Investigating Router Attacks

An attack must be investigated to establish countermeasures that could possibly prevent the success of future attacks. An investigator must keep in mind that the router to be investigated can be in any state and must be returned to its preattack state. The following guidelines should be kept in mind during a router investigation:

- Start with a security policy and develop a plan that includes collecting and defining data.
- Create a reconnaissance methodology that provides information about the target.
- Perform an analysis check to identify incidents and review default passwords and default information.
- Develop an attack strategy for analyzing commands to access the network, access control lists, firewalls, and protocols.
- The investigator must be careful while accessing the router, as valuable evidence can be lost if the router is mishandled.
- Intrusion analysis is vital to identifying the attacker and preventing the success of future attacks.

Investigation Steps

The following steps should be carried out during the investigation of a router attack:

1. Seize the router and maintain the chain of custody.
2. Perform incident response and session recording.
3. Access the router.
5. Identify the router configuration.
6. Examine and analyze.
7. Generate a report.

Seize the Router and Maintain the Chain of Custody

Before starting the investigation process, the investigator should seize the router so that nobody can change its configuration. Chain of custody must be maintained throughout an investigation. Chain of custody is a record of the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence. It is essential to maintain the chain of custody to prevent mishandling of evidence. Doing so also prevents the individual who collected and handled the evidence from being confused while giving testimony during a trial. This record must be handled carefully to avoid claims of corruption or misconduct during a trial. These claims could possibly compromise a case.

The chain of custody must document the following:

- The source of any evidence
- When evidence was received
- The individuals who provided the evidence
- The methods applied to gain the evidence
- The reasons for seizing the evidence
- The evidence handlers

A chain of custody form should include the conditions under which the evidence was collected, who actually handled the evidence, the time of collection, the duration of custody, the security conditions while the evidence was handled and stored, and how the evidence was transferred. A sample chain of custody form can be seen in Figure 4-2.