D3.1 Report on existing tools, their evaluation and the gap to be filled by DOGANA development

Work Package:	WP3
Lead partner:	PROPRS Ltd. (PRO)
Author(s):	C. Dambra, A. Gralewski (PRO), E. Frumento, R. Puricelli, F. Valentini (CEFRIEL), A. Mamelli, M. Russo (HPE), N. Weiss (ELTA), B. Pacheco (INOV), O. Segou (NCRSD), J. Beaume (THA), F. Custodio (VIS)
Submission date:	<submission date here>
Version number:	1.00 **Status:** Final

Grant Agreement N°:	653618
Project Acronym:	DOGANA
Project Title:	Advanced Social Engineering and Vulnerability Assessment Framework
Call identifier:	H2020-DS-06-2014-1
Instrument:	IA
Thematic Priority:	Trustworthy ICT
Start date of the project:	September 1st, 2015
Duration:	36 months

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Horizon 2020 European Union Funding for Research & Innovation

Project co-funded by the European Commission under the Horizon 2020 Programme.

Revision History

Revision	Date	Who	Description
0.00	23/05/2016	C. Dambra	D3.1 template
0.01	02/06/2016	C. Dambra	First full draft with tools evaluations from partners of Task 3.1
0.02	27/06/2016	C. Dambra	Final draft ready for review
0.03	29-30/05/2016	A. Poitevin	Linguistic Review
0.04	01/07/2016	C. Dambra	Updated with internal reviewers' comments (M. Busch and X. Letizia)
1.00	03/07/2016	C. Dambra	Final version ready to be submitted to EC

Quality Control

Role	Date	Who	Approved/Comment

Disclaimer:

Table of Contents

List of figures

List of Tables

Definitions and acronyms

Term	Definition
API	Application Programming Interface
HAV	Human Attack Vector
IG	Information Gathering
IGAS	Information Gathering and Analysis Services
N/A	Not Available
OSINT	Open Source INTelligence
PHI	Protected Health Information
PII	Personally Identifiable Information
SDVA	Social-Driven Vulnerability Analysis
SMS	Short Message Service
SN	Social Network
SQL	Structured Query Language
SW	Software
TAHP	Tools for the Attack and Hook Preparation
TEAT	Tools for the Execution of the Attack
TIAR	Tools for the Information Aggregation and Reporting
UC	Use Case
VCS	Victim Communication Stack
XSS	Cross-Site Scripting

1 Executive Summary

The scope of Deliverable D3.1 was to provide an up-to-date description of which are the existing tools from which the DOGANA development will benefit and the corresponding gap analysis.
The scope has been subdivided into the following steps:

1. To identify the open source (or similar) and commercially available tools to implement a Social-Driven Vulnerability Assessment (SDVA).
2. To implement a high-level ranking of the identified tools according to the experience of the partners involved.
3. For those that have reached a good ranking in the above step, to implement a detailed ranking based on the metrics identified in Deliverable D2.2.
4. To identify the major gaps for each phase of the SDVA.

Steps 1 and 2 have been implemented using an on-line questionnaire filled by all DOGANA partners, and have led to the identification of 48 different tools subdivided into the categories corresponding to the four main phases of an SDVA: information gathering (IGAS), attack and hook preparation (TAHP), attack execution (TEAT) and information aggregation and reporting (TIAR).
The tools have been subject to a detailed evaluation based on the metrics defined in Deliverable D2.2: only 32 tools have passed the threshold and have been selected for the gap analysis.
The gap analysis has drawn the following conclusions:

- The available tools in the open source (or similar) domain are sufficient for the attack preparation (TAHP) and execution (TEAT) phases only.
- The information gathering (IGAS) phase lacks tools for both the information gathering and data analysis functionalities.
    - For what concerns the information gathering functionality, the major gap is the absence of a performant tool to passively extract information from social networks. This gap shall be filled either by the adoption of commercial tools or by the development of the required tools within DOGANA.
    - For what concerns the data analysis functionality, it is necessary to perform a more detailed analysis of the requirements before defining the exact tool to be developed.
- Also information aggregation and reporting (TIAR) phase shows a lack of efficient and complete toolset. Here the recommendation is to consider generic tools available in the public domain for data analytics.
- In the TAHP phase there is the need to consider the SET tool despite its low ranking (only 0,53) since the tool offers some functionalities that may be important to consider for the next steps of DOGANA framework.

