Docs on SwarmLab.io !

Πίνακας περιεχομένων

Lab docs

Internet of Things. Is as a networked interconnection of devices in everyday use that are often equippedwith ubiquitous mechanism.

The Internet of Things (IoT) is based on processing of large amount of data in order to provide useful service. Along with physical objects, the IoT is composed of embedded software, electronics and sensors.

Security is defined as a set of mechanisms to protect sensitive data from vulnerable attacks and to guaranteeconfidentiality, integrity and authenticity of data.

1. Prepare your development and test environment

1.1. Install docker

Docker is a set of platform as a service (PaaS) products that use OS-level virtualization to deliver software in packages called containers.

Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels

2. Internet of things (IoT)

2.1. Intro IoT

How It Works, Apps, Swarm: The Five Principles of Swarm Intelligence

3. Security

Security is defined as a set of mechanisms to protect sensitive data from vulnerable attacks and to guaranteeconfidentiality, integrity and authenticity of data.

Network security, in a cloud environment **(IaaS, PaaS, and SaaS) OR Cloud of Things** consists of the security of the underlying **physical environment** and the **logical security** controls that are inherent in the service or available to be consumed as a service.

- Physical environment security ensures access to the cloud service is adequately distributed, monitored, and protected by underlying physical resources.
- Logical network security controls consists of link, protocol, and application layer services.

In a **cloud environment**, a major part of network security is likely to be provided by virtual security devices and services, alongside traditional physical network devices.

Typically, the inspection and control of network traffic do not pass through physical interfaces where classical control devices can analyze or block them.

This is the reason why effective controls require the integration with the software layer - *network security architecture, security gateways (firewalls, WAF, SOA/API), Security Products (IDS/IPS, Sub Tier Firewall, Security Monitoring and Reporting, Denial of Service (DoS) protection/mitigation, and secure "base services" like DNSSEC and NTP*.

3.1. Scan and network statistics

This tutorial demonstrates some common **nmap** port scanning scenarios and explains the output.

3.2. Network analysis

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

3.3. Network Filter

Netfilter offers various functions and operations for **packet filtering**, **network address** translation, and **port translation**, which provide the functionality required for **directing packets** through a network and **prohibiting packets** from reaching sensitive locations within a network.

iptables is a command line utility for configuring Linux kernel firewall implemented within the Netfilter project. The term "iptables" is also commonly used to refer to this kernel-level firewall. It can be configured directly with iptables, or by using one of the many

3.3.1. Traversing of tables and chains

When a packet first enters the firewall, it hits the hardware and then gets passed on to the proper device driver in the kernel.

Then the packet starts to **go through a series of steps in the kernel**, before it is either **sent to the correct application** (locally), or **forwarded to another host** - or whatever happens to i

3.4. Iptables with shorewall! - Three-Interface Firewall

Shorewall is an open source firewall tool for Linux that builds **upon the Netfilter (iptables/ipchains)** system built into the Linux kernel, making it easier to manage more **complex configuration schemes** by providing a higher level of abstraction for describing rules using text files.

3.5. virtual private network (VPN)

A **virtual private network (VPN)** extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were **directly connected to the private network**.

3.6. SSH Tunneling

SSH Tunneling, is the ability to use ssh to **create a bi-directional encrypted network connection** between machines over which data can be exchanged, typically TCP/IP.