Automated Social Engineering Tools Revisited - An Extended Overview and Comparison with Respect to Capabilities and Detectability

Dominik Dana
St. Pölten UAS
St. Pölten, Austria
email: is191805@fhstp.ac.at

Timea Pahi
St. Pölten UAS
St. Pölten, Austria
email: timea.pahi@fhstp.ac.at

Sebastian Schrittwieser
CD-Labor AsTra, University of Vienna
Vienna, Austria
email: Sebastian.Schrittwieser@univie.ac.at

Simon Tjoa
St. Pölten UAS
St. Pölten, Austria
email: simon.tjoa@fhstp.ac.at

Peter Kieseberg
St. Pölten UAS
St. Pölten, Austria
email: Peter.Kieseberg@fhstp.ac.at

***Abstract*—The manual effort required by social engineers to obtain information about people and organizations that are in their focus can be extremely high in case of targeted attacks. Attackers, therefore, strive to automate processes as much as possible. With a few menu entries and selections, it is already possible to export email addresses from social media profiles, as well as to send friend requests and phishing messages to a large number of people. In this paper, we analyze the most popular frameworks for modeling Social Engineering attacks and generate a simplified and generalized meta-model. Based on this model, it was analyzed which parts of Social Engineering attacks can be automated using state-of-the-art tools that are readily available. The capabilities of these tools were thoroughly evaluated, including ready-to-use system environments. This work is an extended version of our work conducted presented at ICCGI 2024.**

***Keywords*-Automated Social Engineering; Social Engineering Frameworks; Social Engineering Models; Technical Social Engineering.**

I. Introduction

This paper is an extension of our work [1] published in the *Nineteenth International Multi-Conference on Computing in the Global Information Technology ICCGI 2024* and expands the original text. Major new parts, aside modernization and changes throughout the text, include a more conclusive and comprehensive analysis of related attacker models, the inclusion of OSINT (Open Source INTelligence) Link Lists for searching for user data, as well as the discussion of ready-to-use system environments in the reconnaissance phase. Furthermore, key aspects were updated to the current state of the art and the tool selection was expanded.

Social Engineering (SE) is an emerging threat that has evolved along with networking and social media and has attracted increasing attention in recent years. While fraud existed long before, the widespread use of social media and cyberspace provides fertile ground for traditional fraud, as more and more personal information is shared but little awareness and measures are in place to protect it [2]. Especially the widespread and constantly available Social Networking Sites (SNS), are a playground to carry out various forms of phishing attacks [3]. There are advanced phishing attacks that spread through sharing SNS posts that can lead to information leakage [3], but also targeted attacks, where users working for a specific company are identified and contacted through SNSs and their confidential information is stolen, e.g., via direct messages [4]. Last but not least, habituation effects also lead to various links being clicked, posts being copied, liked, shared and pasted, which ultimately promotes Social Engineering [3]. However, Social Engineering requires a great deal of time spent cultivating relationships, building trust, and then exploiting users to obtain classified information [5]. The tools used for this purpose are, in terms of basic information retrieval, mostly located in the Open Source Intelligence (OSINT) area and rely on a large collection of publicly available information on the Internet about people and organizations. From the social engineers' point of view, the attacks need to be automated, in order to reach many victims and they should behave human-like, so that more victims fall for them [6]. Automation is especially interesting in the reconnaissance phase, as e.g., in the context of an initial information gathering phase, known users would have to be searched for manually for hours on various platforms and social media channels. this task can already be performed by proprietary search engines, across hundreds of platforms, with just a few mouse clicks. It is a similar story with creating phishing messages, or phishing sites. Instead of designing websites yourself that are used for water-holing or phishing attacks, or instead of sending out a high number of phishing messages via email yourself, a few menu selections or clicks in the respective tools are enough.

This paper describes current automation possibilities which can be used for Social Engineering. The structure of this paper, after a brief introduction and analysis of related work in Section II, it is divided into three main sections, where relevant legal and ethical aspects for the work are considered (Section III), a comparative analysis of Social Engineering phase models and frameworks (Section IV), and the application of the Social Engineering tools themselves (Section V) is

conducted. Section VI provides a conclusion and suggestions for future work, including answers to these research questions:

- RQ1: To what extent are freely available Social Engineering supporting tools already automated and what does this mean in terms of Social Engineering?
- RQ2: Which phases of Social Engineering can be handled with the tools?
- RQ3: How do the different tools interact with each other, are there tool suites that start and accompany a complete Social Engineering process?
- RQ4: How reliable are the results of the tools?

II. Related Work

In this section, we provide an overview on the most important techniques, tools, advanced attacks, as well as trust factors and alternative frameworks.

A. Techniques and tools

In addition to the literature by Mitnick [2] and Hadnagy [3], publications by Talamantes [6] and Kim [7] were analyzed, in which the first tools from the OSINT domain and the first automated tools, including the Social Engineering Toolkit (SET) and Maltego, were already mentioned. Handnagy additionally describes in [8] the Social Engineering pyramid as another Social Engineering phase model. An important distinction into the attack categories ”Computer Based” and ”Human Based” within Social Engineering, is made by Wang et al. in [9], similarly in Aldawood and Skinner’s work [10]. In their paper, Wang et al. also state that technical attacks are becoming increasingly difficult and therefore Social Engineering attacks are on the rise. Furthermore, they assumed the most important attack media to be e-mail, websites and the telephone. Banire et al. also describe in [11] that these also represent the most common attack methods from which phishing, vishing and smishing attacks result. In [10], it is also concluded that virtual communities, after personal data is often stored in these platforms, are the largest source of Social Engineering attacks, as little technological know-how is needed once trust has been established with the victims (see also the study from Kenya [12]). Other techniques and tools, especially from the OSINT domain and people-search engines, are described in [13]. However, their main area of application extends to the USA, as application within the EU, due to the General Data Protection Regulation (GDPR), is not allowed as the GDPR requires operators of the tools to ask for consent when collecting personal data.

B. Advanced attacks and automation

A definition of automation is simplistically and naively made in [14] as systems that take over the execution of tasks from humans and thereby simply reduce the amount of work, or attention, that humans need to devote to these tasks. Wang et al. state in [15] that the wide adoption and availability of SNSs, the Internet of Things (IoT), industrial Internet, and mobile devices, have created greater attack surfaces for Social Engineering. The reason behind this is that due to huge amounts of data generated by their use and that people in today’s world share more information about their own personal identities, activities, relationships, locations, and personal interests, as well as their work and work environments on social media combined with the availability of Social Engineering tools, facilitates large-scale Social Engineering attacks. Automated tools, mentioned by Wang et al. in [15], in addition to ways to bypass phishing and deep learning detection, include the automated chat bots of Huber (ASE bot) [16], Lauinger et al. (Honeybot) [17], amongst others. According to their own statements, compared to the ASE bot, Honeybot moves one step further, by not having humans communicate directly with a bot, but instead initiating a conversation between two real people, with Honeybot acting as a ”Bot in the Middle”, interposed in between. The behavior of Honeybot by changing, replacing, or deleting parts of messages, is individually controllable and the chance, for example, to click on links, which are inserted, or changed by Honeybot, is greatly increased, compared to other chat bots. The project ”Social Network Automated Phishing with Reconnaissance” (SNAP_R) [18] on the other hand, interacts with users on the Twitter platform and sends a machine-generated tweet to its targets, which mostly contains a shortlink. Broken English and shortlinks are accepted on Twitter due to the character limit, which is why the authors see SNAP_R as an extension to SET to automatically distribute phishing messages to a larger target group. The ASE bot, Honeybot and additionally the Koobface bot, spreading as malware through the Facebook social media platform, are also cited as automated Social Engineering tools in a study by Kaul and Sharma [19].

C. Trust factors as the basis for automation functionality

The trust factors that enable Social Engineering to be successful, are described by Kano and Nakajima after an experiment [20]. The fact that people are more likely to open suspicious links in messages from Facebook friends than from, e.g., their bank is also addressed by Stern at Kaspersky [21]. The latter go on to state that it is also widespread to clone unrestricted Facebook profiles and send friend requests to friends of this original profile. The goal is to use the cloned profile to send convincing phishing messages or to get the Facebook friends to click on phishing links.

D. Alternative Frameworks

In addition to the classical frameworks and Social Engineering models, presented in a subsequent section, models such as the one described by Tong Wu et al. in [4], consisting of Social Engineering Sessions (SES) and Social Engineering Dialogues (SED) and the models in [22], which are still in early stages of development represent alternative approaches for new Social Engineering models.

III. Legal and ethical aspects

When compiling and searching for information in the context of Social Engineering, data and information from and about specific individuals are used. This also holds true for the experiments conducted in this study. While malicious attackers

will not care about legal or ethical issues regarding private data retrieval, this had, of course, been an issue during our research. Data and information that can be traced back to individuals is considered as personal data in the current version of the General Data Protection Regulation (GDPR), under Article 4 [23], the processing of which is considered to be lawful if there is consent for processing for one or more specific purposes and these are processed appropriately for the purpose and in accordance with the principle of data minimization [23] and appropriate protective measures have also been taken by the processor for the required storage period. Even if information about individuals and institutions can be found freely on the Internet, from an ethical point of view, it cannot and should not be assumed that this information is also freely available for use. However, information can also be interpreted differently in the wrong circumstances, leading to unintended and unfavorable outcomes for the individuals concerned. Another dilemma is that the OSINT sample is minimized or selected depending on the needs of the collector [13]. Thus, important sources might indeed be intentionally neglected in order to achieve a particular result. The handling of legal and ethical aspects is quite different in the related work. This ranges from permissions and questionnaires requested in advance, to simply conducting experiments. Debriefing with participants is rarely held. In order not to unknowingly turn participants into experimental subjects, which has already raised serious ethical concerns [24], own outdated and already known leaked data was searched for first tests with the tools. When processing the data and information found, an attempt was made, despite automation, to take into account the principle of data minimization and purpose limitation as far as possible. Attention was paid to emerging and possibly disadvantageous combinations of the results. The search and test results were not saved after the application of the different tools. In some cases, the tools automatically created log files that contained the results of the search queries. These log files were also deleted at the end of the tests.