Finally, the tool's landscape will be updated in the Deliverable D3.1b "Revised report on existing tools, their evaluation and the gap to be filled by DOGANA development" due at M22.

2 Scope of Report

The scope of Deliverable D3.1 was to provide an up-to-date description of which are the existing tools from which the DOGANA development will benefit and the corresponding gap analysis.

The scope has been subdivided into the following steps:

5. To identify the open source (or similar) and commercially available tools to implement a Social-Driven Vulnerability Assessment (SDVA).
6. To implement a high-level ranking of the identified tools according to the experience of the partners involved.
7. For those that have reached a good ranking in the above step, to implement a detailed ranking based on the metrics identified in Deliverable D2.2.
8. To identify the major gaps for each phase of the SDVA.

This document will be updated across the project's life and reported at M22 as D3.1b "Revised report on existing tools, their evaluation and the gap to be filled by DOGANA development".

3 Identification of the tools

3.1 The categories of tools

As reported into the Deliverable D2.2 "DOGANA Metrics for the Evaluation of the Existing Tools", four different categories of tools have been identified, corresponding to the typical phases of a SDVA:

1. Information Gathering and Analysis Services (IGAS)
2. Tools for the Attack and Hook Preparation (TAHP)
3. Tools for the Execution of the Attack (TEAT)
4. Tools for the Information Aggregation and Reporting (TIAR)

The four different categories are described in Table 1 as described in D2.2.

Table 1 - The categories of SE tools and their purpose

Category	Purpose of the phase	Purpose of the tools
Information Gathering and Analysis Services (IGAS)	To do some research on the target and collect enough information to build a successful hook.	To harvest information from several sources, collect and organize the information to allow the attacker to perform searches and analyses.
Tools for the Attack and Hook Preparation (TAHP)	To set things up for a successful attack, create a scenario and build trust with several elements (pretexting, fake websites)	To help during the attack planning (selection of the best target, including possible strategies and identification of psychological levers), help during the scenario creation (pretexting, creation of fake website, fake profiles, creation of phishing emails, chat bots, etc.).
Tools for the Execution of the Attack (TEAT)	To maintain the charade and strengthen the control of the relationship long enough to extract the information and, optionally, close iteration without arousing suspicion. Create the actual attack vector (i.e., attach a malware to a file like a PDF, docx, etc.).	Creation of the actual attack vector by combining a malware with a premade document (prepared during the previous phase), by creating some "interesting SW" (e.g. fake patch/update for well-known SW, infected fake free SW, etc.) or by setting up some remote attack tool that can work once the victim as visited a link. Tools increasing the chances of success of the attack by obfuscating the malicious code or altering it to avoid any antivirus available to the victim. Tools that can help maintaining the charade: proxies, ambient sound generators or audio files (e.g. vishing), automatic message writer for social network (e.g. to plan interaction at scheduled times).

Category	Purpose of the phase	Purpose of the tools
Tools for the Information Aggregation and Reporting (TIAR)	To organize the collected data and extract only the useful information and to write down an attack report.	To collect and store a large amount of data of different formats (e.g. text, images, sounds, captured data traffic, etc.), to automatically generate full or partial reports on the attack providing the selected amount of information. To generate graphs and tables. The reports must be available in different formats

3.2 Ethical and privacy implications of the use of different categories of tools

DOGANA ethical and privacy implications are discussed in detail in both WP5 "Legal and ethical foundations" and WP9 "Ethics requirements".
In particular, while gathering and reporting information and executing attacks with (semi)automated tools, SDVA is facing, similarly to Big-Data analytics tools, the risk of collecting sensitive data and creating automatic data linkages between seemingly non-identifiable data to paint a broad portrait of an individual thus infringing civil rights.
None of the identified SDVA tools have specific (semi-)automated functions to detect and remove (stripping) sensitive information - e.g. Protected Health Information (PHI) and Personally Identifiable Information (PII) - from collected data sets.

