Universidade de Aveiro
2022

Bruno Jorge Silva Caseiro

Defesa por ataque: Simulando ataques para promover fortes políticas de segurança organizacional

Defense by offense: Simulating attacks to promote strong organizational security policies

Universidade de Aveiro
2022

Bruno Jorge Silva Caseiro

Defesa por ataque: Simulando ataques para promover fortes políticas de segurança organizacional

Defense by offense: Simulating attacks to promote strong organizational security policies

> "*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*"
>
> — Sun Tzu

Universidade de Aveiro
2022

Bruno Jorge Silva Caseiro

Defesa por ataque: Simulando ataques para promover fortes políticas de segurança organizacional

Defense by offense: Simulating attacks to promote strong organizational security policies

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Cibersegurança, realizada sob a orientação científica do Doutor António Manuel Duarte Nogueira, Professor auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, e colaboração científica do Engenheiro Ricardo Torres Martins, responsável pelo Gabinete de Cibersegurança na Universidade de Aveiro.

o júri / the jury

presidente / president	Professor Doutor João Paulo Silva Barraca Professor Auxiliar da Universidade de Aveiro
vogais / examiners committee	Professor Doutor Leonel Filipe Simões Santos Professor Adjunto do Instituto Politécnico de Leiria
	Professor Doutor António Manuel Duarte Nogueira Professor Auxiliar da Universidade de Aveiro

Palavras Chave

Red Team; Penetration Testing; Engenharia Social; Hacking Físico; Pentesting Físico; TIBER-EU

Resumo

O cibercrime está continuamente a crescer nos tempos atuais devido à constante digitalização das atividades do quotidiano. Recentemente, após a pandemia de COVID-19 ter atingido o planeta, este efeito foi ainda mais acentuado. Com mais atividade digital, o cibercrime tem também uma tendência a aumentar. A simulação de adversário como ferramenta de testagem é um dos instrumentos mais importantes quando se avalia a segurança de uma organização. Testes de intrusão não são suficientes, pois os atacantes recorrem a muitos outros métodos como à engenharia social e às respetivas técnicas (phishing, personificação, tailgating, etc.). O conceito "red teaming" é introduzido através da simulação de um ataque de larga escala com restrições mínimas. Nesta dissertação houve uma tentativa de executar um teste de red team à Universidade de Aveiro com o objetivo de avaliar, testar e melhorar as políticas de segurança da organização. No entanto, devido a restrições legais e bureocráticas relacionadas maioritariamente com políticas de proteção de dados e outras medidas a favor da privacidade, o plano inicial ficou apenas pelo planeamento de um teste red team. O TIBER-EU Framework foi também introduzido, contendo as normas consideradas como estado da arte no que toca a red teaming na Europa. Estas diretrizes foram seguidas durante o planeamento do teste, o que me permitiu, como autor da dissertação e único membro da red team simulada, encontrar algumas falhas de segurança na Universidade através de breves sessões de análise de threat intelligence.

Keywords

Red Team; Penetration Testing; Social Engineering; Physical Hacking; Physical Pentesting; TIBER-EU

Abstract

Cyber crime is continuously growing in current times due to the constant digitization of everyday activities. Recently, after the world was hit with the COVID-19 pandemic, this effect was even more noticeable. With more digital activity, cyber crime has a tendency to also increase. The simulation of adversaries as a testing tool is one of the most important instruments when evaluating an organization's security. Penetration tests are not enough, as attackers resort to many other methods such as social engineering and its techniques (phishing, impersonation, tailgating, etc.). By simulating a full scale attack with minimal restrictions, "red teaming" is introduced. There was an attempt to perform a red team assessment to the University of Aveiro in order to evaluate, test and improve the security policies of the organization. However, due to legal and bureaucratic restrictions related mostly to data protection policies and other privacy measures, the plan was cut short to merely the planning of the red team. The TIBER-EU Framework was also introduced, representing the state of the art guidelines to red teaming in Europe. This framework was followed during the planning of the assessment, which allowed me, the author of this thesis and also the emulated red team, to find a couple of flaws in the University's security by executing brief threat intelligence analysis sessions.

Contents

List of Figures

Acronyms

CED Conselho de Ética e Deontologia

CISO Chief Information Security Officer

CF Critical Functions

DETI Department of Electronics, Telecommunications and Informatics

DDOS Distributed Denial of Service

DPO Data Protection Officer

EQL Event Query Language

GTL Generic Threat Landscape

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IDS Intrusion Detection System

IP Internet Protocol

IPS Intrusion Prevention System

NDA Non-disclosure Agreement

OSINT Open-source Intelligence

Q&A Questions and Answers

RFID Radio-frequency Identification

SE Social Engineering

SSO Single Sign-On

TIBER-EU Threat Intelligence-based Ethical Red-teaming - Europe

TTI Threat Targeted Intelligence

TTP Tactics, Techniques and Procedures

XSS Cross-site Scripting

Chapter One

Introduction

The number of cyber attacks has recently reached a peak during the COVID-19 pandemic, and it probably will not slow down any time soon. A living proof of this statement is the fact that a week before the time of this writing, a major vulnerability in a Java library was found, putting hundreds of millions of devices at risk (Log4j vulnerability).

Even though technical vulnerabilities are continuously being found and disclosed, most major attacks involve weak security policies or "hacking the human" behind the computer, called Social Engineering (SE). Attacks which have their roots related to a technical vulnerability usually come in waves. As soon as a zero day vulnerability is discovered, attackers and defenders race each other: attackers try to scan and exploit every machine possible across the entire internet, while defenders are focusing on trying to patch every recently vulnerable machine. For this reason, after a vulnerability or exploit is made public, several cyber attacks are launched, which makes it look as they were coming in waves.

But what if the breach originates from a SE attack? There is not a patch in the world that can fix weak security policies or an easily manipulated employee (this can be trained and taught, but it must not be seen as the employee's fault). A company's network can be almost impenetrable from a technical point of view: fully patched systems, up to date applications, firewalls, correctly configured IDSs (Intrusion Detection System) and IPSs (Intrusion Prevention System), user input is made through prepared statements and so on, but the moment an employee is phished, most of those technical security measures go down the drain and become next to useless.

This is not to say that technical defense mechanisms should be disregarded or anything similar, because they really are quite useful. Automatic scanners and exploits are constantly being thrown at virtually every open port on the internet, and those mechanisms are the first line of defense. But traditionally, organizations focus their full attention on these and do not usually give too much importance to SE attacks and high level security policies. Fortunately, this has been changing in recent times, more and more companies are raising awareness on this topic and providing employees with training.

But "how do you know you can take a punch, if you have never taken a punch?" [1]. How would organizations know they are ready for an attack if they haven't been attacked before? [2] Well, "Penetration Testing" and "Red Teaming" have just entered the room. These concepts will be discussed and explained in depth in Sections 1.1 and 1.2, but some key ideas should be kept in mind when performing these types of tests. First, they should be performed by an external entity so the assessment or security evaluation is not biased, like Micah Zenko said in his DefCon 27 talk, "you can't grade your own homework" [3]. It is also important to keep in mind that the vulnerabilities (technical, physical or just poorly trained employees) are already present before the test, so avoiding a pentest or a red team assessment is not a fix. Red teaming/Pentesting is about showing where the vulnerabilities are. If they are not known yet, they still exist, the organization just does not know about them. [3]

The goal of this dissertation is to conduct a red team assessment (note that it is not a penetration test) to University of Aveiro in order to better understand the process, demonstrate how and if the documented red teaming methods and techniques are effective and finally, to help improve the security of the organization. Several simulated attacks will be conducted against some departments of the University. It is important to debrief with each of them, or at least with those with weaker security in order to raise awareness and perhaps change their security policies for the better.

The attacks will not be performed sequentially by department, but by phases (discussed in 1.2). This means that the information gathering phase, for example, will be conducted for all targets in a row for a few weeks. The actual exploitation and attacks will also be performed during a small time span in order not to raise unwanted attention for other departments. For instance, if department A is attacked and a few weeks later department B is also attacked, employees and the security of department B might have already heard about department A's attack, disrupting the nature of a red team assessment. There are some bureaucratic matters to take care of before proceeding with the attacks, since it is not legal to social engineer employees and get access to some types of information. There will be a chapter dedicated to legal matters during this dissertation.

1.1 Penetration Testing

As mentioned before, Penetration Testing is a tool or process which allows an organization to test how well they are prepared for a cyber attack. It is also known as pentest and/or ethical hacking, but it should not be confused with a vulnerability assessment. A vulnerability assessment consists in purely enumerating, ranking and evaluating as much vulnerabilities as possible, but it does not go further than that. Meanwhile, a penetration tester is allowed to exploit found vulnerabilities and attempt to go as deep as possible given that he does not leave the scope of the test. A penetration test can be classified in one of three types: white box, when the information regarding the underlying system is given to the tester (source code, technologies used, etc.); black box, when the tester knows nothing about the asset being tested; gray box, which is a mix of both.

The scope of a test should be very well defined, as organizations are probably ready for the suspicious requests or inputs sent by penetration testers. Perhaps a company might want to test an asset which is not in production yet, failing to respect this scope might interfere with business itself or even the work of internal employees. Obviously, it can happen that a penetration tester provokes a denial of service or somehow crashes a system, but organizations should be ready to deal with that fairly quickly. This is one of the reasons that it is not recommended that live assets are tested. Testing versions of systems (not in production) should be used, so the penetration tester has more room for exploiting and testing the asset without worrying about something bad happening.

With this being said, it is trivial to understand how and why this type of security audit is useful. It is assumed that if a system is tested by a skilled (group of) pentester(s) and the found vulnerabilities are fixed, the chances of an actual attacker breaking in are greatly reduced. But this is not always the case.

"Hackers" are also usually classified in three types: white hat hackers or "ethical hackers", which are mostly penetration testers or security auditors that perform authorized tests only; black hat hackers, the malicious ones which do not respect rules and usually act for personal gain; and finally, gray hat hackers, a mix of both. Gray hat hackers can have good intentions but act beyond the law, or perhaps the other way around, the definition of a gray hat is not very clear and can be somewhat subjective. For example, in [4], it is said that black and white hat hackers are only distinguished by two factors, the purpose of the hacking activity and whether or not prior consent has been granted by the victim. Black hat hackers do not have any kind of restrictions (laws, ethics, scope, permissions, ...) so a penetration test, depending on its specifications, might not fully emulate an attack. Adding to this, a penetration test focuses solely on a technical asset or a group of assets, these can be a simple web site, a group of IP addresses or a server. But a hacker will not be restricted to the list of IP addresses which an organization wants to test. An advanced hacker will not even be tied to exploiting only technical vulnerabilities. In this case, the scope is infinite.

From phishing emails and phone calls to lock picking doors or simply walking in a restricted room, an attacker has endless ways of breaking in. A penetration test is not enough to test security to its entirety.

1.2 Red Teaming

Before introducing the topic of red teaming, it is imperative to understand how important it is to think and act like an attacker when doing these tests. It cannot be stressed enough and it has been proved throughout history, for example, by the likes of the "Trojan Horse" story in ancient Greece or by Sun Tzu and Niccolo Machiavelli. The following two very popular quotes in the book The Art of War [5] perfectly represent the mindset of cyber security in general: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." and "Attack is the secret of defense; defense is the planning of an attack". Another great quote but not as popular as these, from the book The Prince [6]: "The lion cannot protect himself from traps, and the fox cannot defend himself from wolves. One must therefore be a fox to recognize traps, and a lion to frighten wolves."

The concept of a "Red Team" can be somewhat subjective, but it is almost universally agreed that these teams are professionals in the offensive side of security, experts in attacking systems and disrupting their defenses. Red teaming is a popular term in military operations, when a group plays the role of an enemy to try and understand their line of thought. Such as in the research paper [7], a red team simulated the planning of a terrorist attack to try and predict their decisions. The team started by identifying possible targets and gathering information about them, then found a location to plan the attack, and finally prepared it by carrying out reconnaissance operations in person. This is quite similar to the methodology of a red team attack, described in depth during 2.5. This exercise works best when a "Blue team" is also present.

Blue teams have the exact opposite goal, to defend against cyber attacks and threats. In reality, a blue team professional spends most of their time monitoring logs and tools, making sure there is no suspicious traffic in an organization's network. Blue teams can also perform risk assessments and predictions such as calculating business costs in case of breaches, but never actually testing their own defenses, that would be the role of a red team.

A constant friendly war between red and blue teams promotes a continuous improvement to the security of organizations. In the end, both teams must collaborate and debrief in order to better understand what is being done correctly and what there is to improve. Some even call this "Purple teaming" [8]. There is no point in the red team "winning" if they do not share their knowledge with the blue side.

Although these two concepts are frequently confused, the difference between a red team assessment and a penetration test is quite large. While a pentest is usually very limited in terms of scope and focused solely on technical assets, red teams have very broad scopes, usually the entire organization. There are also barely any methodology restrictions and the objective is not to find vulnerabilities, it is to break in by "any means necessary". Quotes are necessary in this statement because small restrictions can be set by the target organization (still not as strict as in a penetration test) and red teamers are not free of legal risks [9].

Red teamers should be very careful if they come across electronic financial data, credit reports, employee data or any other type of sensitive information. Laws regarding this kind of data must be analyzed carefully before proceeding. In summary, testers should not be putting an organization in any additional risk. Before moving on from legal matters, it is crucial for red team members to always carry an authorization letter, usually from an employee with high authority in the organization (a senior manager, usually). In case the attacker is caught, either by employees or by law-enforcement, they can still prove they are not doing anything wrong. It is also suggested to avoid running away when/if caught, the red teamer is not doing anything wrong. It should also be heavily avoided to escalate things to the point of involving law-enforcement. Property damage and physical injuries are also not tolerated.

Expanding on this last statement, the real disadvantage of red team exercises is that real adversaries are not bound by laws or ethics and are not concerned with damages done to the organization. In a research paper [10], it was concluded that some organizations might even avoid red team exercises altogether because trust among employees can suffer. This might or might not be a positive outcome.

But how exactly is an assessment like this performed? There is a well known, state of the art methodology for the European Union, TIBER-EU or Threat Intelligence-Based Ethical Red-teaming (see 2.5). However, in general, a red team usually starts by gathering as much information as possible from the target. This information can be collected online (OSINT), by SE or even by physical observation. Next, the team will plan and execute the attack based on the information that was collected. The attacking techniques are endless and will be discussed soon. Finally, a debrief is performed with who asked for the attack (usually a Chief Information Security Officer (CISO) or a head of security) and the blue team, if there is one. Many times overlooked, the debriefing is the most important phase of a red team assessment, as organizations have the opportunity to fix the most severe vulnerabilities and raise some security awareness inside the organization, especially for the employees who "fell" for the red team's attacks or SE techniques. Positive finding should also be reported and discussed. It is highly recommended that C-Level executives be present in these debriefing meetings [2].

According to [11], there can be three categories of red team assessments: Covert, Overt and Hybrid. Covert are the typical assignments, where the red teamers attack stealthily and avoid being caught at all costs. Meanwhile, an overt assignment is usually performed after a covert one, it involves a Q&A and a walkthrough of the attack performed, demonstrating how and what was exploited to the CISO and discussing how it could be fixed. It is somewhat similar to a debrief, but during an overt assessment the red team is allowed to perform "louder" tests, which would have been easily detected during a covert assessment. For example, using a lock pick gun will result in a lot of noise, raising a lot of unwanted attention. The lock might be very weak, but it would probably not be tested during a covert assessment.

The word "probably" in the last statement leads to a very important question that should be analyzed when planning red team attacks. Is the attack going to be performed during business hours or after hours? There are a lot of different factors involved, and this is why protecting an organization can be so hard. The universe of opportunities for an attacker is huge, an attack cannot be described in an algorithm (currently; this will be discussed in section 2.6) and creativity will also play a big role.

With this being said, attackers have very distinct personalities and skills which must be emulated by red team members. It is important to be inside the mind of a threat actor, to think and act like one (within the defined boundaries). For this reason, the personalities and skills of attackers and red teamers overlap in many areas. The main common characteristic is the ability to stay calm, collected and confident in stressful situations, as well as the ability to always think with an "outside-in" perspective and always play the "devil's advocate" [12]. As it was mentioned during a DefCon presentation [11], being a "professional liar" and "staying cool" are the most important traits. It is even suggested to take acting classes to improve the quality of red team assessments, this is due to the importance of SE (see section 2.2).

A lot of penetration testers would not make good red teamers, since IT workers are usually very introverted. On the other hand, some red teamers might not be good at the technical nature of a job like penetration testing, but they might still be very valuable for a red team, as the team composition should be quite diversified [12]. However, the main skills of a red team are still technical security and hacking-related skills such as computer networks, programming, proficiency in some specific tools, electronics in general and even lock picking.

On the other side of the spectrum there are the SE skills, which are a fraction of some topics such as Cyber Intelligence (cyber action + SE) or PsyOps (psychological operations; SE + physical security), these terms are used in the military and even in intelligence-based government agencies [13]. The reason to resort to SE is very simple: it almost never fails if performed correctly. Perhaps a server hosted in Amazon's Web Services is very secure, but the user who logs in the server is not. Human beings are vulnerable to biases and other psychological tricks used by social engineers (more in section 2.2).

Before proceeding to the next chapter to discuss current techniques more in depth, the diagram represented in Figure 1.1 made by Ivan Kovačević and Stjepan Groš [14] attempts to accurately capture the difference between the skills of a red team and a real life threat actor.