New regulations will also result in new ethical and legal requirements, especially when dealing with personal information. Regarding the utilization of automation for Social Engineering this is especially important, as SE touches two very important aspects: Privacy, as already outlined in this section, but increasingly also the use of Artificial Intelligence (AI) methods. This is especially important with respect to regulations like the AI Act [25] and the Data Act [26], which are first attempts to regulate the use of information in AI. While these are currently limited to the European Union, these regulations could be exemplary for other legal regimes as well. Of course, real attackers will not care about the legality of their tool utilization, the topic is far more important for white hat social engineers that use the tools for enhancing SE security in companies: Since modern machine learning techniques require training with quite large amounts of high quality data, the question of the availability of legal training data needs to be solved. This also includes issues like membership inference attacks, where attackers can try to infer the existences of certain persons in the training data of a trained model, which could, again, pose a privacy problem. Further challenges result from the lack of explainability of modern Machine Learning (ML) tools [27], i.e., it is currently impossible to explain, why a specific model arrives at a specific solution, even in full knowledge of model, training and processing data. While this is certainly no problem in case of criminal use of the tools, it becomes a problem when white hat social engineers need to be able to fully determine the inner workings of attack tools in order to find countermeasures. In addition, even the white hat use of certain tools could pose potential legal problems, which has to be decided in the near future by the respective courts.

IV. Social Engineering models and frameworks

A standardized formulation of a Social Engineering attack, as well as the sequence and temporal events, allows researchers to compare different Social Engineering attacks with each other. Next, we will compare the following most common phase models and frameworks that divide Social Engineering attacks into phases: The *Cyber Kill Chain (M1)* [28], the *Social Engineering Cycle (M2)* [2], the *Social Engineering Lifecycle (M3)* [29], the *Social Engineering Pyramid (M4)* [8], the *Social Engineering Attack Framework (M5)* [30], the *Cycle of Deception (M6)* [31], the *Social Engineering Attack Spiral (M7)* [32], the *Session and Dialogue Based Framework (M8)* [4], and the *Phase based and Source based Model (M9)* [33].

Following, we give a short overview on the most important models.

A. The Cyber Kill Chain

Originally developed by Lockheed Martin [28], the Cyber Kill Chain is one of the oldest and best known models that saw some extensions and changes since 2011, e.g., by IBM Security [34]. It consists of the following phases:

1) *Reconnaissance*: In the reconnaissance phase, targets (persons, institutions or specific persons in institutions) are selected and as much information as possible is obtained about them. Any information, no matter how small and seemingly unimportant, can be of significance for the further course of the attack.
2) *Weaponization*: In this phase, an attack is prepared based on the information previously obtained. On the one hand, a pretext suitable for the attack target is drafted and on the other hand, usable tools are compiled.
3) *Delivery*: In the delivery phase, the execution of an attack is started. Prepared phishing messages are sent to selected targets, prepared data carriers are deposited or water-holing pages are activated.
4) *Exploitation*: In the exploitation phase, security gaps and vulnerabilities of the attack target are exploited. This is also where vishing calls take place, which can persuade the attack target to co-operate and help.
5) *Installation*: In this phase, malware is installed unnoticed on the devices of the targets. This can happen via the

previously prepared data carriers or via one of the activated water-holing pages.

6) *Command and control*: In this phase of the Cyber Kill Chain, the previously installed malware is used to obtain data, further personal information or access data.
7) *Action on Objectives*: In the final phase of the Cyber Kill Chain, the attacks are concretised, systems are compromised and data and access data obtained are exploited to complete the attack.

A major criticism of the kill chain is its focus on malware, as well as on the pure attacker perspective, a criticism that it shares with many of the other models [35]. Furthermore, it is neither cyclic in nature, nor does it allow for the repetition of intermediate phases in the original version, which makes in rather cumbersome to model realistic targeted attacks with attackers moving inside a system and gradually taking it over. This is especially problematic in the light of Advanced Persistent Threats (APT), where attackers are highly persistent and probe the system in many ways [35]. Due to its acyclic nature. the Cyber Kill Chain focuses on a single intrusion attempts, which does not reflect attacker behavior in the case of APTs. Due to the popularity of the Cyber Kill Chain, several enhancements have been proposed, e.g., by providing a holistic model that also includes legal aspects and policy making [36].

B. Social Engineering Cycle and similar approaches

In contrast, the Social Engineering Cycle by Mitnick and Simon [2] has a non-technical focus, which can be seen in the four phases that, again in contrast to the Cyber Kill Chain, are defined as a cyclic approach: (i) Research, (ii) Developing rapport and trust, (iii) Exploiting trust and (iv) Utilization of information.

An attack begins with the *Research phase*, in which information is gathered and research is carried out on the respective target. This can be done via all possible channels (e.g. public sources, annual reports, marketing documents, newspaper articles, websites, content from social media). With more detailed information and insider information, identities are assumed and references are made to people known to the victim. In the next phase, *relationships and trust are developed*, which are then exploited in the subsequent phase. In the *exploitation of trust* phase, the victim is asked for favours and actions. A special form of "reverse sting" also occurs here, in which the victim asks the attacking side for help. In the final phase, the *information gathered is utilised*. If it turns out in this phase that something is still missing to finally achieve the goal, it is possible to return to an earlier phase of the cycle. This continues until the attacking side has achieved its goal.

When searching for social engineering life cycles or phase models, the *Social Engineering Lifecycle* of the internationally active IT security company Imperva [29] needs to be mentioned. Imperva also uses a 4-phase model to illustrate the life cycle of social engineering attacks, similar to Mitnick's model, but with different phases and names: (i) *Investigation*, where the foundations for an attack are prepared. The victims of the attack are selected, background information about them is gathered, and suitable attack methods are chosen. (ii) *Hook*, where the aim is to deceive the victims of the attack and gain a foothold with them. Contact is made with the target, they are deceived with an invented story and control is taken over interactions. (iii) *Play*, which revolves around information that is retrieved over a certain period of time. The implantation from the previous phase is deepened, attacks are carried out, business processes are disrupted and/or data is siphoned off. Finally, (iv) the *Exit* phase, where the attack is completed, ideally without arousing suspicion. To this end, all traces are covered, malware is removed and the pretext, the story that was invented in the hook phase, is brought to a natural conclusion. This is rather different to the model of Mitnick and Simon which does not explicitly tie up lose ends and go for a safe exit.

The *Social Engineering Pyramide* by Hadnagy [3] is also very similar to the Social Engineering Cycle, with the notable deception that it is linear instead of cyclic. Furthermore, it is the only one of the models analyzed in this work that has an explicit reporting step included, which was especially included by Hadnagy, as he used this approach for penetration tests for customers, thus reporting was of the utmost importance.

Another approach derived from the works of Mitnick and Simon is the *Social Engineering Attack Framework* by Mouton [30], which was explicitly stated to be an extension in order to cover shortcomings in the original cycle. In comparison, the social engineering attack framework generally consists of several more phases and is more detailed, especially at the beginning, as the target of the attack cannot yet be clearly defined at the start and it is not yet clear which target persons could possibly help to achieve the desired goal. For this reason, Mouton et al. introduced an additional "Attack Formulation" phase. Furthermore, the "Information Gathering" phase is more detailed in terms of the evaluation of the information gathered, as this is of great importance for the further course of the attack and the subsequent trust relationships to be established are heavily dependent on the quality of the information obtained from this phase. Another important and additional phase, "Preparation", in which data is prepared and attack vectors are selected, is found before the "Develop Relationship" phase, which is very similar but differs in the entry point. The "Exploitation Relationship" phase is also described in more detail in this framework. Finally, there is the additional debriefing phase in which the target persons are to be put back into a normal emotional state (maintenance process). The idea here is to make the target person feel good so that they do not feel as if they have been attacked, in order to counteract feelings of guilt from (unauthorised) disclosure of information and thus avoid unforeseen consequences. In the transition process within the final phase, a decision is made as to whether the target of the attack has been achieved or whether it is necessary to return to an earlier stage (e.g. to obtain more information). As this approach is far more complex when compared to the others, the original figure from the original paper [30] is provided as Figure 1.

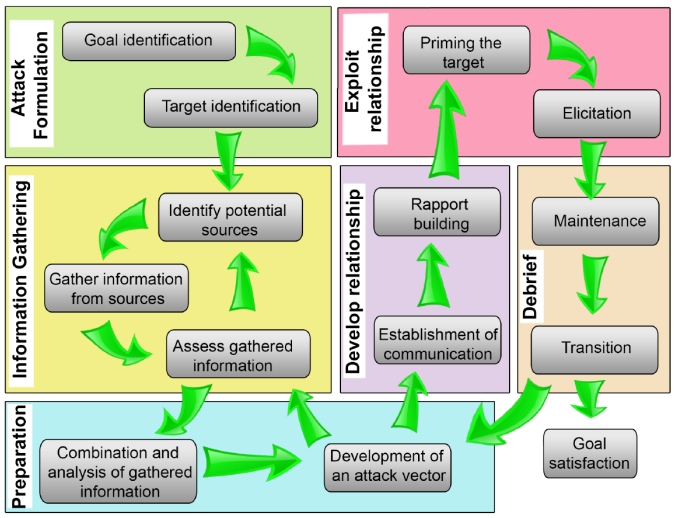

Figure 1. Social Engineering Attack Framework by Mouton et al. [30].