The process of stripping datasets of all information that could identify individuals, either directly or through linkages to other datasets, is called **de-identification**.
Generated by the rapid development of the Big-Data analytics sector, de-identification discussions and approaches appeared quite recently in both academic papers (see for example [1], [2] and [3]) and guidelines from authorities, like the guideline developed by the U.S. Office of Civil Rights [4] for PHI data and by the U.S. National Institute of Standards and Technology (NIST) [5].

There are also some software products for de-identification and anonymisation of data sets to be considered as references for the development of the DOGANA toolbox:

- The IBM Universal De-identification Platform (UDiP)[1], still at the research level, offering de-identification of XML-based documents, DICOM objects, database query results, data in CSV format, spreadsheets and also free text anonymization.
- The Privacy Analytics® CORE[2] that combines risk-based de-identification and masking capabilities to de-identify personal information for data sets of all sizes.
- The HIPAA-compliant de-identification SW[3] from Universal Patient Key Inc. that combines and analyses healthcare data from many sources without compromising patient confidentiality.

[1] https://www.research.ibm.com/haifa/projects/software/udip/
[2] http://www.privacy-analytics.com/software/privacy-analytics-core/
[3] http://universalpatientkey.com/hipaa-de-identification-software/

A more thoroughly investigation on the de-identification and anonymisation aspects will be carried out in the WP3 tasks specifically addressing the implementation of the DOGANA tool chain.

Finally, before starting the integration and use of the considered SDVA tools, it is felt appropriate to ask stakeholders questions similar to the following that are strictly linked to the tools to be used during SDVA:

- Is it ethical to include private information about the workers in the SDVA?
- Is it ethical to mislead a participant when it comes to the goal of the test (*i.e.* social engineering awareness research)?
- Is it ethical to profile the employees through the collection of information (s)he spread on the network (the so called digital shadow)?
- Is it ethical to collect personal information of employees from social media platforms?
- Is it ethical to share information about employees with external third parties?
- Is it ethical to use fake profiles to deceive an employee in order to obtain more information about him?

The answers to the above questions may lead to the adoption or rejection of some of the tools from the toolkit in some organisations depending on national/international legislations and/or the employment contracts/conditions.

3.3 The on-line survey

3.3.1 The on-line questionnaire

An on-line questionnaire has been set-up to collect from all DOGANA partners the list of candidate tools to be used in WP3.
The questionnaire has been built using Google Forms© and it is visible in Appendix 1.

3.3.2 The results of the on-line survey

The on-line survey has received 49 responses from 16 different participants. Out of the 49 tools identified only one duplication was present: the list of the 48 tools is available in Table 2.
The 48 identified tools are subdivided into the categories identified in section 3.1 as described in Figure 1 (some of the tools belong to more than one single category).

Table 2 - List of identified SE tools

Name of the proposed tool	Official web site of the proposed tool	Which category do you think the proposed tool belongs to?
Metasploit	http://www.metasploit.com/	Attack execution tools
Maltego	https://www.paterva.com/web6/	Information gathering services

