Detection and Validation of Network Security Incidents

Objectives:

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

Understand why detection and validation of network security incidents is important for IH&R team members.

Explain what are the common techniques that should be followed by incident handlers to detect and validate network security incidents.

Identify common tools that can be used by incident handlers to detect and validate network security incidents.

External Resources:

Detection and Validation of Network Security Incidents

Incident responders need to validate if suspicious events represent an attack / incident by performing analysis of the indicators reported by victims, users, or employees.

The process also includes monitoring of logs for suspicious network connections, correlation of logs, and event time line analysis.

Incident responders can detect and validate the network incidents by the following techniques:

```
▪ Monitoring Network Traffic - The incident responder should monitor the
incoming and outgoing traffic as all types of network activities create
traffic. Network monitoring tools record all types of activities over the
network which can include the details of the users, such as IP address, MAC
address, time, date, protocols, ports, type of connection, systems/URLs
accessed, and size of files shared. Incident responders can use these details
to find the suspicious events.
```

You can use tools like Wireshark, Colasoft Network Analyzer, and Observer Analyzer to monitor network traffic.

```
▪ Sniffing Network Traffic  - A sniffer enables responders to monitor and
analyze data packets, by extracting complete data packets and storing them on
a system for analysis. As a first step, a baseline for network operations
needs to be created to help determine what the "normal" usage of the network
looks like by capturing network performance and bandwidth consumption during
regular traffic hours. Ensure that the sniffer application captures all the
data passing through the networks including wireless connections.
```

You can use tools like Wireshark, Tcpdump, Cain & Abel, and Kismet to sniff network traffic.

```
▪ Performing Packet Analysis - the process of capturing data packets
transmitted through a network and analyzing them to gather details about the
packet such as network, ports, protocols, devices, issues in network
transmission, and other network specifications. Network sniffing and packet
capture tools include Wireshark and NetworkMiner. Use tools such as ngrep to
search for particular strings, binary structures, or patterns across the
captured packets. Incident responders can also deploy a hex editor to view the
raw bits of the packet that include data such as metadata of a file.
```

Some of the tools that can used to perform packet analysis include Cain & Abel, dSniff, ettercap, Network Grep, OmniPeek, Snoop, and Tcpdump.

```
▪ Performing Log Analysis - Log files are the records of devices that include
the processes performed using them over the logging duration. Log analysis
can take place either manually or with the help of log analyzing tools. After
analyzing the logs, apply filters to avoid unnecessary data.


▪ Performing Host Analysis - You can perform static malware analysis
techniques like file fingerprinting, local and online malware scanning,
performing string searches, identifying packing/obfuscation methods, finding
the portable executables (PE) information, identifying file dependencies, and
malware disassembly. In addition, dynamic malware analysis techniques can also
be performed, such as port / process and registry monitoring, Windows services
monitoring, startup programs monitoring, event logs monitoring/analysis,
installation monitoring, files and folder monitoring, device drivers
monitoring, network traffic monitoring/analysis, DNS monitoring/resolution,
and API calls monitoring.
```