sandbox environments.

▪ Identify the type of capture required (e.g., limited capture, full packet
    capture) while performing network data capturing.

▪ Determine appropriate capture device deployment location and ensure the
integrity and security of the network after introduction of a capture device.
```