Name of the proposed tool	Official web site of the proposed tool	Which category do you think the proposed tool belongs to?
SET (Social Engineering Toolkit)	https://www.trustedsec.com/social-engineer-toolkit/	Attack and hook preparation tools, Attack execution tools
Browser Exploitation Framework (BeEF)	http://beefproject.com/	Attack execution tools
Phishing Frenzy	https://www.phishingfrenzy.com/	Attack and hook preparation tools, Attack execution tools, Information aggregation and reporting tools
The Harvester	https://code.google.com/p/theharvester/	Information gathering services
Lumify	http://lumify.io/	Information aggregation and reporting tools
Apache Zeppelin	http://zeppelin-project.org/	Information aggregation and reporting tools
Elasticsearch	https://www.elastic.co/products/elasticsearch	Information aggregation and reporting tools
Recon-ng	https://bitbucket.org/LaNMaSteR53/recon-ng	Information gathering services
SpeedPhishing Framework (SPF)	https://github.com/tatanus/SPF	Attack and hook preparation tools, Attack execution tools, attack simulation tool
Lucy	http://phishing-server.com	attack simulation and testing
QuickJack	http://samy.pl/quickjack/	Attack execution tools
Social Engineering Toolkit (SET)	https://www.trustedsec.com/social-engineer-toolkit/	Attack and hook preparation tools, Attack execution tools
gophish	https://getgophish.com/	Attack and hook preparation tools, Attack execution tools, Information aggregation and reporting tools
CreePy	http://www.geocreepy.com	Information gathering services, Information aggregation and reporting tools
FullContact	https://www.fullcontact.com	Information gathering services, Information aggregation and reporting tools
FOCA	https://www.elevenpaths.com/labstools/foca/	Information gathering services, Information aggregation and reporting tools
Scythe	https://github.com/ChrisJohnRiley/Scythe	Information gathering services
Kali Linux	https://www.kali.org/	Attack and hook preparation tools
social-searcher	http://www.social-searcher.com	Information gathering services
basKet Note Pads	http://basket.kde.org/	Information aggregation and reporting tools

Name of the proposed tool	Official web site of the proposed tool	Which category do you think the proposed tool belongs to?
Dradis	http://dradisframework.org	Information aggregation and reporting tools
Dan's Tools - Javascript Obfuscator	http://www.danstools.com/javascript-obfuscate/index.php	Attack and hook preparation tools
Dan's Tools - Javascript Minifier	http://www.danstools.com/javascript-minify/	Attack and hook preparation tools
Dan's Tools - CSS Minifier	http://www.cleancss.com/css-minify/	Attack and hook preparation tools
Selenium	http://www.seleniumhq.org/	Information gathering services, Attack execution tools
HTTrack	https://www.httrack.com/	Information gathering services, Attack and hook preparation tools, Attack execution tools
peekyou.com; zoominfo.com	peekyou.com zoominfo.com	Information gathering services
OWASP Zed Attack Proxy Project	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	Attack and hook preparation tools, Attack execution tools
Facebrok	https://sourceforge.net/projects/facebrok/	Information gathering services
S.E.F. - Social Engineering Framework	http://spl0it.org/projects/sef.html	Information gathering services, System integration, testing and maintaining tools
GeoTweet	http://geotweet.altervista.org/	Information gathering services
SimplyEmail	https://github.com/killswitch-GUI/SimplyEmail	Information gathering services
Pupy	https://github.com/n1nj4sec/pupy	Attack execution tools
ATSCAN	https://github.com/AlisamTechnology/ATSCAN	Information gathering services
Spiderfoot	http://www.spiderfoot.net/	Information gathering services
SEES (Social Engineering Attack/Audit Tool for Spear Phishing)	https://github.com/galkan/sees	Attack and hook preparation tools
WifiPhisher	https://github.com/sophron/wifiphisher	Attack and hook preparation tools, Attack execution tools
PyPhisher	http://sneakerhax.com/pyphisher/	Attack and hook preparation tools, Attack execution tools
sptoolkit	www.sptoolkit.com	Information gathering services, Attack and hook preparation tools, Attack execution tools

Name of the proposed tool	Official web site of the proposed tool	Which category do you think the proposed tool belongs to?
Automater	http://www.tekdefense.com/automater/	Information gathering services, System integration, testing and maintaining tools
URLCrazy	http://www.morningstarsecurity.com/research/urlcrazy	Information gathering services
Metagoofil	http://www.edge-security.com/metagoofil.php	Information gathering services
Twoif	https://digi.ninja/projects/twofi.php	Information gathering services
Inteltechniques (API Social Network)	https://inteltechniques.com/intel/menu.html	Information gathering services
Phish5	https://phish5.com/	Attack and hook preparation tools, Attack execution tools, Information aggregation and reporting tools
SecurityIQ	https://securityiq.infosecinstitute.com	Attack and hook preparation tools, Attack execution tools, Information aggregation and reporting tools

