A network intrusion attack is an unauthorized attack on a digital network in various ways. Stealing network resources and jeopardizing social networks is a part of it.

## Phases of Network Intrusion Attacks

There are six phases of a network intrusion attack:

### Reconnaissance

The first step of the attack involves getting familiar with the target. All open-source information that is available over the internet plays a crucial role in this step. The documents regarding the organization and information related to associated people are also a critical aspect.

**Solution:** It is best if you stop the hacker at this very initial stage by installing devices for security. Penetration tests can assist you at this stage.

### Initial Exploitation

If a hacker gets past the reconnaissance stage they then proceed towards initial exploitation. In this phase, they get access to the target network by spear phishing, water-hole attacks, SQL injection attack, or exploiting a known CVE vulnerability.

**Solution:** You still have time to defend your network by regularly updating it. Secondly, you should also make sure that your network is not relying on users for the correct decision. It is also important to set up best security practices such as setting up least amount of privilege, whitelisting applications and segmenting parts of network.

### Establish Persistence

When a hackers get into the network, they aim to establish persistence. Thus, in this phase, the hacker escalates privileges, finds the running keys or gets into the scripts.

**Solution:** Whitelisting is the key to stopping hackers to proceed any further. Through Whitelisting you can separate some assets from the rest of your network. Thus, even if a hacker runs some unusual activity on your network, your critical assets will remain safe.

### Install Tools

Once hackers are sure that a strong ground is set for them to proceed without getting caught then they launch tools. Beginning with installing small tools, the hacker slowly gets hold of your scripts and programs with the heavier ones.

**Solution:** Anti-virus software can be of little help in this stage. However, you can rely on reputation services. These services can detect malicious attackers and block them from communication.

### Move Laterally

If you are unable to stop the attacker by now, then they start moving laterally in your network. In other words, they begin to search for the target inside your network.

**Solution:** It is better late than never which means you can still stop the attacker from proceeding further by network segmentation and monitoring.

### Extract and Exploit

The attacker reaches the final stage which means they have a strong grasp over the target and just need to extract it. By this stage, there is nothing you can do.

You don’t want to know about a breach after an attacker has already extracted your sensitive information. Hence, it’s important to keep a monitoring plan in place and also create data backup in case attackers steal and erase your data.

## Conclusion

Organizations don't realize about every attack and cannot defend themselves against each of those attacks. However, it is always reliable to equip yourself to protect yourself against network intrusion attacks.

Get in touch with [Aardwolf Security](https://aardwolfsecurity.com/contact-us/) today to find out more about how we can help you with our network penetration testing services.