C. Cycle of Deception

The *Cycle of Deception* [31] is a social engineering framework that not only includes the phases from the perspective of the attackers, but also those from the perspective of the attack victims and their defenders. The model was developed because the frameworks available at the time were considered too simple and at the same time too opaque. According to the authors, it is intended, among other things, as an aid for training purposes, but also as a model for a holistic protection strategy against social engineering. The framework is typically depicted in the form of three concentric circular cycles, with the outermost being the *Attack Cycle*, the next the *Defense Cycle* and the innermost the *Victim Cycle*. Each cycle consists of 5 steps that not only work in circular order, but also relate to their counterparts in the other cycles.

a) Attack Cycle: The Attack Cycle is dedicated to the behaviour and actions of the attackers with its included phase: (i) *Goal & Plan* that includes the aim, purpose and justification of the attack, (ii) *Map & Bond*, where attackers use various search techniques to gather information about the attack targets, (iii) *Execute*, where the attackers carry out an unauthorised or punishable act, (iv) *Recruit & Cloak*, which refers to all activities to conceal traces after an attack has taken place and (v) *Evolve/Regress*, where he attackers learn from the process and create an internal justification for what happened.

b) Defense Cycle: In the direction of the center, the attack target, is the next defense cycle, which is dedicated in phases to the options available to the defenders. In some cases, the role of the defenders can be played either by the victims themselves or by IT professionals: (i) *Deter*, providing a deterrent effect through appropriate guidelines and perceptions of good reporting lines in the event of incidents, (ii) *Protect*, providing a small amount of sensitive data, training measures for employees and an appropriate policy provide protection in this phase, (iii) *Detect* describes the detection of attacks by attentive employees or by technical equipment, (iv) *Respond* by creating ways to easily report social engineering attacks or attempts to do so and (v) *Recover* that includes knowledge of the value of your own data, good existing policies and well-documented, reported attacks in order to learn from them.

c) Victim Cycle: The Victim Cycle is placed directly around the attack target and focuses on the behaviour of the individual victims, to whom the authors believe too little attention is paid when analysing attacks: (i) *Advertise*, the victim (knowingly or unknowingly) possesses something of value that makes them a target, (ii) *Socialize & Expose*, where by interacting with the attackers, the victim can be deceived into giving up their valuables or access to them, (iii) *Submit*, the release of e.g., secret information, (iv) *Accept & Ignore*, referring to the behaviour of the victim after an attack has taken place, in that it was accepted, ignored or not noticed at all and (v) *Evolve/Regress*, describing the development of the attack target into the role of the learner, or into the role of the victim.

D. Comparison and Technical Social Engineering model (TSE)

These models differ most clearly in the area of representation. With M1, the M4, M8, and M9 represent in successive process steps, the M2, M3, M5, M6, and M7, respectively, represent in circuits. The fact that the majority of the researched frameworks use a circular structure to describe Social Engineering attacks, which mostly includes the phases of information gathering, trust exploitation, attack development, and target fulfillment, is also already described in [4]. The circular form provides the possibility of representing the repetition of previous phases when more information is needed, or the goal is not achieved in a single phase [2]. M6 does not provide the opportunity to return to a single previous phase, but provides a sequence of several cycles spherically on top of each other, which makes this framework seem to be very complex at first sight, especially in combination with the inclusion of risks as a three-dimensional component. The models and frameworks also differ in terms of the number of phases. Apart from two models, all other models were designed with fewer than eight phases. M1 is only to a limited extent suitable for Social Engineering attacks, since these types of attacks do not necessarily have to pass through all phases of the framework. Also, the complete section, in which relationships and trust are established, as well as exploited, is completely missing. M4 shows five phases and is the only model that includes reporting as the final step, for traceability and documentation of the process and results. The model M3, as well as model M2, are limited to a total of only four phases with similar names. M2 is seen as a good basis in comparison with M5, but too simplistic, according to [30], as it leaves too much room for interpretation and does not include a debriefing phase, which is intended in M5 to bring the target person back to a normal emotional state. No matter how many phases the respective models and frameworks have, a phase for thorough information gathering is required at the beginning of every successful Social Engineering attack, since the quality of the information obtained contributes significantly to the success of the subsequent phases. Based on the compared models and

frameworks, the Technical Social Engineering model (TSE) was designed, shown in Figure 2, which was reduced to only three common phases, within which automation with tool support is possible.

Figure 2. The Technical Social Engineering model (TSE).

A corresponding assignment of the phases of the previously described phase models and frameworks to the phases of the reduced model can be seen in Table I.

V. Tool-supported automation for Social Engineering

While we tackled a lot of different tools during our analysis, we will only be able to give a short outline on the findings in this section, grouping the tools according to the previously defined TSE model.

The tools in the information gathering phase are used to obtain all kinds of information about a (potential) target. Included in this phase are also tools used in reconnaissance and OSINT, as well as Social Media Intelligence (SOCMINT). Still, as this is not an analysis of OSINT tools, we did not further dive into the extreme amount of apps there. We divided the tools into (i) web-based and (ii) locally installed tools.

A. Web based tools for Information Gathering

1) Searching for user data: Google Dorks are pre-defined searches that can be executed using the Google Programmable Search Engine for automation as Custom Search Engines (CSEs). This allows for fine-tuning and exchange of fine-tuned searches, which can be accesses through catalogs. One of the most prominent of these catalogs is the Exploit-DB [37]. At the time of the research, the then current status of the exploit database was 7,341 Google Dorks. Using the Google Programmable Search Engine [38], it is also possible to save search queries online to Custom Search Engines (CSE). These CSEs are also publicly accessible and usable for the general public. A CSE by Brijesh Singh that is specially tailored to social media platforms is available at [39], while Stefanie Proto lists over 130 other available and directly usable CSEs in the compilations [40] and [41] at the time of research.

Another important source for tool gathering are *OSINT link lists*. During the research on automated social engineering tools, links to lists with hundreds of links to web applications were often provided in relevant forums, which are suitable for OSINT purposes, but which can also support the information gathering process within social engineering. Bellingcat [42], a Dutch-based group of investigative journalists specializing in OSINT investigations, provides a compilation of useful web applications for use at [43] and [44]. Similar information can also be found on the homepage of the OSINT researcher with the pseudonym "Technisette" [45], as well as in the other sources listed below:

- *Technisette Tools [45]*: Web-based OSINT tools and web applications to support online searches, links to other partner platforms, social media online search engines.
- *Bellingcat's Online Investigation Toolkit [43], [44]*: Compilation of several hundred web-based tools to support information gathering, grouped according to application areas (e.g. image search engines, social media, people search and much more).
- *OSINT for Journalists [46]*: Media map and link list with links to various OSINT online search engines, tool collections, links to other extensive link lists, web applications and databases.
- *Search Social Media [47]*: Numerous online search engines grouped according to social media platforms (Twitter, Reddit, Periscope, Tumblr, Facebook, Instagram, YouTube, LinkedIn, TikTok, Telegram, Snapchat, Pinterest). Links to other link lists and search engines for information on people, user names, telephone numbers and email addresses.
- *Ph055a GitHub Repository [48]*: GitHub repositories `Domains_OSINT_Collection` and `OSINT_Collection` contain link lists with numerous links to OSINT resources available online, such as search engines for users across several hundred social media platforms, search engines for information about companies, search engines for searching leaks, but also links to online resources to investigate domains and IoT products, such as subdomain enumerators and crawlers, link checkers, DNS info, similar site search and much more.
- *OSINT Framework [49]*: An animated OSINT tool link collection that offers freely available search engines and web applications for searching and enumerating user names, domains, e-mail addresses and archives as well as documentation and training material.

The number of links in these lists is so extensive that it was not possible to carry out a precise review as part of this work. Random checks showed that not all links were functional and not all tools worked automatically. It also turned out that links to similar pages are included, which in turn contain a large number of tool links. It also turned out that the listed tools, search engines and browser plugins are very often similar.

Regarding Social Media platforms, the web application *CheckUsernames* [50] allows the parallel search of over 300 platforms for user-names and linked profiles. Still, the search is very limited, only allowing for exact (partial) matches without additional intelligence. *ReconTool* [51] provides several additional features, like e.g., mindmapping information for dynamic interaction with the search engine. Even more extended functionality is provided by *HOPain Tools* [52], [53], as it also allows searching for pics, videos, detailed content

TABLE I
PHASE ASSIGNMENT

Model	Information Gathering	Attack Preparation	Attack Execution
M1	Reconnaissance	Weaponization, Delivery	Exploitation, Installation, Command & Control, Action on Objectives
M2	Research	Developing Rapport and Trust, Exploiting Trust	Utilize Information
M3	Investigation	Hook	Play
M4	Information Gathering	Attack Planning	Perform Attacks
M5	Information Gathering	Preparation	Exploit Relationship
M6	Map & Bond	Execution	
M7	Recon	Relationship Building, Attack Scenario Building	Execution, Action on Objectives
M8	Attack Preparation		Attack Implementation
M9	Using suitable gates of SNSs to gather information about victim	Using suitable gates of SNSs to reach the victim	Attack

like postings (also allowing filtering like time frames, location or number of likes), as well as bitcoin addresses. Social media platforms can be searched individually or in groups, for many platforms require a respective account.