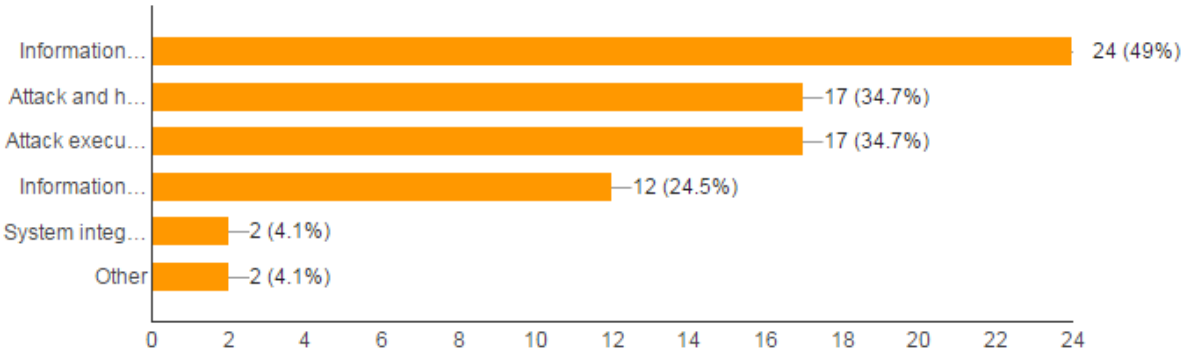

Figure 1 - The number of identified tools per category

The most populated category has been the information gathering (IGAS at 49%) phase, followed by the attack and hook preparation (TAHP) and the attack execution (TEAT) categories (34,7%) phases and finally by the information aggregation phase (24,5%).

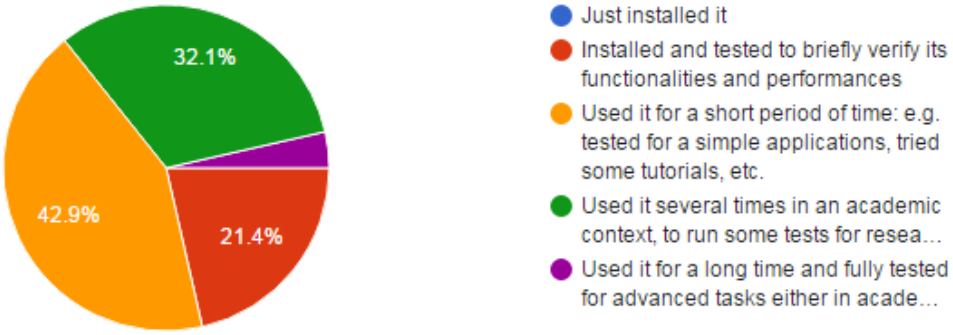

Figure 2 - The familiarity of the respondents with the SE tools

Respondents have been interviewed about their specific knowledge of the identified tool (see Figure 2 for the related statistics) and, in case of good familiarity due to direct usage or knowledge from literature review, they have been asked to provide a synthetic evaluation of the quality of the considered tool (the result of the synthetic evaluation is synthesised in Figure 3).

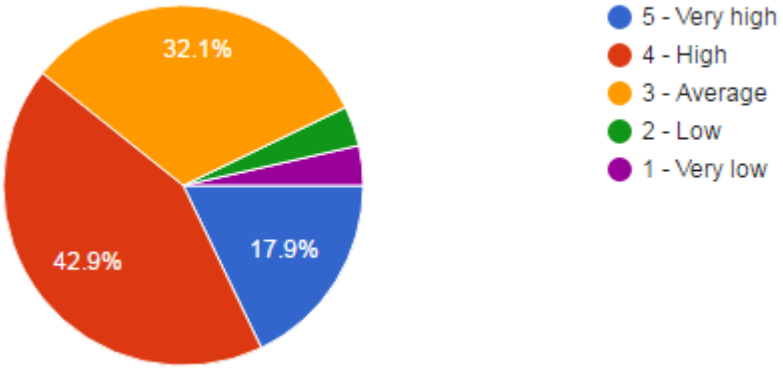

Figure 3 - The quality of the tested tool (only those that have been ranked)

On the basis of the synthetic evaluation, only the tools with a “Very High” or “High” quality evaluation have been shortlisted and passed to a more extensive evaluation.
This shortlist has been extended with the tools identified but not synthetically evaluated in the on-line survey. This was done to ensure that all identified tools have passed through at least one evaluation stage.

