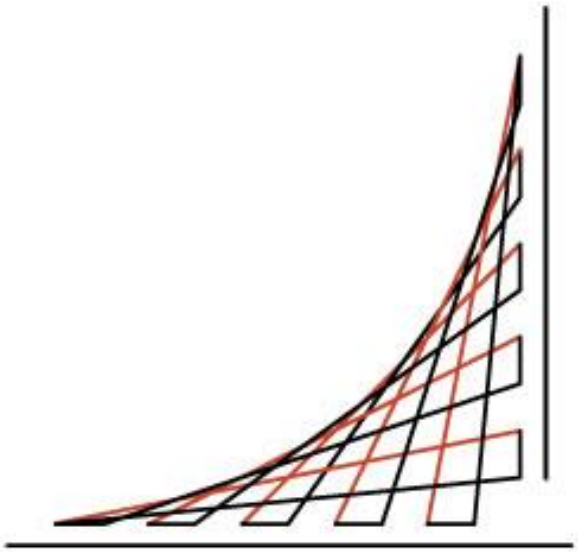


INGENIERIA DE SISTEMAS – SPTI 2021-1

LABORATORIO 1:

# Conceptos Generales y Clasificación de activos de Información

GERSON DAVID QUINTERO RODRIGUEZ

Autor:

Torres Segura Duck James Alexander

# INTRODUCTION

In this laboratory we will learn to classify the assets of a company or company using tools such as Simple Risk, which helps us with the characteristics of the asset and its classification, we will continue learning a little about the CID triad Confidentiality, integrity and availability, all thanks to to the formal definitions used in cybersecurity.

1. SECTION ONE: Security for Internet of Things (IoT).

- Explain what is Internet of Things (IoT).

  the Internet of Things is made up of devices from simple sensors to smartphones and wearables connected together.

- List at least 5 examples of Internet of Things devices that can be found in your surroundings.

  - smart refrigerator.
  - security cameras.
  - robot vacuum cleaners.
  - smart microwave.
  - smart vehicle.

- View the following video about attacks over Internet of Thing devices and answer the following questions:

  - ¿What information assets (Hardware, software, information, network, persons, etc.) were compromised in the attack?

    The electronic and mechanical parts of the car were compromised in the attack using a device inside the car which allowed to decelerate, turn on the radio and turn signals.

  - Identify possible impact (reputational, operative, legal) for the manufactured of the IoT devices which are consequence of the attack. Support your answer with some news or information of similar cases.

    These cases have an impact on the reputation of brands that have vulnerabilities and even more when the IoT era approaches where our vehicles belong to this type of technology.
    We can see the case of Spain and its new 5G implementations on the roads.
    https://www.abc.es/economia/abci-cambiaran-carreteras-espanolas-y-internet-cosas-202101240123_noticia.html?ref=https:%2F%2Fwww.google.com%2F

- ¿How was affected each one of the information security principles (CIA)?

  The principle of confidentiality was affected due to the modification of the car giving all the data to an external person.

  The principle of integrity was affected by modifying the autonomous capacity of the vehicle at the will of a third person.

  The availability principle was affected when the vehicle stopped working correctly for the customer.

## 2. SECTION TWO.

- Describe a real case where you consider that your personal information was vulnerated. Describe which were the attack consequences and what you did after the attack.

  One case was the cloning of my home wireless network by another with the same name and to enter it required the router password again, the attack managed to obtain my wireless network password automatically after I managed to change it.

## 3. SECTION THREE: National cyber-defense and critical infrastructures.

- ¿What is cyber-defense, cyber-attack, and cyber-intelligence? ¿What are the differences between these concepts?

  Cyber defense:
  Cyber defense is all about giving an entity the ability to thwart cyber attacks on the go through cyber security. It involves all processes and practices that will defend a network, its data, and nodes from unauthorized access or manipulation.

  cyber attack:
  Cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks.

Cyber intelligence:
Cyber intelligence can be defined as monitoring, analyzing, and fighting digital security threats.

The difference that these concepts have is the ability to modify, the three work together from the cyber-attack that can only be controlled with cyber-defense and analyzed with cyber-intelligence.

- ¿What is considered critical infrastructure?

  Critical infrastructure includes any system and data, whether physical or virtual, so vital to the state that the destruction of such systems and data would have a debilitating impact on national economic security and Environmental security.

- View the following video about attacks over critical infrastructures and answer the following questions:

  - ¿What information assets (Hardware, software, information, network, persons, etc.) were compromised in the attack?

    In the attack, the data of the people, their Routers, was compromised, as well as the information of the nation kept in the defense ministry.

  - ¿How was affected each one of the information security principles (CIA)?

    The principle of confidentiality was affected by the access to the personal routers of each home that was vulnerable, which allowed obtaining the data of this person.

    The principle of integrity was affected by modifying the operation capacity of their computers connected to the attacked Router.

    The principle of availability was affected when the web service of the attacked ministry could fail imminently due to the attack.

- ¿What can be done against these kinds of threats? Explain your answer.

  In the face of this type of threat, a cyber defense plan must be in place so that governments avoid incidents that may cause a failure in essential services in the country.

