Security Assessment of the Oeiras Municipality IT Infrastructure

(extended abstract of the MSc dissertation)

José Pedro Ferreira Gomes
jose.pedro.gomes@tecnico.ulisboa.pt
Instituto Superior Técnico

Advisor: Prof. Ricardo Jorge Fernandes Chaves
Advisor: Prof. Nuno Miguel Carvalho dos Santos

***Abstract*—Information security has become a primary concern for organizations. Due to the complexity of modern IT infrastructures, it is difficult to prevent individuals with malicious intent to gain illegitimate access to information and/or cause damage to data or services maintained by enterprises and public institutions. With each passing month, the number of vulnerabilities discovered easily exceeds the number of the previous month. Thus, at a time when computer attacks are increasingly elaborate, any entity needs to have a robust physical and technological defense. In this work, we focus on a specific organization – the Oeiras Municipality – and our goal is to assess the security of the IT infrastructure of this entity. The complexity of this task comes from the fact that this infrastructure has grown to a considerable scale without following a comprehensive, laid out security architecture. As a result, it is currently difficult to understand to what extent this organization is vulnerable to potential cyber-attacks. To address this problem, this thesis presents a systematic security study of the Oeiras Municipality IT infrastructure which involved a three-pronged methodology: (1) we deployed an in-house SIEM to assess whether it would help to gain visibility of the security events ocurred in the network, (2) performed a manual vulnerability analysis using commonly used pentesting tools, and (3) conducted a field study to assess the social awareness of employees. We identify several vulnerabilities and provide a set of recommendations to improve the security of this IT infrastructure.**

***Keywords:* Cybersecurity, Vulnerabilities, Scanning tools, Information Security, SIEM, Infrastructure, Social Engineering.**

I. Introduction

The world relies on technology now more than ever before. As a result, digital data creation has grown exponentially. Nowadays, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Unfortunately, devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization.

Devices, as well as human beings play a fundamental role in cybersecurity. Cybersecurity is referred mainly as information security, and the practices of ensuring its integrity, confidentiality and availability. It involves tools, technologies, and best practices to protect networks, devices and data from attacks or unauthorized access. Unfortunately, cyber attacks are increasingly damaging to organizations. Nearly 70 percent of consumers believe organizations are vulnerable to hacking and cyber attacks, and say they are less likely to continue or start doing business with organizations that have been compromised [1]. A SOC uses a range of tools that collect data from across the network and various devices, monitors for anomalies and alerts of potential threats. This thesis aims to explore and study these tools in order to analyze, understand and correct vulnerabilities found. To this end, this work aims to study the Oeiras Municipality IT infrastructure in its entirety, and understand the various vulnerabilities and risks that may be present, both digital and behavioral.

This work intends to deliver the following main contributions around the matter of cybersecurity applied to this public entity infrastructure:

- Deployment and analysis of the applicability of the SIEM deployed in-house, to improve the visibility of events occurring in the infrastructure i.e., Splunk
- Manual vulnerability assessment of the IT infrastructure using standard pentesting tools
- Field study involving the employees of the Oeiras Municipality in order to characterize the level of social awareness in this public entity.
- Recommendations on how to improve the security of the IT infrastructure and social awareness.

II. Background

Ensuring the integrity, availability and confidentiality of information incorporates many tasks, from configuration management to ensure a robust system, effective cybersecurity and security policies to workforce training. The importance of all these aspects has been growing as the digital world evolves, forcing those in charge of each organization to do the same, evolving.

In this chapter we resume the subject of our study, the IT infrastructure of the Oeiras Municipality. Then provide an overview of the main security risks: vulnerabilities, lack of visibility and social engineering.

A. Oeiras Municipality Computational Infrastructure

There are six critical services whose assets and networks, whether physical or virtual, are critical to the Oeiras Municipality. Their incapacitation or deactivation would have

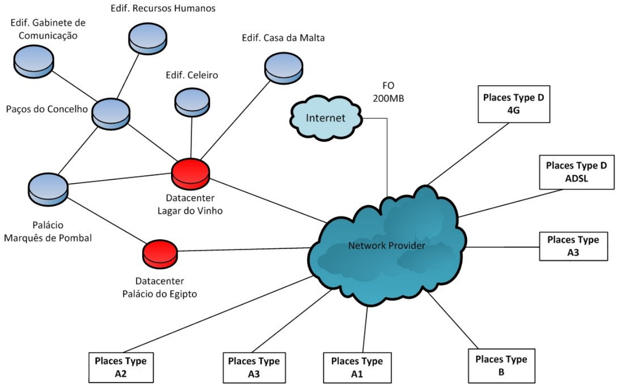


Figure 1. Oeiras Municipality network topology.

a debilitating effect in all the services that the municipality provides causing serious inconvenience at all levels of the institution

- Technological Platform
- Security Platform
- Virtualization Service
- Databases Service
- Internet Provider Service
- Website Hosting Service

B. Definitions: Risks and Vulnerabilities

The study of vulnerabilities and their mitigation is the main objective of this work. There is no universal definition of what a vulnerability is, but all have a tendency to describe the concept in the same way. In the next paragraphs we will describe how global organizations define a vulnerability, as well as the impact and why it is important to discover vulnerabilities at the perimeter of the network.

Impact:: The impact of a vulnerability is defined by the consequences that a company suffers because of that vulnerability. It is composed of two factors, the technical impact, which includes the availability, confidentiality and integrity of information at the mercy of vulnerability, and the impact from the point of view of the business in which the financial, legal or privacy consequences resulting from the loss or exposure of information are analyzed.

