TEK-UP University

Tunisian Republic
Ministry of Higher Education and Scientific Research

Private Higher School of Technologies and Engineering

Computer Science Engineering Curriculum

Internship Report

An OSINT investigation using modern OSINT techniques

Submitted by
Ghassen Landoulsi

Company : Pwn & Patch

Academic Year: 2021/2022

TEK-UP
Ecole Supérieure Privée
Technologie & Ingénierie

Tunisian Republic
Ministry of Higher Education and Research
Private Higher School of Technologies & Engineering

وزارة التعليم العالي والبحث العلمي

SUMMER INTERNSHIP REPORT

Level : TIC

An OSINT investigation using modern OSINT techniques

By GHASSEN LANDOULSI

realized within Pwn&Patch

Professional supervisor : LESIS Oussama

Period of the internship :
17/07/2023 - 17/08/2023

Scholar year: 2022 - 2023

Contents

General Introduction

As part of the preparation for my engineering degree at the Private Higher School of Technologies Engineering, I wanted to have my internship in a company that meets these challenges of the future in CyberSecurity. Pwn&Patch uses the latest cybersecurity techniques and methodologies to ensure that organizations are safe by securing critical IT infrastructures and sensitive information. The combined competence and perseverance of Pwn&Patch's employees gave me a great environment to further enrich and develop my skills and knowledge and I'm forever grateful for their help.

First, we will describe Pwn&Patch and its mission and I present the direction where I spent my internship. My second chapter was a look at OSINT's history and its general steps. The third chapter describes the investigation I was tasked with, and I end with a conclusion where I resume what I learned during this internship.

Chapter 1

The General framework of the internship

1.1 The General presentation of the host organization

1.1.1 Presentation of Pwn&Patch

Pwn&Patch is a cyber security consulting company that offers several services to help all types of businesses protect themselves against the security risks that are increasing day by day. With a qualified and certified team by several international organizations, Pwn&Patch aims to create a safer digital world for customers to focus on what matters to them.

Figure 1.1: Pwn & Patch

1.1.2 Pwn&Patch's services:

Threat Intelligence and public exposure analysis :
Discover what hackers can find about your organization and your publicly exposed assets.

Red Team Operations :
Emulate the behaviors and techniques of a potential attacker in the most realistic way possible

Infrastructure Penetration Testing :
Detect vulnerabilities and security loopholes in your network and give you the ability to prevent them from being exhibited by an attacker

Web Application Penetration Testing :
Secure your web applications and eliminate any risk around them

Mobile Application Penetration Testing :
Perform a security audit that includes the study of the application's logic, a technical analysis, and the analysis of elements that could be extracted (reverse engineering)

Social Engineering simulation :
Test the awareness of your employees with highly customized Social Engineering campaigns.

1.2 Organizational chart of the company

Pwn&Patch is structured as such:

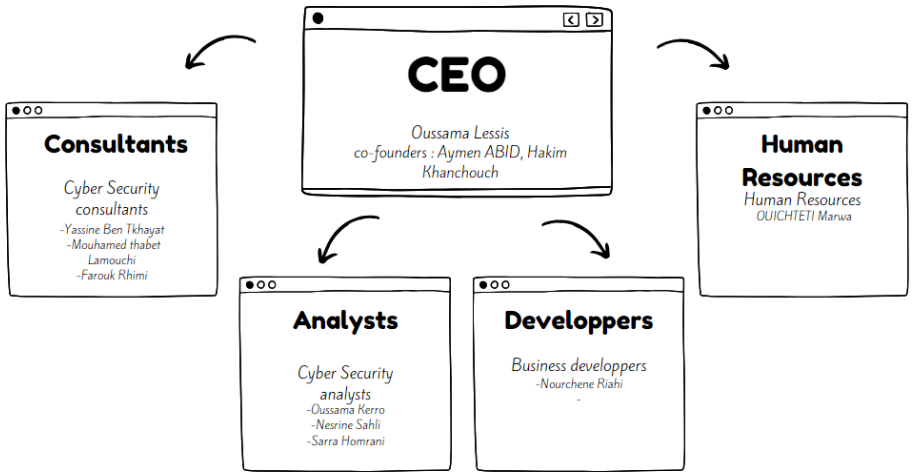

Figure 1.2: Pwn&Patch's organizational Chart

1.3 Conclusion

In this chapter, I present Pwn&Patch, its missions, and its organizational chart.