2) Technology checks: In order to expand the possibilities of pretexts and impersonations for Social Engineering in organisations, it can be helpful to examine existing websites for the technologies used and possible vulnerabilities. The following tools can be used as an alternative to considerably more expensive systems due to higher licence and operating costs. The result of a scan with *BuiltWith* [54] shows the technologies, plugins and hosting provider used for a website, but also other websites that use the same hosting provider, as well as the duration and the respective public IP address under which they were accessible. However, the results can only be viewed to a limited extent in the free version, but are sufficient for searching for *Common Vulnerabilities and Exposures* (CVE) entries and for developing pretexts. Technological information, telephone numbers, email addresses, CVE vulnerabilities with the corresponding CVE number, public IP addresses used, open ports, domain names, cybersquatting domains and much more to determine further attack surfaces and risks of a website can also be found out very conveniently with *SpiderFoot* [55]. The *SpiderFoot HX* [56] version offers an even greater scope and an intuitive, graphical interface that can display all this information in the form of a node graph, where each node can be selected individually. The scan results were surprisingly comprehensive and consistently correct in the short time available and in view of the basic version used. Regarding the analysis of industrial (IoT) devices, Shodan [57], ZoomEye [58], Spyse [59] and Chaos [60] seem to be the most popular. Shodan provides many filter options and requires a familiarisation period in order to achieve useful results. The search results depend on the time in which Shodan has scanned the target system, but contain a high level of detail about the scanned target system. Despite language barriers, ZoomEye could be used with translation software at the time of the research and the presentation of the search results was very similar to Shodan. Surprisingly, Spyse was only able to deliver a few results during the application and using identical target systems and is therefore not very suitable for Social Engineering purposes. Chaos was still at an early stage of development at the time of the research. On the other hand, SynapsInt [61] is a freely available tool that also fits into this categorisation. It provides search results for domains, IP addresses, SSL certificates, email addresses, telephone numbers and Twitter accounts, as well as searching for ransom bitcoin addresses and CVE numbers. The results of a scan with the same inputs as before quickly delivered correct results, a current screenshot of the page, a VirusTotal analysis, the last available entry in the Internet archive Wayback Machine, open ports and information on the hosting provider used. In addition, all domains that can be reached under the same IP address, all subdomains, internal links and related social media links are listed and checked to see whether it is included in various blocklists. The blacklist check also works with entered email addresses. The leak check and the Twitter account check did not work with a private email address that has already been leaked many times.

3) Generate valid email formats: In order to generate the formats for E-Mail addresses of targets, we had a look at the search engines *Email-Format* [62] and*Hunter.io* [63]. Hunter, as well as Email-Format, derive patterns for corresponding email address formats from a large number of email addresses collected via web scans. Of the target domains entered for testing, around a third did not return any search results. The email address formats derived in both web applications appear correct, and sample data is also displayed freely in both applications, although it is not always up to date. Email address format offers, in addition to the identified conventions, a larger list of representative email addresses, as well as (depending on the payment plan) the option of downloading them. In comparison to Email Format, Hunter tends to limit the output, but in addition to more up-to-date data records, it also shows the occurrence of the representative email addresses, which are used to derive the logics for the email addresses.

4) Data breaches and data leaks: Regarding searching data breaches and data leaks, the IntelligenceX platform [64] retrieves results from Dataleaks, Wikileaks, paste sites and even the darknet for search queries, such as email, Bitcoin, MAC and IP addresses, domains, URLs, telephone numbers,

credit card numbers and much more. IntelligenceX offers a so-called "Third Party Search", in which the search scope can be extended again to several search engines (simultaneously via pop-ups) and, for example, Vehicle Identification Numbers (VIN) can also be searched for. There are separate search functions for social media channels, links to OSINT link lists, as well as file and encoding tools. The test searches carried out delivered surprisingly accurate results. A privately used, knowingly leaked email address that was no longer in use was found, including the password used at the time of use. For another, still privately used email address, it was possible to find out in which data breach the email address appeared and which platform was affected by the breach. Valid access data was also found for other email addresses in the private sphere; Reverse image searches from the third-party search category with randomly uploaded images from private collections and quick Google searches, mostly referred to Adobe stock images, however; three out of ten uploaded images were found. The VIN search was also tested with two different VIN numbers from our own stock, but the search yielded no results.

5) Detecting online times: Online times of targets are especially interesting for targeted attacks. The tool *SleepingTime* [65] was analysed for the SNS platform Twitter and successfully used with several Twitter accounts. SleepingTime analyses the last 1000 tweets of a Twitter account and derives an estimated "sleep schedule" from the time stamps of the respective tweets, in which the account is least active and in use. *WhatsApp Monitor* [66] is a similar tool that works with browser notifications when a specific WhatsApp contact is available online. The use of the tool sounded very interesting during the research, but could not be used at the time of the tests, as the website was not accessible at the time of the tests.

6) Searching for personal information: Regarding searching for personal information. Suche nach Personendaten, *Webmii* [67] compiles publicly available information about people on the Internet and uses it to generate an online score that is intended to show the availability of the person. Webmii usually lists the results in four sections. (i) the results list, containing the names of people who have interacted with the target person on social media channels, (ii) search results from various newspaper articles, (iii) results from various social media channels and (iv) search results obtained via a Google CSE. At first glance, *IDCrawl* [68] offers a wider range of functions, as it can be used to search not only for people's names, but also for user names across 17 SNSs. A reverse phone search is also offered. IDCrawl offers the option of an "opt-out", where you can exclude yourself from search results. During the test and the search for own findable information, IDCrawl was only able to verify one search result as correct, but the topicality of the result was doubtful, as in this specific case the user profile picture did not match and had already been replaced some time ago. However, the accuracy of the data is not guaranteed in large quantities at Webmii either, as only parts of the information could be considered correct as well. The majority of the search results were not usable, and in some cases links to results could not be opened at all.

B. Locally installed tools for Information Gathering

1) Maltego and alternatives: The data mining tool Maltego [69] is one of the best-known tool suites in the OSINT environment and is almost unique in its range of functions. Depending on the licence and the added plugins, the scope anc capability of the software change. For the tests and the tool comparison with a similar tool, the registered, free Community Edition with eight free plugins was used, which provides a certain number of credits depending on the query used. With six out of one hundred available credits, it was already possible to find domain information, whois entries, company owner data, email addresses, telephone numbers, public IP addresses, all plugins used on the website, as well as archived versions of these since 2009. Audit reports from American companies in the same business sector were also found in the Maltego document cloud. However, these were not related to the exemplary target company. As part of the research, a comparable alternative, or supplement, to Maltego could be found, which, despite critical voices [70], was implemented, licensed and tested for comparison: Lampyre [71], which is only available on Windows platforms and offers a similar overview to Maltego's Transformation Hub in the so-called "List of requests". The advantage of the software is that the plugins do not have to be installed individually; a selection (and like Maltego, the entry of a corresponding API key) of the modules to be used, the underlying and desired tasks, as well as the required parameters, is sufficient for the start.

In direct comparison, Maltego is clearer and more structured to use. Lampyre is simpler in terms of usability, the results are mostly displayed in tabular form and graphical dependencies are only possible in isolated cases. Furthermore, it is partially unstable, e.g., during the application tests, various result tabs suddenly stopped responding and could no longer be selected, meaning that the results could no longer be viewed.

Of the plugins already included, Lampyre offers a selection of search criteria that could not yet be found in Maltego and vice versa. These included, for example, the search for IMEI numbers, WLAN SSIDs or Vehicle Identification Numbers (VIN) in Lampyre, while Maltego offers the Wayback Machine, Movie Database, Blockchain.info or Google Maps Geocoding, which are regularly updated and expanded in both applications. Within Maltego, the origins of the search results and the use of the search providers are traceable. At first glance, it is not possible to recognise where Lampyre obtains the results of the transformations if the search provider is not described in the tasks. In the transformations to the same target organisation, more search results could be achieved with Maltego with less known data. The reliability of the data was also higher in Maltego; for example, the public company Facebook account could be found with Maltego, whereas Lampyre returned error messages for these transformations.

2) Searching for user and personal data: Regarding searching of account or personal data, *CrossLinked* [72] allows for automated searches in LinkedIn by filtering external search engine results, so-called *Search Engine Scraping*, thus not

requiring account data for searching. When verifying the results, it was found that although they were plausible (by randomly comparing the results with the online employee directory), but the results also included every person who had specified St. Pölten UAS in their LinkedIn profile, not only employees. When searching for another organisation without results, it turned out that links from search engines were also counted as results. The tools UserReCon [73] and Userrecon-py [74], Nexfil [75], Sherlock [76], Us3R-F1nD3R [77] and Thorndyke [78] promise similar functionalities with search scopes spanning several hundred social media platforms. From the own descriptions and command references of these tools, it is clear that Sherlock is the only application that can process several search entries as well as prepared lists in one search run. The tools are very similar in their use and appearance, as are the results. In addition to existing social media accounts, the Instagram test account `@dominikhatkeininsta` could also be found as a registered user on several platforms according to the search results. As the test account was only created for Instagram, it can be assumed that the search results are not valid, except for the Instagram platform. This was confirmed when checking the search results for the Twitter and Reddit platforms. Buster [79] can also find users on social media platforms, but the search scope is extended to the generation of email addresses, which are provided from possible data breaches, pastes and reverse-whois queries. Buster also shows the sources of results, as the services of Hunter.io, among others, are used in the background.

3) Technology checks: Regarding checking for technology, *TheHarvester* [80] is already pre-installed under Kali Linux and offers searches for domain information and Google dorks in 38 different search engines. Corresponding API keys are required for use, and the search results can be limited in scope. In the test, the search engines did not work properly under version 4.0.3, despite reinstalling the tool; under version 3.2.2, search results could at least be obtained via Google, although most of them were not valid. Raccoon [81] is basically an extension of nmap. The tool is still in the development stage and the focus is on simplicity. The convenience of using Raccoon lies in the fact that the parameterisation of the nmap scans is already predefined by the tool. In addition to the possibilities of nmap scans and subdomain enumeration, Raccoon should also be able to search cookies, recognise web application firewalls and provide information on CMS, web servers and Whois queries. However, this did not work in the test (without nmap scan). A coherent subdomain enumeration could be carried out using three different domains, including that of the St. Pölten University of Applied Sciences, with Sublist3r [82], Sn0int [83] and Frogy [84], whereby Frogy also uses Sublister in the enumerations. Sublister also offers the option of a port scan and a brute force scan, which were not performed. Under Sn0Int, the subdomain enumeration is only a small part of the functionalities. Frogy was still under development at the time of research and testing. In addition to finding IPs, domains and subdomains, it is also designed to find live websites and login portals. What is particularly interesting about this tool is that it can access the Chaos-database. Another tool suggested in the information retrieval communities is ReconSpider [85], which is a tool for the automated scanning of IP and e-mail addresses, websites, telephone numbers, DNS and domain information, but also for searching data breaches. ReconSpider was able to consistently return correct data in the test entries, but occasionally crashed with Python errors when making entries in the menus for whois and domain queries.