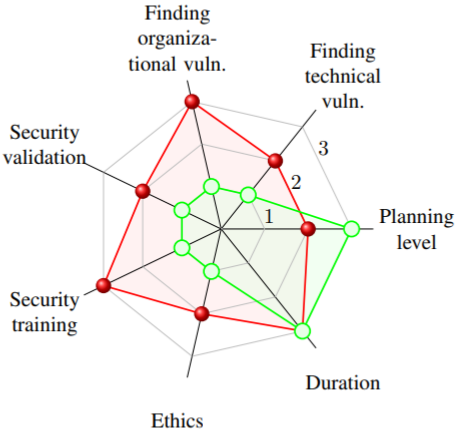


Figure 1.1: Skill distribution of red teams (red) and real threat actor (green)

Another diagram is shown in Figure 1.2, one that thoroughly represents the skills of a red team, made by members of the University of Brasília [13]. The four skills displayed in the outer, gray circles are referred as "macro" skills, the four skills resulting from their intersection are considered secondary while the blue ones are mentioned as tertiary skills for a red team. This article was developed in the military context, but it heavily overlaps with cybersecurity.

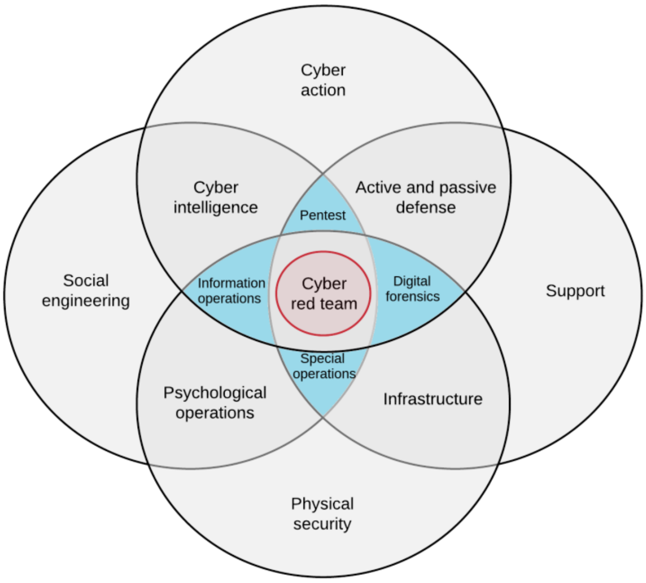


Figure 1.2: Skills for a red team in a military context

1.3 Purpose of this dissertation

This dissertation aims to achieve tangible results by testing, evaluating and possibly reviewing the security policies set at the University of Aveiro. Hopefully,by the end of the dissertation the University becomes a safer place to work and study, its employees and even students will be given training or shown small workshops about information security, and finally, more awareness about security topics in general will be raised.

In order to achieve these set goals, the rest of this document will resume by going over the state of the art of penetration testing and red teaming, where some common techniques and exploits are researched, including social engineering and a deep dive into human psychology. The TIBER-EU framework is introduced, as well as some innovative red teaming techniques.

The third chapter describes the legal and technical preparation that was required to attempt a red team assessment, while the penultimate chapter is exclusively dedicated to the planning of a red team test following the TIBER-EU guidelines. The dissertation ends with a brief conclusion and an outlook to the possible continuation of the elaborated thesis.

Chapter Two

State of the art

This chapter will begin by providing an in-depth revision of techniques that are currently used in red team assessments. Some of the techniques listed in 2.1 might partially involve a small application of SE, leading to the second section of this chapter which describes SE, the techniques related to it and the psychology involved in a very detailed manner. Before closing this chapter, the TIBER-EU framework will be mentioned and characterized, as it is the most up-to-date, state of the art method to perform red team tests. Finally, some futuristic and innovative approaches to red teaming are enumerated. Those are not quite state of the art as they are not used frequently nor they are completely viable, so they are closer to "prototypes" or perhaps even a guess to what the state of the art of red teaming might look like in a few years.

2.1 Common techniques and exploits

This section is dedicated to the enumeration of commonly utilized techniques in red teaming; roughly starting from the most technical to the least. Some of these can require SE, either before performing them, during the exploitation or even after. For instance, in some cases OSINT gathering will only be useful if paired with SE techniques.

2.1.1 Network scanning and exploitation of services

This is a very technical method, which consists in running scanner tools such as "Nmap" to discover open ports and services running on a designated network. It is usually performed either remotely, in case of public networks, or from inside the organization, in order to scan and analyze the private and internal network. It is very important and common for attackers, as it allows for the discovery of the type of servers running, potentially vulnerable services or even security misconfigurations. It is specially dangerous when performed in private networks, as enterprises commonly use Microsoft Windows' Active Directory, which is fairly easily to exploit when inside access is available. Needless to say, exploiting and scanning a network requires an enormous amount of technical knowledge.

2.1.2 Application analysis and exploitation

Application security is not as similar to network security as one might think. Exposed applications are usually web applications (WebApps) or websites. These are the most common assets that are usually in scope during a penetration test, but they are still very important during red team assessments. If a WebApp is "vulnerable enough", it is not required to perform in-person attacks. Even if a web application is somewhat secure with a few vulnerabilities such as user enumeration for example, it is already enough to leverage a more dangerous attack. Some examples of other commonly exploited vulnerabilities are cross-site scripting (XSS), SQL injection, broken access control, security misconfigurations, identification and authentication failures, etc. [15]

In a very bad scenario, a successful exploitation of these vulnerabilities can lead to access to entire servers, databases or even networks. Most of the time, these vulnerabilities are exploited in order to leverage bigger and more dangerous attacks. Naturally, these also require high levels of information security knowledge and hacking skills in general.

2.1.3 Network Sniffing

Network sniffing, snooping, eavesdropping or even "Man in the middle" attacks are similar to network scanning, to some degree. It consists in intercepting traffic and monitoring communications inside a given network. It can result in captured passwords or some other pieces of data which can be leveraged into more dangerous attacks. It is usually performed from a private network of an organization, so about halfway through a red team assessment. Usually it requires previous SE skills or very good technical knowledge in order to reach a situation where the internal network is accessible. A popular software used for intercepting communications is Wireshark.

2.1.4 RFID card/badge cloning

Nowadays every organization uses some kind of RFID card for authorization, identification or/and even authentication mechanisms. Students have a school or university card, some supermarket chains make employees use RFID cards to check-in to work which also double as badges, etc. And the organizations which do not rely on RFID cards usually have some type of badge to identify employees. There are many types of RFID cards but up to 70-80% of companies use low frequency, unencrypted RFID cards, which are by far the most insecure and the easiest to clone [1]. Empty RFID cards and card cloners can be found for sale online for very cheap prices and some smartphones are even capable of doing it as well.

If an organization opts for badges, it is even easier to exploit these. All that is required is a few photoshop skills and a printer. An attacker can easily break into an organization's building by combining badge cloning and some SE skills. The image below shows two very obviously fake badges which were successfully used during a red team assessment [11]. The authors even stated the following: "if you can't clone badges, just build fake ones".

Cloning RFID cards requires a lot of SE skills since an attacker must be very close to the cloned card, but building fake ones as depicted in Figure 2.1 requires only some information gathering. These badges can be found online especially in company meetings, parties, barbecues or LinkedIn posts. This is an example of a very common technique which also requires some OSINT.

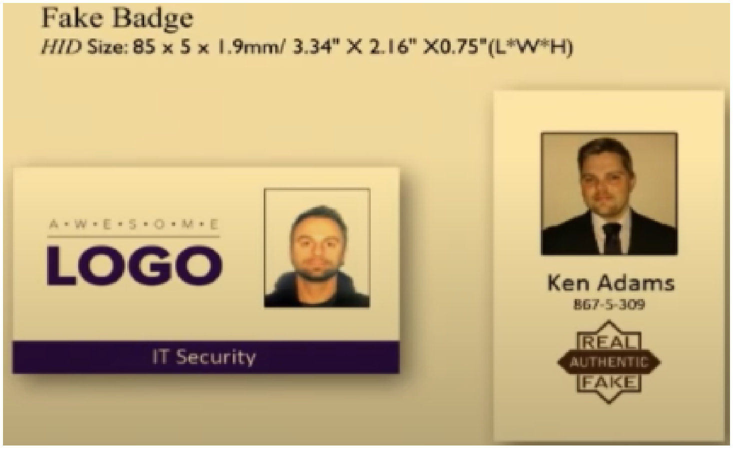


Figure 2.1: Fake badges used during a red team assessment

Cloning and copying of fake badges is usually done before an attack or during the in-person reconnaissance. Depending on the usage that the organization has for the cards/badges, a successful exploitation of cards and badges can lead to many unauthorized accesses, mostly to rooms and spaces inside buildings.

A medium level of information security knowledge is required in order to understand that these cards can be cloned and, regarding the badges, that they can be openly found online. The technical knowledge required is minimal, as anyone can order a card cloner online, read the instructions and quickly start stealing identities.

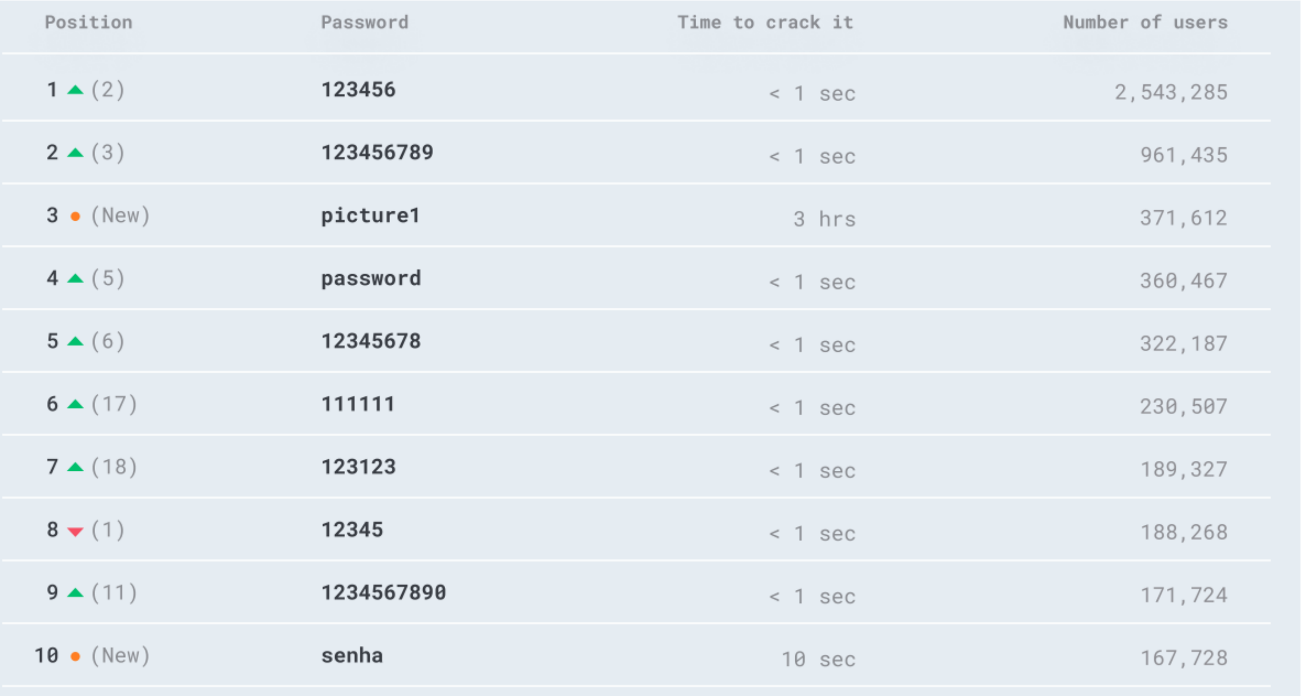
2.1.5 Password spraying

Password spraying is the act of inserting several passwords in hopes of guessing an easy password of a user. This technique is similar to password brute forcing, but it is usually done when a list of usernames is known. The passwords used are either default credentials for a given system, such as "admin", "root", "password" or in some cases even a blank password. Once again, this method can be effective if paired with OSINT or SE, so a username is known beforehand.

The timing of this technique varies immensely, as it can be used in several occasions during a red team assessment. Penetration testers can also use this technique in order to test for weak credentials. Sometimes hacking is as simple as guessing an easy password.

A successful exploitation of weak credentials can lead to unauthorized access to computer systems, either remotely or physically. One neat red teaming trick to bypassing keypads is to look at the dirty and washed buttons for easy pin codes [16]. Although with a lower probability of working, this can also be attempted on smartphones, particularly for unlocks with sliding patterns.

There is not a high level of technical knowledge involved when performing this attack. It is one of the most important techniques even though only some familiarity with basic information security policies is required. Not everyone knows that systems have default credentials or that there are lists of the top 10 most used passwords during a given time period, but an attacker does not have to be a security expert to find that out.



Position	Password	Time to crack it	Number of users
1 ▲ (2)	123456	< 1 sec	2,543,285
2 ▲ (3)	123456789	< 1 sec	961,435
3 ● (New)	picture1	3 hrs	371,612
4 ▲ (5)	password	< 1 sec	360,467
5 ▲ (6)	12345678	< 1 sec	322,187
6 ▲ (17)	111111	< 1 sec	230,507
7 ▲ (18)	123123	< 1 sec	189,327
8 ▼ (1)	12345	< 1 sec	188,268
9 ▲ (11)	1234567890	< 1 sec	171,724
10 ● (New)	senha	10 sec	167,728

Figure 2.2: Top 10 most used passwords in 2020, according to NordPass, a company providing password management services

2.1.6 Open-source intelligence (OSINT)

OSINT stands for Open-source intelligence and in very simple terms it consists in gathering information on a given target through legal and openly available sources. These sources can be online records, the target's employer's website, specific tools designed for OSINT or even LinkedIn or Facebook posts.

The type of information collected can be anything from first and last names to buildings' layouts. Emails, phone numbers, addresses, family members' names, company ranks etc. can all be collected when preparing an attack. For example, Google Maps can provide a good overview of what a company's site might look like. If there is a lot of movement or not, if security is present, what do the surroundings look like and so on. Other examples of popular but more advanced OSINT tools are Maltego and Shodan.io. Maltego provides a library for discovery of data through open sources. it is very similar to what some free online services provide such as the websites listed on the OSINT framework (https://osintframework.com/). The OSINT framework is a collection of online tools for OSINT, there are search engines for people, phone numbers, business and public records, the list goes on.

OSINT is mostly used before a red team assessment in order to better prepare an attack. it is a large portion of the work in the digital forensics world, which by itself says a lot about its importance when preparing a red team assessment. The technique alone is not very useful, but it can be used as leverage for very dangerous attacks such as phishing and its variations.

OSINT is in the middle of the Technical-SE spectrum, so it will be mentioned again in the next section.

The knowledge required to gather information on a target is not a lot, but it requires that the gatherer knows where and how to look for this information. In the United States, official and government records are publicly and widely available and a portion of the population knows about it. In other countries, OSINT can become somewhat harder to perform. Google can also be considered an OSINT tool if the user takes advantage of all its features. Sometimes sensitive information is unintentionally disclosed and an in-depth Google search can do the trick.

2.1.7 Lock picking

Lock picking is the art of unlocking a lock, usually a door's lock, by using tools and gadgets to manipulate it instead of using a traditional key. Some red teamers are more skilled than others in this trade, but almost all of them run their assessments with some kind of lock picking gun. A lock pick gun is a loud gadget that automatically attempts to pick a lock, it is usually effective against weaker ones. However, a good quote to keep in mind by Jayson E. Street is "No point in being a locksmith if people can let you in" [16]. Once again, it hints at the importance and effectiveness of SE.

Lock picking is usually done during red team assessments, but a lot has to be kept in mind such as the surroundings, the attention drawn and the time of day. it is obviously performed to break into unauthorized rooms, but it is also possible to pick different kinds of locks and not just door locks.

Lock picking is another technique which almost falls in the SE category, but fundamentally there is no human interaction required to objectively pick a lock. Perhaps it is required to reach a situation where a lock can be picked, but the technique itself requires no social interaction.

The technical knowledge required is null (from an information security expert's point of view) and so is the SE skills (taking into consideration the above perspective), but it might require some handiness, craftiness and maybe previous experience on the topic.

There are other more specific techniques which are mostly a combination or a deeper dive into the ones listed above, but these are definitely the most common during a red team assessment. But the SE piece of the puzzle is still missing, a red teamer is not a penetration tester, and he can enjoy other techniques which are highly more effective.

A study even attempted to investigate how technology could replace SE [17], but it ends up in a cycle, always leading to human vulnerabilities. The author claims hydrogen bombs (technology) can prevent wars just by provoking fear alone, instead of having to negotiate or manipulate world leaders. But in the end, a strong emotion is associated with the hydrogen bomb, fear. And that is what is preventing the war, fear; not the hydrogen bomb itself. For that reason, social engineering was not replaced, it was just used in an indirect manner. In what seems like a comical tone, the author suggests a woman is more easily convinced to accept a IUD (intrauterine contraceptive device) instead of taking a birth control pill every day. But in the end, social engineering is still present. The technology of the IUD was used to overcome "bad" emotions for the woman, the burden of having to take a pill every day and not running the risk of forgetting it by accident.

In the following section, social engineering will be explained in depth, some techniques will be listed and described just as they were in the previous one. Finally, the psychology behind it and a more analytical explanation will be given. It sounds counter intuitive that techniques focused on manipulating emotions can be (partially) analytically explained, but there are still a few common pillars in humans' minds that can almost always be manipulated in order to obtain information.