## 4. SECTION FOUR: Identify information assets in a company.

- Download a local instance of the solution SimpleRisk from: https://www.simplerisk.com/download.

  - In step 1 select "Use a pre-installed SimpleRisk Virtual Machine Image"

  - In step 2 download a vmware or virtualbox ovf/ova file

  - In step 3 read the document to import, bootstrap the virtual machine, set an IP address and get web access to the interface.

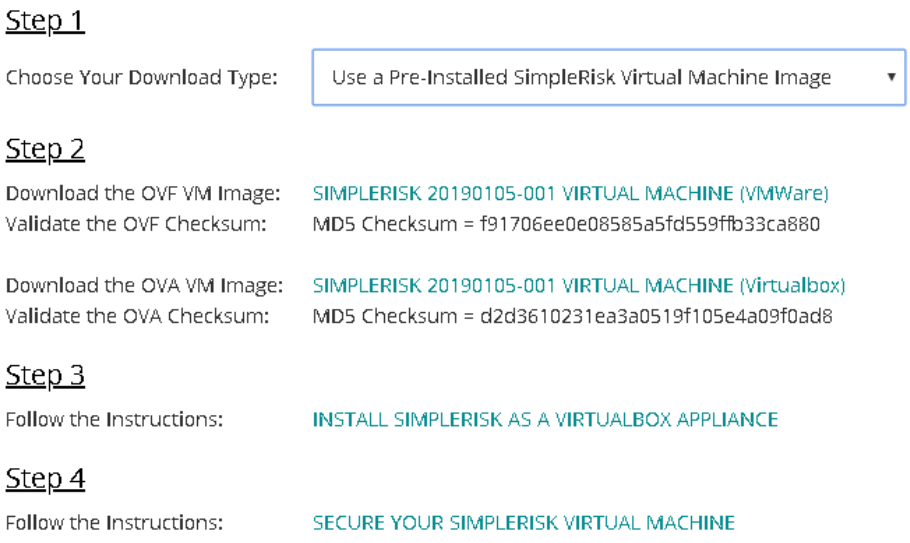


*Figure 1: installation steps*


*Figure 2:installation complete*

- Network configuration: Set the network card of the virtual machine in “bridge mode”, taking care of having mark at least on adapter (Wifi or Ethernet) as show in the following image:

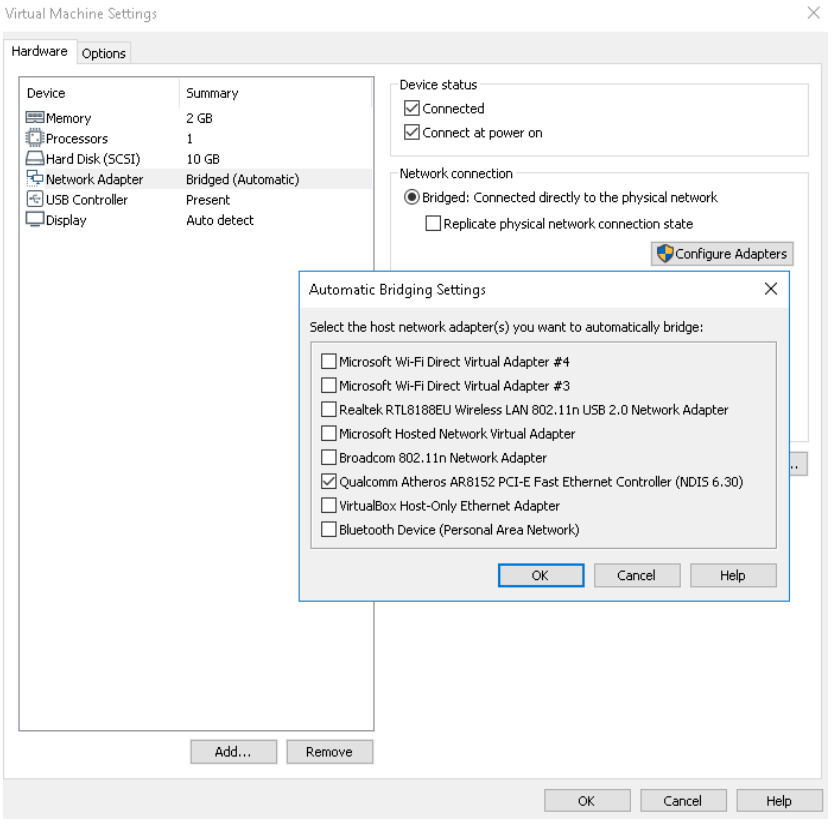


*Figure 3: configuration done*

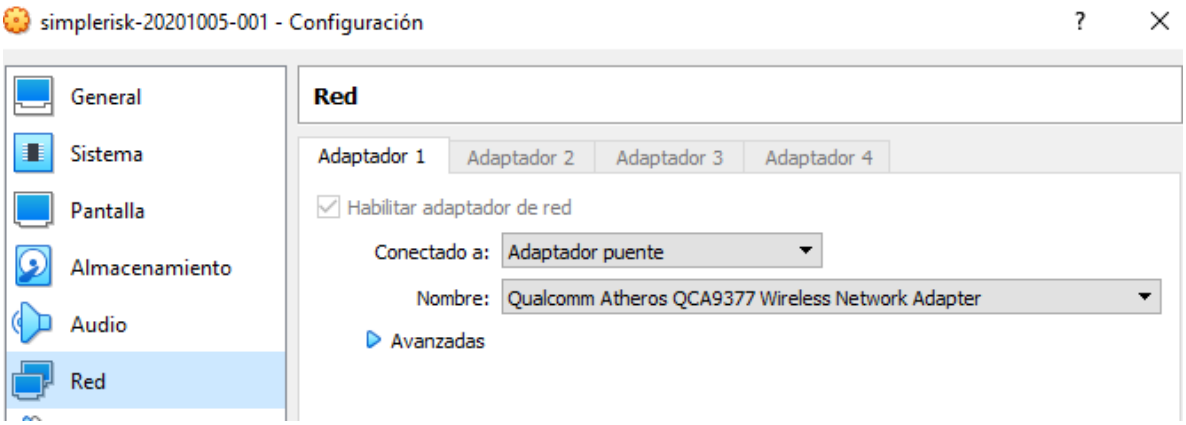


*Figure 4: configuration done.*

- Bootstrap the virtual machine, unlock (decrypt) the disk using password: simplerisk
- Login using credentials: simplerisk/simplerisk

```
Ubuntu 18.04.5 LTS simplerisk tty1

simplerisk login: simplerisk
Password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-122-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Feb  2 06:08:33 UTC 2021

  System load:  0.02              Processes:           94
  Usage of /:   38.1% of 4.90GB   Users logged in:     0
  Memory usage: 29%               IP address for eth0: 192.168.0.13
  Swap usage:   0%

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

0 packages can be updated.
0 updates are security updates.


simplerisk@simplerisk:~$
```

*Figure 5: login*

- Use the ifconfig -a command to see the name of all the interfaces you have in your virtual machine. In my case I had two ones: ens33 and lo.

```
simplerisk@simplerisk:~$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.13  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe83:74da  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:83:74:da  txqueuelen 1000  (Ethernet)
        RX packets 582  bytes 816890 (816.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 447  bytes 33782 (33.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 1540 (1.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 1540 (1.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

simplerisk@simplerisk:~$ _
```

*Figure 6: command done*

- As Simplerisk is installed on Ubuntu 18.04 platform, set the IP address modifying the following file /etc/netplan/01-netcfg.yaml in the following way:
    - For this case I chose the IP: 10.10.3.113/24 with gateway 10.10.3.1 and DNS 10.1.0.17.
    - In the Networks Laboratory you can chose any available IP from the range 10.2.77.X/16 with gateway: 10.2.65.1 and DNS 10.2.65.60.

**Netplan file before being modified**

```
 GNU nano 2.9.3                          /etc/netplan/01-netcfg-bck.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
```

*Figure 7: configuration done*

**Netplan file after being modified**

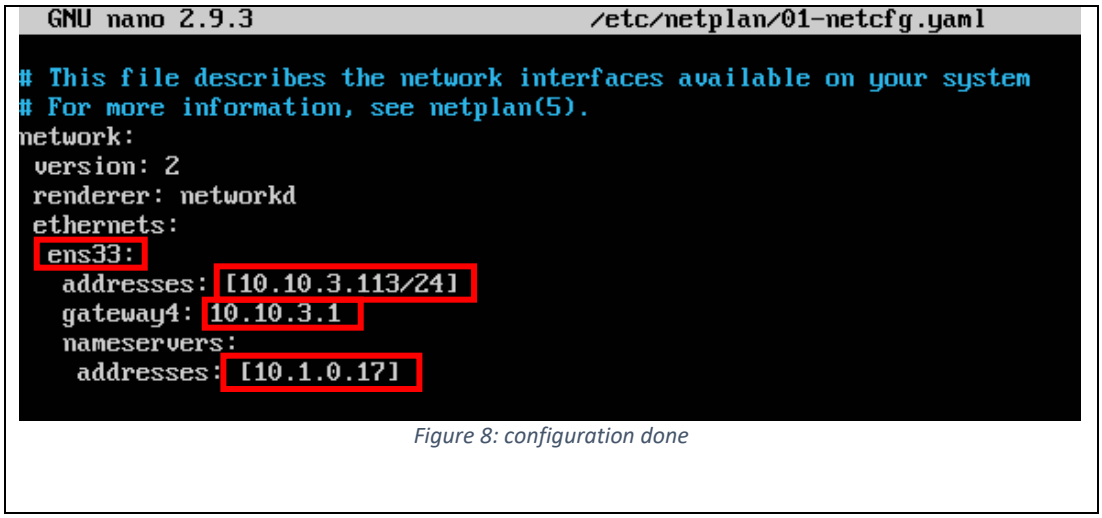


*Figure 8: configuration done*

Netplan do not accept TABS and is strict with identation, so only use spaces inside the 01-netcfg.yaml document.

- Apply changes typing: sudo netplan apply
- In configure, go to "Add and remove values" and in status delete all existing status and create the followings: Accepted, Avoided, Mitigated and Transferred.