4) Export data from social media: Regarding the export of data from social media profiles, ReconSpider can display information of Facebook, Twitter and Instagram accounts, but this is limited to the name, number of followers and profile description and cannot be exported. The tool OSINTGram [86] on the other hand requires a valid Instagram account to be usable. For export, optionally in *.txt and *.json file formats, all addresses that can be read from posted image material, all texts and comments that have been added to posted images, the number of followers of the target account, as well as the number of accounts that the target account follows, account information, as well as the number of all likes, hashtags, a list of all links of the target account and a list of all accounts that have commented on posts of the target account at any time are available. The ”fwersemail”, ”fwingsemail”, ”fwersnumber” and ”fwingsnumber” functions are particularly interesting features for Social Engineering purposes, each of which creates a list of telephone numbers and email addresses (if specified in the respective accounts) of the followers and followings. In the test application with the Instagram account of the St. Pölten University of Applied Sciences, several thousand pieces of data were found. With a private test account, the consistently correct information could be provided in lists within a short time. Sterra [87] also exports follower and following accounts, including their account ID, user name, specified name, biography, number of posts and links to the respective account in CSV files. Within the application, it is also possible to compare follower lists with each other and filter them for similarities or differences. As Sterra works directly with Instagram’s API, the reliability of the data is guaranteed. List comparisons can also be carried out with the Python tool Insta-Extract [88] and these are simpler in the application than within Sterra, but not as extensive. What works well on the social media platform Instagram in the test applications also works with two other applications on the Twitter platform. Twi1tter0s1nt [89], also known as TWINT and twosint, offers pretty much the same functions on the command line that TinfoLeak [90] also offers in a GUI. These include general searches for user names, searches for geocoded tweets (if the geolocation data in the tweets can be read), tweets in a specific time window, filtering for specific terms, but also exporting the number of followers. In addition to exports in several file formats, TWINT also offers to translate tweets directly into other languages using Google Translate. A time limit between individual scrapes can also be set for scraping tweets using the ”min-wait-time” parameter. TinfoLeak is easier to use with the graphical user interface, where the desired operations are simply ticked and provided with the corresponding values or

data.

C. Ready-to-use system environments

The information procurement phase is very extensive due to the large number of applications available. Automation is largely attempted to be created within an application in order to automate and positively influence time and effort through recurring activities and queries (for example, the same searches for different user names on social media platforms). Applications such as Maltego and Lampyre use plugins from various manufacturers and developers to offer automation with various and different search queries within their own application. During the research for social engineering tools with automation and possibilities for this, two Linux distributions could also be found, with which no complete automation can be created in the process of information retrieval, but the effort is greatly simplified by the convenient operation.

1) Tsurugi-Linux: Similar to the Linux distributions Kali and BlackArch, the ready-to-use distribution of the Tsurugi Linux project [91] is structured in a similar way. The distribution is completely free and includes a variety of tools that can be used for the purposes of digital forensics and malware analysis. The distribution is based on Ubuntu and is available for download in three versions. Two of the three versions are available as a live system, while the third version can be downloaded as a ready-to-use image for Oracle VirtualBox. Tsurugi is a double-bladed sword used by Japanese monks. The metaphor of the double-bladed sword has also been transferred to the distribution: there is a profile switcher that switches from the digital forensics environment to the OSINT environment, making numerous tools for information gathering and reconnaissance purposes conveniently available in the start menu with just a few mouse clicks. A list of pre-installed tools can be viewed at [91], some of which were also discussed in this paper independently of this distribution. Similar to Kali and BlackArch, the tools must be started manually, but the ease of use is increased by the profile switcher and thus simplifies the process of information retrieval.

2) CSI-Linux: The Linux distribution CSI-Linux [92] is also designed for digital forensics. CSI-Linux optimises the time and effort involved in the process of obtaining information by using several tools, which have also already been discussed in this paper, to enable the pre-parameterised starting of applications with a so-called "case management" and to store the search results clearly in a corresponding folder structure. Each new investigation process starts with the creation of a new case file, after which the desired type of investigation is selected. This can be ”Social Media Intelligence (SOCMINT)”, for example. The respective launcher is kept so simple, even when selecting a different investigation (e.g. ”Domain and Website OSINT”) that you only need to select what you want to search for. Special knowledge of and in programmes and applications, as well as the parameters required for use, is therefore not necessary. The handling of API keys, some of which are subject to a charge, is also kept simple and clear with this workflow-like user interface. Keys can be added, exchanged or removed conveniently with just a few mouse clicks. CSI-Linux is also available as a ready-to-import image for Oracle VirtualBox. In addition, it is also offered as a bootable image in the form of a forensic RAW image. For support, there are also instruction videos and walkthroughs for various application purposes at [92].

D. Tools for the attack preparation phase

The attack preparation phase includes those tools that, depending on the selected attack scenario, are useful for preparing attacks, e.g., for preparing payloads or phishing messages.

1) Preparing Payloads: To prepare suitable payloads, already generated and available versions [93] can be used, or new ones can be generated. In addition to one of the best-known tools, the Social Engineering Toolkit (SET) [94], the PowerShell script [95] designed by Matt Nelson and Matt Robinson is also suitable for this, which creates an Excel document after the run that creates a Meterpreter shell when called on the target system. It also persists in the Windows registry and in the user directory so that it can be executed again when the system is restarted. A connection to the infected system can be established via Meterpreter Reverse HTTP and HTTPS. The MacroPack tool from Emeric Nasi [96] is more up-to-date and has an extended range of functions compared to the PowerShell script and requires a functioning and registered Office installation on the system on which the payload is to be integrated into an Office file. The tool also offers the service of code obfuscation so that the malicious code in the Office markers is not so easily recognisable and it supports all Microsoft Office document versions and shortcut files in the community version. The Pro version offers an even wider range of functions and can be used on existing Office files. During the tests, the generation of payloads with the PowerShell script did not work, despite changes in the execution guidelines, which originally prevented the execution of the script. For the execution and use of MacroPack, it is recommended to adjust the Windows security settings, as these prevent execution and classify the tool as a serious threat. The tool Social_X, which was supposed to be able to generate Trojans with its own reverse shell and in the form of an *.exe file, unexpectedly failed to install correctly and terminated after several start attempts. Documentation for the tool was not available at the time of testing and a linked YouTube video was no longer available. Social_X is therefore only mentioned as another possibility, as the last commit on GitHub was only a few months old and the error could possibly be fixed soon.

SET, which is included in every current installation of Kali-Linux, offers the option of automatically manipulating data carriers, so that malicious code can be automatically executed on removable media via the autorun function. This can be done via an executable file, which is executed via the autorun.inf file contained on the removable storage device, or via a file format exploit to bypass any security warnings. TrustSec also provides detailed documentation on SET. SET worked out of the box and, with the TrustSec documentation, was simple and reliable.

2) Recognising tone and emotions in texts: In order to test messages for the effect of emotions, the Tone Analyser [97] from IBM was tested during the research into automated Social Engineering tools. The Tone Analyzer can be freely tested online in a web form and recognises the emotions and tones of voice contained in an entered text via machine learning analysis. The Node.js version of the Tone Analyser [98] offers free analyses and support for several languages and files directly for the first 1000 API calls per month after registration in the IBM Developer Cloud. To quickly test the analysis, the following sample texts were entered for analysis:

- *Positive emotion: "Dominik likes doing his master thesis all night long :-)"*
- *Negative emotion: "Dominik does not like doing his master thesis all night long :-("*

Tone Analyzer carried out the analyses with respect to the emotions "Confident", "Joy" and "Sadness" and classified the strength of the expressions in the messages with different colours. In further tests, with different text fragments, Tone Analyser also classified in the direction of "Analytical" and "Tentative". We did not conduct any further tests, as this work is not focusing on the capabilities of emotion detection, but on the general usability of the tools.

3) Bot preparation: Parts of a Social Engineering attack can also be carried out by bots, depending on the target and attack scenario selected. Implementations of Twitter bots, modelled on Realboy [99] or SNAP_R [100], for example, can be used in the attack execution phase for the automated distribution of phishing links. In the attack preparation phase, corresponding Twitter accounts can be created, filled with content and equipped with a network of followers and followings to make them more credible. Both bots, Realboy and SNAP_R, were not tested and evaluated in this work, as there exists ample recent work analyzing bot preparation for Social Engineering.

E. Tools for the attack execution phase

The attack execution phase includes all those tools that can directly execute a Social Engineering attack. While researching the relevant tools, it emerged that the automation of attack tools is described almost exclusively in terms of phishing with website cloning, mass emails and occasionally the use of bots.

1) Phishing with website cloning: SET [101] offers the possibility to clone any website into a website with phishing or hosting multiple attack methods. The cloned page is ready for use as soon as it is entered, and the user data entered is displayed in colour directly on the command line. Zphisher [102] works in a similar way, also with regard to website cloning. Unlike SET, however, Zphisher only offers ready-made templates for phishing pages and does not clone individual pages. This is also the case with phishEye [103], although it is the only tool listed that also offers the option of cloning websites for mobile devices. During the application tests, it was found that although Blackeye [104] provides a number of templates for social media platforms, these could not be tested directly as an error occurred when generating the phishing links and no links were generated or output for use. SocialFish [105] could also not be fully tested and evaluated, as module error messages occurred within the main application when the application was started, despite all installed requirements and dependencies. The documentation for the app is very brief and rudimentary, so the error could not be rectified. Cloning the GitHub repository again did not help either. StormBreaker [106] extends the list of phishing tools mentioned in this subsection with a tool that cannot clone websites like the others mentioned so far, but instead generates pages and links with the help of Ngrok with a maximum of two inputs, which enable access to the camera, microphone and location data of the end devices. The location data is returned with a Google Maps link. StormBreaker also offers an "OS Password Grabber" function, which is designed to transfer the passwords entered. During the tests, there were difficulties with this part of the function, as either the links to be sent were not generated or the application did not respond to inputs. However, the functionality of accessing the microphone, camera and location data of the potential target's device is only possible if all phishing warnings displayed by the current browser generations are ignored when the page is accessed and authorisation to access the microphone, camera or location is granted accordingly.