2.2 Social engineering, common techniques and the psychology behind it

Social engineering is the process of psychologically manipulating people in order to obtain information. Obtaining information is always the key, although the end goal might be to gain unauthorized access to a system or physical space. It is a very important field in information security and also a very deep one in psychology. This will be discussed later during this section.

Social engineering is one of the most effective and under researched cyber crimes, as of now [18]. Its effectiveness comes from the fact that humans consider themselves to be in a state of absolute security at all times, but a small unnoticed mistake can turn into losses of millions of dollars. Nowadays, hackers will not attempt to break into as many systems as possible, that is in the past. Today, the biggest systems have state of the art security, but still require humans to some degree. Professional attackers will aim for a human target instead [19]. Many recent attacks have started through social engineering, usually through phishing, but this art has been around for a few decades. It first appeared during the age of phreakers ("phone hackers"), when they would chat about SE techniques but describe them as "bullshitting to get information" [20].

Humans are so easily exploited because social engineers take advantage of social errors and cognitive biases, while the attackers' techniques are only limited by their creativity [21]. It also helps that victims might not be aware of the value of the information they possess [22], adding to this, people do not usually expect bad things to happen until they happen [16]. Technical malware can assist SE, combining psychological, social and technical aspects in one single attack, such as in phishing [23].

A social engineer's success will heavily depend on his or her ability to develop trusting relationships [23], since the six human tendencies he or she will rely on will be authority, likeness, reciprocation, consistency, social validation and security [19]. The psychology in social engineering will be discussed deeply when closing this chapter, but for now it is important to understand it from a high level: a social engineer is always pervasive, persistent and persuasive [23].

Humans are vulnerable to social engineers, mostly when these are acting confident and know the roots of the manipulative strategies they are using inside out. These attacks can take up to weeks, if not months, including several physical visits to the target. In an edition of "2600: The Hacker's Quarterly", someone got a job as a janitor within a company only to access critical information [24]. Unlike exploiting technical vulnerabilities, social engineering attacks can take much longer because they require a lot of preparation. Kevin Mitnick, one of the most famous hackers ever, claims there are four stages in a social engineering cycle: research, developing rapport and trust, exploiting trust and utilizing the information [19].

Below are some of the most common social engineering techniques and how they can be used to exploit a target.

2.2.1 Phishing

Phishing is somewhere in between social engineering and "technical hacking", as it requires some expertise to set up but on the other hand the vulnerabilities being exploited are human emotions. In general terms, phishing is sending a fraudulent message to a victim in order to trick them into revealing sensitive information. There are some variations of the term, such as "vishing" (voice + phishing) when performed over the phone, smishing, when the message is delivered via SMS and spear phishing, which is when the attack is highly targeted.

Phishing has been very popular in the last few decades through emails. These would be sent in mass with a generic message, usually asking nicely for money for a specific reason (such as an investment with guaranteed return) or by blackmailing with made up information, which might or might not be true about the target.

These phishing emails were not very effective, but since they were sent at such large scale, attackers would still profit. However, the most common and effective technique nowadays is spear phishing [23]. The concept is the same and it does not have to be delivered via email, but the message is personalized for each target. Recently discovered 0-day vulnerabilities and spear phishing are the two biggest starters of cyber attacks.

There was a study performed while training future cyber security professionals in spear phishing using a method called SiEVE (Social Engineering Vulnerability Evaluation), which appears to be a conventional way to map and evaluate the steps to perform a spear phishing attack [25]. From previous research done by the authors, they concluded that most enterprise attacks result of spear phishing. During the actual study, it was found that posing as a known individual for the target increases the chance of success by 4.5 times. Also, the previous research about a target does not need to be as deep as it sounds, sometimes all the information needed can be found on a social network such as Facebook. The method had three main phases: 1) Identify the target; 2) Profile the target; 3) Craft the spear.

The usual purpose of a phishing attack is to collect the credentials from the target user. Vishing usually has different objectives, but still aims to retrieve sensitive information. From there, other more dangerous attacks can be leveraged.

2.2.2 Dumpster diving

Dumpster diving is considered a social engineering technique although no social interaction is required. Just as the name implies, it consists in looking through the thrash cans of the target. Organizations which deal with sensitive information usually have shredders spread through the office, but sometimes a really persistent attacker can still make sense out of the stripes of paper in the thrash. The solution is cross cut or micro cut shredders, which decimate the paper in a way that makes it extremely hard for anyone to puzzle it back together.

On the other hand, most individuals do not have a paper shredder at home. Sometimes having access to prescriptions, medicine packages, bank statements, mail exchanged with administrations and government organizations, etc. is as easy as looking in a thrash can.

2.2.3 Shoulder surfing

Shoulder surfing is another technique which requires minimal to no social interaction, and it is very simple to conduct. It simply means to look over someone's shoulder while they are dealing with sensitive information. Standing behind the target while they insert their password is the most common situation that qualifies as shoulder surfing.

2.2.4 Impersonation

Social engineering techniques do not have to be complicated. People will not expect and attacker to be impersonating another person, especially in person. A characteristic of this technique that is sometimes looked over is that when posing as someone with high authority, the target will be thinking twice before accusing the social engineer [19].

Impersonating and phishing are two most usual techniques used by red teamers, and neither requires high levels of technical knowledge.

2.2.5 Name dropping

Name dropping is a speech technique that exploits human emotions directly. It is usually tied with either phishing or impersonation. The attacker mentions people from inside the company (drops names), which makes the victim assume that both parties are familiar with that same person. This can work in two ways: as Mitnick states in his book [19], name dropping high ranked people in the company can leave the target more comfortable and/or intimidated when providing inside information. Explaining and understanding how and why social engineering works is very complex, but the execution can be as easy as saying a few names.

2.2.6 Tailgating

In the common world, it is usually called tailgating when a car driver is so close to the car in front that if the first stops, there is undoubtedly going to be a collision. In a way, "tailgating" for hackers and red teamers can have the same definition, but it is carried out in very specific situations. Many organizations have spaces restricted via access cards or biometric data which should be required by each and every person accessing the given space. Tailgating circumvents that need, an attacker simply sticks behind someone at a distance that will not allow the door (or whatever physical barrier) to close and ask for authorization again. The tailgater accesses the space without having to provide an authorization token.

2.2.7 Escalating requests

Escalating requests is something that can be used after the first impression is made. it is very common for scammers to do this. It consists in first starting with a very small favor to which the victim would not mind complying. The following requests are gradually larger.

In a hypothetical scenario of a woman scamming a man by invoking a sexual desire, which is very common in the internet, the first request could be a couple of dollars for a meal. The next request could be a slightly larger sum for a week of rent. Finally, a third request could be a large sum of money to pay for a flight to supposedly meet the man. The last request seems a lot more plausible after complying with the two former ones.

This is connected to a psychological event called the "sunk-cost fallacy" [26]. The sunk-cost fallacy is when someone hesitates on abandoning a bad strategy since they already have invested a lot of resources into it. It is especially common in gambling. The sunk-cost fallacy and the technique of escalating requests can almost be seen as the vulnerability (psychological bias) and the exploit.

2.2.8 Company lingo

Using "company lingo" during speech can give a false sense of confidence in the attacker. It acts almost exactly as name dropping but instead of names, the attacker uses internal words. For example, dropping several internal departments names and their respective acronyms would be considered usage of company lingo, which leaves the victim more likely to trust the attacker.

2.2.9 Reverse social engineering

Reverse social engineering provides instant credibility [19]. In order for this technique to work, the attacker must already be inside the mind of the victim as someone who is available to help. The attacker then creates a problem for the victim without them knowing about it. Faced with the problem, the victim will recall how the attacker is able to help them solve it. The attacker is happy to help, but he or she can use this as leverage when asking for something in return.

Reverse social engineering can have some variations of the general example depicted above. It might seem hard to conduct but the possibilities are endless. As an example, let us build an hypothetical scenario. Attacker (A), through previous OSINT collected, calls target-employee (E) and introduces himself as a substitute for a help desk employee who is taking a couple of days off. Through his or her speech, 'A' drops a lot of authority names and uses company lingo in order to establish a false sense of confidence. The details are not important, but let us assume 'E' believes that 'A' is, in fact, part of the organization's help desk. Later, 'A' sends spam emails in mass to the internal email address of 'E'. As this is not a common occurrence, 'E' needs help from the help desk and will remember how 'A' is available to help. The attacker can now ask a series of questions to "verify" the identity of the employee, retrieving the answer to the security questions of the employee's account. Now the attacker can successfully complete the "reset password" process while posing as the target employee.

Social engineering and technical knowledge can be combined in numerous ways. Social engineering can be split into several categories, according to [27]. One of the categories is "sociotechnical", which includes phishing, spear phishing, using malicious devices or even baiting victims to use the devices themselves. Figure 2.3 shows a diagram made by the authors, which lists SE attacks, its vectors and channels. The only technique which has not been mentioned is waterholing: compromising a website of interest to the victims.

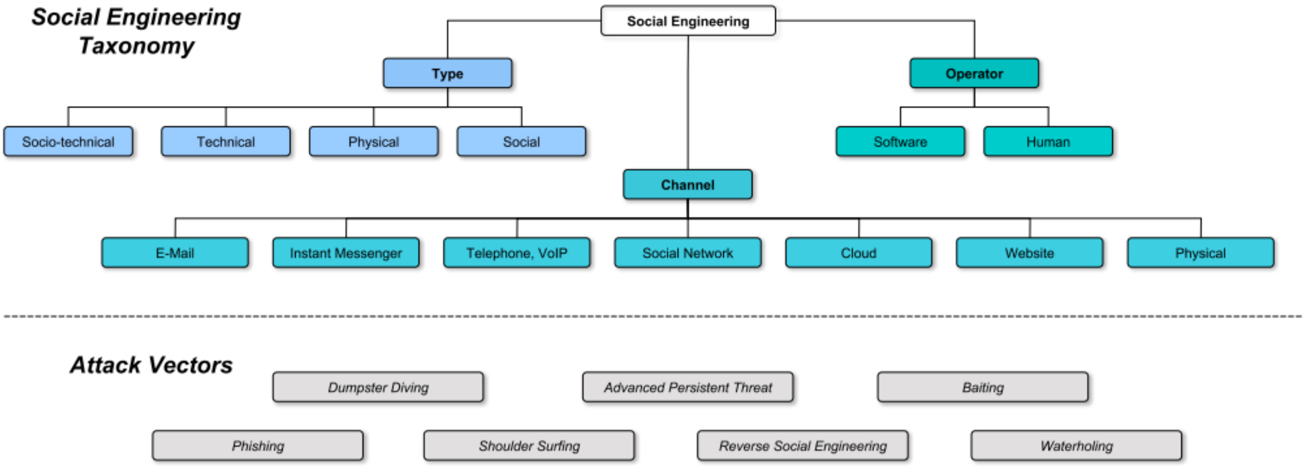


Figure 2.3: Overview of SE attacks, channels and vectors

Two very good sources to understand the psychology behind social engineering are these books which have been frequently cited during this dissertation: [26] and [19]. Although their fields of work are different, in practice they can overlap, and so do their findings. Kevin claims a victim of social engineering will always remember the start and end of an interaction better, and this aligns with Kahneman's "Halo effect": first impressions will always weigh more and influence later interactions. Kevin Mitnick also explains in his book how people do not expect anything to go wrong except when it does, which gives the benefit of the doubt when dealing with social engineers. Once again, Daniel Kahneman describes two biases which agree with Mitnick's findings: the "Planning fallacy" - always assuming the best case scenario will happen - and the "Confirmation bias" - the human mind tends to favor evidence and facts which support something it already believes.

The most common emotions vulnerable to exploitation are authority, likeness, reciprocation, consistency, social validation, scarcity, the desire to be helpful (empathy), a tendency to trust people, fear and willingness to cut corners (greed) [19] [28] [23].

In an attempt to materialize the exploitation of these emotions, an attacker could use techniques such as diffusion of responsibility ("I'm the authority, if it goes wrong it is my fault, do not worry"), promising future rewards, forcing a moral duty or invoking guilt ("guilt tripping"), identifying with the victim in order to create feelings of empathy, etc. [18]. Manipulative people have very attractive personalities, they are quick thinkers and are able to distract the victim from their own thoughts, even acts that do not require social interaction can be considered manipulative such as staying at the scene of the crime longer than necessary to avoid suspicion. Even the timing of the attack can influence the outcome, as people are more easily influenced when they are overloaded with work or other tasks [26]. Adding to all of this, the authors of [3] concluded that 85% of people believe they are less biased than the average person, which only makes the scenario better for social engineers.

An article called "Hacking the Wetware!" [29] labeled some of these tendencies in three different categories: normative commitment, feeling obligated to return gestures and favors; continuance commitment, feeling obligated to behave consistently according to a past decision (sunk-cost fallacy); affective commitment, feeling obligated to provide information because of the need to be socially accepted. it is very interesting how the attacker does not force the victim into doing anything, but instead invokes feelings of moral obligation. Obviously, the author claims humans who demonstrate high levels of normative, continuance and affective commitment are more vulnerable to social engineering.

It is usually not something that is given much thought, but the ethics of red teaming is something interesting to analyze, since an actual attacker will have absolutely no limits on ethically wrong behaviours [4]. It is a very subjective topic that can be evaluated through different ethical theories such as utilitarianism, which only evaluates the consequences of an act, or Kantian deontology, which argues that isolated, objective acts should be morally evaluated. Kant's theory is completely against red teaming assignments since tricking employees and hacking systems would be considered unethical. On the other hand, utilitarianism would support red team tests if the advantages outweigh the disadvantages. For example, if some employees suffer emotionally after the assignment, the ethical value of the test can be questioned.

The author of [4] claims the term "ethical dilemma of social engineering in penetration testing", characterized by first distinguishing black and white hat hackers: they differ by 1) the purpose of their hacking activity and 2) whether prior consent has been granted by the victim. All of this is highly subjective, but there would be a solution for this dilemma. First, the designation "ethical dilemma of social engineering in penetration testing" is somewhat conflicting as a penetration test does not involve humans, but red teaming does. Secondly, a red team assessment aligns with white hat hacking in the first condition (purpose of the hacking activity) but does not fulfill the second one (no prior consent granted by the victim). A well prepared organization could state in the employee's contract that red team assessments could happen during the lifetime of the contract. There are two advantages to this, extra awareness for information security and the ethical dilemma would disappear, even though the importance of ethics, morals and the dilemma itself can and will always be questioned.

2.3 Current landscape of cyber attacks

This next brief section will go over a few of the latest and largest cyber attacks in order to prove how social engineering plays such an enormous role in state of the art information security, as well as a recently discovered vulnerability which is causing chaos in many enterprises. Red team assessments should be as close to a real life threat actor as possible, so studying and learning from those who are being emulated is the best strategy.

As it was mentioned before, spear phishing is the most common and effective technique to leverage more dangerous attacks. Red teams diverge from denial of service tests, but in today's world, a variation of it is by far the attack which is more usually seen in the wild - ransomware.

The word "ransomware" originates from the combination of two different words, "ransom" and "malware". A computer infected with ransomware would have its files encrypted in a way that only the attackers are able to decrypt them. The hackers would then ask for a large sum of money, the ransom, in exchange for rescuing the encrypted data. Victims are usually infected with ransomware through spear-phishing and the worst part is that this malware is sometimes able to spread sideways to other computers in the same network.

Some claim the ransom should not be paid as it encourages future attacks, or perhaps the current attackers would only rescue part of the information and ask for an even larger ransom for the rest of it. In some occasions, the information is never released anyway. Opinions are still divided for this topic, but one thing is very clear: frequent backups are an essential tool to fight ransomware.

- Log4Shell

  Log4j is a popular Java framework that allows for data logging. The technical details of this zero-day vulnerability are not important, but the key point to take from it is how 93% of enterprise cloud environments were affected by it. The vulnerability had been privately disclosed to the Apache Software Foundation around 2013 but it was not patched. Meanwhile, it was released to the public on the 24th November 2021. For 8 days there was no patch for it, leaving millions of devices vulnerable to the Log4Shell attack [30].

  Automated scans and exploits were being launched against millions of devices throughout the internet with absolutely no social interaction necessary. At the time of writing (January 2022), some machines are still being exploited. A successful exploitation leads to remote code execution, which is the worst possible outcome.

  Social engineering did not play a part in these attacks, but zero-days occasionally appear, and if taking systems offline is not an option, waiting for a patch with a vulnerable system online is the only solution.

- Grupo Impresa

"Grupo Impresa" is a Portuguese media group which holds all SIC TV channels, the Expresso journal among others. The exact details of this attack are still not known for certain, but it is widely believed it started with a phishing attack to a high level employee. Credentials for Impresa's Amazon's Web Services were phished and soon the SIC and Expresso's websites were both defaced, with a ransomware-like message [31].

SIC's archives were allegedly deleted and a lot of personal information was accessed by the hackers. The hacker group is called "Lapsus$" and have targeted Brazilian government organizations in the past. What is interesting about this attack is that no ransom has been requested, but Impresa's files have still been encrypted and although the attack has not been solved yet, it appears they are currently either negotiating or haven't disclosed all the details yet.

- Robinhood Markets

  Robinhood Markets is an American company which provides financial services. They suffered this attack in November of 2021 and 5 million customer email addresses were stolen, while another 2 million users had their full names taken [32].

  The attack was performed resorting to vishing, when an employee was social engineered through the phone. Besides the data previously mentioned, the attacker also gained access to additional personal information such as dates of birth and ZIP codes of a smaller group of people. The hacker then asked for an extortion payment to rescue the information. Some of the data ended up being leaked [33].

