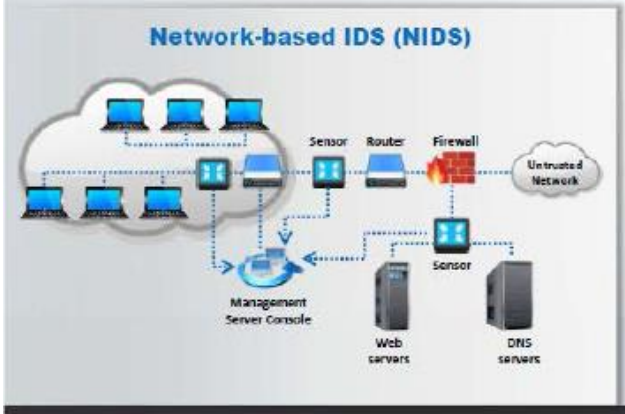
Types of Intrusion Detection Systems

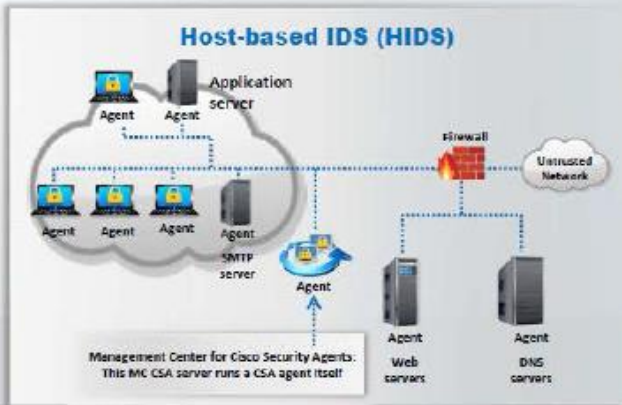
Network-Based Intrusion Detection Systems — 01

- These mechanisms typically consist of a **black box** that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion
- It detects malicious activity such as **Denial-of-Service attacks**, port scans, or even attempts to crack into computers by monitoring network traffic

Host-Based Intrusion Detection Systems — 02

- These mechanisms usually include auditing for events that occur on a **specific host**
- These are not as common, due to the overhead they incur by having to **monitor each system event**





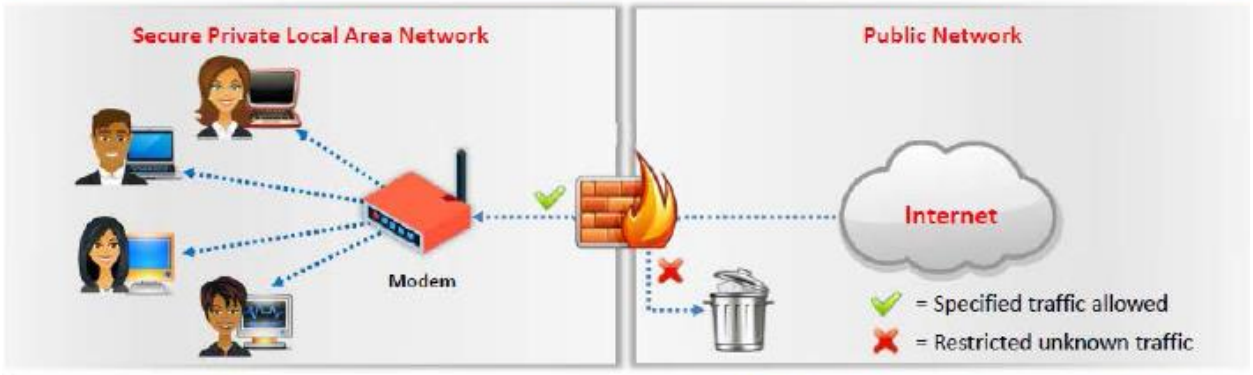
Firewall

Firewalls are hardware and/or software designed to prevent **unauthorized access** to or from a private network

Firewalls **examine all messages entering or leaving the Intranet** and blocks those that do not meet the specified security criteria

They are placed at the junction or **gateway** between the two networks, which is usually a private network and a public network such as the Internet

Firewalls may be concerned with the type of traffic or with the **source** or **destination addresses** and ports