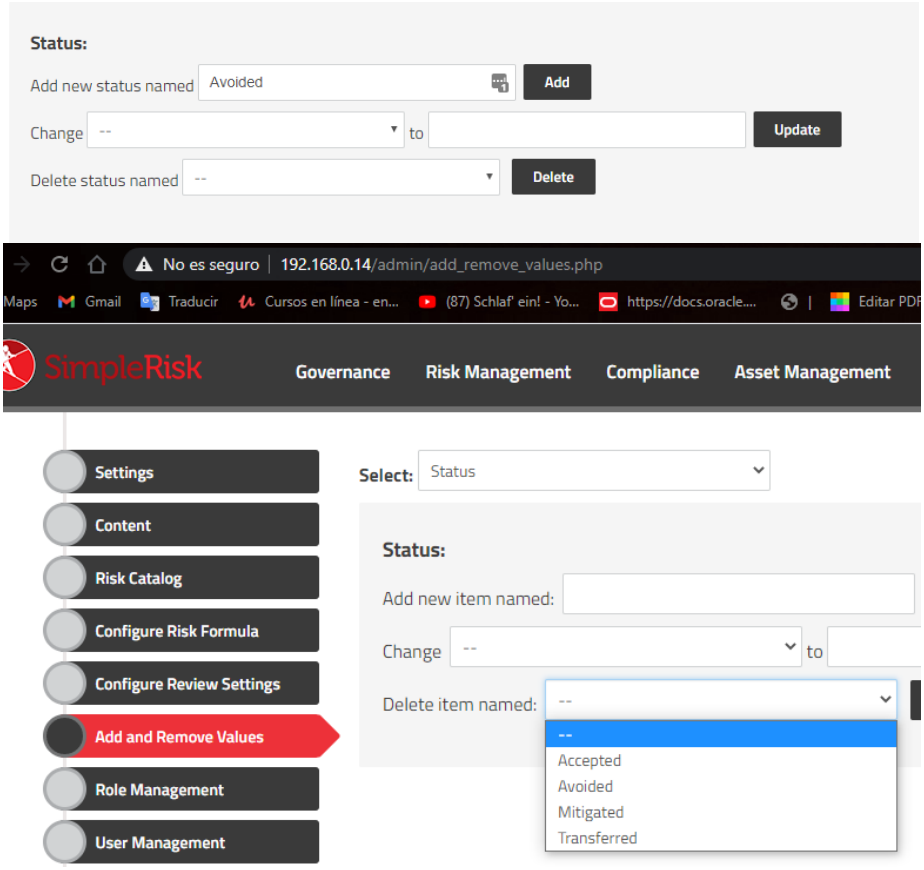


*Figure 9:configuration SimpleRisk*

After setting the network card you should be able to start a browser and access the SimpleRisk interface where you can log in using the credentials admin/admin:

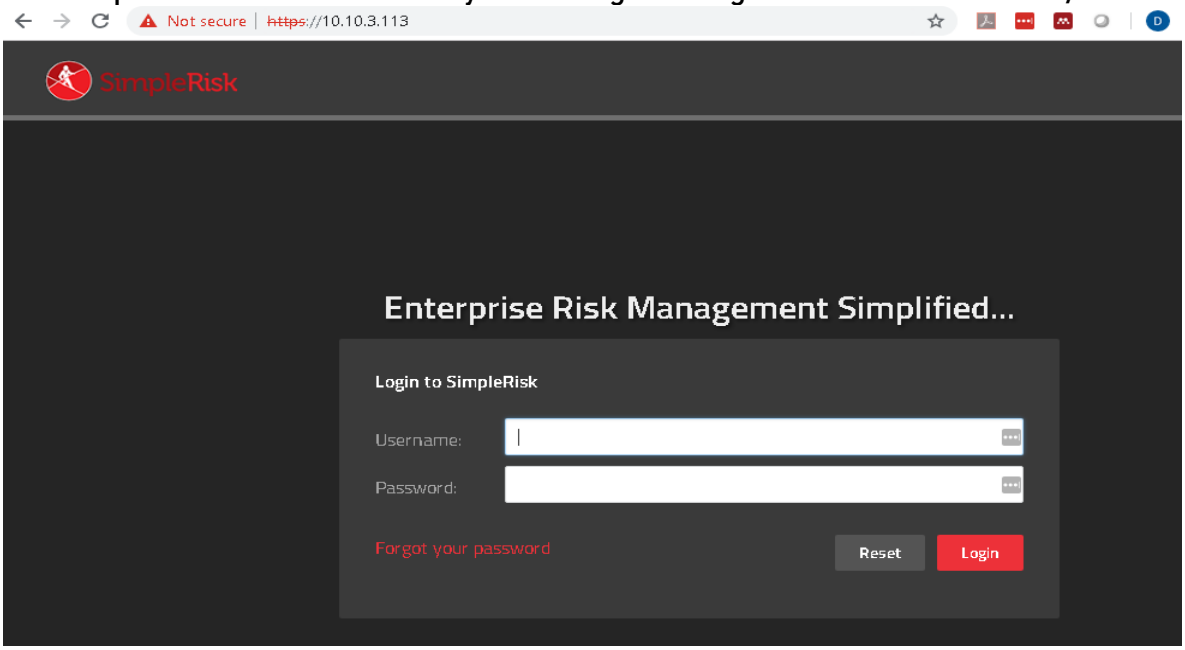


*Figure 10: login*

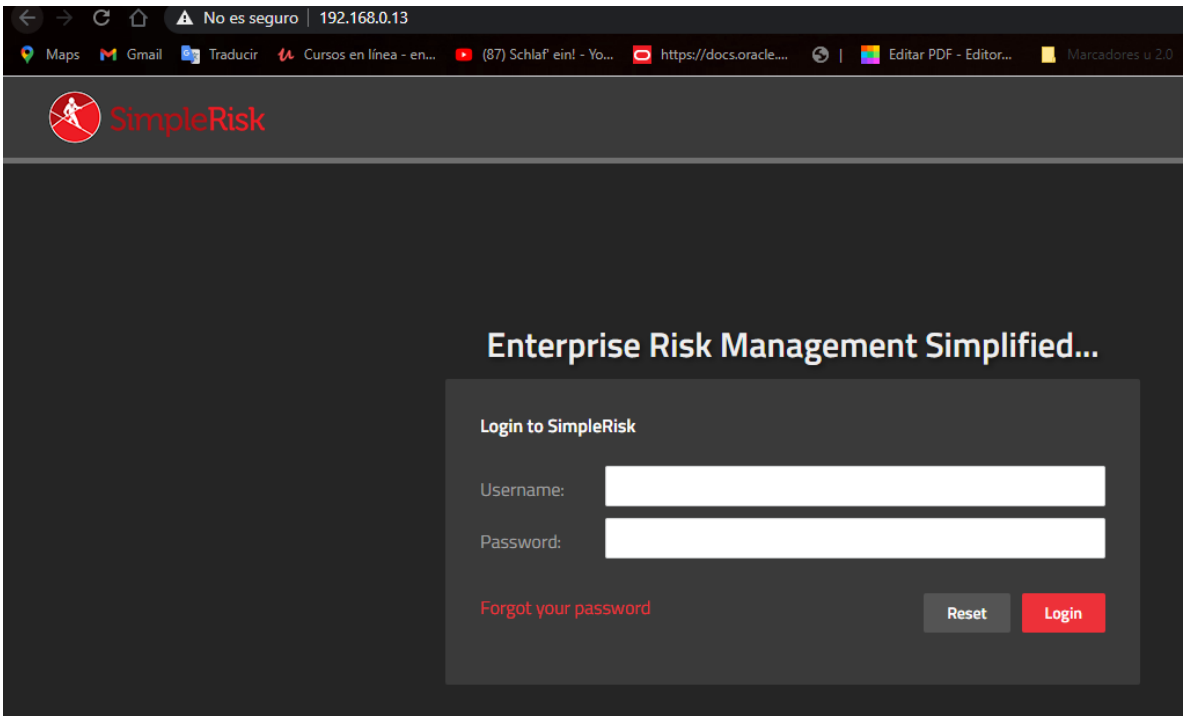


*Figure 11: login done*

Fll out the “Asset Management” section in SimpleRisk. For each asset fill: Asset name, IP Address, Site/location, Team and Asset Details. In Asset Details you must place the following information:

1. Name of the owner
2. Name of the responsible
3. Name of the custodian
4. Name of the area or process where the assets belongs
5. Type of asset (Hardware, software, information, network, persons, etc)
6. Asset users
7. Classification (Publico, Uso interno, Reservado, Confidencial)
8. Impact to availability [1-5]
9. Impact to confidentiality [1-5]
10. Impact to Integrity [1-5]
11. Total Impact

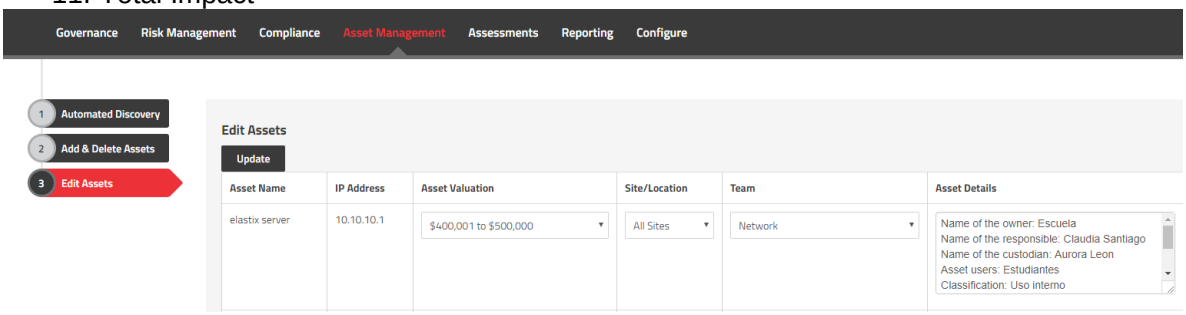


*Figure 12: configuration assets*

Use the following table to evaluate impact:

| | |
|---|---|
| **5: Critico** | * Genera perdidas de alto costo, como sanciones, multas o demandas que impidan la ejecución normal de las tareas |
| | * Se impacta la imagen y se pierde la confianza con los usuarios de la entidad. |
| **4: Alto** | * Podría generar pérdidas de alto costo, como sanciones, multas o demandas que impidan la ejecución normal de las tareas a corto plazo |
| | * Podría causar un impacto negativo en la imagen y confianza en los usuarios de la entidad. |
| **3: Medio** | * Podría generar pérdidas de costo moderado, como sanciones, multas o demandas que impidan la ejecución normal de las tareas a mediano plazo |
| | * Podría impactar la imagen de la entidad negativamente, en áreas, servicios o sectores de usuarios de la SIC. |
| **2: Bajo** | * Podría generar pérdidas de costo bajo, como sanciones, multas o demandas que no afecte considerablemente la ejecución normal de las tareas |
| | * Podría generar un impacto poco considerable en áreas, servicios o sectores de usuarios de la SIC. |
| **1: Insignificante** | * No genera costos significativos para la ejecución de las tareas |
| | * No afecta la imagen de la entidad. |

*Table 1: impact*

Use the following table to evaluate classification:

| **Descripción** | **Nivel de clasificación** |
|---|---|
| **El activo puede ser consultado por todo el mundo** | Publico |
| **El activo pude ser consultado solo por personal de la entidad** | Uso Interno |
| **El activo se considera información Reservada por ley o mandato (Ley 1581 de 2012, Ley 1266 de 2008, etc)** | Reservado |
| **El activo puede ser consultado solo por un grupo de personas en particular** | Confidencial |

*Table 2: classification*

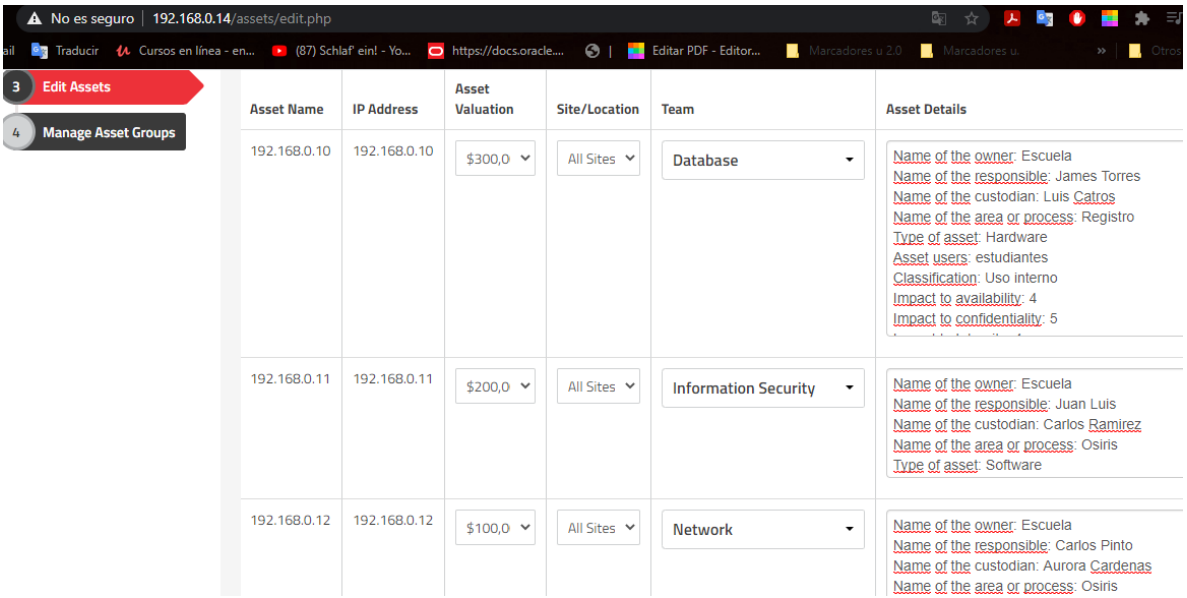


*Figure 13: configuration assets done*

- Prepare an Executive Summary with the analysis of the information assets that you have just filled in the Excel. Use graphics to represent the information. The executive summary must allow the company manager to know the impact of the assets and make decisions about how to protect the assets.