The goal of this chapter was to lightly present different types of cyber attacks that could happen in organizations. Log4j was a "simple" zero-day vulnerability which encourages hackers to scan the internet looking for vulnerable machines while Robinhood's data breach was a "good old-fashioned" ransomware with a small twist: vishing instead of phishing.

Then, there is the case of Grupo Impresa, which is somewhat uncommon as it appears the attackers are not looking for money. However, not all details have been disclosed. For this reason, it is still hard to conclude what are the motivations and objectives of the attackers with great confidence.

2.4 How to not be a victim of social engineering

Being aware of a social engineering attack is not something that is at the top of employees' head, especially when there are important tasks to finish or when they are overloaded, a situation when the employee's thinking is not at its best. Adding to this and according to Kahneman [26], the status quo bias will not be helping either, as people have a slight preference for the current state of affairs. This means employees will always show slight resistance to acknowledging that there is something wrong, either when they are actually under attack or when questioned about the company's bad security policies.

It is critical to understand how an attacker might operate, and after all the analysis described during this document, we can conclude some warning signs of an attack might be:

out of ordinary requests, claims of authority, stressing urgency, refusal to give a callback number, threatening, name dropping and even flirting or flattery [19]. it is important to remember how a social engineer attack is only limited by the attacker's imagination and creativity, therefore, it is impossible to enumerate all possible scenarios of attack.

The solution is to always verify identities and classify information. Data should be classified in different categories, for example: public, internal, private and confidential. Identity verification should be performed in order to understand if another employee can access a given category of information. The exact procedures for this verification are various, but they include requesting digitally signed emails, dynamic passwords (daily renewable tokens only known by internal employees), vouching (by another trusted employee), contacting a supervisor or manager, etc.

Security policies inside an organization will depend on the type data being handled as well as various other factors, so they should be discussed deeply and defined not with a "everything is going to be okay" mentality, but with frame of mind such as "it is impossible that something will go wrong". With this being said, there are some general policies that can be implemented in almost every enterprise, such as never speaking passwords over the phone, not leaving passwords lying about (in sticky notes, paper, etc.), using cross shredders, implementing caller ID technology [28], not giving out personal information, using firewalls and antivirus software, not visiting HTTP websites (trust only HTTPS) and, of course, regularly testing the company's defenses with thorough red team assessments [18].

2.5 TIBER-EU Framework

Before mentioning the TIBER-EU Framework, the cyber kill chain should be mentioned. "Kill chain" by itself is a military concept which identifies the structure of an attack [34]. In general, the kill chain would consist in identifying a target, dispatching forces to the target, initiating the attack and finally, destruction of the target.

Recently, Lockheed Martin, a corporation with numerous interests, one of them being information security, came up with the "cyber" version of the kill chain - the cyber kill chain. Although it is not universally accepted or described in great detail, it is a very well known concept. The TIBER-EU framework takes some concepts from the cyber kill chain (see figure 2.4), expands them and applies them to red teaming.

TIBER-EU [35] is the true state of the art framework used to guide red teams on their assessments. It is mainly directed toward financial institutions and its infrastructures, but the framework can be applied to other organizations as well. It claims to mimic the tactics, techniques and procedures (TTPs) of real-life threat actors in order to test the critical functions (CFs) of an organization and its systems, including the people involved. The framework stresses how important it is to not resort to "internal teams that have grown accustomed to the internal systems, people and processes". Other pre-conditions which have already been mentioned during this dissertation are also present in the TIBER-EU framework, such as the risk of testing live systems during a red team assessment.

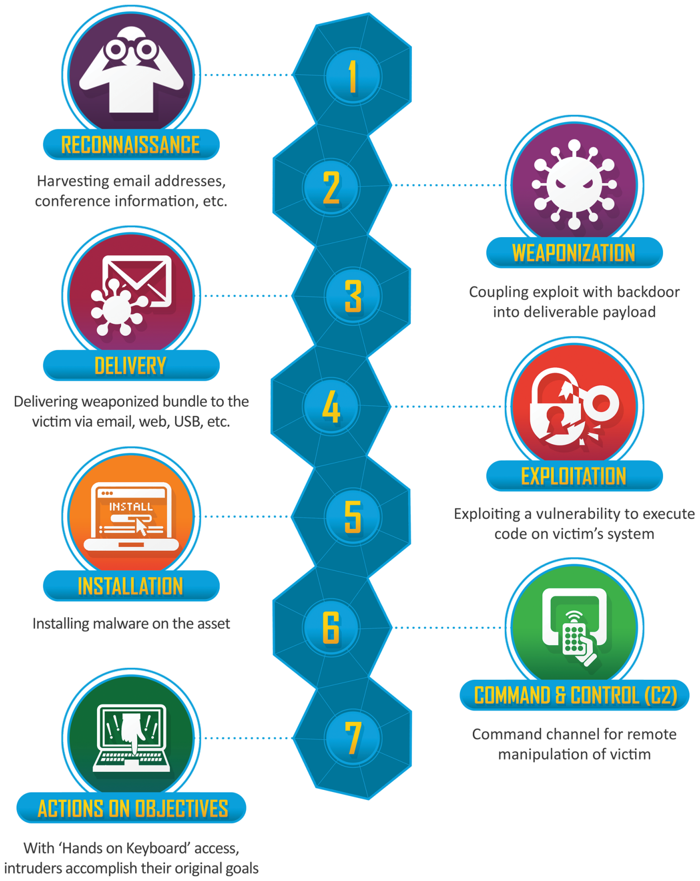

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 2.4: The Cyber Kill Chain

From a high-level point of view, the TIBER-EU framework consists in three main processes: preparation, testing and closure; with some flexibility associated to their specific details. The red team assessments to the University of Aveiro, performed during the practical half of this dissertation, will be loosely based on this framework.

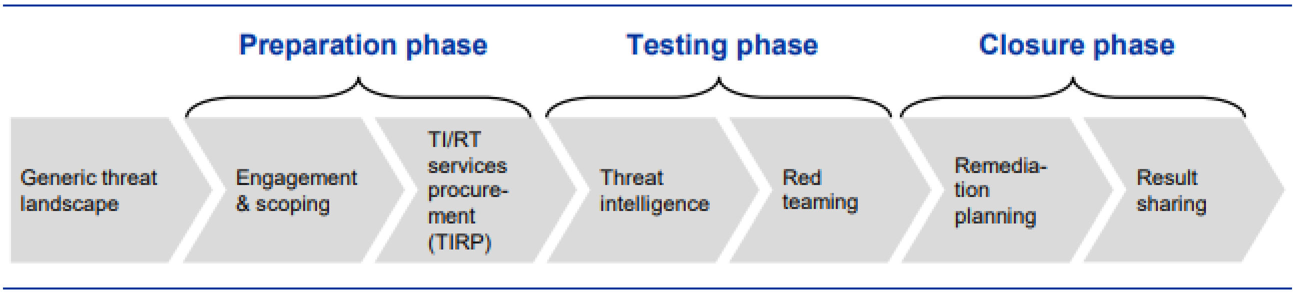


Figure 2.5: TIBER-EU process

The flexibility of the framework is very important as countries with different laws and rules will probably have slightly different implementations of the framework. Although the document is very deep and detailed regarding its birth, rules, government procedures and other non-essential information (to the actual red team assessment), this chapter will focus mostly on the red teaming process.

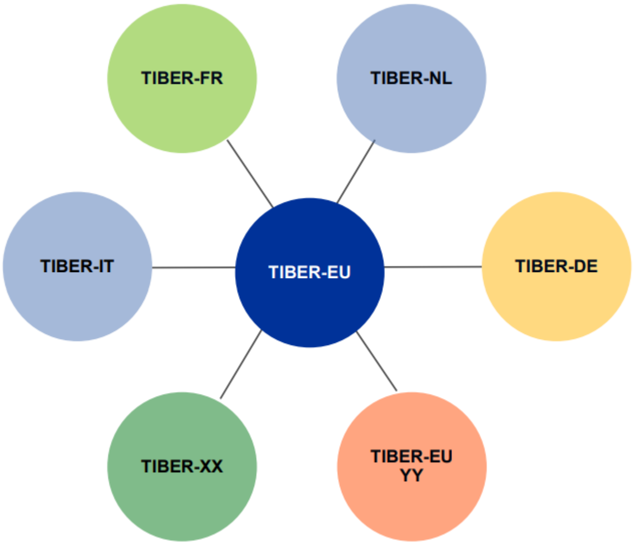


Figure 2.6: TIBER-EU European implementation guides

Just like this thesis will have a "Legal and Technical Preparation" chapter in order to gather permissions to conduct some activities, the TIBER-EU framework also lists some techniques which may be performed to "fully replicate a real-life attack". The list is not exhaustive and other activities might also be carried out. Loosely transcribing from the document, these are:

- Gathering OSINT on the target entity and it is suppliers
- Gathering data from other sources (government sharing platforms, etc.)
- Gathering data from the dark web
- Deploying disguised people to gather intelligence
- Creating fake scenarios to social engineer people using the information gathered
- Gathering data on employees and customers of the target
- Gathering credentials from employees and service providers of the target

Following the diagram in Figure 2.6, the first step (Generic threat landscape) consists in describing the general scenario of the threat landscape, such as identifying TTPs of real-life threat actors, who might these threat actors be and specifically which assets are likely to be targeted. This is the only optional phase in the TIBER-EU framework.

The preparation phase is short: scopes are defined, teams are established, and everything is validated by relevant authorities. The red team is given permission to carry out the test. Even though it is a quick phase, the importance of it cannot be overlooked.

The actual assessment happens during the test phase. It starts by having a TTI report developed, or "Targeted Threat Intelligence Report". Threat scenarios and other useful information is present in it. The scenarios should be intelligence-led and specifically target CFs and its associated people and processes.

The closure phase - the red team provides a test report, showing its findings and observations. Advice on improving security policies, technical adjustments and even awareness and education can be included. Executives and other highly ranked employees should now be aware of the assessment in order to have the red team walk through the issues while discussing them (described as overt assessments in [11]). A remediation plan must be developed and executed or else all the testing would be in vain. In the next sections, some smaller details of each phase will be enumerated and described.

2.5.1 Preparation phase

Besides what was already mentioned in the above overview of the three phases, during the preparation phase it is also ensured that the red teamers meet appropriate standards to conduct the test, they must also undergo a formal TIBER-EU certification and accreditation process.

The scope is also very well defined, other functions can be added to the CFs already listed. it is important to note how a CF is not a system but a critical function.

After the scope is set, the "flags" to be captured are defined. A "flag" is the objective, target or goal that the red team must achieve to consider the assessment as finished, assuming they are not caught or interrupted. Flags can be dynamically changed during the assessment, as sometimes it is interesting to push deeper into an organization to truly test its limits.

2.5.2 Testing phase - threat intelligence and scenarios

The target entity should now write a Generic Threat Landscape (GTL) report with specific attack scenarios they may be faced with. These include who might be threat actors and what assets they will target. This allows for more realistic testing since the red team now has a clearer idea of how the assessments should be performed. The GTL can be updated frequently since the threat landscape is constantly evolving with new TTPs and threat actors constantly entering the cyber security world.

After the red team has the GTL, they can proceed in developing a TTI (Threat Targeted Intelligence) report. This report includes all gathered information on the target in order to create a realistic attack scenario. The importance of this report cannot be stressed enough as real-life threat actors have weeks, if not months, to gather all the information necessary and prepare an actual attack. Some difficulties might arise due to natural limitations such as ethical and legal boundaries, and time and resource constraints.

The TTI should mainly focus on two key areas, the target and the threat. The target being the potential attack surfaces across the entire entity being tested, while the threat are potential threat actors and threat scenarios. Target identification is generally carried out by thoroughly identifying weak points in the various systems, including employees. Meanwhile, threat identification relies on past cyber attacks and potential threats which might have the resources and can benefit the most from an attack to the entity in cause.

In summary, the TTI should consist in tailored scenarios, threat actors and their goals/motivations and finally, evidence that a post-test remediation and improvement will be effective in reducing business risk.

2.5.3 Testing Phase - red team testing

The actual testing can now begin, which should reasonably take around 10-12 weeks in a professional enterprise setting (this number varies according to the organization's size and complexity). The duration should be allocated beforehand by considering some factors such as the scope, the target entity's resources and any other external requirements for the assessment. The methodology can vary and is flexible to some degree, but below is the example given in the official TIBER-EU framework document:

- Reconnaissance

  The first phase focuses on collection of information. This includes technologies used by employees, their routines, security policies, etc. It differs from the previous information collected when creating the TTI since this phase may involve physical presence at the target's infrastructures. The position of security cameras and personnel schedules are some examples of what type of information might be collected.

- Weaponisation

  With the help of the information gathered in the reconnaissance phase, a picture of the target starts being formed. A preparation for the operations on the targeted assets is carried out.

- Delivery

  In the delivery phase, the red team starts executing the actual attack and carrying out actions such as social engineering, scanning networks, planting malicious devices, etc.

- Exploitation

  The true "breaking-in" happens in the exploitation phase, which heavily depends on the previous phase. While the delivery phase consists in executing the "malicious" actions, the exploitation is when the red team takes advantage of what was achieved previously. In a hypothetical scenario, after a network is scanned and vulnerabilities are found during the delivery phase, the exploitation would consist in the red team proceeding to take advantage of those same vulnerabilities and gaining access to critical systems.

- Control and movement

  This phase is what is commonly known as "moving laterally" or "privilege escalation" in the information security world. After the red team successfully exploits a given machine, they attempt to propagate their control over to other machines especially ones with higher privileges (privilege escalation). Sometimes moving laterally to other systems with the same privileges is necessary in order to follow a clearer path to a higher-value system.

- Actions on target

  The final phase of testing happens when the red team attempts to achieve the flag previously agreed upon. Sometimes the employee of the target organization who requested the assessment might ask the red team to capture another flag, or to push the (in)security limits of the organization. On an off-topic note, some red teamers suggest pushing as much as possible after capturing the flag and only finishing the assessment when caught [11]. However, this should be discussed in the beginning stages of the test.

2.5.4 Closure phase

Although the actual testing has ended, the closure phase gives utility to the red team assignment. A remediation plan is developed and the results from the red team are shared, in order to actually enhance the security of the target. All relevant stakeholders should be involved in the closure phase.

After a red team report is submitted, the blue team is supposed to develop their own report with counter measures to the attacks presented by the red side of the attack. This is important because soon there will be a replay workshop: the red team walks the blue team through the techniques used to conduct the attack while discussing what is wrong, what is right and what can be done to improve security.

A 360-degree feedback meeting must be held including all participants. The meeting is not supposed to focus on the security itself, but on the TIBER-EU process. From each of their perspectives, parties should cover important topics such as which activities or aspects of the TIBER-EU process worked well, which must be improved and how it can be improved. Obviously, any other feedback is also welcome.

After the 360-degree feedback meeting, it is time to submit the final version of the remediation plan and the test summary report. The remediation plan is based on test results, which describes improvements to mitigate vulnerabilities in order to reduce business risk. Meanwhile, the test summary report is less technical and does not contain information regarding weaknesses or vulnerabilities. Its goal is to summarise the overall test process, as well as other documents such as the red and blue team test reports, the TTI report, the remediation plan and so on.

2.6 Futuristic views on Red Teaming

Red teaming is still somewhat new to the world, almost everyone outside the information security will not be familiar with the concept. But this does not mean information security professionals are not constantly innovating and developing new tools and techniques. it is a vast field which is rapidly growing almost in a parallel universe, as most people will not be noticing the fast development of security techniques unless it directly affects them.

With this being said, this chapter will now go over some projects by other authors which are paving the way to the evolution of red teaming, it can even be considered "beyond state of the art", as some of these cannot be implemented yet while still obtaining good, practical results.

The first project to be discussed will be from a conference talk, blackhat USA 2019 - "Fantastic Red-Team Attacks and How to Find Them" [36]. The first note is that this does not involve actual red teaming, but penetration testing. However, the concept is interesting and red teaming involves exploiting systems, similar to penetration testing, so this talk is still relevant. What is shown during this talk is a project called "Atomic Red Team", which is an open source project for testing for security controls. It is based on YAML and the tests can be run in a single command line, easy and simple. It makes use of what they call EQL, "Event Query Language", which is useful in hunting and detecting sequences of events. A example of EQL is shown in Figure 2.7.

```
process where
    process_name == "svchost.exe" and
            not (command_line == "* -k *" or
            parent_process_name = "services.exe")
```

Figure 2.7: EQL code snippet example

EQL is capable of matching many types of events, even sequences of them in a specific order. Objects such as PIDs, parent processes, subprocesses can all be searched and traced back with EQL. This is useful to gather an initial set of suspicious activity and reduce it to a manageable data set.

EQL can only be used in local systems, so after a potential attacker already managed to gain a foothold on the system. It does not protect or counteract, as it can only be used almost as a local IDS. It seems closer to a tool for incident responding and digital forensics than a red teaming one, but it is still interesting to research how the blue side of things is evolving.

Moving on to other studies, the following two focus on automating the red teaming process and turning it into an algorithmic system, which is something that does not seem viable when humans, emotions and feelings are involved. Adding to this, as it has been mentioned before not only by the author of this dissertation but cited from other articles and studies, the limits of an attacker are set by his or her imagination and creativity. The concepts are not poorly thought out, but technology has just not evolved enough to develop such systems.

An interesting article [37] explains the concept of "Computational Red Teaming" or CRT. It analyzes "Building Information Models" (BIMs) and assesses security from there. BIMs are converted to a node graph. Each node represents a building which is connected to neighbor zones (other nodes). Each node has some security parameters such as time to set up an explosive or the location of blue agents (security guards, for example).