2) Mass mailer: In addition to individual (spear) phishing messages, the Social Engineering toolkit SET [101] can also be used to set up the sending of mass emails. The email addresses of the recipients can be provided via a separate text file, and a separate mail server or sending via Google Mail (gmail) can be selected for sending. The message content is accepted in both HTML and plain text formatting. A test mailing with SET was carried out using our own mail server. As expected, the e-mail message was classified as SPAM and filtered accordingly. In many cases it is not clear before sending a message whether it will be blocked by a mail server or whether it will be delivered without any problems. In order to check the behaviour of mail servers when a message is received, a check can be carried out in advance using Phishious [107]. According to its own information, Phishious is the only tool to date that makes it possible to scan phishing attacks via email. Phishious analyses the header data of undeliverable messages and can therefore predict whether a message will be delivered or classified as spam or junk mail. Another mass mailer tool can be seen in Catero [108]. In addition to the option of cloning websites, Catero offers various ways of sending automated messages and can be controlled entirely via the Command Line Interface (CLI). Catero supports sending messages via Twillo accounts for sending SMS messages, sending via LinkedIn accounts and WebMail services, Google Voice and iMessage.

3) Bot utilization: Another type of automation of Social Engineering using bots is the preparation for the use of SMSRanger[109], which is based on a Telegram bot. SMSRanger sends automated messages to people, in each case on behalf of a bank, and asks them to enter OTP codes (One Time Password) in corresponding websites or in an automated call via a voice bot using the telephone keypad. The service contains daily updates, is available in various languages and is subject to

a charge. At the time of research, calls from and to various countries, including German-speaking countries, were also included for USD 425 per month. SMSRanger is controlled via a Telegram chat. This bot was also not activated for security, legal and ethical reasons. With Honeybot [17], Tobias Lauinger et al. have already shown that conversations between two people can be started and influenced and controlled by the bot-in-the-middle, which can also be used to carry out attacks. The *Honeybot* tool is only mentioned in this section and was not tested or evaluated in this paper, as this has already been done in related work.

VI. Conclusion and Future Work

In this section, we provide some conclusion, but also references for future work in this fast evolving topic.

A. Conclusion

In order to better understand automation in the area of Social Engineering and to be able to search for suitable tools and tool suites, but also to be able to classify automation in different phases of Social Engineering, various Social Engineering frameworks were analyzed and compared with each other. It was found that the various models often differ in the number of phases and that classifying automated tools into individual phases in this way is not purposeful. Therefore, a compression to common phases of all models was carried out and from this, the *technical Social Engineering model* was derived. Furthermore, the individual phases of the described frameworks from other works were assigned to the phases of the technical Social Engineering model, using phase mapping. A similar and comparable abstract model could not be found by the time of writing this paper. For the listing and clustering of the automation-supported Social Engineering tools within Section V, the individual phases of the technical Social Engineering model were used. The clustering of the corresponding tools shows that in the information gathering phase there exists a lot of diversity and a large number of tools allowing for the most automation possibilities, as there is a large community of interested parties and contributors from the OSINT area. This was shown not only in the short intervals, in which tools and updates to existing tools are published, but also in the linguistic diversity in which the applications are written. The short intervals make it impossible to list and test all of the available tools. A selection of over 140 tools, written in German or English language, were subjected to a practical application and comparison, where it was found that information retrieval within the European Union has become more difficult since the introduction of the General Data Protection Regulation, and that web applications for information retrieval in particular largely only provide results in the states of the USA. There are, in the applications that are available free of charge, often query limits implemented that only allow a small number of queries within a certain period of time. Registering to receive an API key, shifts the query limits, depending on the chosen tariff and tool, but also the up-to-dateness, as well as the amount of data provided. Within this work, only freely available tools and API keys free of charge were used. Furthermore, it became apparent that results must be manually checked for plausibility and validity before further use, since the results of automated tools, with the exception of those that read information directly from social media platforms, are not necessarily correct or appropriate. When using the tools to gather information from social media platforms, most of the platforms require a registered account. When using the tools to prepare for attacks, it has been shown that automation can be summarized to the preparatory generation and creation of payloads and bots, as well as support in the formulation of texts. When using the tools in the attack execution phase, the researched and mentioned tools could be summarized into the categories ”phishing with website cloning”, ”mass mailers” and the ”use of bots”. A completely end-to-end automated software that can map a complete Social Engineering attack in all of its phases could not be found. The two tools Maltego and SET are, after completion of the tests and comparisons, the most functional and reliable tools.

B. Answering the research questions

The research questions posed at the beginning of the paper can thus be answered as follows.

a) RQ1: The freely available Social Engineering tools are automated in the sense that recurring query and search work can be performed automatically, thus significantly reducing manual effort. Searches can be performed via web applications, but also locally installed tools. Web applications shine with simpler operation and fast availability. The automation possibilities are greater when using the APIs of the search providers and platforms, since the results can be processed further in an automated manner if the appropriate output is available. A completely automated solution could not be found and is correspondingly difficult to develop, since Social Engineering can be very dynamic and the validation and decision as to, whether data and information fit a current target and scenario, must be made manually by the social engineers themselves. Automation is also already available in the execution of attacks and in the corresponding preparation, and the corresponding tools are already very easy to use. During the application and writing of the paper, it has become evident that the selection and availability of automated tools for the purpose of information retrieval is the largest. One justification of this can be the availability of a large community from the OSINT domain. Another reason can be seen in the greater availability of these tools, among other things for awareness-raising measures. With regard to quality, it was stated in the paper that the scope of the search and the number of permitted searches are subject to certain limitations, depending on the platform and are only increased with paid subscriptions. This also affects the reliability of the search results. Regarding availability, interesting tools could be collected during the research phase, but during the testing and application phase a few weeks later, they were no longer available and applicable. The free availability of automated Social Engineering tools means that these tools are available to any person, can be used by any

person, and thus any person can easily use Social Engineering techniques, without much effort or in-depth knowledge. Due to the availability of ready-to-use system environments, pre-configured systems are provided, which, with a simplified graphical user interface, can deliver usable results within a short period of time, even for beginners.

b) RQ2: The various frameworks and phase models differ in terms of the number of phases, as well as the processes within the phases themselves. Generally speaking, the phases of reconnaissance and the phases, within which attacks take place, are best served and supported by automation. Due to the number of differences between the various Social Engineering models, it was not possible to map the automated tools to all models, which is why the abstract technical Social Engineering model was derived from the other analyzed frameworks.

c) RQ3: Records must be manually selected, validated, and formatted for the next tool. Toolsuites, which offer multiple options and whose functionalities can be extended with plugins, such as the mentioned tools Maltego, Lampyre, or also Spiderfoot HX, can transfer results into new searches most easily. These tools cannot guide a complete Social Engineering process, but they accompany a large part of it very reliably.

d) RQ4: The results of the tools depend very well on the respective mode of operation itself. While some of the tools, in order to deliver search results, make use of searching in archive databases or searching crawled and scanned websites, some tools access live data directly. In free program versions, live data was only analyzed by tools that search across social media platforms, for example Tinfoleak or OSINTGram, and required a corresponding user account. Searching crawled pages affects the reliability and the up-to-dateness of the results.

C. Future Work

As an extending future work, paid API keys of the applications, offering higher-value subscriptions, can be purchased and the results compared between the premium versions. Under appropriate legal and ethical coverage, extended use of the tools, including for awareness and training purposes, is conceivable. In the light of the increasing number of phishing messages, the comparison and use of professional Social Engineering tools, such as CanIPhish, GoPhish and SET, in the corporate context is a possibility. From this, organizational countermeasures, suitable for the respective organization, can be derived and an anti-Social Engineering framework can be designed. In the analysis of free tools, it was found that search platforms, including Hunter.io, Shodan.io, as well as _IntelX, were used in common by some tools. In the context of a future work, the comparison of which and how many search engines and databases are used in the background, together and whether the results, despite use of same sources, differ. Also, the development of an automated Social Engineering application, which can link the applications and results of different Social Engineering tools together, can be initiated.

Acknowledgments

Part of this work was funded by the Christian Doppler Laboratory for Assurance and Transparency in Software Protection, Research Group Security & Privacy, Faculty of Computer Science, University of Vienna. The financial support by the Austrian Federal Ministry of Labour and Economy, the National Foundation for Research, Technology and Development and the Christian Doppler Research Association is gratefully acknowledged. Part of this work was funded by the COIN project "Secure Supply Chains for Critical Systems" (SSCCS, 883977). The financial support by the Austrian Research Promotion Agency (FFG) is gratefully acknowledged.

References

[1] D. Dana, S. Schrittwieser, and P. Kieseberg, "Automated social engineering tools-overview and comparison with respect to capabilities and detectabilitys", in *Proceedings of the Nineteenth International Multi-Conference on Computing in the Global Information Technology (ICCGI 2024)*, IARIA, 2024.

[2] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, 2003.

[3] C. Hadnagy, *Social Engineering: The Art of Human Hacking*. John Wiley & Sons, 2010.

