**What Is a Network Attack**

**A network attack is an attempt to gain unauthorized access to an organization’s network, with the objective of stealing data or perform other malicious activity. There are two main types of network attacks:**

**Passive network**

**Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.**

**Active network**

**Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.**

**Types of network attacks**

**Here are the various types of network attacks.**

**1. Unauthorized access  
Unauthorized access refers to attackers accessing a network without receiving permission. Among the causes of unauthorized access attacks are weak passwords, lacking protection against social engineering, previously compromised accounts, and insider threats.**

**2. Distributed Denial of Service attacks  
Attackers build botnets, large fleets of compromised devices, and use them to direct false traffic at your network or servers. DDoS can occur at the network level, for example by sending huge volumes of SYN/ACC packets which can overwhelm a server, or at the application level, for example by performing complex SQL queries that bring a database to its knees.**

**3. Man in the middle attacks  
A man in the middle attack involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.**

**4. Code and SQL injection attacks  
Many websites accept user inputs and fail to validate and sanitize those inputs. Attackers can then fill out a form or make an API call, passing malicious code instead of the expected data values. The code is executed on the server and allows attackers to compromise it.**

**5. Privilege escalation  
Once attackers penetrate your network, they can use privilege escalation to expand their reach. Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.**

**6. Insider threats  
A network is especially vulnerable to malicious insiders, who already have privileged access to organizational systems. Insider threats can be difficult to detect and protect against, because insiders do not need to penetrate the network in order to do harm. New technologies like User and Even Behavioral Analytics (UEBA) can help identify suspicious or anomalous behavior by internal users, which can help identify insider attacks.**

## How to Prevent Network Attacks

## There are many different ways to defend against network-related threats which are.

### **1. Install antivirus software.**

**One of the first lines of defense against malware and other viruses is to install**[**antivirus software**](https://www.forbes.com/advisor/business/software/best-antivirus-software/)**on all devices connected to a network (Roach & Watts, 2021). Antivirus software can detect and prevent malicious files from being installed on a system, and it should be updated regularly to include the latest definitions.**

### **2. Create strong passwords.**

**Another essential step in protecting a network is to create strong passwords. Passwords should be at least eight characters long and include a mix of letters, numbers, and symbols. They should also not be easy to guess—for instance, the user’s name or the name of the company.**

### **3. Enforce security policies.**

**A third way to reduce risk of attacks on a network is to enforce security policies. Security policies can help ensure that all devices on a network are protected against viruses and malware and that users are using strong passwords.**

### **4. Use firewalls.**

**Firewalls are another essential tool in defending networks against security threats. A firewall can help prevent unauthorized access to a network by blocking incoming traffic from untrusted sources.**

### **5. Monitor activity.**

**Finally, it’s important to monitor activity on the network. Tracking logs and other data enables suspicious activity to be identified quickly, allowing security personnel to take steps to investigate and mitigate potential threats.**