The red team will now attempt to penetrate each zone in the facility with several different methods/paths while calculating the fastest time to do so. If they are successful, a report is submitted to the blue team, which attempts to implement the required defenses to prevent a similar attack. The cycle is repeated until no more defenses are required or all the resources are exhausted. Some parameters for the red team can be configured, such as the tools they use. These can be set to anything from a rock to an electric drill or even explosives.

Another project presented in [38] attempts to create an automated model for red teams. After going through the article several times, it appears the authors refer to penetration testing as red teaming, which is not very accurate. Pentesting is a portion of red teaming, but the terms are not interchangeable.

The process starts by developing a threat model - a data flow diagram of an application, enumerating vulnerabilities and ranking them with a realistic and consistent method. Finally, there should be a process for threats to be eliminated or mitigated.

Another concept explained by the authors in the article is "Attack trees". Roots are the goals of an attacker, while leaf nodes represent different methodologies to achieve that goal. Nodes can be considered OR-nodes or AND-nodes. OR-nodes can occur if any of its children occur, while AND-nodes occur only if all of its children also occur.

Threat modeling and attack trees will be useful to aid through the process. The next step is to design use cases for individual attacks, while enumerating specific tools, info, hardware etc. that the attacker would need. This goes in an XML file, in a format similar to what is shown in Figure 2.8.

```
<KNOWLEDGE>
    <PROGRAMMING>
        <LANGUAGE NAME="HTML">
            <CONCEPT> TAGS </CONCEPT>
        </LANGUAGE>
```

Figure 2.8: Automated attack model for red teams - Example of XML file for enumeration

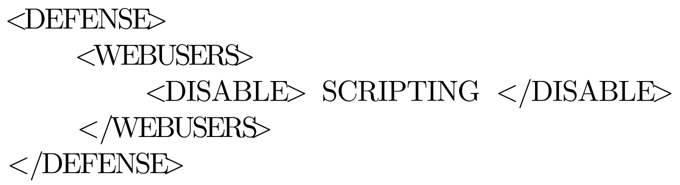
Regarding the use cases, pseudocode can be used to describe an attacker's steps, decisions and thinking. UML-based charts help. The train of thought can also be described in an XML file with custom tags.

```
<AND>
    CONSTRUCT A URL CONTAINING MALICIOUS CODE
    <AND>
        POST A MESSAGE EMBEDDING THE CRAFTED URL IN A DISCUSSION
FORUM TO MAKE THE VICTIM READ THE MESSAGE AND FOLLOW THE URL
    <OR>
        E–MAIL THE CRAFTED URL PERSUADING THE VICTIM TO FOLLOW THE
MALICIOUS LINK
    </OR>
    </AND>
</AND>
```

Figure 2.9: Train of thought described in XML

Regarding the defenses, another XML is required to define them. At the moment, this does not automate attacks but the authors claim it might be possible in the near future since models such as these facilitate planning.

Automated red teaming seems very far from the current reality, even if talking about penetration testing only. There are numerous automated scanners which result in a ton of false positives, and that is a problem by itself. In the case of red teaming, if physical security, humans, emotions, psychology, feelings and physical spaces are added into the equation, the concept seems far too utopian. One sentence from this article about automated red teaming that really stood out was the caption of one of its images - "Pseudocode describing the



```
<DEFENSE>
    <WEBUSERS>
        <DISABLE> SCRIPTING </DISABLE>
    </WEBUSERS>
</DEFENSE>
```

Figure 2.10: Possible defenses in XML

attacker's steps and decisions in a XSS attack". Decision making is an entire field of study by itself and it is heavily studied in economics, business, psychology and even sports. It cannot be described in a few lines of pseudocode.

Although the efforts to go beyond the state of the art are appreciated and are definitely pushing the limits for offensive information security, it is still not viable enough for its use to be considered in the real world.

Chapter Three

Legal and Technical Preparation

Initially, the idea of performing a red team assessment to the University of Aveiro as a dissertation seemed perfect: it is directly related to the cybersecurity Master's degree; it is purely based on offensive security, which besides being a personal interest, is a branch of cybersecurity that is not usually explored as much in academic contexts; and finally, if everything went according to the plan, the results would be tangible and very useful for the University.

But as I started discussing my dissertation with teachers and supervisors, the path to materializing the initial plan became exponentially longer and perhaps even impossible due to legal and privacy-related matters. Several meetings were held: at least one dissertation supervisor was present in each of them, as well as myself, as expected. The University's Data Protection Officer (DPO) also attended some of these gatherings.

3.1 Permissions for a red team assessment

The first few meetings involved discussing general details such as the need for a "get out of jail free" card, how some tools like pen drives or fake access points would be useful, the number of departments that could collaborate, etc. Some more specific ideas were also brainstormed. For example, how building blueprints are hung on most departments walls, the possibility of exploring the android application, as well as other technical procedures.

Even before presenting the plan to the University's DPO, some conclusions were drawn: a lot of data would probably have to be censored in the final document; credentials and other sensitive data could not be used or stored (if a phishing experiment would be performed, it could only be noted that an employee fell for the attack, but not their credentials); in case any type of data needed to be stored, and encrypted machine in the University's network would have to be used.

Finally, we agreed that I, as student, would have to list all the activities that could potentially be performed and send them to the DPO and the Ethics and Deontology Council (CED). The list would have to be split in technical activities and SE activities.

3.1.1 List of Red Team activities

The first document sent to the CED and the DPO was loosely divided in 3 sections: SE activities, exploitation of technical vulnerabilities and some other important notes.

Not all activities will be listed here, but enough of them to understand how difficult a red team test would be with the conditions established by the University rules.

Social Engineering Activities

- Deceive employees (in person, by email or by phone)
- Enter rooms where students do not have permission to
- Impersonate employees or external entities
- Phishing
- "Steal" and use useful items to the red team, such as keys, cards, ...
- Collect personal data such as names, passwords, IDs, emails and phone numbers (which might be useful, for example, when impersonating someone)

Exploitation of technical vulnerabilities

- Insert pen drives or run commands on the University's computers
- Evil twin Wi-Fi attacks
- Accessing unauthorized files on a given computer, or in others connected to the University's network (not a "single activity" *per se*, but something that might happen as a consequence of other attacks)

These lists are certainly not exhaustive, as the goal of section 3.1 is to demonstrate, in a general manner, the process that the student and the personnel involved had to go through before reaching an agreement. The original lists were vastly larger, but it is not necessary to present the entire list here since it ended up not being approved.

3.1.2 University's Review

A few months later, the University reviewed the document and commented on some of the activities, namely to impose heavy restrictions and limitations. Once again, the following table is not exhaustive and only shows the reviews of the activities mentioned in the previous subsection.

The first column lists the activities (same as above), the second column shows the limitations or notes given by the University, while the third and final column materializes some thoughts and reactions I had to the reviews. The first half shows SE activities, while the bottom half of the table is for technical activities.

For each activity, each review sounded extremely similar. The red team could write down that they could do it, but never actually do the activity. This completely destroyed the entire purpose of a red team assessment. The vulnerabilities could never be exploited or escalated.

If I had proceeded with these restrictions, all these tests would appear to be more of a "physical security vulnerability analysis" than a red team assessment, as they could not be chained. For example, It could be useful to phish an employee in order to gain access to some type of room security code. With these restriction, I could only note that an employee fell for a phishing attack, but I would not even be allowed to look at the credentials

Activity	University's review	Personal thoughts and reactions
Deceive employees	OK as long as no collected information is stored, only note that you could obtain it	What is the point of deceiving someone just to say that I could deceive them? The goal is to escalate to other things such as unauthorized accesses or obtaining credentials
Enter rooms which students do not have permission to	Note that you could enter, but do not do it	In other words, I can not do it
Impersonate employees or external entities	OK as long as you only note you were able to impersonate someone	Why would I do it if I cannot get any additional information from the act?
Phishing	Note that an employee fell for the phishing attack, but do not escalate to anything else	The entire point of a phishing attack is to steal credentials
"Steal" and use useful items to the red team, such as keys, cards, ...	Simulate that you could, but do not actually do it	Same as in the second row. Basically, no permission
Collect personal data such as names, passwords, IDs, emails and phone numbers	OK, note that you could collect it, do not store it	Why collect the information if I cannot use it?
Insert pen drives or run commands on the University's computers	As long as the owner of the computer is present	If someone is watching, they would probably not allow me to use their computer
Evil twin Wi-Fi attacks	OK	Surprised I had no notes here. Perhaps I forgot to mention that the goal would be to steal Single Sign-On (SSO) credentials
Accessing unauthorized files in a given computer, or in others connected to the University's network	Mention only that you could obtain access to files, but do not copy or open them	Pointless, similar to the other activities

Table 3.1: Table summary of potential red team activities

3.1.3 Exploring alternatives

Initially after receiving the University's notes, I found myself in denial. It was risky to bet the initial idea would completely go through, but at this point in time, halfway through the second semester, I did not have time to start a new dissertation.

My first alternative consisted in doing a series of tests that would align with the imposed restrictions. For example:

- Try to deceive employees, but as soon as it seems as I will be successful, stop the test
- Attempt to phish several employees but only note how many fell for the attack
- Note how it would be possible to steal some items, for example, if an employee leaves a key unsupervised

This idea was quickly crossed off, as a tiny mistake could easily lead to legal troubles. Also, a big variable would be the reactions of the "victims". Although the point of these tests would be to strengthen the University's security, it is impossible to tell how a given employee was going to react to being lied to, even if the end goal was good willed.

Unfortunately, everyone involved agreed that it would be very hard or perhaps even impossible to conduct any red team activities for a student's dissertation. The teachers were very understandable with the situation and agreed that I should not abandon the good dissertation I had so far, but instead opt for an alternative: I would go as far as possible with a red team assessment to the point of planning the activities with as much detail as I can, but without ever actually performing them.

I agreed, but before elaborating on this, I wondered why are not organizations ready for this? Perhaps the fact that I am a student and not a professional had some impact, but I am positive that most companies never heard about this kind of assessment. Everyone suddenly cares about security when an attack actually happens. "Preventing" is not always the first thought in enterprises, companies think attacks will not happen and security is a waste of money. This led me to research about white hat hacking and its legal components, specifically in Portugal.

3.2 White Hat Hacking (in Portugal)

White hat hacking has been discussed here before, when security professionals such as penetration testers or red team members were also mentioned. Pentesting appears to be a slightly easier topic when it comes to legal matters, as the goal is to find vulnerabilities and not exploit them. So, if a given vulnerability would give access to tons of personal data, the security professional could just report it without actually exploiting it. But it all depends on contracts, non-disclosure agreements (NDA), etc.

For a red team, things might get a bit more complicated. Stealing items? Lying to employees? Impersonating somebody else? And the victims are not aware of all of this, unlike in a pentest. Portugal is a bit behind when it comes to this type of security, so information or even laws about red teaming specific to the country will be very hard to find, if not impossible.

Some articles and laws were collected and reviewed, although not directly related to red teaming, some of them mention penetration testing, white hat hacking or something that sounds similar. A few of them are just opinions from knowledgeable Portuguese authors in the information security niche, but they serve their purpose and it is possible to draw a picture of the governments views on white hat hacking.

The first article analyzed was about "Técnico's Security Team" (STT) [39], a group of university students that enjoyed learning about security during their free time. The mindset of the interviewees is great, but they never mention legal matters. The group leader, Pedro Adão, claims that "knowing how to attack is essential in order to understand how to defend". He also used a quite clever metaphor when asked if he was afraid the members would do something unethical: there is a very popular locksmith in Lisbon that knows how to pick door locks, but he does not wander around town stealing from everybody's homes.

By the end of the article, something interesting is mentioned. Some students found vulnerabilities in government websites and sent several emails reporting them. The replies were not very pleasant. A few months later, they decided to publicly publish the vulnerabilities. Following up on this story, the students state that ethics are very important in this field and every white hat hacker respects them, but they never mention the law or any legal restrictions.

The second article [40] did not mention white hat hacking directly, but there was an indirect reference to Portuguese laws. When talking about Rui Pinto, a Portuguese activist known for the creation of Football Leaks [41], the author says he attempted "to benefit from the status of whistleblower or cooperator, apparently unknown to our criminal proceedings, but present in other jurisdictions".

This is the only reference to legal matters, but there is also an interesting perspective described in the article. A bigger problem than whistleblowers is the integrity of the data revealed by them. Files can be edited to align with the whistleblower's intentions. The legality of whistelblowing itself is not discussed in depth, instead the article focuses on how so many people encourage the act (while resorting to illegal hacking techniques) without understanding that data can actually be altered and modified.

"Portugal em guerra digital" [42], which literally translates to "Portugal at digital war", was an article written by someone which frequently writes about cybersecurity topics and is also involved in the field professionally. Maintaining the pattern from previous articles, laws were not mentioned. But there were some suggestions given on how to improve Portugal's information security policies.

He starts by pointing out that Portugal's software supply chain must be improved and government systems should have minimum security requirements. The "Centro Nacional de Segurança" (National Security Center) should also perform surprise audits on national companies with large revenues.

Adding to this, national organizations with revenue above a certain threshold must perform yearly penetration tests. He also recommends that the government launches a bug bounty program for their websites, as well as public companies'. Although I personally do not see the government doing any of this any time soon, this line of thought is great and aligns with what this dissertation is trying to achieve: to get inside the mind of the threat actors.

Collecting these articles and trying to find news and stories about Portugal's legal position on white hat hacking already gives away that the country simply does not care about ethical hacking, for that reason I decided to look directly at the laws [43], [44] and perhaps draw some conclusions.

The Portuguese Law nº 109/2009, from 15th September is commonly known in Portugal as "The cybercrime law". Articles 3rd, 6th and 7th from Chapter II were the most interesting for the purpose of this dissertation.

Article 3rd is not related to white hat hacking but there are some very curious statements, such as "(...) who, with the intentions of deceiving legal decisions, (...) (modifies data) (...), with the intention that these are considered or used for legally relevant purposes, is punished (...)".

The statement is obviously not original and was translated, but the phrasing does not seem the most correct even in its original language. Perhaps because it is a very recent law. For example, can someone modify data if they are not deceiving any legal decisions? What if someone modifies data with other intentions other than to use them in legal contexts, and afterwards they are taken to court and use the tampered data as evidence for something? Their initial intentions were not to use the modified data for legal purposes, for that reason they cannot be punished according to this article. This is all not very clear, and laws should not be subjective.

Article 6th is about illegal access to data, and probably pertains to white hat hackers. The first statement is very clear and there is no room for interpretations: "Who, without legal permission or without authorization from the system owner, in any way accesses a computer system, is punished (...)". According to this, maybe a white hat hacker can find the vulnerabilities as long as they do not exploit them or access any private data. But "computer system" (sistema informático) is not defined anywhere in the article.

It is also mentioned that the selling or distribution of computer malware is not authorized and can be punished (paraphrased). The punishments vary according to how and why the information was obtained.

The last relevant article of the cyber crime law is article 7th, regarding illegal interception. It is a very simple and concise statement. Once again paraphrasing, the law simply says no one can intercept computer data transmissions happening inside a computer system (incoming or outgoing are also included) without permission from the owner. This means that, for example, running Wireshark in the mall's public Wi-Fi without authorization can put someone in jail for up to 3 years.

Hackers love to bend the rules. Black hat hackers will not care at all about legal matters, but gray hats sometimes favor from different interpretations of the law. Meanwhile, white hat hackers should be at least somewhat aware of these, even more so if they work on their own or without authorization (which we now know it might not be legal, but sometimes companies will welcome bug reports). If the hacker is protected by a legal contract, things are quite different.

With laws, bureaucracies and preparations out of the way, it is time to focus on the second half of this dissertation, which should be more "hands-on" and less theoretical. But first, I shall expand on the alternative I took due to the permissions problem with the red team assessment.

3.3 The alternative

For this academic white paper, laws will not be a problem, at least for the most part. The plan is to follow the planning phases of the TIBER-EU framework as closely as possible without ever engaging in any kind of practical assessment.

Technical exploitation is still fair game, as long as I let someone in charge of the system know I will be doing a variation of a penetration test. This is useful if, for instance, some data regarding members of the University can be accessible through some type of vulnerability. To materialize this plan, it is only required that I state the vulnerability exists, but I should still never access any data.

Other forms of information gathering are also valid. OSINT will always be legal since the information is, as its name states, "Open-source". Gathering information in person can also be done, as long as no rule is broken. In other words, I will be looking around, in places I am allowed to go and without even coming close to breaking any rule, for information that could potentially be used by an attacker.

Another important change is that the planning will only be done for one department, since they would all be extremely similar. The major differences would be noticed during the actual execution of the assessment. With this alternative, there is no point in creating different plans. Perhaps the plan for the Department of Electronics, Telecommunications and Informatics (DETI) would be slightly different, due to having servers and other computational systems hosted inside, but other than that, the variations would be minimal.

This alternative approach also comes with some advantages, such as less planning restrictions or higher levels of autonomy. The plan will be approached exactly like a professional red team assessment, so I will not worry about restrictions of any kind (the law still applies, as discussed before).

The higher autonomy for me comes from the fact that I will not be depending on entities besides myself to write the dissertation, for the most part. No authorizations are needed from departments, I will not have to schedule the assessments with them (maybe the departments would have required this), no waiting for replies from University's personnel, etc.

Although I was somewhat aware of the difficulties my dissertation would pose, my personal thoughts range from "disappointed that the initial plan was not possible" to "extremely thrilled to start planning a red team assessment with barely no restrictions". All in all, while the outcome was not perfect, it was still quite good.