[4] K. Zheng, T. Wu, X. Wang, B. Wu, and C. Wu, "A session and dialogue-based social engineering framework", *IEEE Access*, vol. 7, pp. 67 781–67 794, 2019.

[5] E. D. Frauenstein and S. V. Flowerday, "Social network phishing: Becoming habituated to clicks and ignorant to threats?", in *2016 Information Security for South Africa (ISSA)*, IEEE, 2016, pp. 98–105.

[6] J. Talamantes, *The Social Engineer's Playbook: A Practical Guide to Pretexting*. Hexcode Publishing, 2014.

[7] P. Kim, *The Hacker Playbook 2: Practical Guide to Penetration Testing*. Secure Planet, LLC, 2015.

[8] C. Hadnagy, *The Science of Human Hacking*. Wiley Publishing Inc., 2018.

[9] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: A domain ontology and knowledge graph application examples", *Cybersecurity*, vol. 4, pp. 1–21, 2021.

[10] H. Aldawood and G. Skinner, "An advanced taxonomy for social engineering attacks", *International Journal of Computer Applications*, vol. 177, no. 30, pp. 1–11, 2020.

[11] B. Banire, D. Al Thani, and Y. Yang, "Investigating the experience of social engineering victims: Exploratory and user testing study", *Electronics*, vol. 10, no. 21, p. 2709, 2021.

[12] J. Obuhuma and S. Zivuku, "Social engineering based cyber-attacks in kenya", in *2020 IST-Africa Conference (IST-Africa)*, IEEE, 2020, pp. 1–9.

[13] N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*. Springer, 2018.

[14] C. P. Janssen, S. F. Donker, D. P. Brumby, and A. L. Kun, "History and future of human-automation interaction", *International Journal of Human-Computer Studies*, vol. 131, pp. 99–107, 2019.

[15] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity", *IEEE Access*, vol. 8, pp. 85 094–85 115, 2020.

[16] M. Huber, "Automated social engineering, proof of concept", *Royal Institute of Technology Stockholm*, 2009.

[17] T. Lauinger, V. Pankakoski, D. Balzarotti, and E. Kirda, "Honeybot, your man in the middle for automated social engineering.", in *LEET*, 2010, pp. 1–8.

[18] J. Seymour and P. Tully, "Weaponizing data science for social engineering: Automated e2e spear phishing on twitter", *Black Hat USA*, vol. 37, pp. 1–39, 2016.

[19] P. Kaul and D. Sharma, "Study of automated social engineering, its vulnerabilities, threats and suggested countermeasures", *International Journal of Computer Applications*, vol. 67, no. 7, pp. 13–16, 2013.

[20] Y. Kano and T. Nakajima, "Trust factors of social engineering attacks on social networking services", in *2021 IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech)*, IEEE, 2021, pp. 25–28.

[21] A. Stern, "Social networkers beware: Facebook is a major phishing portal", *Kaspersky Lab*, vol. 23, 2014.

[22] K. Kikerpill and A. Siibak, "Mazephishing: The covid-19 pandemic as credible social context for social engineering attacks", *Trames: A Journal of the Humanities and Social Sciences*, vol. 25, no. 4, pp. 371–393, 2021.

[23] EUR-Lex, *Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)*, 2016.

[24] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites", in *2009 International Conference on Computational Science and Engineering*, IEEE, vol. 3, 2009, pp. 117–124.

[25] EUR-Lex, *Regulation (eu) 2024/1689 of the european parliament and of the council of 13 june 2024 laying down harmonised rules on artificial intelligence and amending regulations (ec) no 300/2008, (eu) no 167/2013, (eu) no 168/2013, (eu) 2018/858, (eu) 2018/1139 and (eu) 2019/2144 and directives 2014/90/eu, (eu) 2016/797 and (eu) 2020/1828 (artificial intelligence act)*, 2024.

[26] EUR-Lex, *Regulation (eu) 2023/2854 of the european parliament and of the council of 13 december 2023 on harmonised rules on fair access to and use of data and amending regulation (eu) 2017/2394 and directive (eu) 2020/1828 (data act)*, 2023.

[27] R. Goebel *et al.*, "Explainable ai: The new 42?", in *International Cross-Domain Conference for Machine Learning and Knowledge Extraction*, Springer, 2018, pp. 295–303.

[28] Lockheed Martin Corporation, "The cyber kill chain", [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (visited on 03/17/2025).

[29] imperva, "What is social engineering", [Online]. Available: https://www.imperva.com/learn/application-security/social-engineering-attack/ (visited on 03/17/2025).

[30] F. Mouton, M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework", in *2014 Information Security for South Africa*, IEEE, 2014, pp. 1–9.

[31] M. Nohlberg and S. Kowalski, "The cycle of deception: A model of social engineering attacks, defenses and victims", in *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, University of Plymouth, 2008.

[32] A. Cullen and L. Armitage, "The social engineering attack spiral (seas)", in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, IEEE, 2016, pp. 1–6.

[33] A. Algarni, Y. Xu, and T. Chan, "Social engineering in social networking sites: The art of impersonation", in *2014 IEEE International Conference on Services Computing*, IEEE, 2014, pp. 797–804.

[34] P. Pathak, "Is your soc overwhelmed? artificial intelligence and mitre att&ck can help lighten the load", [Online]. Available: https://securityintelligence.com/is-your-soc-overwhelmed-artificial-intelligence-and-mitre-attck-can-help-lighten-the-load/ (visited on 03/17/2025).

[35] M. S. Khan, S. Siddiqui, and K. Ferens, "A cognitive and concurrent cyber kill chain model", *Computer and Network Security Essentials*, pp. 585–602, 2018.

[36] J. Happa and G. Fairclough, "A model to facilitate discussions about cyber attacks", *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, pp. 169–185, 2017.

[37] Offensive Security, "Google hacking database", [Online]. Available: https://support.google.com/websearch/answer/2466433 (visited on 03/17/2025).

[38] Google, "Programmable search engine", [Online]. Available: https://programmablesearchengine.google.com/about/ (visited on 03/17/2025).

[39] B. Singh, "One-stop cse for social media", [Online]. Available: https://cse.google.com/cse?cx=73dda67fd05b4405f#gsc.tab=0 (visited on 03/17/2025).

[40] S. Proto, "Stefanie proto's custom search engines", [Online]. Available: https://docs.google.com/spreadsheets/d/1fBPz6KHsFXryhu6JNrj1l-Rl04bEKLfinyCgCIqTyzU/edit?fbclid=IwAR3niqdKoD6Zx1DL4ZPvM9yXMUo8Hhr6zK2MpELKvyvegQ2Ea7xWqLELiM0#gid=436019663 (visited on 03/17/2025).

[41] S. Proto, "Sprp77's osint resources", [Online]. Available: https://drive.google.com/drive/folders/1CBcemFdorkAqJ-Sthsh67OVHgH4FQF05 (visited on 03/17/2025).

[42] Bellingcat, "Bellingcat - the home of online investigations", [Online]. Available: https://www.bellingcat.com/ (visited on 03/17/2025).

[43] Bellingcat, "Bellingcat's online investigation toolkit", [Online]. Available: https://docs.google.com/spreadsheets/d/18rtqh8EG2q1xBo2cLNyhIDuK9jrPGwYr9DI2UncoqJQ/edit?fbclid=IwAR2gnqA0CUujpYiS4Kg6Jvwch0Sg-tR1g9_s9gfofwRyIz75ioy-PzdQRto#gid=1919065780 (visited on 03/17/2025).

[44] Bellingcat, "Bellingcat osint landscape - start.me", [Online]. Available: https://start.me/p/ELXoK8/bellingcat-osint-landscape (visited on 03/17/2025).

[45] Technisette, "Tools - technisette website", [Online]. Available: https://technisette.com/p/tools (visited on 03/17/2025).

[46] 16.OSINT-IO, "16.osint-io", [Online]. Available: https://start.me/p/1kOJ9N/16osint-io (visited on 03/17/2025).

[47] Sourcesource, "Search social media", [Online]. Available: https://start.me/p/RMKeQv/search-social-media (visited on 03/17/2025).

[48] Ph055a, "Ph055a (ph055a) / repositories", [Online]. Available: https://github.com/Ph055a?tab=repositories (visited on 03/17/2025).

[49] J. Nordine, "Osint framework", [Online]. Available: https://osintframework.com/ (visited on 03/17/2025).

[50] KnowEm, "Checkusernames", [Online]. Available: https://checkusernames.com/ (visited on 03/17/2025).

[51] R. Tool, "Osint recon tool", [Online]. Available: https://recontool.org/%5C#mindmap (visited on 03/17/2025).

[52] HOPain, "Hopain osint search tools", [Online]. Available: https://osint.hopain.cyou/ (visited on 03/17/2025).

[53] HOPain, "Github - hopain complex osint search tools", [Online]. Available: https://github.com/HOPain/OSINT-Search-Tools (visited on 03/17/2025).

[54] BuiltWith Pty Ltd, "Builtwith technology lookup", [Online]. Available: https://builtwith.com/ (visited on 03/17/2025).

[55] S. Micallef, "Spiderfoot", [Online]. Available: https://www.spiderfoot.net/about/ (visited on 03/17/2025).

[56] S. Micallef, "Spiderfoot hx", [Online]. Available: https://sf-c824cc8.hx.spiderfoot.net/scaninfo?id=48f74883e9c61198ca1d8356ad0d38e9cc42584e208317542c21b56afbbbb890 (visited on 03/17/2025).

[57] Shodan Search Engine, "The shodan search engine", [Online]. Available: https://www.shodan.io (visited on 03/17/2025).

[58] KnownSec, "Zoomeye", [Online]. Available: https://www.zoomeye.org (visited on 03/17/2025).

[59] SPYSE, "Spyse - internet assets search engine", [Online]. Available: https://spyse.com (visited on 03/17/2025).