Chapter 2

OSINT

2.1 Introduction to OSINT

OSINT : Open Source Intelligence is the collection of information from published or public sources for intelligence purposes. It can be used to gather data on potential threats or "Cyber-attacks"

2.1.1 History of OSINT

OSINT existed way before the technological boom of our days, back in early military settings (WWII, Cold War ...) where it was used for espionage and strategic intelligence gathering. Agents would often listen to Open Radio Broadcasts for valuable information, they also searched for newspapers, journals and interviews . In general, any type of information that can be related to said target is of use. OSINT came to flourish after the social media boom information that was hard to gather before became publicly available. The future of OSINT is very promising as many new technologies are starting to be applied to this field, such as machine learning and automation which helped replace repetitive workflows.

2.1.2 OSINT investigation

Five steps of the OSINT cycle consist of Planning, Gathering, Analysis, Dissemination, and Feedback :
Information Sourcing The initial phase where the individual identifies potential sources from which information may be gathered. Sources are documented and detailed notes are written down for later use.

Data Harvesting Information is collected and harvested from the selected sources and other sources that are discovered throughout this phase.

Data Processing Harvested information is processed for actionable intelligence by searching for information that may assist in the investigation.

Data Analysis The individual performs data analysis of the processed information using OSINT analysis tools.

2.1.3 Report writing

In the "Report writing" phase, the insights learned from the OSINT investigation are documented within a comprehensive and well-structured report. This involves the trans-

formation of collected data, analysis, and conclusions into a clear and organized narrative. The ensuing report serves as a vital tool for decision-makings.
The report writing phase encompasses the following fundamental components:

Executive Summary: Encapsulating the investigation's objectives, methods, significant findings, and overarching conclusions.

Introduction: In this segment, the investigation's backdrop and context are outlined. A restatement of the objectives is provided, coupled with a reaffirmation of the OSINT revelations.

Methodology: Elaborating on the specific tools and techniques harnessed during the OSINT exploration, this section describes the collection, processing, and analysis of the data. Ensuring the transparency and replicability of the used methods.

Findings: Here, each finding is substantiated by evidence gathered during the investigation, with references to the sources. The visual augmentation, facilitated by graphs, charts, and screenshots, helps the presentation of findings.

Analysis: In this phase, the data is interpreted and contextualized. The report relies on the significance of the findings compared to the investigation's aims. Patterns, trends, and correlations within the data are explained.

Conclusions: The conclusions are tailored to address the specific objectives of the investigation, giving insights into the findings's implications.

Recommendations: If applicable, recommendations are dispensed, outlining actions to help remedy the found complications. These recommendations could serve as directives for decision-making or as pointers for future research.

Limitations: The report acknowledges any constraints or challenges encountered during the OSINT investigation. It shines a spotlight on potential biases, sources of error, or areas marked by incomplete or unreliable data.

References: This section compiles a comprehensive list of all utilized sources. By citing sources, the report's credibility is upheld.

Finalization: The report undergoes thorough review and editing to ensure cohesion and accuracy. This polishing phase is vital to presenting a report of high quality.

2.2 Conclusion

In conclusion, Open Source Intelligence (OSINT) is a valuable tool for gathering and analyzing information from public sources. It has a long history, starting from its use in military settings for intelligence purposes. With the rise of technology and the internet, OSINT has become even more powerful. Looking ahead, OSINT's future is bright. New technologies like machine learning and automation are being used to enhance the OSINT process. However, it's important to remember that the success of OSINT still relies on skilled analysts who can find and interpret relevant information accurately. In today's information-driven world, OSINT remains a crucial tool for obtaining insights and making informed decisions.

Chapter 3

The Investigation

3.1 Introduction to our Targets

We have two targets who will remain unnamed for privacy purposes. The first target is a big name in casinos and gambling facilities. The second target is an electricity, oil, and gas company. these two targets are big players in their respective fields and they asked for an OSINT investigation to identify publicly available information about their companies and employees. Below I detail the steps I took in this investigation and the tools that aided my research.

3.2 Planification

The same steps were used for both companies, first of all, we start by enumerating the list of publicly available sources then we collect the needed tools and proceed with our investigation

3.3 Information Sourcing

One of the most important parts of an OSINT investigation is to find as much accurate information as possible, that's why it's important to diversify the sources to have a better chance of getting the desired result.