Chapter Four

Planning a red team assessment according to the TIBER-EU framework

During this chapter, the actual planning of the red team assessment will be done. The structure will closely follow the TIBER-EU framework but, naturally, some steps will have to be adapted or perhaps even skipped entirely due to the nature of this dissertation. For instance, subsection 4.3.2 (red teaming) inside the Testing phase (4.3) will likely be quite short.

Some phases require an entire report just by themselves, so those will probably be shorter than in a real red team assessment. Note that even the planning of this type of test can take more than just a few days or weeks.

The target department will be the DETI. With this being said, the first step of TIBER-EU is the Generic Threat Landscape. Before proceeding, it should be kept in mind that TIBER-EU is designed towards the financial sector but still adapted to other sectors in the professional world. That is exactly what will be done in the following sections and subsections, the framework's structure will be adapted to the academic sector.

4.1 Generic Threat Landscape

Creating a Generic Threat Landscape is marked as "optional" in the official TIBER-EU guidelines. Adding to this, a GTL report is maintained for each national implementation. For example, if there was a TIBER-PT framework, a single GTL report would be used as reference for each red team assessment in Portugal, in a give sector. Even though this is typically of the responsibility of national authorities, it is still possible to do our own assessment of a generic national threat landscape.

There are three main steps to take when developing a GTL report. The first is outlining the entities involved and their respective specific roles in the sector. The second step is to identify relevant high end threat actors and their relevant tactics, techniques and procedures used to target the previously enumerated entities.

Finally, the report ends by linking the threat actors and their TTPs to the specific entities initially mentioned. Since the framework allows for this flexibility, in this GTL report the second subsection where high end threat actors are enumerated will already link those to specific targets and TTPs. This will be helpful later when developing attack scenarios.

Entities involved

- DETI (the target)

  The target department should obviously be part of the list of entities involved. Its role in the academic sector is to teach students while providing them with the necessary infrastructures and resources to facilitate their education. Resources range from classrooms to computers and access to the internet. It is also the workplace for professors and other employees with different functions: security guards, janitors, secretaries, etc.

  Besides being a place for education, DETI also hosts some of the university's servers, which makes it especially important from a security point of view. Some of them are critical to the well-functioning of classes and other activities, even outside the department.

- Other departments and university's branches

  Although, other departments are not being targeted by the red team, they are still involved in the sector. Students from other areas of study might take classes about computer science or electrical engineering. Besides, they are dependent on DETI due to university's servers being hosted there.

  For simplicity, other branches of the university are also included here such as the university's social services, administration buildings and even the canteens. There is some innate constant collaboration between all the smaller entities under this bullet point, and that is the reason for them to be grouped.

- Members of the department

  Students, professors and other employees will all be considered members of the department. This group basically includes anyone who attends the building, even students enrolled in other courses other than DETI's.

  Other than classes, students from other departments can enter the department for various reasons, studying during their free time, using the vending machines or even to take part in social events. In general, all departments are accessible to some degree to all students, for that reason they all belong to this group.

Depending on the scope, the list could be a lot more extensive, such as if government branches that focus in education were included. In fact, scholarships in Portugal are paid by the government to students. So it would not be unreasonable to add those branches of the government to this list, if the scope was large enough.

High end threat actors

- Students

  Although it seems a bit conflicting that a student would attack their own institution, it has happened before and it will very likely continue to happen. DETI students in particular might have some technical knowledge to conduct simple or easily automated attacks.

Even recently the university was targeted by a Distributed Denial of Service attack (DDoS). Some claim it was ordered by some DETI students since the dates of the DDoS overlapped with online exams happening in the department. This is just a theory and was never confirmed, the only thing that was certainly known was that the attack originated from a botnet. This made it extremely hard to counter, leaving the university with no internet access for a few days.

Some of the university's intranet pages are known to be vulnerable, for example, to cross-site scripting. There have been no known attacks, but it is still a possibility. Perhaps students do not have the technical requirements to be able to conduct an attack like this. Or maybe the fact that they would be required to log in to attack the intranet pages is enough to repel them (no anonymity for the attacker).

- Hacker groups

  At the time of this writing, in recent months there have been numerous hacker groups successfully targeting several companies and even hospitals in Portugal. Their TTPs and motivations were the same as in the stereotypical hacker group attack: encrypt everything and ask for money to undo the process. In other words, ransomware attacks.

  Every company should be worried about ransomware, as anyone can be a target, from single individuals to large enterprise companies. Ransomware by itself would not be a problem if the initial entry points did not exist, these are usually phishing or some kind of social engineering.

- Non-technical robbers, muggers and burglars

  A red team assessment also considers offline attacks, so the typical mugger or burglar who might resort to knives, guns or other common weapons is also part of the GTL report. And attacks like this have happened in previous years.

  Robbers mostly targeted students. More specifically, DETI students since most of the time they are required to carry their own laptops. Adding to this, by the nature of their interests, these students carry high end technology (better laptops, high end smartphones, expensive audio devices, etc).

In an official TIBER-EU document, the GTL may be validated and reviewed by relevant national entities. If possible, these entities should help update the report on an ongoing basis as new threat actors and TTPs emerge and pose new risks to the sector.

4.2 Preparation phase

The preparation phase is the first mandatory phase of TIBER-EU. A pre-launch meeting would be held with the red team (me, the student), the professors involved with the dissertation and DETI, CED and university representatives. This is the official start of the TIBER-EU testing process for each entity.

The security team of the target would have been mapped, as well as system administrators or people in charge of the security of critical systems. If this meeting would have been conducted, Ricardo Martins, who is in charge of the university's cybersecurity department, would have been part of this map. Coincidentally, he is also helping with this dissertation.

Other details which cannot be emulated without having the actual meeting would have to be discussed. For example, contractual considerations, security protocols, stakeholder roles and responsibilities, etc. Signing an NDA and assuring a free, safe and secure flow of information would have been crucial in this phase, even more so given the relationship between the red team and the target entity (student/university).

4.2.1 TI/RT services procurement (TIRF)

In a real red team test following the TIBER-EU framework, the university would now proceed by ensuring that I had the appropriate standards to conduct the assessment. Since Portugal does not have a national TIBER-EU process, there is also no entity that conducts accreditation processes or certifies red teams to assure they meet the desired standards.

For that reason and according to TIBER-EU, the university could conduct their own procurement process, assuring I was capable of conducting a red team assessment and dealing with confidential and private documents and data.

By the end of this sub-phase: the university's procurement process should be well established; all entities must have agreed to act in compliance with the TIBER-EU framework and respective legal matters; conditions must have been established to manage the confidential sharing and retention of intellectual property rights.

4.2.2 Engagement & scoping

It is time to set the scope of the test, as well as to enumerate the target entity's CFs. Additional non-critical functions can be included in the scope, as long as these do not affect the testing of CFs.

In sum, CFs are the people, processes and technologies that are required to the good functioning of the core service of the entity. In the case of DETI, we can enumerate the following CFs:

- DETI's desktop computers
- DETI's secretary and respective employees
- Internet access
- Professors
- Security guards
- Servers hosted inside DETI's infrastructures

Some of these are self explanatory and do not require further clarification. For example, in the case of the servers, professors or internet access.

The security guards made the list, since the official definition of CFs by TIBER-EU says "the people (...) if disrupted, could have detrimental impact on (...) the entity's safety and soundness".

The secretary and its employees provide stability by performing daily tasks which do not seem very important at first sight. However, the department would likely not function at its best and struggle to deliver core services if this section was disrupted.

Critical Functions	Key systems and services	Flags
DETI's desktop computers	- Power; - Internet access (each student has their desktop synced across all computers, so logging in with different accounts results in different files being displayed); - A valid login account.	- A specific file on someone's desktop.
DETI's secretary and respective employees	- Power; - Internet access; - Physical access to the secretary.	- Items/tokens placed in spaces which only secretary employees have access to.
Internet access	- Power; - Routers, access points and other networking gear; - Clear environment for radio communications (WiFi only, vulnerable to jamming).	- Someone's login credentials, but obtained only through network-related attacks (e.g. evil twin attacks).
Professors	- Their respective offices; - Their IDs; - Laptops, USB devices and other gear potentially used for lectures or academic work.	- A specific file only professors have access to; - Items/tokens inside their offices; - A target professor's ID.
Security guards	- Security cameras; - IDs; - Security guard uniform and tools.	- Items/tokens at security guard's desk; - A target security guard's ID.
Servers hosted inside DETI's infrastructures	- Power; - Potential backup power generators; - Ventilation devices.	- Items/tokens in server rooms; - A specific file in a server's file system.

Note: "Power" refers to electric power/electricity

Table 4.1: CFs, respective key systems/services and potential flags to be captured

DETI's core services would be the well functioning of classes, maintenance of the university's servers and the preservation of a good environment for the students, even if they are not studying or taking classes.

The testing should be performed on DETI's live systems and infrastructures, although testing, backup and pre-production systems might be included in the scope. Personally, I am not aware of how the backups and testing systems are managed, so this could have been a point of discussion in an actual meeting about scoping.

The GTL report can be referred to in order to contextualize a potential business impact analysis, which is also recommended.

Finally, flags to be captured must be defined. This is achieved by first specifying the key systems and services that underpin and support each CF. Flags can be changed on an iterative basis as the red team test evolves. Table 4.1 represents the previously enumerated CFs, some of their respective key systems and services, and finally potential flags that could be set.

To close this phase, flags must be approved by everyone and the scope must be agreed at the board level of the university. In case it is necessary, the business model of the university, its CFs, systems underpinning them and respective purposes should be explained to everyone involved in the red team assessment.

4.3 Testing phase

During this phase of the TIBER-EU framework, one of the key components will be threat intelligence-based scenarios, that is the reason why a GTL report was developed earlier.

4.3.1 Threat intelligence

Another valuable tool related to threat intelligence is the TTI report. A smaller variation of one was written in the previous phase, when research about past threat actors was done as well as some enumeration regarding CFs. However, OSINT on the target entity is still a missing component.

Firstly, the information gathered should mostly be focused on CFs and their underpinning systems, but valuable data regarding the entity in general can also be included. New targets and attack surfaces can be revealed, as it can help the red team provide a deeper and more focused testing.

OSINT

- Android application analysis

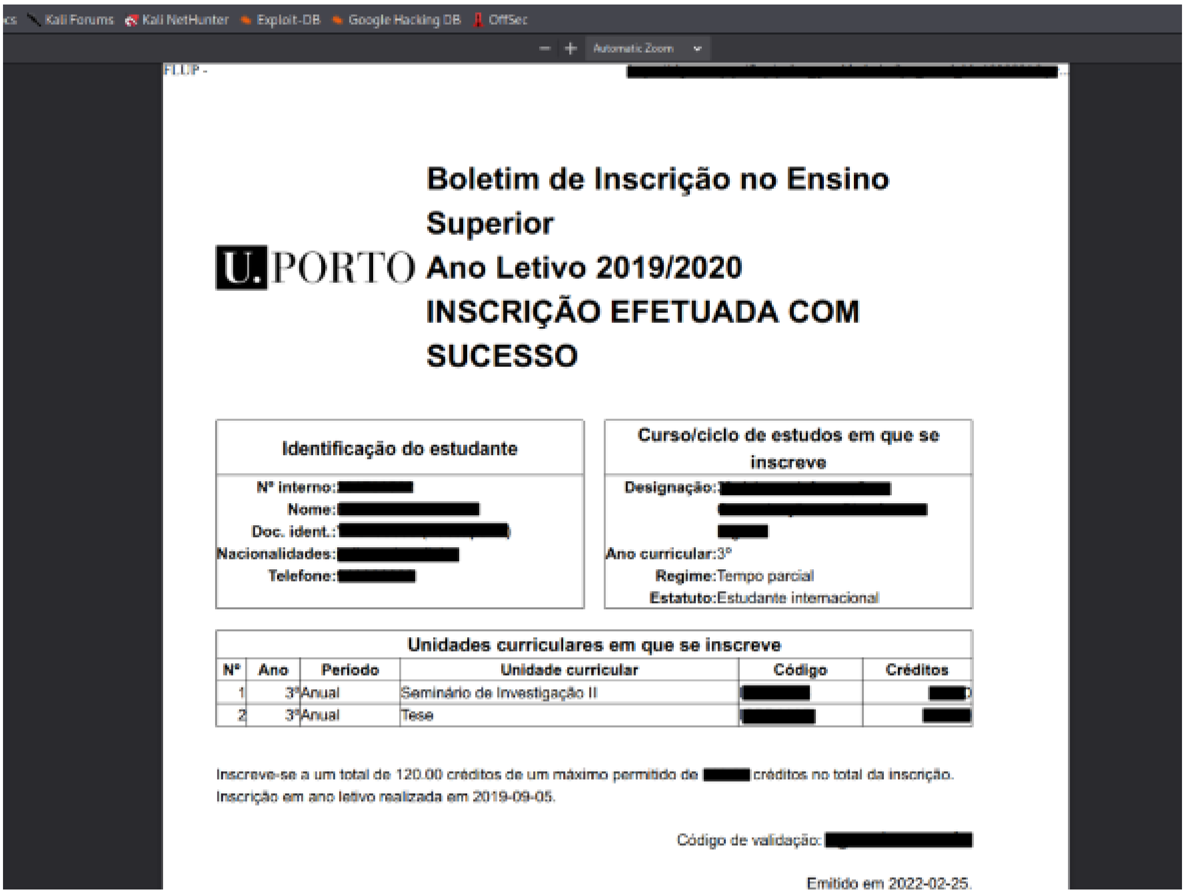
  Luckily, during the first semester of the present year, some cybersecurity master's students did a vulnerability assessment of the UAMobile Android application. This was for the course "Analysis and Exploration of Vulnerabilities", and the following students created the report that was provided to me (respective student number in parentheses): Dinis Cruz (93080), Duarte Mortágua (92963), João Laranjo (91153), José Sousa (93019), Pedro Santos (93221) and Tiago Oliveira (93456), under the guidance of Professor João Paulo Silva Barraca.

  The exact details of each vulnerability will not be discussed in this thesis, only a general overview of each and its respective impact.

  The first vulnerability can be considered a broken access control or perhaps even an insecure direct object reference. By intercepting a request when hitting the "Grades" menu, it is possible to edit a parameter which is associated with a document. This document can be downloaded regardless of user permissions, as long as its identifier is correct. For example, the students were able to access the document shown in figure 4.1.

  Obviously a simple identifier does not allow an attacker to choose which document to access, but through trial and error or brute forcing, various documents can be downloaded without authorization.

  Another similar vulnerability present is the possibility of impersonating another user when sending messages. The concept is really simple. First, by intercepting a request to send a message from user A (attacker) to V (victim), it is possible to find an identifier of V. Afterwards, if A wants to impersonate V to send a message to T (third-party),



FLUP - [redacted]

U.PORTO

Boletim de Inscrição no Ensino Superior
Ano Letivo 2019/2020
INSCRIÇÃO EFETUADA COM SUCESSO

Identificação do estudante

Nº interno: [redacted]
Nome: [redacted]
Doc. ident.: [redacted]
Nacionalidades: [redacted]
Telefone: [redacted]

Curso/ciclo de estudos em que se inscreve

Designação: [redacted]
Ano curricular: 3º
Regime: Tempo parcial
Estatuto: Estudante internacional

Unidades curriculares em que se inscreve

Nº	Ano	Periodo	Unidade curricular	Código	Créditos
1	3º	Anual	Seminário de Investigação II	[redacted]	[redacted]
2	3º	Anual	Tese	[redacted]	[redacted]

Inscreve-se a um total de 120.00 créditos de um máximo permitido de [redacted] créditos no total da inscrição.
Inscrição em ano letivo realizada em 2019-09-05.

Código de validação: [redacted]

Emitido em 2022-02-25.

Figure 4.1: Document downloaded by exploiting a vulnerability in the Android application

then all there is left to do is intercept a request of a legitimate message from A to T and tamper the sender identifier: switch A's with V's.

One more very serious vulnerability is the improper authentication when accessing conversations. With a very similar method to the previously explained vulnerabilities (tampering IDs), it is possible to read chat conversations between any two arbitrary users.

And with almost the exact same technique, it is possible to access details of courses which a user does not have access to. The concept is similar to the previous vulnerabilities, solely by changing an identifier parameter for the course, any course can be accessed.

Lastly, and perhaps this is considered a feature, blueprints for buildings are freely available in the application. This can be useful for an attacker in order to plan attacks or break-ins. Figure 4.2 shows a screenshot of what is being mentioned. This was not included in the vulnerability assessment report of the first year students.