[60] projectdiscovery.io, "Projectdiscovery.io | chaos", [Online]. Available: https://chaos.projectdiscovery.io (visited on 03/17/2025).

[61] M. Garciaguirre, "Synapsint", [Online]. Available: https://synapsint.com/index.php (visited on 03/17/2025).

[62] Email-Format, "Email-format", [Online]. Available: https://www.email-format.com (visited on 03/17/2025).

[63] Hunter Web Services, Inc., "Find email addresses in seconds - hunter", [Online]. Available: https://hunter.io (visited on 03/17/2025).

[64] Kleissner Investments s.r.o., "Intelligencex", [Online]. Available: https://intelx.io/ (visited on 03/17/2025).

[65] A. Agarwal, "Sleeping time", [Online]. Available: http://sleepingtime.org/ (visited on 02/08/2024).

[66] R. Ahmad, "Whatsapp monitor - whatsapp contact online monitoring tool", [Online]. Available: https://github.com/rizwansoaib/whatsapp-monitor (visited on 03/17/2025).

[67] Webmii, "Webmii people search engine", [Online]. Available: https://webmii.com/ (visited on 03/17/2025).

[68] IDCrawl, "Idcrawl free people search", [Online]. Available: https://www.idcrawl.com/ (visited on 03/17/2025).

[69] Maltego Technologies, "Maltego", [Online]. Available: https://www.maltego.com (visited on 03/17/2025).

[70] M. Krueger, "Be careful what you osint with", [Online]. Available: https://keyfindings.blog/2020/03/23/be-careful-what-you-osint-with/ (visited on 03/17/2025).

[71] DATA TOWER Kft., "Lampyre: Data analysis & osint tool for everyone", [Online]. Available: https://lampyre.io (visited on 03/17/2025).

[72] m8r0wn, "Crosslinked: Linkedin enumeration tool to extract valid employee names from an organization through search engine scraping", [Online]. Available: https://github.com/m8r0wn/crosslinked (visited on 03/17/2025).

[73] vijaysahuofficial, rly0nheart and HanslettTheDev, "Userrecon: This is a simple username recognition tool.", [Online]. Available: https://github.com/vijaysahuofficial/UserReCon?%5C%5Cfbclid=IwAR0NAexz0KEyNDvJSOfSyOzsw9Z0Hc9j7AtB38ZK5AsI-5vupj46Dh95o-o (visited on 03/17/2025).

[74] [lucmski], "Recognition usernames in 187 social networks", [Online]. Available: https://github.com/lucmski/userrecon-py (visited on 03/17/2025).

[75] thewhiteh4t, "Nexfil: Osint tool for finding profiles by username", [Online]. Available: https://github.com/thewhiteh4t/nexfil?%5C%5Cfbclid=IwAR0NAexz0KEyNDvJSOfSyOzsw9Z0Hc9j7AtB38ZK5AsI-5vupj46Dh95o-o (visited on 03/17/2025).

[76] sherlock-project, "Hunt down social media accounts by username across social networks", [Online]. Available: https://sherlock-project.github.io (visited on 03/17/2025).

[77] machine1337, "Userfinder: An osint tool to find user's all over the internet including social media platforms", [Online]. Available: https://github.com/machine1337/userfinder?%5C%5Cfbclid=IwAR3sCrgnkLvCUuLHP5VT6X8pVUvfyb8W0DZPenHVDA-VTIq3Et3zwMldWL0 (visited on 03/17/2025).

[78] rly0nheart, "Thorndyke: Lightweight username enumeration tool", [Online]. Available: https://github.com/rly0nheart/thorndyke?%5C%5Cfbclid=IwAR1qnLkHJOC0a-OdlRXk1svN8ypAo6BvuQTrA8L5E4VY%5C%5CxbgI4UzVXLUz6PE (visited on 03/17/2025).

[79] sham00n, "Buster: An advanced tool for email reconnaissance", [Online]. Available: https://github.com/sham00n/buster (visited on 03/17/2025).

[80] c. Martorella, "Theharvester | kali linux tools", [Online]. Available: Https://www.kali.org/tools/theharvester/ (visited on 03/17/2025).

[81] E. Meged, "Raccoon: A high performance offensive security tool for reconnaissance and vulnerability scanning", [Online]. Available: ttps://github.com/evyatarmeged/Raccoon (visited on 03/17/2025).

[82] aboul3la, "Sublist3r: Fast subdomains enumeration tool for penetration testers", [Online]. Available: https://github.com/aboul3la/Sublist3r (visited on 03/17/2025).

[83] kpcyrd, "Sn0int: Semi-automatic osint framework and package manager", [Online]. Available: https://github.com/kpcyrd/sn0int (visited on 03/17/2025).

[84] Iamthefroggy, "Frogy: Subdomain enumeration script", [Online]. Available: https://github.com/iamthefrogy/frogy (visited on 03/17/2025).

[85] bhavsec, "Most advanced open source intelligence (osint) framework for scanning ip address, emails, websites, organizations", [Online]. Available: https://github.com/bhavsec/reconspider (visited on 03/17/2025).

[86] G. Criscione, "Osintgram is a osint tool on instagram. it offers an interactive shell to perform analysis on instagram account of any users by its nickname", [Online]. Available: https://github.com/Datalux/Osintgram (visited on 03/17/2025).

[87] Novitae, "Instagram osint tool to export and analyse followers | following with their details", [Online]. Available: https://github.com/novitae/sterraxcyl (visited on 03/17/2025).

[88] J. Sánchez, "Instagram osint tool to scraping user information", [Online]. Available: https://github.com/JavideSs/insta-extract (visited on 03/17/2025).

[89] L. Zaccagnini and falkensmz, "Tw1tter0s1nt: Python tool that automates the process of twitter osint investigation using twint", [Online]. Available: https://github.com/falkensmz/tw1tter0s1nt (visited on 03/17/2025).

[90] V. Diaz, "The most complete open-source tool for twitter intelligence analysis", [Online]. Available: https://github.com/vaguileradiaz/tinfoleak (visited on 03/17/2025).

[91] G. Rattaro *et al.*, "Tsurugi linux", [Online]. Available: https://tsurugi-linux.org/index.php (visited on 03/17/2025).

[92] J. Martin *et al.*, "Csi linux", [Online]. Available: https://csilinux.com/ (visited on 03/17/2025).

[93] D. Kitchen, "Usb-rubber-ducky wiki", [Online]. Available: https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads (visited on 03/17/2025).

[94] D. Kennedy, "The social-engineerin toolkit (set)", [Online]. Available: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set (visited on 03/17/2025).

[95] M. Robinson and M. Nelson, "Generate-macro: This powershell script will generate a malicious microsoft office document with a specified payload and persistence method", [Online]. Available: https://github.com/enigma0x3/Generate-Macro (visited on 03/17/2025).

[96] E. Nasi, G. Michel, and J. Goldberg, "Tool used to automatize obfuscation and generation of office documents, vb scripts, shortcuts, and other formats for pentest", [Online]. Available: https://github.com/sevagas/macro%5C_pac (visited on 03/17/2025).

[97] IBM Watson Developer Cloud, "Tone analyzer demo", [Online]. Available: https://tone-analyzer-demo.ng.bluemix.net/ (visited on 03/17/2025).

[98] IBM Watson Developer Cloud, "Sample node.js application for the ibm tone analyzer service", [Online]. Available: https://github.com/watson-developer-cloud/tone-analyzer-nodejs (visited on 03/17/2025).

[99] Z. Coburn and G. Marra, "Realboy - believeable twitter bots", [Online]. Available: http://ca.olin.edu/2008/realboy (visited on 03/17/2025).

[100] J. Seymour and P. Tully, "A machine learning based social media pen-testing tool", [Online]. Available: https://github.com/zerofox-oss/SNAP%5C_R (visited on 03/17/2025).

[101] D. Kennedy, "The social-engineerin toolkit (set)", [Online]. Available: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/ (visited on 03/17/2025).

[102] T. Rayat, "Zphisher: An automated phishing tool with 30+ templates.", [Online]. Available: https://github.com/htr-tech/zphisher (visited on 03/17/2025).

[103] A. Kumar, "Phisheye is an ultimate phishing tool in python.", [Online]. Available: https://github.com/sky9262/phishEye?%5C%5Cfbclid=IwAR1hdh%5C_rgxK24YB4gi%5C_2FYtY4D7Qrxt05WPwU2ZKGa1g%5C%5CXCh7ln7MF0RfmyI (visited on 03/17/2025).

[104] An0nUD4Y, "Blackeye: The ultimate phishing tool with 38 websites available", [Online]. Available: https://github.com/An0nUD4Y/blackeye (visited on 03/17/2025).

[105] UndeadSec, "Socialfish: Phishing tool & information collector", [Online]. Available: https://github.com/UndeadSec/SocialFish (visited on 03/17/2025).

[106] A. Moghaddas, "Storm-breaker: Tool social engineering with ngrok", [Online]. Available: https://github.com/ultrasecurity/Storm-Breaker?%5C%5Cfbclid=IwAR2HX8B5RRQ2f-yRlWndAjxZM1PKfZxVZq-GM-9C%5C_f317IFWGjdAVhcRHaY (visited on 03/17/2025).

[107] Reis, "Phishious: Ein open-source-evaluierungs-toolkit für secure email gateway (seg)", [Online]. Available: https://github.com/Rices/Phishious?%5C%5Cfbclid=IwAR2OhR2kRNkAyyGS7skSzOwlRPEWDcxzFwzohAFuj%5C_coi%5C%5CQFlMdq7t9wlh%5C_k (visited on 03/17/2025).

[108] Section9Labs, "Cartero - social engineering framework", [Online]. Available: https://github.com/Section9Labs/Cartero (visited on 03/17/2025).

[109] smsranger.io, "Smsranger is the most advanced sms capture bot on the market", [Online]. Available: https://smsranger.io/ (visited on 03/17/2025).