Normally, four types of vulnerabilities are defined:

- *Hardware vulnerability:* This type of vulnerability includes, above all, changes at the physical level of the system, such as the addition of devices or interruption of traffic.
- *Software vulnerability:* Includes modifications of the software present in the host or its elimination. The most illustrative examples are trojan horses, information leaks and viruses.
- *Data vulnerability:* Includes the security, confidentiality and evaluability of data. Improper access to insider information is the most recurrent case of such attacks, as well as loss of data or alteration of data for personal benefit.
- *Web-based vulnerability:* The most common way to present and share information over the Internet is to do so based on web applications, making it one of the most used attack vectors.[2]

Importance of vulnerability assessment: With the expansion of cyber attacks and online dangers, it is critical to have a consistent beware of the security escape clauses that could turn into a pathway for hackers. These assessments permit security teams to apply an understandable and clear way to deal with and resolve security breaches in the IT infrastructure. This exercise, which must be done regularly, helps in distinguishing dangers and points of failure at the most punctual time conceivable and work on mitigation to close any breaches present in the system. This assessment assumes a crucial job in guaranteeing that an association meets cybersecurity consistency and rules.

C. Social Engineering

Human actions, whether intentional or not, are a major threat to platform and information security across all organizations. Regardless how robust the technology, any individual with access to an organization's systems and data, it is a potential vulnerability – a response to a phishing message, a mistakenly downloaded file or an opened email attachment containing a virus are the most significant and common weak points. Social Engineering is defined by social-engineer.org as "Any act that influences a person to take an action that may or may not be in their best interest". The idea behind this approach is to take advantage of a potential victim's natural tendencies and emotions to obtain information [3]. These attacks can be performed in any process where human interaction is involved and come in many different aspects, and the most common are the following:

- Baiting;
- Vishing;
- Phishing;
- Impersonation.

D. Security Information and Event Management

In the early days, there were relatively few IT security tools, which included antivirus for host monitoring, firewalls for perimeter protection and IDSs for intrusion detection. There was no integration between the various technologies, each one presenting its own interface depending on who developed it and relating the various events throughout the infrastructure was a complicated task, given the lack of compatibility between the various tools. SIEM tools were developed to be able to, in real-time, collect, filter, store, select, correlate, and create alerts for security-relevant events. The main functionality of this type of system is the ability to correlate events from different sources and in large quantities and normalize them in a common representation to all, turning this information into knowledge that can trigger measures and actions of defense, so that companies are able to establish and maintain a situational picture.

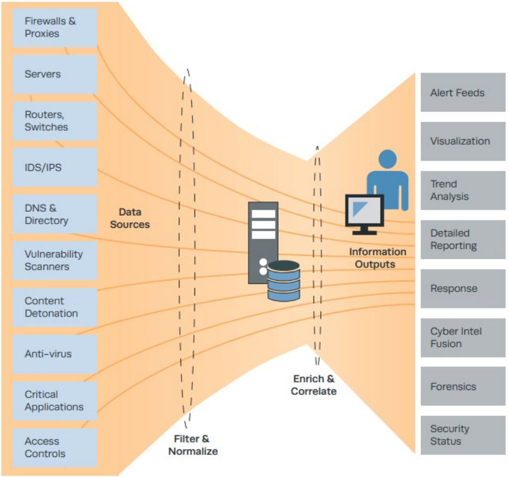


Figure 2. Architecture of a SIEM system [4].

E. Vulnerability Scanners

There are different vulnerability scanners accessible in the market today. The vulnerability scanning process can be done at four main levels: application level testing for vulnerabilities, failures and bugs; host level diagnostics, which includes hardware, all software present in it and configurations; network level testing that looks for failures in access controls and packet operations; database identification in search of sensitive information that should be protected. The following tools are broadly used as they are open source and give the best results. Next, the most relevant tools are presented.

- OpenVAS;
- Nmap;
- OWASP Zap;
- Nikto;
- WPScan

F. Splunk

Splunk presents itself as one of the most popular SIEM solutions in the market. It has incorporated analytics and network and machine data can be monitored on a real-time basis as the system scans for potential vulnerabilities. It triggers alerts that can be defined by the user and tuned to match the organization needs. As interaction it counts with a very simple interface which first presents a basic overview of an incident before displaying in-depth observations on the event. The Asset Investigator feature flags for malicious actions using correlation rules, and allows the user to track and classify a security event. It works with any machine data, on cloud or on-premises and its automated actions and workflows enable a quick and assertive response to incidents.

The customization of dashboards and visualizations was one of the requirements and Splunk presents itself as the solution that best fills this gap in the available solutions. As far as the rest of the functionalities are concerned, all the tools presented work in a similar way, varying in the simplicity of their interface and a possible exclusive functionality. All of them have variable prices, which was also a selection criteria. After the gathering of all functionalities described above and the selection criteria, as well as the fact that it is available as soon as possible so that it can be implemented, tested and put into production, the solution chosen was Splunk.

III. Related Work on IT Security Monitoring

Several publications have been made over time on vulnerability and security monitoring in IT infrastructures. On [5][6][7][8] different methods used for intrusion detection and cybersecurity are discussed along with the most common breaches detected on infrastructures. When it comes to vulnerability analysis using pentesting tools, it is studied in [9][10] how it is possible to provide active cyber defence using Vulnerability Assessment and proactive actions taken to solve vulnerabilities and stop possible attack. In [11][12][13] some premium/open source VAPT tools have already been approached.

Related work to analysis of log events and how it can enable the detection of anomalous events relevant to cybersecurity have been studied previously in [14][15]. As the applicability of SIEM to analyze security events in previous publications [16][17].

In [18][19] it is identified the compliance of employees with the information security policy (ISP) of an organization and how it can improve end user's behavior [20]. Social engineering attacks have already been discussed too in several publications helping to the conclusion that the human interaction is the weakest link in a cybersecurity environment [21][22][23].

IV. Deployment and Assessment of In-House SIEM

This chapter presents the first contribution of this thesis which consists of the deployment and evaluation of a SIEM in the IT infrastructure of the Municipality of Oeiras. Our objective is to combine a theoretical and practical implementation of a SIEM tool to assess whether it is an added value to improve visibility in the infrastructure of the Municipality of Oeiras, giving its employees a better understanding of relevant events and incidents and at the same time make it safer. We include a brief presentation of Splunk's architecture and highlight the steps that were necessary to implement it in our deployment scenario. Lastly, we describe some case studies put into practice, whose results will then serve to justify the conclusions and evaluations of this chapter.