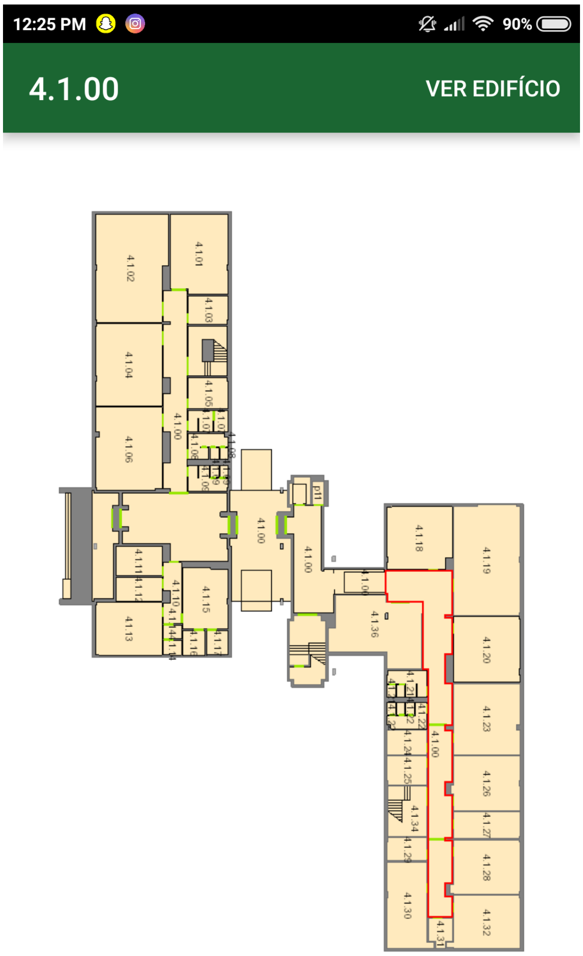


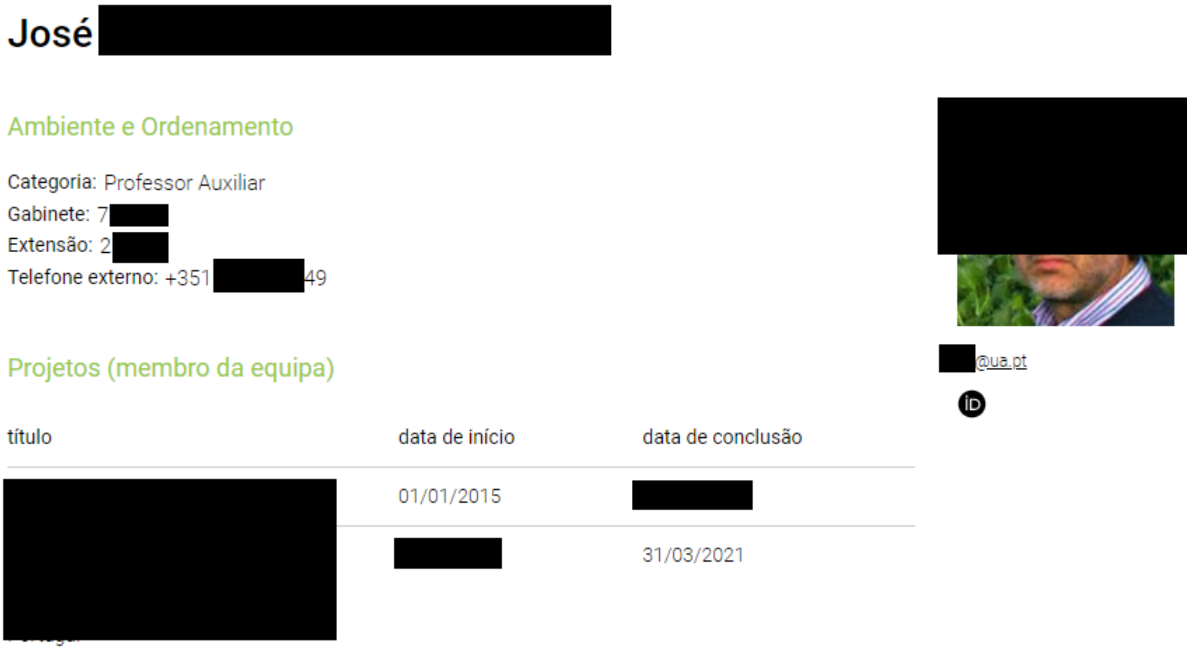
Figure 4.2: Screenshot of a building blueprint in the Android application

- Web OSINT

  Up until recently, it was possible to see the exact schedule of a student just through his or her student number. PACO, the university's online portal, could be used to check a student's own schedule through the link `https://paco.ua.pt/secvirtual/horarios/desenho_horario.asp?tipo=101&value=STUDENT_NUMBER`. Note that the student number could be altered to any number. For example, I recall that groups of friends would use this vulnerability by switching the value of the parameter from their own number to a friends' number in order to find a good time to meet each other outside classes. Obviously, it is harmless in this context, but an attacker could plan attacks around people's schedules. In the end, the university did a good job to fix this vulnerability, as this no longer works.

  I do not consider the following points vulnerabilities per se, since they can be considered extremely valuable for the students. But a lot of information about classes, professors and even students are available online. For example, a professor's page shows his email, phone number, office number and a list of projects.

The link under the picture redirects to some sort of portfolio website, which lists activities, qualifications, etc. of the professor. This can be seen in figure 4.3. Even though his details are censured, this information is widely available, so anyone with a bit of dedication can find out who is the exact person shown below. The person in question was chosen at random.



José [redacted]

Ambiente e Ordenamento

Categoria: Professor Auxiliar
Gabinete: 7[redacted]
Extensão: 2[redacted]
Telefone externo: +351 [redacted]49

[redacted]

[redacted]@ua.pt

Projetos (membro da equipa)

título	data de início	data de conclusão
[redacted]	01/01/2015	[redacted]
	[redacted]	31/03/2021

Figure 4.3: Screenshot of UA's website showing details of a professor

- Field work

  A few minutes were taken to explore the department and find some vulnerabilities in the physical space. First, and even though this is probably intentional, the blueprints are hung in the departments walls, as seen in figures 4.4 and 4.5.

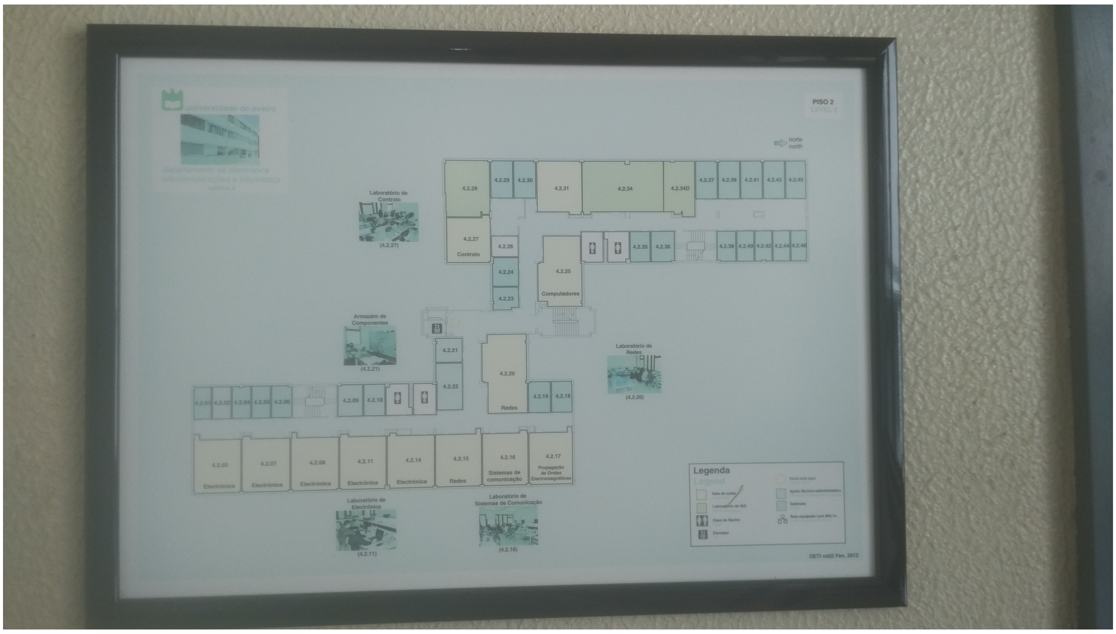


Figure 4.4: Blueprint inside the department

An electrical control cabinet was found open, as seen in figure 4.6.

There is a small space reserved for the professor's mailboxes. The space to insert documents or any other items meant for the teachers is relatively large, which allows for the insertion of things like hooks to remove documents in the inside or even cameras to peek in. The mailboxes are shown in figure 4.7.

A room with the label "Warehouse" was seen with the door completely wide open. I did not enter the room, but it appears some kind of machinery was being stored inside. The purpose of this warehouse is not certain, nor if it is supposed to be open. This can be seen in figure 4.8. The picture's contrast and brightness were edited due to bad lighting.

Finally, and what appears to be the most interesting, the departments secretary has a window to the outside. If we look through the window, a computer monitor can be seen with several sticky notes attached to it. I did not put much effort into reading what was written in those, but this is definitely not a good practice. Figure 4.9 shows the entrance of the department and the window in question. For privacy reasons, I did not attempt to photograph the sticky notes.

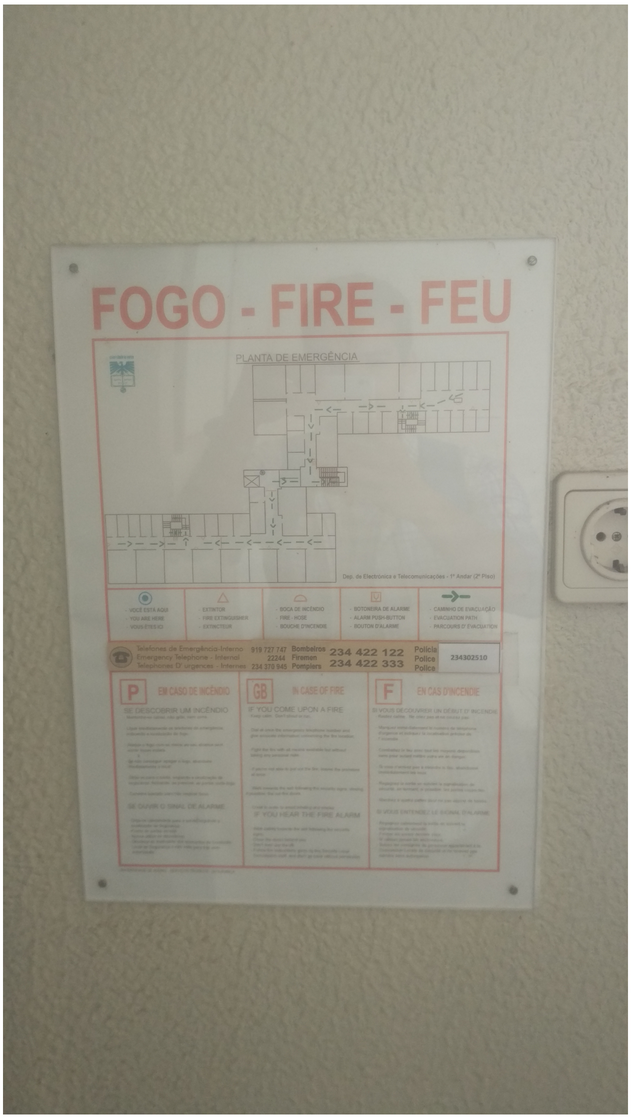


Figure 4.5: Another blueprint inside the department

Figure 4.6: Open electrical control panel

Figure 4.7: Professor mailboxes

Figure 4.8: Open warehouse

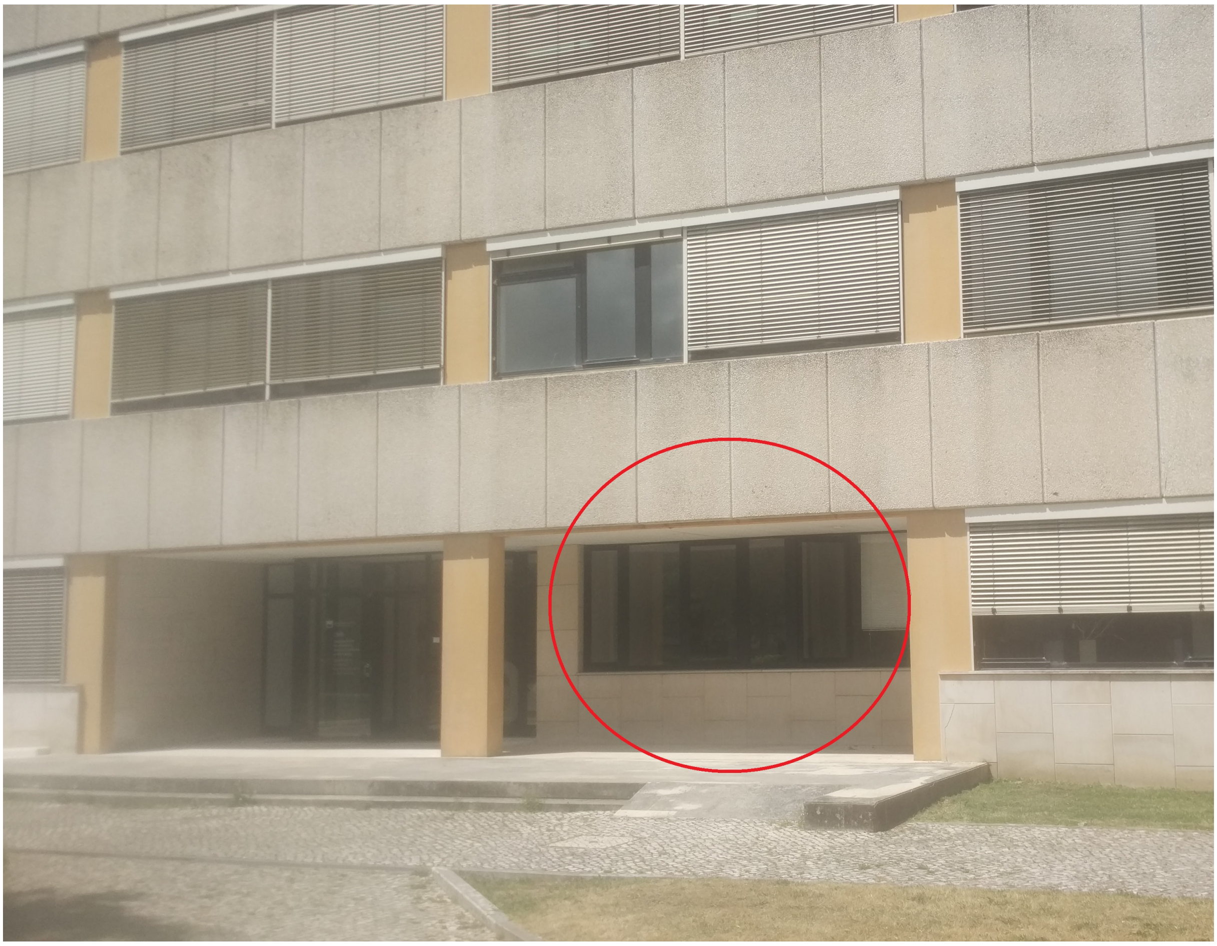


Figure 4.9: DETI's entrance

Attack Scenarios

This list is not exhaustive and these are only a couple of possible attack scenarios after a brief brainstorming session. In a true TIBER-EU assessment, this report must be noticeably more thorough.

The following attack scenarios are based on the previous threat intelligence research performed. And to reiterate, the possibility of attack scenarios are only limited by imagination, so these are only a few examples.

- Android app impersonation

  Given the vulnerabilities mentioned above in the android application, it is possible to impersonate someone when sending a message. An attacker can also check course details without permission.

  Chaining these two vulnerabilities, an attacker could send messages as a professor and seem credible due to the fact that they are aware of the specifics of the course. Let us assume a student would like to cause some kind of "physical denial of service" attack. Perhaps to postpone an exam that the students were not prepared for. The attacker could send a message as the professor to all the students claiming the exam was cancelled or postponed.

- Professors' office break in

  I did not figure out if the electrical cabinet was meant to control the given hall, floor or even the entire building. Let us assume it was the least dangerous case and it just controlled the hall.

  An attacker could easily look at the office's labels in that hall and figure out which offices belong to whom. With a bit of trial and error, an attacker could figure out through the android app which courses does a given professor teach, it would probably be possible to figure out the professor's schedule.

  Well, the door locks are not manual (unlocks with ID card), so by turning off all the switches in the electrical board, the locks would probably stop working. If the professor is giving a lecture... His or her office is now wide open.

- Secretary credentials in the post-it

  Depending on the type of information written in the post-it notes in the secretary, different attacks can be conducted. Usually these notes either hold "to-do lists" or login credentials.

  If they have credentials, it is a matter of time until an attacker gets hold of the entire network. The network is running Windows' Active Directory, which, as it has been mentioned in the first few chapters, is fairly easy to exploit from the inside. Even easier if the attacker has access to staff credentials.

- Premature access to exams

The professors have their numbers exposed online. Phone numbers can be spoofed. Mostly during exam preparation classes, the professors, as a joke, tell the students they have the exams right in front of them. And the exams are actually right there, fresh from the printer, in order to help the lecturer conduct the exam preparation class.

Students know the exams recently came from the printer, so maybe it would be possible to spoof the professor's phone number and call the place in the university where they make copies of the exams. "Hello, this is professor X, could you please print an extra copy of the exam I left there recently? Leave it in my mailbox after. Thank you".

Soon, the attacker knows a copy of the exam is in the professor's mailbox. With some creativity, it is possible to fetch things from inside those mailboxes. Nothing too fancy is required, a quick amazon search for "foldable pick up tool" brings up the item shown in figure 4.10.

Figure 4.10: Pick up tool that can be used to steal items from professor's mailboxes

These scenarios loosely represent a draft of the red team's test plan. At this point, stakeholders, the red team and the target entity would hold a threat intelligence workshop. The reports and scenarios would be displayed and any feedback from any entity is welcome. The red team should specifically mention the CFs, flags, start and stop dates and potential "leg-ups".

A "leg-up" happens when the target successfully defends itself from a given attack, so in order to let the red team proceed, they are given access to a system, internal network, etc. so the assessment can continue. This can also be seen as a simulation of an attack starting from an insider.

4.3.2 Red teaming

After all the preparation work, it is time to deploy the red team. The methodology can be flexible, but it is usually a variation of the cyber kill chain. The recommended methodology by the TIBER-EU framework was already described in detail previously, its main phases were reconnaissance, weaponisation, delivery, exploitation, control and movement, and actions on target.