3.4 Tools selected for the evaluation

The process described in section 3.3 has led to the identification of 35 tools to be submitted to the detailed evaluation. The complete list for the detailed evaluation is available in Table 3.

Table 3 - SE tools selected for extensive evaluation

Name of the proposed tool	Tool's category	Synthetic evaluation
Twoif	Information gathering services	Very high
Inteltechniques (API Social Network)	Information gathering services	Very high
FullContact	Information gathering services, Information aggregation and reporting tools	Very high
Dan's Tools - Javascript Minifier	Attack and hook preparation tools	Very high
URLCrazy	Information gathering services	High
SimplyEmail	Information gathering services	High
Selenium	Information gathering services, Attack execution tools	High
SecurityIQ	Attack and hook preparation tools, Attack execution tools, Information aggregation and reporting tools	High
Pupy	Attack execution tools	High
Maltego	Information gathering services	High
FOCA	Information gathering services, Information aggregation and reporting tools	High
Dan's Tools - Javascript Obfuscator	Attack and hook preparation tools	High
CreePy	Information gathering services, Information aggregation and reporting tools	High
Browser Exploitation Framework (BeEF)	Attack execution tools	High
WifiPhisher	Attack and hook preparation tools, Attack execution tools	N/A
sptoolkit	Information gathering services, Attack and hook preparation tools, Attack execution tools	N/A
SpeedPhishing Framework (SPF)	Attack and hook preparation tools, Attack execution tools, attack simulation tool	N/A
Social Engineering Toolkit (SET)	Attack and hook preparation tools, Attack execution tools	N/A
SEES (Social Engineering Attack/Audit Tool for Spear Phishing)	Attack and hook preparation tools	N/A

Name of the proposed tool	Tool's category	Synthetic evaluation
S.E.F. - Social Engineering Framework	Information gathering services, System integration, testing and maintaining tools	N/A
Recon-ng	Information gathering services	N/A
QuickJack	Attack execution tools	N/A
PyPhisher	Attack and hook preparation tools, Attack execution tools	N/A
Phish5	Attack and hook preparation tools, Attack execution tools, Information aggregation and reporting tools	N/A
peekyou.com; zoominfo.com	Information gathering services	N/A
OWASP Zed Attack Proxy Project	Attack and hook preparation tools, Attack execution tools	N/A
Lumify	Information aggregation and reporting tools	N/A
Lucy	attack simulation and testing	N/A
gophish	Attack and hook preparation tools, Attack execution tools, Information aggregation and reporting tools	N/A
GeoTweet	Information gathering services	N/A
Facebrok	Information gathering services	N/A
Elasticsearch	Information aggregation and reporting tools	N/A
Dradis	Information aggregation and reporting tools	N/A
basKet Note Pads	Information aggregation and reporting tools	N/A
Apache Zeppelin	Information aggregation and reporting tools	N/A

The synthetic evaluation of the tools has given the following results:

- There is at least one tool for all the phases with a "Very High" ranking for all the phases but the attack execution.
- The attack execution tool phase, even if without a tool with a "Very High" quality evaluation, has at least two alternatives with "High" ranking.

More significant evaluations are reported in section 5 "Gaps to be filled".

4 Tools evaluation

4.1 The adopted metrics

Since the evaluation of the tools in Task 3.1 is essentially a desk evaluation based on available public data and partner's expertise, the metrics developed in D2.2 "DOGANA metrics for evaluation of the existing tools", have been analysed to verify their usability within Task 3.1 context.
The result of the metrics' usability analysis is reported in the following tables (from Table 5 to Table 8). As it is possible to see from the analysis all the metrics proposed in Deliverable D2.2 are usable for the desk evaluation of the tools in Task 3.1.