A SIEM is necessary for handling the increase of the information level as well as the centralized analysis of logs. This technology was created based on the principle that it is necessary to gather, relate, and store relevant events and incidents in an infrastructure that are produced in different sources and in a non-homogeneous way. Splunk was the tool with the best qualities and possibilities to deliver the desired results. The Splunk Enterprise version has all the features

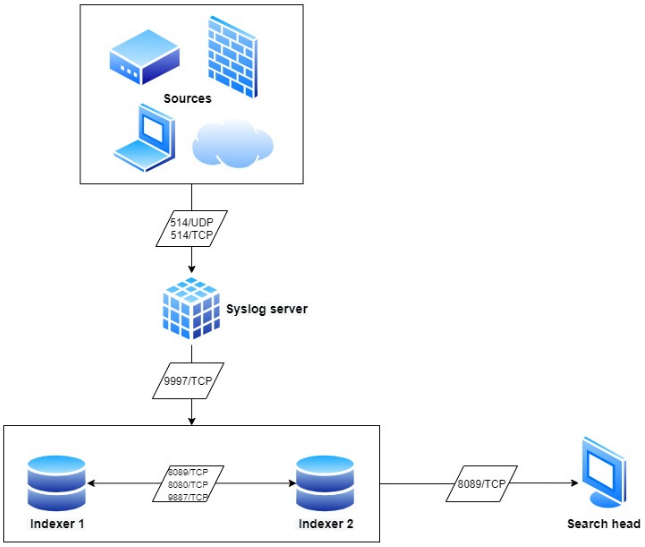


Figure 3. Splunk architecture.

listed as necessary and allows you to collect, search, analyze, and view data from various types of sources and devices.

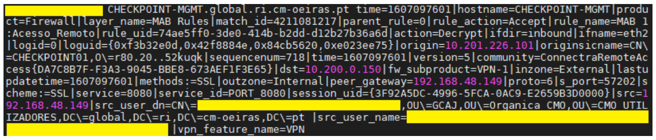
A. *Customized Splunk Architecture*

Splunk consists of three main components: Universal Forwarders, Indexer, and Search Head. The first one is present in the source and is responsible for collecting the information and then forwarding it to the Indexer, which is the component in charge of receiving, transforming, and organizing the information into an index. Upon request from Search Head also looks for specific data. Finally, Search Head is responsible for interacting with the user and presenting the results back, after forwarding the requests to Indexer. These results can be presented as tables, charts or even raw data. For searching, filtering and presentation of results, Splunk uses Search Processing Language (SPL), its own language developed for use in the tool, which is based on SQL and Unix syntax, with more than 140 commands [**?**]. Our implemented architecture is mirrored in the diagram depicted in Figure 3, composed of two indexers, a search head and a syslog server.

One component that is not mandatory but which we have used in our deployment is a machine that will work as a Syslog server. Syslog is a client/server protocol for the transmission of messages whose destination is usually called Syslog daemon/server. The addition of this node allows continuing to receive data from sources even when the Splunk service is down, for reasons of updates or new configurations.

The following discusses all necessary changes and adjustments to Splunk's system components and software. To start the data collection process it was necessary to decide which nodes of the IT infrastructure of the Municipality of Oeiras would be in the scope of the SIEM build. Note that the ultimate goal of this part of the project is to create a SIEM that can correlate and link events that occur horizontally across multiple machines and vertically across multiple levels of infrastructure. After this phase of analysis, it was possible to finally start the project. To configure the Syslog server it was necessary to make sure that ***rsyslog*** service, native to the Linux operating system was running and then indicate in the configuration file located in the path ***../etc/rsyslog/conf.d*** the various IP addresses of the sources. This was configured to populate seven log files with information from Checkpoint Firewall and VPN, where each one of the files would represent one of the last seven hours of data. This information would be rotated to a different file every hour, guaranteeing that in the one called **chkp.log** would be always the most recent information and in the **chkp.log.6** the oldest information.

The event used to demonstrate the configuration and treatment of data focuses on account logon activities in the Municipality. The following listing extracted from the log file is an example of a VPN login. Note that the anonymized data is personal data of a user that has not been authorized for public processing within this work.



```
[redacted] CHECKPOINT-MGMT.global.ri.cm-oeiras.pt time=1607097601|hostname=CHECKPOINT-MGMT|produ
ct=Firewall|layer_name=MAB Rules|match_id=4211081217|parent_rule=0|rule_action=Accept|rule_name=MAB 1
:Acesso_Remoto|rule_uid=74ae5ff0-3de0-414b-b2dd-d12b27b36a6d|action=Decrypt|ifdir=inbound|ifname=eth2
|logid=0|loguid={0xf3b32e0d,0x42f8884e,0x84cb5620,0xe023ee75}|origin=10.201.226.101|originsicname=CN\
=CHECKPOINT01,O\=r80.20..52kuqk|sequencenum=718|time=1607097601|version=5|community=ConnectraRemoteAc
cess{DA7C8B7F-F3A3-9045-BBE8-673AEF1F3E65}|dst=10.200.0.150|fw_subproduct=VPN-1|inzone=External|lastu
pdatetime=1607097601|methods:=SSL|outzone=Internal|peer_gateway=192.168.48.149|proto=6|s_port=57202|s
cheme:=SSL|service=8080|service_id=PORT_8080|session_uid={3F92A5DC-4996-5FCA-0AC9-E2659B3D0000}|src=1
92.168.48.149|src_user_dn=CN\=[redacted],OU\=GCAJ,OU\=Organica CMO,OU\=CMO UTIL
IZADORES,DC\=global,DC\=ri,DC\=cm-oeiras,DC\=pt |src_user_name=[redacted]
 |vpn_feature_name=VPN
```

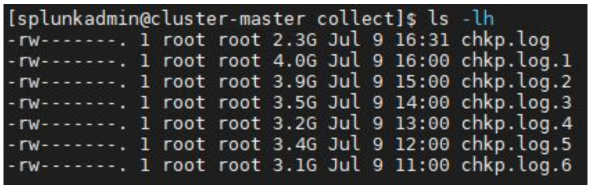
Figure 4. Example of VPN session login log.