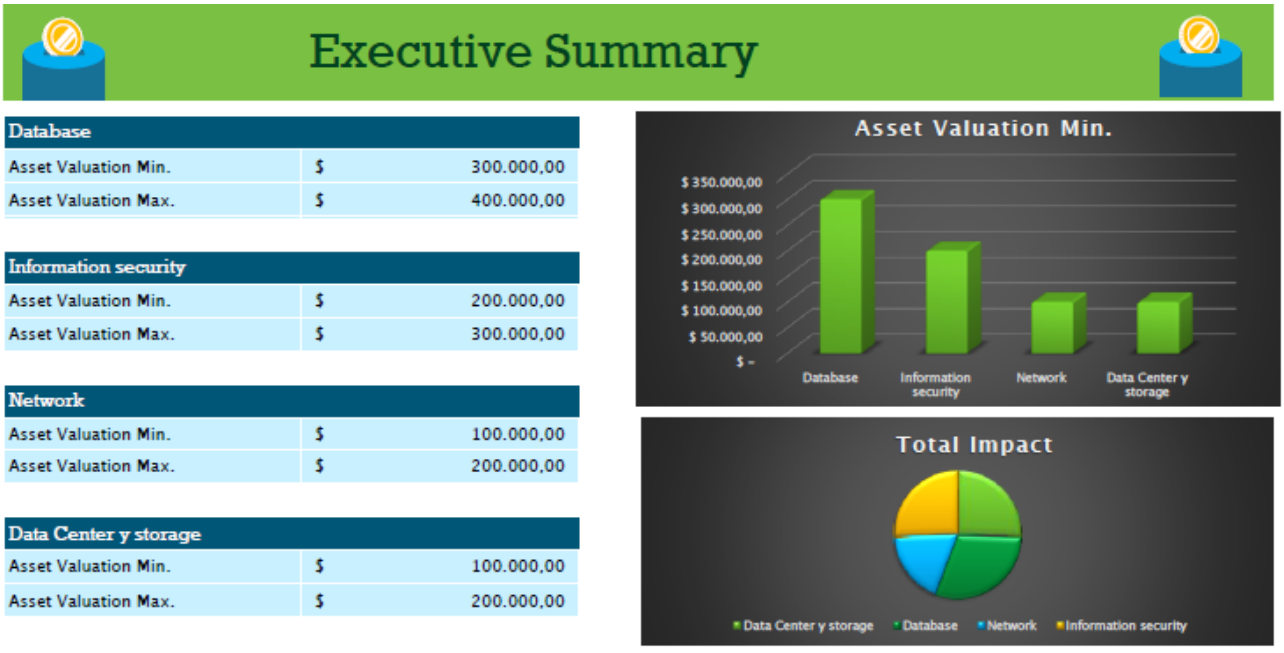


*Figure 14: Executive Summary*

## 5. SECTION FIVE

- For each laboratory session, each student must find out about some security threat that is published by some media. Each class, the teacher can select one student and ask him/her to describe the threat. Some examples of media are:

    - https://cyberstreetwise.com/
    - http://www.bbc.com/news/technology
    - http://www.theguardian.com/media-network/information-security
    - http://www.telegraph.co.uk/technology/internet-security/
    - http://www.bloomberg.com/topics/cybersecurity

- Understand the basic metrics from the CVSS Score 3.0: https://www.first.org/cvss/specification-document Play a bit with the following CVSS Score calculator: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:H

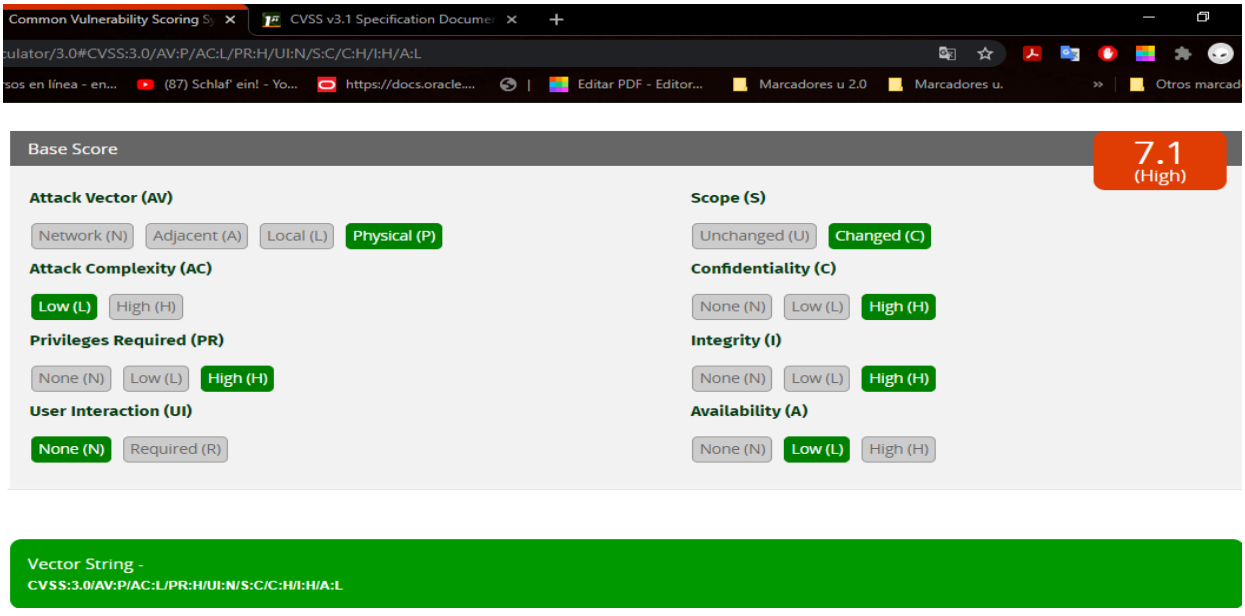


*Figure 15: CVSS done*

The Common Vulnerability Scoring System (CVSS) captures the principal technical characteristics of software, hardware and firmware vulnerabilities. Its outputs include numerical scores indicating the severity of a vulnerability relative to other vulnerabilitieS.

- Go to the following link: https://source.android.com/security/bulletin/index.html and describe which was the last Android security bulletin, publication date, number and kinds of security patch levels. For two vulnerabilities included in the bulletin, specify: description of the vulnerability, severity, operative systems affected.