3.3.1 WHOIS Databases

WHOIS databases contain domain registration information and can offer details about website ownership, It can also provide the Registrar, the Registrant Country, and IP addresses related to the domain.

3.3.2 Search engines

Google, Bing, and other search engines can provide a wealth of information. Using advanced search operators and techniques (Dorking) can help narrow down our search and provide information that's not simply queried when searching.

3.3.3 Social Media Platforms

Facebook, Instagram, Twitter, Linked-In, and other social media platforms can provide valuable insights as many users mindlessly publish private information which can be their home addresses, personal emails, and phone numbers. Such valuable information can be a dangerous tool in the hands of malicious people.

3.3.4 Government Websites

When dealing with sensitive government-related investigations, government websites can be a source of some data that's not supposed to be accessible to the public. Government websites often offer reports, statistics, and official statements that may contain addresses and emails to some high-ranking officials, such emails can be used to further enumerate vulnerabilities in a governmental structure.

3.3.5 Archive Websites

Archive.org also called The Wayback Machine can help you access historical versions of websites and track changes over time to find what information was hidden or falsely published and removed from a website.

3.3.6 Leaks

Leaks can be of many forms as some pirates like to publish their findings after getting into password databases either for free or for a hefty sum to the interested buyer, these findings present thousands and millions of passwords to a vast number of accounts, Knowing that many people use the same password for every platform this can present a danger if a user's password gets leaked.

3.3.7 Services

In the instance where a target is a website or a Web application a service enumeration can be done, which is a search for open ports on said websites to find what services are open on which ports, in this case using an older version of a service on a port can lead to having it exploited to gain unauthorized access to a system related to said target.

3.4 Data Harvesting

Once the potential sources have been identified, the next step involves initiating the data harvesting process from these sources. This entails utilizing the previously mentioned tools to gather pertinent information. Each tool serves a distinct purpose: WHOIS for domain ownership details, HUNTER.io for email addresses, Intelx.io for data leaks, and Amass for mapping attack surfaces, among others. By leveraging these tools effectively, a wealth of diverse data points can be gathered efficiently.

3.5 Using the tools for data harvesting

To aid our research we got the help of some important OSINT tools

3.5.1 WHOIS

WHOIS is a query and response protocol that queries databases that contain resources of registered users, domain names, IP address blocks, and other information

Figure 3.3: who.is

Using who.is a whois reverse search engine we found for example that our websites have registrars in the Ivory Coast

3.5.2 HUNTER.io

Hunter provides search and verification for email addresses from publicly available online sources

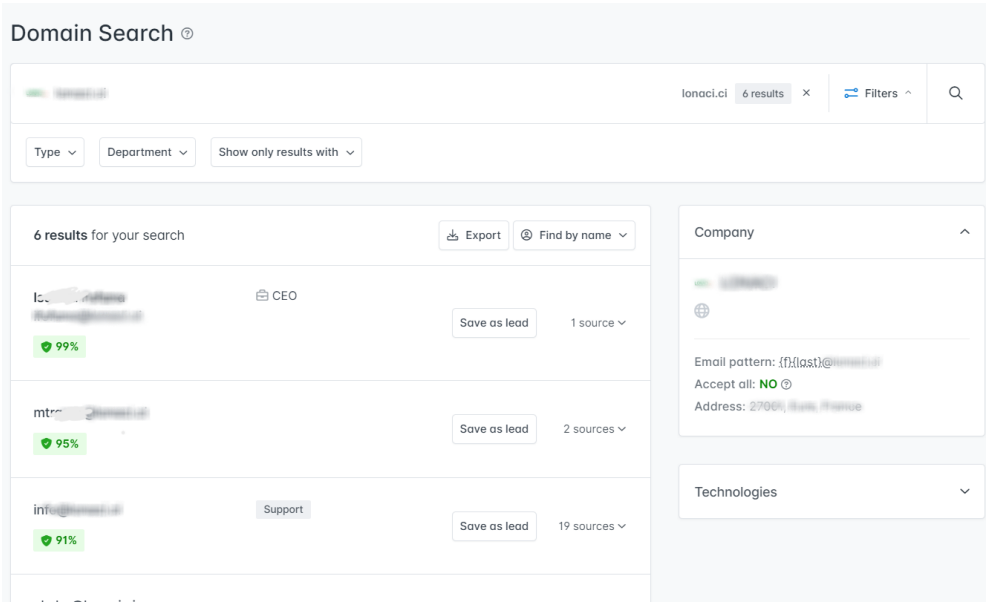

Figure 3.4: hunter.io

After entering our target's domain into Hunter.io's search engine we got the following results which were a list of email addresses found from publicly available reports that were left and forgotten on parts of the company's website or in some cases other websites.