The first step in dealing with this type of event is to determine which elements are relevant to be processed by the SIEM. The amount of information that arrives per second in the system required that only the necessary information is collected and kept in processing.

This data is evaluated in the content of the fields and the evaluation of the results can only be done through validation and use of the fields. The main fields that were identified were name of the sensor that generated the event, IP addresses and user information like name and domain data.

At this point in the project, we were faced with a problem that we were not aware of. The team responsible for hiring the Security Information and Event Management license did not have the sensitivity to calculate the size of information that would need to be uploaded to the platform. This failure translated into the number of sources and amount of data that could be redirected to the system as the contracted license proved to be quite short in order to cover the needs of the Municipality, whose ultimate goal was to be able to correlate events that take place in the infrastructure at all levels. The license purchased consisted of a limit of 15GB of data per day allowed for treatment in Splunk. This limit was exceeded everyday in about 5 hours, simply with data from the VPN and Firewall, taking into account that most of the Municipality's collaborators were remote working.

This made it impossible to configure all the previously spoken sources in the SIEM. A new hiring process was



```
[splunkadmin@cluster-master collect]$ ls -lh
-rw-------. 1 root root 2.3G Jul 9 16:31 chkp.log
-rw-------. 1 root root 4.0G Jul 9 16:00 chkp.log.1
-rw-------. 1 root root 3.9G Jul 9 15:00 chkp.log.2
-rw-------. 1 root root 3.5G Jul 9 14:00 chkp.log.3
-rw-------. 1 root root 3.2G Jul 9 13:00 chkp.log.4
-rw-------. 1 root root 3.4G Jul 9 12:00 chkp.log.5
-rw-------. 1 root root 3.1G Jul 9 11:00 chkp.log.6
```

Figure 5. VPN and firewall log files size.

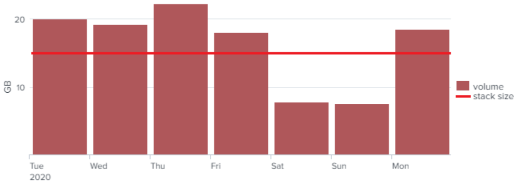


Figure 6. Average daily license usage per week.

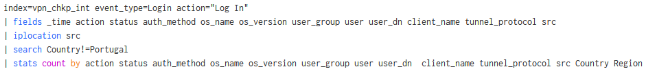
started with a daily data value of 100GB, however until it was finalized it was necessary to decide which sources to load the system with. Once again, the context in which most employees found themselves ended up making the decision to be to upload information from the VPN instead of other sources of input. From this moment all the implementation and evaluation of Splunk technology was affected by this constraint of only being possible to configure one data source.

In particular, we configured Splunk with rules to trigger alerts for three specific events: successful logins from foreign countries, VPN brute-force login attempts, and webmail brute-force login attempts. Next, we provide an account on how these rules were set up and present our main findings while running Splunk for the time period between June and September.

B. Success Login from Foreign Country

The first developed alert exploits the information of an access login after being handled by the platform which was created in order to understand where this same access had been made from. It arose from the need to try to minimize the risks of having the network security perimeter completely open, with some employees having to work with personal computers whose content and state is unknown. This rule aims to understand or at least help define whether a given access when made from a given country by someone who is or is not in that geographical point, is undue or not, confirmed later with possible contact with the user.

Events related to VPN index and Login event type are filtered and data fields like time, status, auth_method, os_name, user_group and user_dn are extracted. Then the location of the source host is calculated taking into account the IP address with the src field, to which we just asked to be returned access information outside Portugal. Finally, the data is grouped by the same fields from which information was extracted.

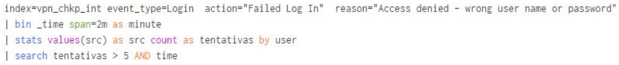


```
index=vpn_chkp_int event_type=Login action="Log In"
| fields _time action status auth_method os_name os_version user_group user user_dn client_name tunnel_protocol src
| iplocation src
| search Country!=Portugal
| stats count by action status auth_method os_name os_version user_group user user_dn  client_name tunnel_protocol src Country Region
```

Figure 7. Search rule that alerts for undue access.

C. VPN Brute-force Login Attempt

This alert was developed to detect cases where the same user account had several failed VPN login attempts in a short time. This kind of situations can be translated in the so-called brute force attack [24]. For this the following rule was implemented and put into production:



```
index=vpn_chkp_int event_type=Login  action="Failed Log In"  reason="Access denied - wrong user name or password"
| bin _time span=2m as minute
| stats values(src) as src count as tentativas by user
| search tentativas > 5 AND time
```

Figure 8. Search rule that alerts for several attempts of login.

Events related to VPN index and Login event type were filtered and data fields like action, and the reason for that was extracted as well. The time range for this alert to be triggered was set to 2 minutes. The number of attempts was calculated taking into account the same user account to which we just asked to be returned those cases where there were more than five failed attempts. Next, the data was grouped and returned by the same fields from which information was extracted. This alert was also triggered some time after being put into production. It stated that a user account had 6 failed attempts of login in the VPN.

The limitation described in Section 3.3.2 ended up influencing the possibility of testing to which the technology could have been subjected, making it impossible to correlate events. However, together with the fact that the Municipality's VPN was being used by most of the workforce, this would always be one of the services to be tested regarding integration with the platform. As well as the use of webmail which increased substantially due to its public availability.

The tool provided visualization, alarm generation, and event management which facilitated the tracking of security-related incidents. Although it was not possible to prove and test at the maximum extent, the platform is able to integrate with any kind of security event source, including the presence of some native add-ons for sources such as Checkpoint Firewall and Microsoft Active Directory, with some additional knowledge of the associated syntax and environment. The results of this chapter of the work showed that a SIEM is a technology that when well deployed and maintained can be helpful to increase the knowledge of the events that occurred in the infrastructure,

V. Vulnerability Assessment

The following section presents the second contribution of this work, i.e., an analysis of vulnerabilities present in the IT infrastructure of the Municipality of Oeiras. To this end, we intend to make use of some of the most widely used vulnerability scanning tools available in the market. We aim to make an analysis of their findings, study their possible impacts on the infrastructure, and define resolution measures for them.