As the red team, I should have a plan to manage possible risks to the university that might arise, such as degradation of services or disclosures of sensitive information. These must be kept to the absolute minimum. Below are some controls or general things to keep in mind in order to minimize risks to the entity.

- Disrupting exams and student work might not be a very good idea. So impersonating a professor to cancel an exam is probably out of question. A good alternative could be to do the same for an extra, non-mandatory class, where less students show up and no new material is lectured. These are often called OTs (Orientação Tutorial) or office hours.

- Turning off the electrical board during work hours would probably disrupt at least one professor. This attack scenario could be attempted during the night, and it makes it even more simple since an attacker does not have to think about the professor's schedule.

- Regarding the credentials in the post-it notes, some common sense is required if privileged access is obtained. Nothing too malicious should be done with inside access, or anything that can disrupt anyone's work in general.

- If an attacker gets access to any type of item from a professor's mailbox, an exam for instance, it should not be shared with anyone outside of the red teaming process, as it would heavily disrupt courses (postponing and creation of a new exam, since the old one was exposed).

- Since a large network is running inside the university, it is likely something vulnerable can be found. A contact to the network engineering team should be kept in order to solve any problems that might arise from the red teaming test.

A red team test plan is the output of the activities conducted in the testing phase: detailed attack scenarios (these should be written from the attacker's point of view) and the risk management controls.

Some information regarding CFs and internal systems might not be openly available, so this could be facilitated by the university. Attackers would probably use illegal or unethical methods to obtain this information anyway, so by asking the university directly it is possible to avoid those actions and create a more realistic environment. This can be seen as a grey box testing approach.

By now, the test would be executed in a stealthy manner. The attack scenarios are not meant to be followed precisely and I, as the red team, could show some creativity and adopt alternative paths to the agreed objectives or flags, as real life attackers would do.

4.4 Closure phase

After the test, the closure phase includes a red team test report, which consists in a summary of how the red team test went, a walkthrough replay of the red team test with the company of the blue team, a 360-degree feedback meeting, a remediation plan and finally the sharing of results.

For obvious reasons, some of these will be skipped during this dissertation. Just for the record, Ricardo Martins, the university's CISO, would be considered the blue team of the university. Other relevant members of IT departments or perhaps system administrators could follow along with the red team replay.

The 360-degree feedback meeting would get everyone involved together once again in order to let everyone express their opinions regarding which activities progressed well, which could have been improved and any other relevant feedback.

4.4.1 Remediation planning

Since in this specific case there was no test or test results, let us assume that the attack scenarios were all successful, therefore, a remediation plan is required for each of them.

- Android app impersonation

  The first scenario is heavily technical and would probably require a major rebuild to the android application, as it is heavily flawed in some areas. A deep penetration test to the app would definitely uncover more security holes that would have to be patched as soon as possible.

  This would be the obvious remediation, but some policies could also stop students from impersonating teachers, such as only using emails to communicate with the students instead of e-learning direct messages. Or even course forum posts, which appear to not allow impersonations. The vulnerability is only related to private messages.

- Professors' office break in

  This scenario is simple to prevent: simply be attentive to locked electrical cabinets and lock those. However, if we assume the door locks would indeed stop working if there is no power (the RFID ones), then it would be a perfectly valid idea to implement a backup generator, battery or any kind of system to keep them running for as long as possible.

- Secretary credentials in the post-it

  Do not stick post-it notes with sensitive information anywhere which is remotely in sight of anyone besides yourself. This is a basic, high-level security policy that everyone should be aware of by now. I believe the university should also implement other security policies and even train its employees and teach them more about security.

  In my honest opinion, the university is not a "high value target" for most attackers, so it has been getting by without any major attacks. But if someone more sophisticated would target the university, I sincerely think that our security would crumble, unfortunately.

- Premature access to exams

  Professor's details are sometimes useful for students, so a balance between security and usability should be achieved. I proposed that professor's emails, phone numbers, etc. should be only available to students, professors and other employees. In other words, a user would have to be logged in in order to find those details.

  Regarding the phone number spoofing... there is not a way to fight back, only by implementing security policies which were mentioned in the above scenario. A good policy would be to only provide information in person or after some type of verification. If attacker A spoofed person's V phone number to call C, a good way to verify the attacker's identity would be to have C call the number back to confirm the identity of the caller. This would result in C actually getting in touch with V. This only works if C initially suspects the caller is not who he claims to be.

  Lastly, the professor's mailboxes should have smaller gaps. An entire book could fit in there, in the "worst" case scenario, a student has to drop an assignment or something similar, and even this is starting to get more and more unlikely with everything being done digitally.

  I would suggest the implementation of small lockers, similar to those seen in high schools. High school students used to leave letters to each other all the time. Larger items would not fit, but if something other than a few sheets of paper have to be delivered, then it is meant to be delivered personally or through a safer medium.

4.4.2 Result sharing

The results of the test must be shared with the university. If everyone agrees to it, other entities can also participate in the sharing of results, even if it was not part of the test initially.

If there are any key findings, threats or vulnerabilities that are relevant to the entire sector, it could be interesting to share results with the TIBER-EU Knowledge Centre. This would not only help the whole sector improve its security but also provide better guidelines for future red team assessments.

Chapter Five

Conclusion

Cybersecurity is becoming more prevalent by the second in today's world. In the last few years, companies have been giving more and more attention to information security, especially during and after the times when the COVID-19 pandemic peaked. Virtually everyone had to stay indoors, so remote work became the norm for most workers. Online shopping was preferred to driving to the supermarket. Nearly everything could be done through the internet as service providers attempted to avoid having their businesses working strictly in person.

This led to an exorbitant increase in new online systems and respective users. More users equals more potential victims for cyber attackers, and new systems being released in a hurry is a good environment for vulnerabilities to arise. Note that this problem was already present, but the pandemic managed to make it more obvious and prevalent, as the number of cyber attacks ramped up with huge momentum throughout the entire world.

With this being said, companies and organizations slowly started being more attentive to their information security, but still not as much as they should. Red teaming is the perfect exercise to evaluate the general security level of an organization, as red teamers dedicate their careers to studying and learning the attackers' tactics, procedures and methodologies.

As someone who aims to make an impact and also think and act in innovative ways, for my dissertation I decided to attempt to perform a red team assessment to the university. Many reasons led me to propose this dissertation: offensive security is my main interest inside cybersecurity; the results could have been tangible and actually very helpful for the university; students, professors and members of the university would have a safer environment to work and/or study.

While everything seemed great on paper, in reality it would be an extremely complex process, which leads me to think that organizations are not ready for this type of assessments. On the other hand, attackers will not ask if an organization is ready for them either. Perhaps being a student and not doing the red team test professionally helped the university intercept the initial plan, but the amount of trouble regarding data protection, data collection, permissions to perform some activities etc. was enormous.

Although the starting goal of the dissertation was not achieved, a good amount of knowledge was collected and obtained about red teams and red teaming, especially during chapter 2, State of the art. Articles, conferences, white papers and the TIBER-EU framework were studied in depth. Even though I, as a student of the offensive security art, was already inside this subject, the analysis of all these sources provided me with an immense amount of different insights and perspectives. This definitely helped me learn even more about hacking, as well as expand my creativity for hacking-related matters, which is one of the most important characteristics of red teamers.

The TIBER-EU framework cannot go unmentioned, as it was the framework used for the planning of the red team assessment. Following its guidelines to write a shorter plan was the alternative given by professors and mentors of my dissertation after being denied the permissions for the true red team test. A small reconnaissance step was performed in person, which was the closest thing to a red team assessment that was allowed. Attack scenarios, remediation plans and other specific TIBER-EU concepts were implemented, which gave birth to a minimalist red team report.

5.1 Future Work

For the future, I would expect organizations, namely the University of Aveiro, to become more open minded regarding information security and/or security in general. Penetration tests, red team tests, risk assessments, etc. should all be performed regularly. Conceivably not by a student, but by professional red teamers and their respective employers.

Regarding this dissertation in specific, the attack scenarios, critical functions, high-end threat actors and all the threat intelligence gathered would be a good starting point for a potential future red team assessment. Particularly the attack scenarios and the field work performed could already be useful to DETI's security team, as some of those flaws were detected by simply walking around the department, not doing anything malicious or illegal.

It was unfortunate that the starting plan could not be completed, a change of dissertation theme was even considered when the permissions for it were denied. However, since the research work performed in the first two chapters was very in depth and well written, the teachers agreed to allow me to finish this dissertation with only the planning of a red team test. In the future, every cybersecurity student and hopefully other members of the university will be hoping to see their institution have their security policies and security controls thoroughly tested.

References

[1] J. P. Eric Smith, "Advanced red teaming: All your badges are belong to us," DEFCON 22, 2014.

[2] S. Mansfield-Devine, "The best form of defence – the benefits of red teaming," *Computer Fraud & Security*, vol. 2018, pp. 8–12, Oct. 2018. DOI: 10.1016/S1361-3723(18)30097-6.

[3] M. Zenko, "Red teaming insights and examples from beyond," DEFCON 27, 2019. [Online]. Available: https://www.social-engineer.org/social-engineering/the-sevillage-wrap-up-from-def-con-27.

[4] J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," *Computers & Security*, vol. 83, pp. 354–366, 2019, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.02.012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740481831174X.

[5] S. Tzu, *Sun Tzu on the Art of war*. Lulu. com, 2009.

[6] N. Machiavelli and T. Butler-Bowdon, *The Prince: The Original Classic*. Capstone, 2010, vol. 5.

[7] D. Romyn and M. Kebbell, "Terrorists' planning of attacks: A simulated 'red-team' investigation into decision-making," *Psychology, Crime & Law*, vol. 20, no. 5, pp. 480–496, 2014. DOI: 10.1080/1068316X.2013.793767. [Online]. Available: https://doi.org/10.1080/1068316X.2013.793767.

[8] J. Firch, *Red team vs blue team: What's the difference?* https://purplesec.us/red-team-vs-blue-team-cyber-security/, Accessed: 20-Dec-2021, 2020.

[9] J. V. DeMarco, "An approach to minimizing legal and reputational risk in red team hacking exercises," *Comput. Law Secur. Rev.*, vol. 34, pp. 908–911, 2018.

[10] T. Dimkov, A. van Cleeff, W. Pieters, and P. Hartel, "Two methodologies for physical penetration testing using social engineering," in *Proceedings of the 26th Annual Computer Security Applications Conference*, ser. ACSAC '10, Austin, Texas, USA: Association for Computing Machinery, 2010, pp. 399–408, ISBN: 9781450301336. DOI: 10.1145/1920261.1920319. [Online]. Available: https://doi.org/10.1145/1920261.1920319.

[11] T. R. Brent White, "Skills for a red teamer," DEFCON 25, 2017.

[12] B. Scott, "Red teaming financial crime risks in the banking sector," *Journal of Financial Crime*, vol. ahead-of-print, Sep. 2020. DOI: 10.1108/JFC-06-2020-0118.

[13] J. Junior, W. Giozza, R. Albuquerque, G. Amvame-Nze, E. Canedo, and D. Da Silva Filho, "Competências para os cyber red teams no contexto militar," *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, vol. 02/2020, p. 612, Mar. 2020.

[14] I. Kovačević and S. Groš, "Red teams - pentesters, apts, or neither," in *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, 2020, pp. 1242–1249. DOI: 10.23919/MIPRO48935.2020.9245370.

[15] *Owasp*, https://owasp.org/, Accessed: 5-Jan-2022, 2021.

[16] J. E. Street, "Steal everything, kill everyone, cause total financial ruin!" DEFCON 19, 2010. [Online]. Available: https://defcon.org/html/defcon-19/dc-19-speakers.html#Street.

[17] A. M. Weinberg, "Can technology replace social engineering?" *Bulletin of the Atomic Scientists*, vol. 22, no. 10, pp. 4–8, 1966. DOI: 10.1080/00963402.1966.11454993. [Online]. Available: https://doi.org/10.1080/00963402.1966.11454993.

[18] A. Jain, H. Tailang, H. Goswami, S. Dutta, M. Singh Sankhla, and R. Kumar, "Social engineering: Hacking a human being through technology," *Journal of Computer Engineering (IOSR-JCE)*, vol. 18, pp. 94–100, Oct. 2016. DOI: 10.9790/0661-18050594100.

[19] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. USA: John Wiley & Sons, Inc., 2003, ISBN: 076454280X.

[20] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Computers & Security*, vol. 73, pp. 102–113, 2018, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2017.10.008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817302249.

[21] B. Atkins and W. Huang, "A study of social engineering in online frauds," *Open Journal of Social Sciences*, vol. 01, pp. 23–32, Jan. 2013. DOI: 10.4236/jss.2013.13004.

[22] R. Luo, R. Brody, A. Seazzu, and S. Burd, "Social engineering: The neglected human factor for information security management," *IRMJ*, vol. 24, pp. 1–8, Jul. 2011. DOI: 10.4018/irmj.2011070101.

[23] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society*, vol. 32, no. 3, pp. 183–196, 2010, ISSN: 0160-791X. DOI: https://doi.org/10.1016/j.techsoc.2010.07.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0160791X10000497.

[24] I. S. Winkler and B. Dealy, "Information security technology? don't rely on it. a case study in social engineering," in *5th USENIX UNIX Security Symposium (USENIX Security 95)*, Salt Lake City, UT: USENIX Association, Jun. 1995. [Online]. Available: https://www.usenix.org/conference/5th-usenix-unix-security-symposium/information-security-technology-dont-rely-it-case.

[25] J. J. Meyers, D. L. Hansen, J. S. Giboney, and D. C. Rowe, "Training future cybersecurity professionals in spear phishing using sieve," ser. SIGITE '18, Fort Lauderdale, Florida, USA: Association for Computing Machinery, 2018, pp. 135–140, ISBN: 9781450359542. DOI: 10.1145/3241815.3241871. [Online]. Available: https://doi.org/10.1145/3241815.3241871.

[26] D. Kahneman, *Thinking, fast and slow*. New York, NY US: Farrar, Straus and Giroux, 2011.

[27] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, Oct. 2014. DOI: 10.1016/j.jisa.2014.09.005.

[28] T. Peltier, "Social engineering: Concepts and solutions," *Information Systems Security*, vol. 15, pp. 13–21, Nov. 2006. DOI: 10.1201/1079.07366981/45802.33.8.20060201/91956.1.

[29] S. Applegate, "Social engineering: Hacking the wetware!" *Information Security Journal: A Global Perspective*, vol. 18, pp. 40–46, Feb. 2009. DOI: 10.1080/19393550802623214.

[30] Wikipedia, *Log4shell*, https://en.wikipedia.org/wiki/Log4Shell, Accessed: 10-Jan-2022, 2021.

[31] Observador, *As dúvidas do ataque de hackers que obrigou a impresa a recuar no tempo. o que pode ter sido comprometido?* https://observador.pt/especiais/as-duvidas-do-ataque-de-hackers-que-obrigou-a-impresa-a-recuar-no-tempo-o-que-pode-ter-sido-comprometido/, Accessed: 10-Jan-2022, 2022.

[32] Wikipedia, *Robinhood markets*, https://en.wikipedia.org/wiki/Robinhood_Markets, Accessed: 10-Jan-2022, 2022.

[33] G. Sevilla, *Massive robinhood ransomware attack pulled off via customer support phone call*, https://www.emarketer.com/content/massive-robinhood-ransomware-attack-pulled-off-via-customer-support-phone-call, Accessed: 10-Jan-2022, 2021.

[34] Wikipedia, *Kill chain*, https://en.wikipedia.org/wiki/Kill_chain, Accessed: 10-Jan-2022, 2022.

[35] E. C. Bank, *TIBER-EU Framework*, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf, Accessed: 20-Dec-2021.

[36] R. W. Casey Smith, "Fantastic red-team attacks and how to find them," BLACKHAT USA 2019, 2019. [Online]. Available: https://www.blackhat.com/us-19/briefings/schedule/#fantastic-red-team-attacks-and-how-to-find-them-16540.

[37] T. Tan, S. Porter, T. Tan, and G. West, "Computational red teaming for physical security assessment," in *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent*, 2014, pp. 258–263. DOI: 10.1109/CYBER.2014.6917471.

[38] H. Ray, R. Vemuri, and H. Kantubhukta, "Toward an automated attack model for red teams," *IEEE Security Privacy*, vol. 3, no. 4, pp. 18–25, 2005. DOI: 10.1109/MSP.2005.111.

[39] Observador, *Os piratas informáticos portugueses que nos defendem*, https://observador.pt/especiais/os-piratas-informaticos-portugueses-que-nos-defendem/, Accessed: 17-May-2022, 2017.

[40] ——, *Hacking ao serviço do bem ou destruição da prova?* https://observador.pt/opiniao/hacking-ao-servico-do-bem-ou-destruicao-da-prova/, Accessed: 17-May-2022, 2021.

[41] Wikipedia, *Rui pinto*, https://en.wikipedia.org/wiki/Rui_Pinto, Accessed: 17-May-2022, 2022.

[42] D. Vivo, *Portugal em guerra (digital)*, https://www.dinheirovivo.pt/opiniao/portugal-em-guerra-digital-14587141.html, Accessed: 17-May-2022, 2022.

[43] M. Público, *Legislação cibercrime*, https://cibercrime.ministeriopublico.pt/iframe/legislacao-cibercrime, Accessed: 17-May-2022, 2022.

[44] e-konomista, *Lei do cibercrime em portugal: Factos a reter*, https://www.e-konomista.pt/lei-cibercrime-portugal/, Accessed: 17-May-2022, 2018.