3.5.3 Intelx.io

Intelligence X is a search engine and data archive. It searches for data leaks and the public web by email, domain, IP, and more.

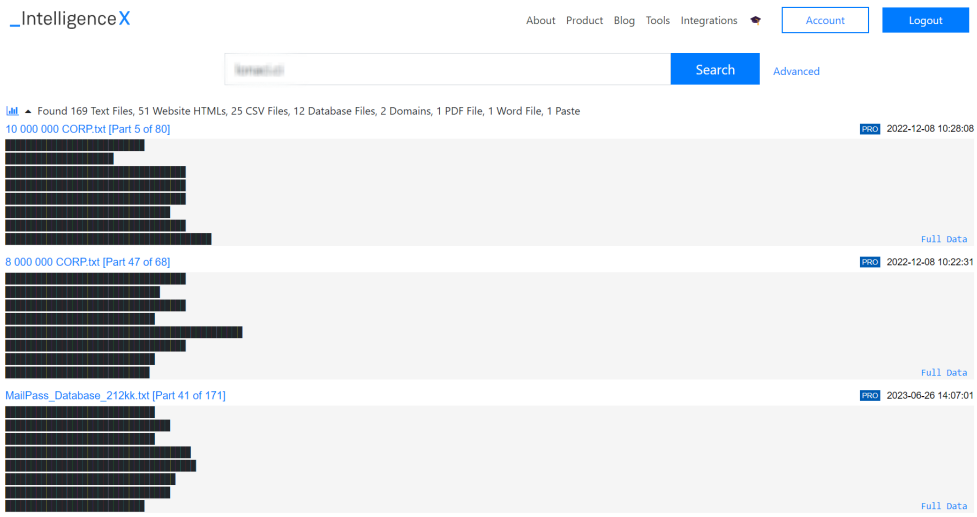

Figure 3.5: Intelx.io

After getting some e-mail addresses earlier it is time to use intelx.io to run a reverse search on some database leaks to find if our target's employees have had their passwords leaked as shown by the screenshot we found many passwords related to our targets. This is a huge security risk that should be solved PROMPTLY.

3.5.4 Amass

Amass is an in-depth attack surface mapping and asset discovery that performs network mapping of attack surfaces and external asset discovery using open-source information gathering and active reconnaissance techniques.

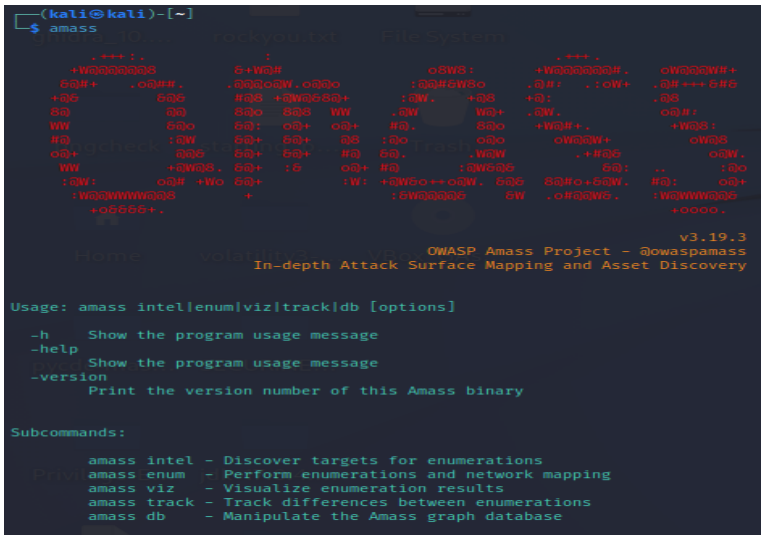

Figure 3.6: Amass

After entering our target's website as an argument in the amass tool we found many subdomains ABOUT our target. These subdomains were subject to the same treatment as the target's main website because if an exploit was found it could help the pirate trace back to the main domain.