Pentesting tools are used to discover vulnerabilities on networked computer systems. These tools were used through a virtual machine deployed in the main infrastructure network of the Municipality of Oeiras. Vulnerability testing was not only carried out in Municipality-owned web sites but in websites hosted externally too and was held for a period of 7 months from February to August 2020. For privacy reasons, the website url, name of the website and IP address will be anonymized

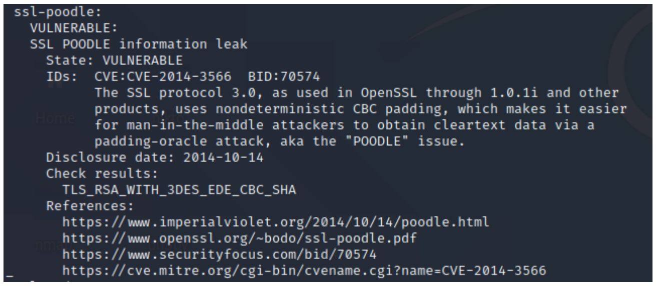
A. SSL/TLS Certificates

The first type of vulnerabilities that we found is related to SSL/TLS certificates. It was found by manual inspection and without the use of any of the tools indicated above. Only then, for confirmation, a testing software tool was used, which is available online and completely free, SSL Server Test from Qualys. Secure Socket Layer (SSL) and its successor Transport Socket Layer (TLS) intend to deliver secure end-to-end communication over the Internet [25]. Based on the model of public keys infrastructures and certificates, it was developed to ensure confidentiality, authenticity and integrity of communications. In the IT infrastructure of the Municipality of Oeiras it was possible to check that some websites did not present certificates, thus maintaining insecure communications. Some others presented certificates with outdated protocol versions, or even self-signed certificates and wildcards, concepts that will be explained later.

Vulnerability to DROWN and POODLE attacks: As we can see in the image above, this website presents a certificate that makes use not only of the SSL version 3.0 and TLS 1.0 and 1.1, all insecure, but also TLS 1.2 which is a recommended version. Since this test was made a few days before version 1.1 became officialy deprecated, the software only gives it a warning state. Two of the vulnerabilities to which this type of certificate is subjected to are the *DROWN* and *POODLE* attacks. The first was discovered in 2016 and its name comes from Decrypting RSQ with Obsolete and Weakened Encryption (DROWN). The attack allows the attacker to break the encryption and obtain passwords or sensitive information that is being exchanged in communication[26].

With the Nmap tool we can also check that this webserver is vulnerable to this attack. Using the command **nmap -sV –script=vuln webserverip**, which makes use of the ”vuln” script available for the tool. This script enhances Nmap’s ability to produce relevant CVE information about the services discovered in the host target.

For these vulnerabilities the only recommendation and that was made to the Infrastructure team, is to update the certificate to one that uses the versions considered safe.

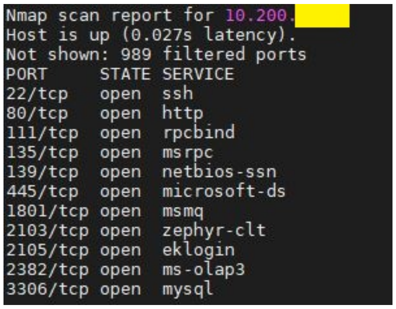


```
ssl-poodle:
  VULNERABLE:
  SSL POODLE information leak
    State: VULNERABLE
    IDs:  CVE:CVE-2014-3566  BID:70574
          The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
          products, uses nondeterministic CBC padding, which makes it easier
          for man-in-the-middle attackers to obtain cleartext data via a
          padding-oracle attack, aka the "POODLE" issue.
    Disclosure date: 2014-10-14
    Check results:
      TLS_RSA_WITH_3DES_EDE_CBC_SHA
    References:
      https://www.imperialviolet.org/2014/10/14/poodle.html
      https://www.openssl.org/~bodo/ssl-poodle.pdf
      https://www.securityfocus.com/bid/70574
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

Figure 9. Presence of the vulnerability POODLE confirmed.

B. Open Ports

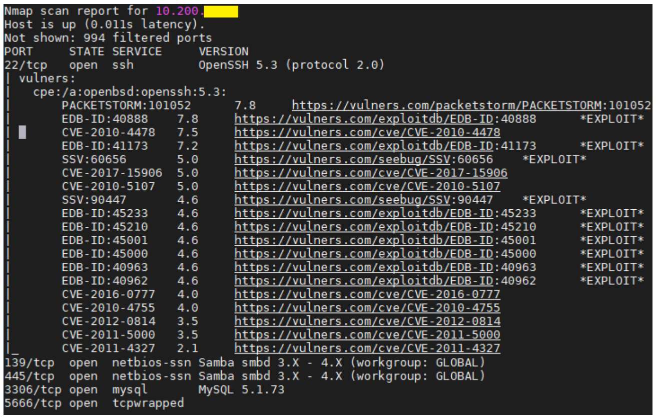
The fact that systems are exposed to external network probing makes the number of vulnerabilities to which systems are subjected even greater. The fact that a port is open to connections can facilitate the establishment of communications but can present itself as a vulnerability. In the figure below it is possible to analyze the open ports at the target of the scan using **nmap -h 10.200.xxx.xxx**. It is also possible to scan which operating system is present on the host, as well as its version, using **nmap -O -v 10.200.xxx.xxx**.