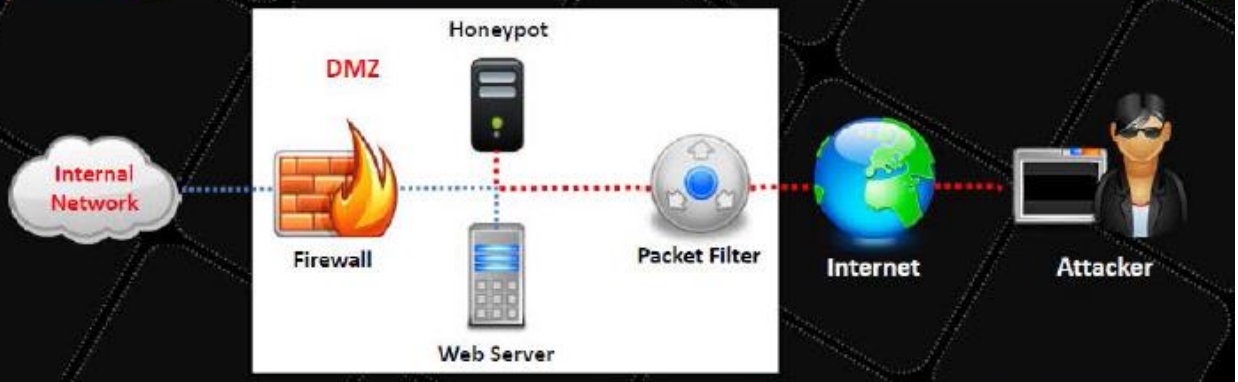


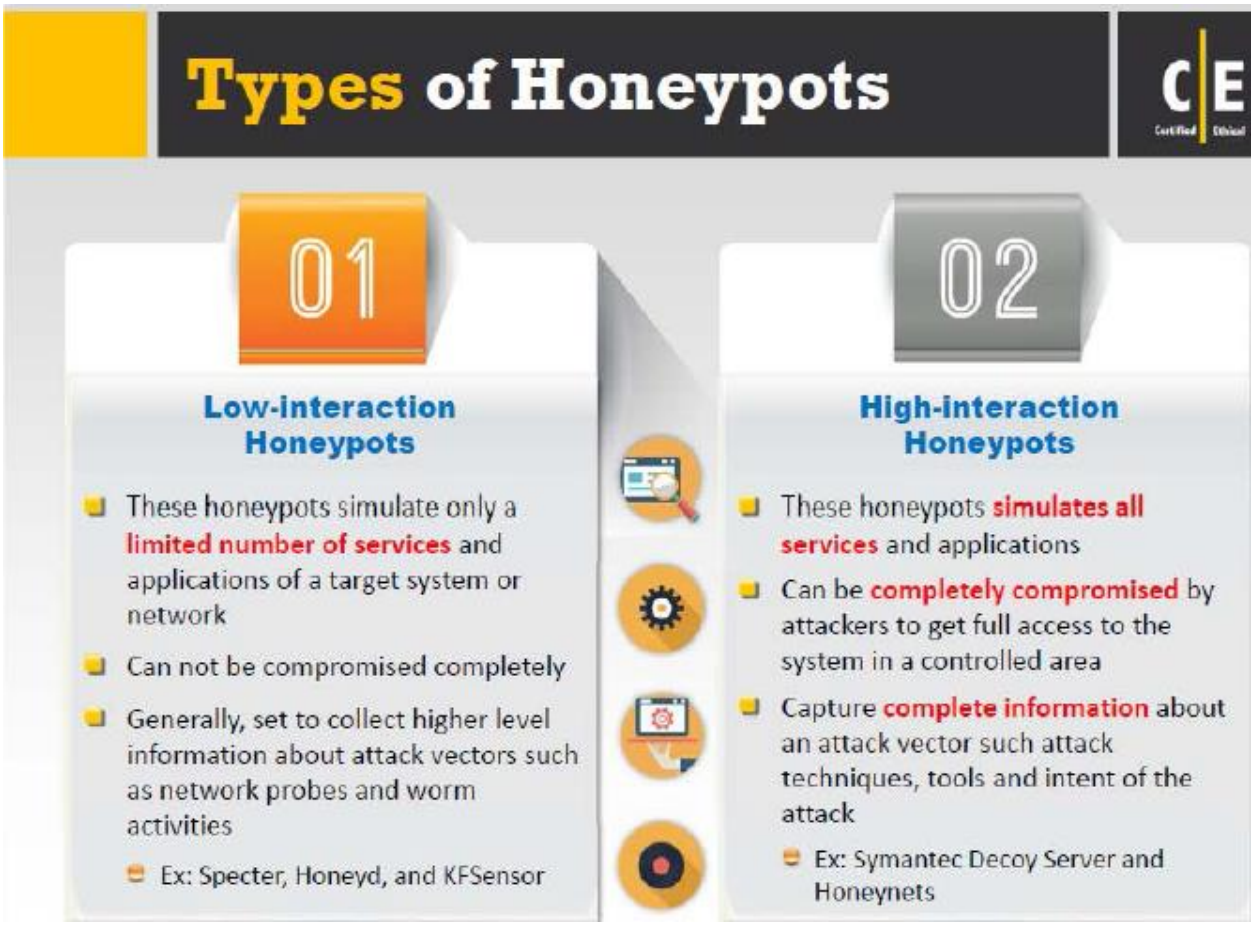
Honeypot

A honeypot is an information system resource that is expressly **set up to attract and trap people** who attempt to penetrate an organization's network

It has no authorized activity, does not have any production value, and any traffic to it is **likely a probe, attack, or compromise**

A honeypot can **log port access attempts, or monitor an attacker's keystrokes. These could be early warnings** of a more concerted attack





How to Bypass an Antivirus using Veil on Kali Linux

```
apt-get update
apt-get install veil
```