3.5.5 Censys.io

Censys helps organizations, individuals, and researchers find and monitor every server on the Internet to reduce exposure and improve security. after entering our target's website in Censys's search engine we were provided with the running services on each domain

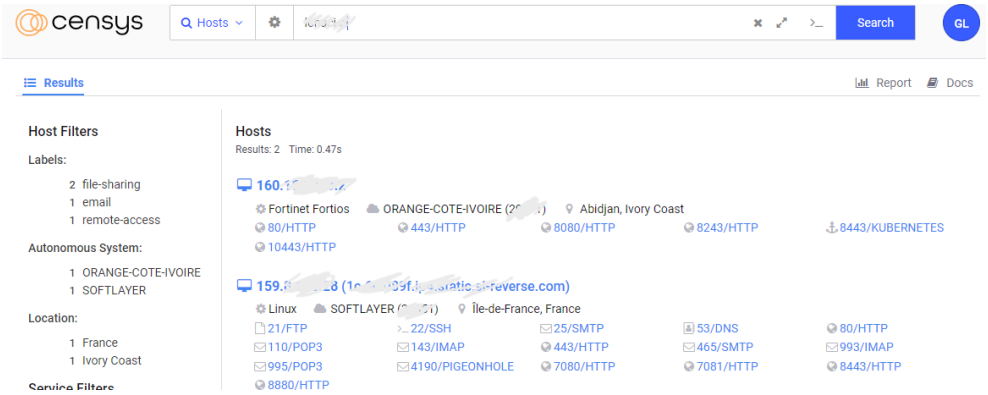

Figure 3.7: Censys

clicking on each service we find the service name and version which can be used to identify any exploit in databases such as exploit-db.com.

3.5.6 Security trails

SecurityTrails enables you to explore complete current and historical data for any internet assets. IP & DNS history, domain, and Open Port intelligence.

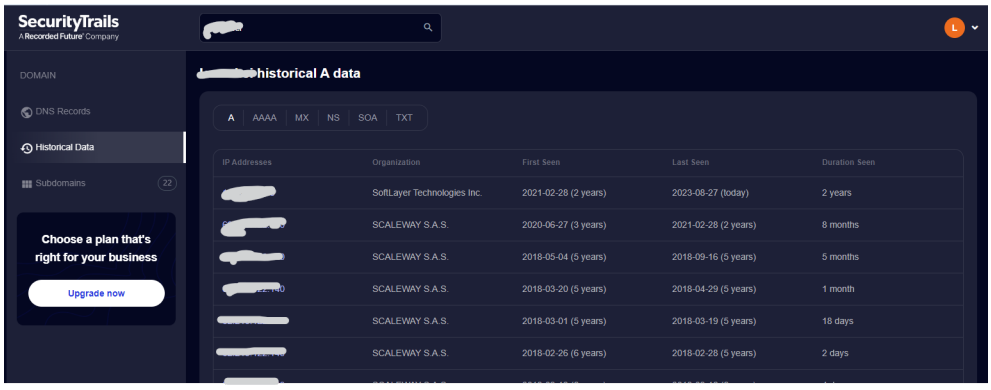

Figure 3.8: Security Trails

using security trails we were able to find out when the changes of hosting organization were made besides giving us more subdomains in a similar way to Amass mentioned previously

3.5.7 LeakIX

LeakIX is a red-team search engine indexing mis-configurations and vulnerabilities online.

Figure 3.9: LeakIX

Using Leakix we made a graph of our target's network to help structure our data and ease our analysis