```
Nmap scan report for 10.200.[redacted]
Host is up (0.027s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2382/tcp open  ms-olap3
3306/tcp open  mysql
```

Figure 10. Port scan result.

Again, if we use the Nmap Script Engine (NSE) with the ”vuln” script, we can find out what kind of vulnerabilities this host presents, given the corresponding ports and services that were discovered. With the command **nmap -Pn -sV –script=vuln 10.200.xxx.xxx** we get the following output:



```
Nmap scan report for 10.200.[redacted]
Host is up (0.011s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:5.3:
|       PACKETSTORM:101052      7.8     https://vulners.com/packetstorm/PACKETSTORM:101052
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       EDB-ID:41173    7.2     https://vulners.com/exploitdb/EDB-ID:41173      *EXPLOIT*
|       SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPLOIT*
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       EDB-ID:45210    4.6     https://vulners.com/exploitdb/EDB-ID:45210      *EXPLOIT*
|       EDB-ID:45001    4.6     https://vulners.com/exploitdb/EDB-ID:45001      *EXPLOIT*
|       EDB-ID:45000    4.6     https://vulners.com/exploitdb/EDB-ID:45000      *EXPLOIT*
|       EDB-ID:40963    4.6     https://vulners.com/exploitdb/EDB-ID:40963      *EXPLOIT*
|       EDB-ID:40962    4.6     https://vulners.com/exploitdb/EDB-ID:40962      *EXPLOIT*
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|       CVE-2010-4755   4.0     https://vulners.com/cve/CVE-2010-4755
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|_      CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: GLOBAL)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: GLOBAL)
3306/tcp open  mysql       MySQL 5.1.73
5666/tcp open  tcpwrapped
```

Figure 11. Vulnerabilities scan with NSE.

With these findings, although they represent only a small sample of an infrastructure that is composed of several publicly exposed virtual machines and web servers, we were able to notice a number of possible open ports that could possibly be closed or with a filtered state, that present several vulnerabilities about to be explored. Although it has not been possible to report all these instances in detail, they should be checked as closely as possible by the teams responsible for the service, so that they can assess what the real need for these conditions is.

C. Web Applications

Given a large number of public websites present in the infrastructure of the Municipality, taking into account the scope of this work, we decided to analyze the security of the web pages. We used Nikto and OWASP Zap tools to test it in the Municipality regarding misconfigurations and security vulnerabilities.

More specifically, we executed the command **nikto -host 142.93.xxx.xxx -p 443** to perform the evaluation of vulnerabilities present in the page under study.

In this analysis we can identify several failures:

- Webserver returns the technology configured in it;
- X-Frame-Options header is not set;
- XSS protection header is not defined;
- The X-Content-Type-Options header is not set;
- The hostname does not match the certificate name;
- It is possible to list indexed directories;
- Possibly vulnerable to BREACH attack [27].

VI. Cybersecurity Awareness

This contribution consists of a field study aimed at assessing the cybersecurity awareness of the employees that work for the Oeiras Municipality and have access to its IT infrastructure. We begin this chapter with a more detailed motivation of this study and an explanation of its main goals. Then we present our methodology which consists of a survey addressed to the employees of the IT Department.

Ignorance or lack of awareness of good cybersecurity practices present themselves as the greatest threats to the security of information systems. Nowadays, it is known that the best way to improve a company's situation regarding the security of its assets is not only through technical solutions but also by increasing the awareness and education of employees who use these same systems. However, these common practices of digital security continue to be ignored in daily use by most individuals, which puts at risk the integrity and confidentiality of a company's data.

A. Survey

The survey was conducted via a questionnaire that aimed at gathering information about the knowledge, behaviors and thoughts related to the topic of cybersecurity on the part of the municipality's employees. It was designed with Google Forms and consisted of a brief presentation of its scope and purpose, a reminder that all data would be treated anonymously, followed by 19 questions, the first 3 of which served to characterize the individual from the point of view of age, gender and function within the department. Then, the questionnaire was divided in three parts:

- Initially the respondent was asked if he or she had ever participated in an awareness-raising or training session on the topic of cyber-security, if he finds the topic relevant and if, in a form of self-reflection, he thinks he knows how to act in a hypothetical case of a cyber-security incident, so that it was possible to understand the level of literacy of the target audience.
- The following questions included some what-if scenarios of use cases and several options of approaches to the same scenario to be chosen. Some questions about notions of digital security were developed and, taking into account the context of a pandemic experienced, questions were also asked about habits and circumstances experienced while users were placed in remote work.
- Finally, the participants were asked to try to classify their workplace from the point of view of physical and computational security, in the most honest way possible.

integrity and confidentiality of a company's data.

B. Social Engineering Attack Scenarios

For a further analysis and evaluation of the behavior of the Municipality's employees in possible attack situations using social engineering techniques, it was necessary to prepare three case studies using different techniques. In order to choose the cases put into practice, their practicality and speed of execution were evaluated, without the need to resort to external resources. The scenarios apply the techniques described earlier.

C. Use Case 1: Vishing Attack

The first example of an attack of social engineering carried out in the scope of this work made use of the *vishing technique*. The plan of attack would have the following description:

> A telephone call would be made to the general and public number of the Municipality of Oeiras, by someone posing as an employee of a technical assistance company of air conditioning systems to try to discover the existence and the respective physical location of the data centers of the infrastructure of the institution. The premise given would be that an intervention would be scheduled. However, no specific information was given about the date and time of the intervention, within the employees of the supposed company. This information would then be part of a larger plan to inflict some physical damage to these data centers.

The scenario was given as finished and the attack as successful.

D. Use Case 2: Baiting Attack

The following scenario intended to make use of the *baiting technique* which, although it seems quite banal, also proves to be one that presents many cases of success. This is because it is a technique that intends to attract the individual and lure him into performing a given action by sharpening his curiosity. The plot of this action was quite simple.

