Intrusion Response

The field of intrusion response deals with the problem of once an intrusion is detected, how can the system be protected? Its goal is to handle the attack in such a way that damage is minimized.

Goal

Handle attempted attack in such a way as to minimize damage as determined by the security policy.

3 categories pf response:

1. Monitor, collect data, perhaps increase amount of data collected
2. Protect, act to reduce exposure
3. Call a human

Incident Prevention

Ideally, intrusion attempts will be detected and stopped before they succeed. This typically involves closely monitoring the system usually with an intrusion detection mechanism and taking action to defeat the attack. In the context of response, prevention requires that the attack be identified before it completes. The defenders then take measures to prevent the attack from completing. This may be done manually or automatically.

Detected and stopped before they succeed
   closely monitoring the system
   take action to defeat the attack

e.g.
   Jailing attackers is an approach that allows the attackers to think that their attacks have succeeded, but places them in a confined area in which their behavior can be controlled and if necessary manipulated.

Intrusion handling

When an intrusion occurs, the security policy of the site has been violated. Handling the intrusion means restoring the system to comply with the site security policy and taking any actions against the attacker that the policy specifies. Intrusion handling consists of six phases:

1. Preparation for an attack
   This step occurs before any attack are detected. It establishes procedures and mechanisms for detecting and responding to attacks.

2. Identification of an attack
   This triggers the remaining phases.

3. Containment of the attack
   This step limits the damage as much as possible.

4. Eradication of the attack
   This step stops the attack and blocks further similar attacks.

5. Recovery from the attack
   This step restores the system to a secure state.
6. Follow-up to the attack
   This step involves taking action against attacker, identifying problems in handling incident, and recording lessons learned.

**Containment Phase**

Containing or confining an attack means limiting the access of the attacker to system resources. The protection domain of the attacker is reduced as much as possible. There are two approaches: passively monitoring the attack and constraining access to prevent further damage to the system.

1. **Passively monitoring** the attack and constraining access to prevent further damage to the system.
   - simply records the attacker’s actions for later use
   - marginally useful
   - possibly learn something about attackers

2. **Constrain actions** by minimizing the protection domain of the attacker while preventing the attacker from achieving their goals.
   - much more difficult
   - Cliff Stoll story of creating a honeypot to occupy the attacker’s attention.

**Eradication Phase**

Eradicating an attack means stopping the attack. The usual approach is to deny access to the system completely or to terminate the processes involved in the attack. An important aspect of eradication is to ensure that the attack does not immediately resume. This requires that attacks be blocked. A common method for implementing blocking is to place wrappers around suspected targets. Firewalls can also be used to prevent access to the system or to re-direct the attacker to a sandbox.

**Follow-Up Phase**

In the follow-up phase, the systems take some action external to the system against the attacker. That action may be legal or technical.

1. Legal Action – criminal or civil
   - filing complaints, law suits

2. Technical Action
   - Technical attack to damage the attackers seriously enough to stop the current attack and discourage future attacks.

Consequences of a counterattack:

1. May harm an innocent party
   - Attacker may be impersonating another site.
   - Attacker may have hacked another site.

2. May have side effects
   - DOS attack

3. Is antithetical to the shared use of a network

4. May be legally actionable