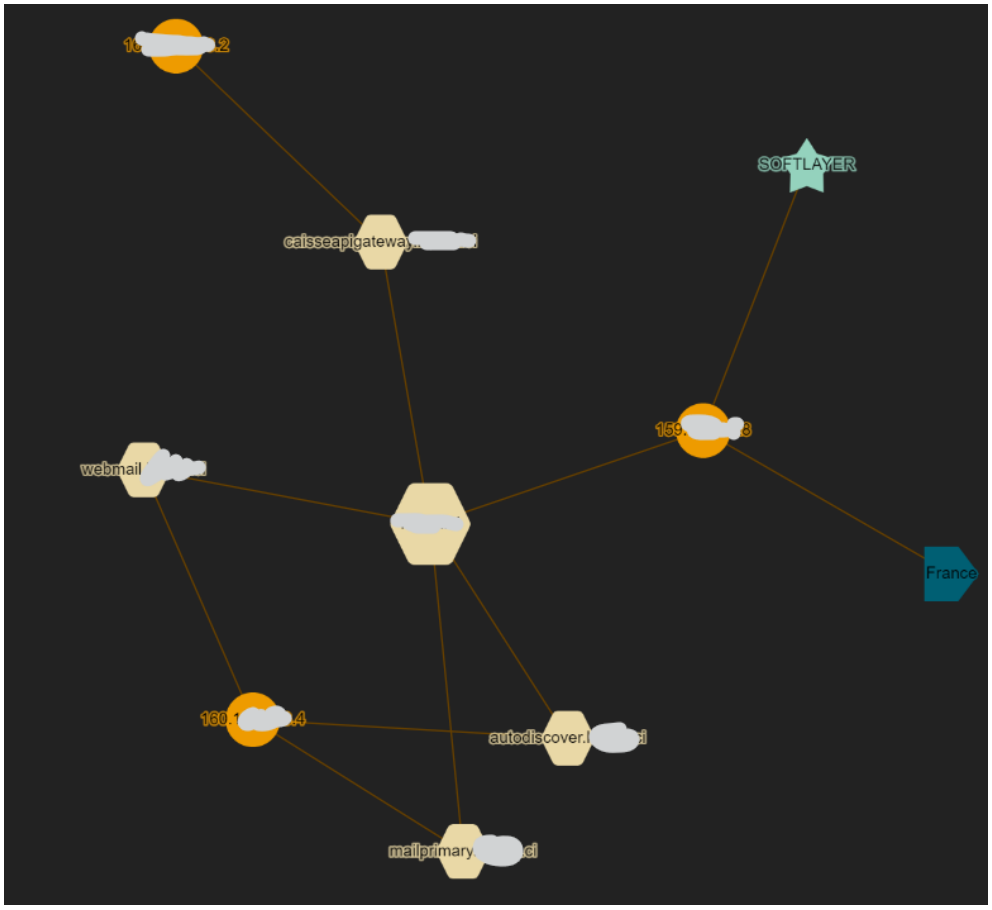

Figure 3.10: LeakIX graph

3.6 Data Processing

After collecting the data, it is unavoidable that some of it while important may not be of use to the investigation that's why it is important to clean it up remove the duplicates and structure the data in a way that makes it easier to analyze especially when working as a team on one investigation.

3.7 Data Analysis

After receiving the processed data, we begin the analysis phase where we draw connections and find insights about our target by cross-referencing data from different sources, we can find relationships, patterns and, vulnerabilities especially when said target is of big online presence

3.7.1 Identifying Vulnerabilities

One of the primary objectives of this investigation is to identify vulnerabilities. These vulnerabilities could range from weak passwords exposed in leaks to improperly secured servers or outdated software versions. Such findings can provide valuable insights to improve security measures.

3.7.2 Mapping Attack Surfaces

Using tools like Amass, we can map the attack surface of the companies. This means identifying all the points of potential entry for cyber attacks. By understanding their attack surface, companies can take steps to strengthen their defenses, this can be helped by running a simulation attack or a pentest to provide a simulated scenario of a cyber attack.

3.7.3 Discovering Insider Threats

Publicly available information might inadvertently reveal potential insider threats or information leakage from employees. Monitoring online activity and identifying suspicious behavior can help mitigate these risks.

3.8 Conclusion

Conducting an OSINT investigation for these two prominent companies has provided valuable insights into their online presence and potential vulnerabilities. By employing a variety of tools and techniques, we've gathered, processed, and analyzed publicly available data to generate meaningful intelligence. The information gathered can guide these companies in enhancing their security measures, mitigating risks, and making informed decisions moving forward.

General Conclusion

My internship at Pwn&Patch has been one of the best professional experiences that I had the chance to have.
During this internship, I learned precious knowledge about Cyber Security in general and OSINT in particular
The investigation that I was tasked with presenting a challenging yet fun experience where I got to finally test my knowledge and learn many new skills that will for sure be of use in my future and this project will be a great stepping stone into the world of Cyber security in general and OSINT, in particular. I hope to have left a good impression of my professionalism and my ability to learn and especially of my Private Higher School of Technologies Engineering.

List of Figures

Liste des acronymes

OSINT :*Open Source Intelligence*

DNS :*Domain Name System*