After a few hours of placing the flash drive, an employee of the IT Department had the "kindness" to return it to the Unit, after realizing who it belonged to and so it was easy to understand who picked up the flash drive and what he did with it. As in the previous case, this action was given as completed and successful.

E. Use Case 3: Impersonation Attack

The third and last scenario intended to make use of the social engineering technique called *impersonation*, in which one individual poses itself as another person to try to gain access to a resource he originally would not have. The plan of this scenario would be that:

> An individual would impersonate an employee of the Department of Informatics to gain access to the video surveillance circuit recorder of Parque dos Poetas, a green space widely frequented in the council, in order to later extract information from it.

During the minutes the attacker was inside the room where the recorder was placed, he was always alone and without any supervision. After a few minutes he left the place quite naturally, stating that the task that had brought him there was finished. Once again and following the previous examples, the attack was given as successful.

F. Survey Results

From the survey we were able to get 29 responses out of a possible 33. When we analyze the survey answers we started to realize that there is a clear lack of training on the subject of cyber security. As shown in Figure 12, over 62% of the participants said they had never participated in a training action on the subject. Although more than half of the participants answered that they had never received training on cybersecurity, most of them, even in a smaller percentage (i.e., about 55%), state that they have sufficient knowledge on the subject for a good performance of their function. Once again it was possible to verify the contradiction in their answers when asked if they thought they had in their possession the instructions on how to proceed in case of a cyber security incident. This question, to which about half answered no, was intended to understand whether the management transmits the necessary guidelines to the remaining employees.

VII. Security Recommendations

After all data collected from the illegitimate accesses to the Municipality's VPN, the illiteracy verified by some users, as well as the presence of some bad practices regarding cyber-security, the work project intended to give some lectures or training to the employees not only of the IT Department, but to all employees of the Municipality. Unfortunately, this initiative was not authorized by higher instances. We continued to work on technical solutions that could be proposed to try to minimize security risks. We present a list of security measures that we recommend to be implemented at the Oeiras Municipality.

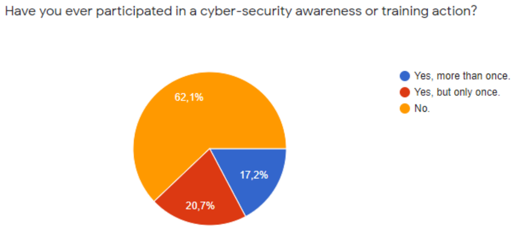


Figure 12. Presence of employees with training in cybersecurity.

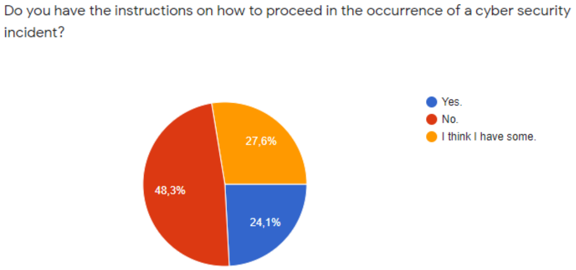


Figure 13. Lack of guidelines from workforce.

- **Two-factor Authentication:** one of the technical measures analyzed and proposed for implementation was the deployment of a dual-factor authentication solution for access to the organization's systems[28]. Given the situations analyzed before, we verified the urgent need to do so, especially in the resources most accessed by employees in telework, such as VPN and webmail.
- **Password Management:** another of the conclusions that could be drawn from the answers to the questionnaire was that the management of employees' passwords is quite negligent, and there are even those who admit to using a document that they keep with them to manage their passwords. The policy in the Municipality establishes that the access passwords to the systems must contain at least 8 characters, including at least one capital letter, one small letter, a special character and a number. It stands to reason then that NIST's recommendations present today a greater relevance in the length of a password and not so much in its complexity when it comes to the mixture of characters[29].
- **Data Encryption:** once again, to overcome the limitations of the human factor in this matter and the fact that most users of the network and files of the Municipality have their computers at home, it became necessary to think about a measure to safeguard the information contained in them in the event of loss or

misplacement. In this sense, it was possible to use disk encryption software. Such a tool would verify the integrity of the hardware and the operating system at computer start-up. If this verification was successful then an encryption key was released which allowed the boot to continue. If the volume is removed from the machine it is practically impossible to read the information within the same [30]

- **Zero-trust Model:** as seen in the sections above, the human being remains the weakest link in security infrastructure of an organization. To minimize the dependency on user actions, it was advised that the Municipality adopts a zero-trust strategy. The current situation provides network users and resources with a static trust-based management that does not make periodic evaluations of access controls or makes use of a policy of "blacklisting" instead of "whitelisting". This type of model aims to improve security in a model that better adapts to the complexity of the network, the hypothesis of roaming workers and at the same time manages to protect users, devices and data, regardless of location.
- **Procedures and Policies:** When the answers to the inquiry were analyzed, we noticed that almost half of the participants answered that they did not know how to proceed in the occurrence of a cyber security incident. But when we asked the person responsible for this information, we reported that there was practically no documentation available to the IT Department employees and the one that existed was completely outdated. As part of this work and in an attempt to provide some procedures to employees in situations related to information security, an Information Security Policy and an Incident Management Policy were developed. Employees who comply with these documents present themselves as a crucial factor in a good evaluation of information security.

VIII. Conclusions

In this work we had the objective of making a study of vulnerabilities present in all the infrastructure that includes the IT Department of the Municipality of Oeiras. For this we divided the work in three parts, the implementation of a SIEM tool to increase the visibility of incidents that occur in the network, the use of tools for pentesting and analysis of vulnerabilities to discover and discuss the existence and resolution of these same vulnerabilities and, to finish, a study of notions and knowledge of cyber security with the employees of the Department that included an inquiry and drills of social engineering attacks.

It should be noted these results were verified in an analysis directed only to the IT Deparment, as far as the other employees of the Municipality are concerned, we can expect an increase in illiteracy and lack of sensitivity on the subject. With this results, we can conclude that awareness has not been cared of and should be improved in all stakeholders. This is where training is recommended, to minimize risks and increase employees' knowledge.