Android Security Bulletin – January 2021.
2021-01-05 security patch levels.
posted in AOSP.

| CVE | Type | Severity (Qualitative) | Severity (Quantitative) | CVSS v3.0 Vector | Describe an exploitation scenario explaining all the metrics included in the CVSS Vector |
|---|---|---|---|---|---|
| **CVE-2021-0313** | DoS | Crítico | 5 | CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Break layout context before and after bidi control carácter. |
| **CVE-2021-0303** | EoP | Alto | 4 | CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | GrpcGraph initializes StreamSetObserver - which triggers a thread to notify GrpcGraph of termination. |
| **CVE-2021-0306** | EoP | Alto | 4 | CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | If a permission owner changes, or a permission level is upgraded, revoke the permission from all packages |
| **CVE-2021-0307** | EoP | Alto | 4 | CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | GrpcGraph initializes StreamSetObserver - which triggers a thread to notify GrpcGraph of termination. |
| **CVE-2021-0310** | EoP | Alto | 4 | CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Add tests for revoking install permissions when definer is uninstalled. |
| **CVE-2021-0315** | EoP | Alto | 4 | CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Protect GrantCredentialsPermissionActivity against overlay. |
| CVE-2021-0317 | EoP | Alto | 4 | CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Revoke permission on non-runtime -> runtime upgrade |
| **CVE-2021-0318** | EoP | Alto | 4 | CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Since there is no check to see if SensorEventConnection has been destroyed, the mEventCache pointer can still be used even after it was freed. |

*Table 3: Andorid security bulletin*

- The Android Security Bulletin just covers Google mobile phones (Pixel and Nexus), so, ¿Who covers the vulnerabilities from phones of other brands? The answer is that each manufacturer should publish its own security updates. Let's check for example Samsung Android Security Updates: Go to the following link: http://security.samsungmobile.com/smrupdate.html and describe which was the last Samsung Android Security Update and publication date. For two vulnerabilities included in Samsung Android Security Update, specify: description of the vulnerability, severity, operative systems affected.

  SMR-FEB-2021
  February 2021
  (SMR) process

| CVE | Type | Severity (Qualitative) | Severity (Quantitative) | CVSS v3.0 Vector | Describe an exploitation scenario explaining all the metrics included in the CVSS Vector |
|---|---|---|---|---|---|
| **SVE-2021-19221** | DoS | alto | 4 | CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | The patch adds the proper input validation to prevent local permanent denial of service. |
| **SVE-2021-18243** | EoP | medio | 3 | CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Improper access control vulnerability in Samsung keyboard version prior to SMR Feb-2021 Release 1 allows arbitrary change in Settings during Initialization State.<br>The patch adds proper access control for additional functions of Samsung keyboard |
| **SVE-2021-18877** | EoP | bajo | 2 | CVSS:3.0/AV:P/AC:H/PR:H/UI:R/S:C/C:N/I:L/A:L/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Lockscreen bypass vulnerability in Secure Folder. |
| **SVE-2021-19482** | EoP | bajo | 2 | CVSS:3.0/AV:P/AC:H/PR:H/UI:R/S:C/C:N/I:N/A:L/CR:L/IR:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H | Unnecessary logs in libhwui library version prior to SMR Feb-2021 Release 1 allows leakage of object address. |

*Table 4: samsung security bulletin*

- Find out and define the following terms: Cyber-criminal, Spies, Hacktivists, Insider attacker, Cyber terrorists, Cyber Warriors, Script Kiddies, and Online Social Hackers.

Cyber-criminal:

Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

Spies:

Cyber espionage is a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.

Hacktivists:

Hacktivism is the act of misusing a computer system or network for a socially or politically motivated reason. Individuals who perform hacktivism are known as hacktivists.

Insider attacker:

An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.

Cyber terrorists:

premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents.

Cyber Warriors:

They are those people who are responsible for committing cyber attacks.

Online Social Hackers:

Social hacking describes the act of attempting to manipulate outcomes of social behaviour through orchestrated actions.

- Find out the meaning of the following terms: Threats, Vulnerability, Security Controls.

Threats:

cybersecurity threat is any malicious attack by an individual or organization to gain access to another individual's or organization's network to corrupt data or steal confidential information.

Vulnerability:

in computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries within a computer system.

Security Controls:

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

- ¿What is the difference between Proprietary, Responsible and custodian for an asset?

The difference is that the owner is the owner of the asset, the person responsible is responsible for its modification, while the custodian is the person who insures the asset.

## CONCLUSIONS

In this laboratory we learned to classify the assets of a company or company using tools such as Simple Risk where we manage to assign their values and managers as well as specific details of the asset, we learned and refined the concepts of the CID triad Confidentiality, integrity and availability , all this thanks to the formal definitions used in cybersecurity.

## REFERENCES


- Trendmicro, cybercriminals, https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals
- Samsungmobile, securityupdate

  https://security.samsungmobile.com/securityUpdate.smsb
- First, cvss, https://www.first.org/cvss/v3.0/specification-document
- Android, security bulletin, https://source.android.com/security/bulletin/2021-01-01
- Ncsc, cyberaware, https://www.ncsc.gov.uk/cyberaware/home
- BBC, technology, https://www.bbc.com/news/technology