IX. Achievements

The evaluation of the functionalities of a Security Information and Event Management tool allowed the conclusion that this type of platform greatly increases the visibility of incidents that occur in the infrastructure. The testbed used was information regarding VPN access, which made the study somewhat limited, but sufficient to understand the added value of this type of tool. As a disadvantage, this platform has its license cost per data size processed, which was one of the causes for the analysis to be so limited. The creation of rules and alerts is also not very intuitive.

The manual vulnerability assessment using open-source pentesting tools returned several interesting findings about the resources present in the infrastructure. It was possible to notice vulnerabilities in the configuration of certificates, servers, web applications, and content management platforms. These flaws, although not all described in the document, reveal that functionality is a priority above security, with some negligence in terms of configuration and maintenance of security services. All the vulnerabilities that have been discovered have a measure of resolution, some of them quite simple and do not clash with the commitment to functionality.

Regarding the field study of cybersecurity knowledge by the Municipality's employees, the inquiry made it possible to conclude that there is a clear lack of knowledge and sensitivity on the subject, although in the answers most of the respondents affirm that they have enough knowledge on the subject to perform their function. As for the field scenarios that tested social engineering in the infrastructure, all of them were successful from the point of view of the attack, which means that from the point of view of security they revealed immense flaws and problems. In this chapter, it was possible to conclude an urgent need for training the Municipality's workforce in the theoretical and practical knowledge of good practice in workplace safety.

X. Future Work

The SIEM tool could be much more productive for the purpose if it was provided with more sources so it could make better use of its event correlation functionality.

The use of vulnerability analysis tools should be done regularly and to all the resources of the Municipality, with a properly documented process to treat the resulting vulnerabilities. In parallel, a standard should be established to perform software updates on the organization's machines.

As a future step of this work, training on cyber-security would be taught to employees of the Municipality of Oeiras, involving issues of social engineering and good practices to have in the workplace.

References

[1] N. A. Joseph Muniz, Gary McIntyre, *Security Operations Center: Building, Operating, and Maintaining Your SOC*, 2nd ed. Indianapolis, 46240 USA: Cisco Press, 2016.

[2] D. M. U. K. Kavita S. Kumavat, Ranjana P. Dahake, "Overview of vulnerability analysis," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 10, October 2013.

[3] Security through Education, "Social engineering defined,," https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/, visited 2019-12-06.

[4] Carson Zimmerman, "Mitre - ten strategies of a world-class cybersecurity operations center," Bedford, 01730 USA, 2014, https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf, visited 2019-10-15.

[5] D. H. Lakshminarayana, J. Philips, and N. Tabrizi, "A survey of intrusion detection techniques," pp. 1122–1129, 2019.

[6] U. Bashir and M. Chachoo, "Intrusion detection and prevention system: Challenges opportunities," pp. 806–809, 2014.

[7] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[8] A. Warzyński and G. Kołaczek, "Intrusion detection systems vulnerability on adversarial examples," pp. 1–4, 2018.

[9] J. Goel and B. Mehtre, "Vulnerability assessment penetration testing as a cyber defence technology," *Procedia Computer Science*, vol. 57, pp. 710–715, 12 2015.

[10] P. S. Shinde and S. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing," *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, pp. 1–5, 2016.

[11] S. Umrao, M. Kaur, and G. GUPTA, "Vulnerabilty assessment and penetration testing," *International Journal of Computer Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371*, vol. 3, pp. 71–74, 01 2012.

[12] P. Xiong and L. Peyton, "A model-driven penetration test framework for web applications," pp. 173–180, 2010.

[13] A. Austin and L. Williams, "One technique is not enough: A comparison of vulnerability discovery techniques," pp. 97–106, 2011.

[14] M. Landauer, F. Skopik, M. Wurzenberger, and A. Rauber, "System log clustering approaches for cyber security applications: A survey," *Computers Security*, vol. 92, p. 101739, 05 2020.

[15] Z. Li, M. Davidson, S. Fu, S. Blanchard, and M. Lang, "Converting unstructured system logs into structured event list for anomaly detection," *ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1–10, 08 2018.

[16] A. Haque, A. DeLucia, and E. Baseman, "Markov chain modeling for anomaly detection in high performance computing system logs," 2017. [Online]. Available: https://doi.org/10.1145/3152493.3152559

[17] M. Landauer, F. Skopik, M. Wurzenberger, and A. Rauber, "System log clustering approaches for cyber security applications: A survey," *Computers Security*, vol. 92, p. 101739, 05 2020.

[18] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," vol. 34, no. 3, 2010.

[19] L. Souza, M. Silva, and T. Ferreira, "The acceptance of information technology by the accounting area," *Sistemas Gestão*, vol. 12, pp. 516–524, 12 2017.

[20] H.-S. Rhee, C. Kim, and Y. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers Security*, vol. 28, pp. 816–826, 11 2009.

[21] R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework," *Computers Security*, vol. 76, 02 2018.

[22] K. Krol, J. Spring, S. Parkin, and A. Sasse, "Towards robust experimental design for user studies in security and privacy," 05 2016.

[23] S. Rahman, R. Heartfield, W. Oliff, G. Loukas, and A. Filippoupolitis, "Assessing the cyber-trustworthiness of human-as-a-sensor reports from mobile devices," 06 2017.

[24] N. R. Z. Z. H. Zhang, D. Yao, "Causality reasoning about network events for detecting stealthy malware activities," *Computers Security*, vol. 58, p. 180–198, 2016.

[25] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The most dangerous code in the world: validating ssl certificates in non-browser software," pp. 38–49, 10 2012.

[26] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Käsper, S. Cohney, S. Engels, C. Paar, and Y. Shavitt, "Drown: Breaking tls using sslv2," 2016.

[27] J. Kelsey, "Compression and information leakage of plaintext," vol. 2365, pp. 263–276, 2002. [Online]. Available: https://iacr.org/archive/fse2002/23650264/23650264.pdf

[28] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," *2009 IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009*, pp. 641–644, 05 2009.

[29] J. F. R. P. Paul Grassi, Elaine Newton, *Digital Identity Guidelines: Authentication and Lifecycle Management*. NIST - National Institute of Standards and Technology, 2017.

[30] J. Kornblum, "Implementing bitlocker drive encryption for forensic analysis," *Digital Investigation*, vol. 5, pp. 75–84, 03 2009.