Table 4 - Metrics' usability – macro-group General

Macro-group General			
Metric Name	**Weight**	**Definition**	**Usable in D3.1**
Understandability	20%	How easy is it to understand and learn how to use the software and its functions?	Yes
Documentation	15%	Is user documentation comprehensive, appropriate, and well-structured?	Yes
Installability	10%	How straightforward is it to build and/or install on a supported system?	Yes
Identity	5%	Is Project/software identity clear and unique? Is it easy to understand who owns the project/software?	Yes
Support	10%	How easy is to understand how the project is run and the development of the software managed? Is there evidence of current/future community and developer support? Is there any evidence of current/future development?	Yes
Portability	5%	Is the software usable on multiple platforms?	Yes
Changeability	15%	How easy is it to understand and test at the source level? Is it easy to modify?	Yes, only if technical partner is an expert user of the tool
Interoperability	20%	Is it interoperable with other required/related software?	Yes

Table 5 - Metrics' usability – macro-group Technique IGAS

Macro-group Technique – IGAS – Information gathering analysis services			
Metric Name	**Weight**	**Definition**	**Usable in D3.1**
Number of sources	5%	Number of information sources like social media, documents, public web sites, blogs that the tool is capable to search for.	Yes
Performance	15%	A measure of software performance including minimum specific system requirements (the less the better) and time spent for information retrieval, processing and output (the less the better).	Yes, only if technical partner is an expert user of the tool
correlation capability	20%	Is there any information correlation functionality? If the answer is yes, how many of them and what is the relevance of the gathered information?	Yes
output quality	40%	How relevant is the collected information with the provided search criteria?	Yes, only if technical partner is an expert user of the tool
Information filtering	20%	Is there any information filtering functionality?	Yes

Table 6 - Metrics' usability – macro-group Technique TAHP

Macro-group Technique – TAHP – Tools for the attack and hook preparation			
Metric Name	**Weight**	**Definition**	**Usable in D3.1**
Automation	20%	What is the level of automation in its functions? For example, in identifying potential targets, bypassing security challenges, interacting with a “chat environment”.	Yes
Templating	25%	When it comes to create fake identities, fake profiles or custom made fake web pages, what is the available level of customization? Is it possible to provide different templates or is there only a limited set of premade resources?	Yes
Impact	20%	Are the most famous social networks and communities included among the exploitable	Yes

Macro-group Technique – TAHP – Tools for the attack and hook preparation			
Metric Name	**Weight**	**Definition**	**Usable in D3.1**
		ones? Are there premade versions of famous web sites and/or logos?	
Level of variety of the target	10%	How many target social networks, communities and web sites can be targeted/exploited? Do the targets belong to just one category (e.g. only social networks, only chats, etc.) or multiple ones?	Yes
Properties of the fake entity that has been created	25%	How good is the tool in emulating human behavior (e.g. chat skills, fake profile creation, etc.) or web pages (e.g. cloning a web site, writing fake emails, etc.).	Yes, only if technical partner is an expert user of the tool

Table 7 - Metrics' usability – macro-group Technique TEAT

Macro-group Technique – TEAT – Tools for the Execution of the attack			
Metric Name	**Weight**	**Definition**	**Usable in D3.1**
Multi-attack availability and combination	30%	What is the range of attack vectors and strategies offered by the tool? Is it possible to combine different kind of attacks together? Is it possible to create sequences of attacks?	Yes
Automation	30%	Is it possible to automatize the attacking process, either as a whole or in single steps?	Yes
Mass attack level	5%	Is there any functionality regarding the handling of mass attack campaigns? If the answer is “yes”, how many different targets can be attacked in an hour time?	Yes
Attacker's identity concealment and or spoofing	30%	Is it possible to hide attacker's identity or assume a fake one? How good are the spoofing/hiding capabilities of the software?	Yes
Persistence	5%	Is the tool able to provide some form of persistent access to the target after a successful attack execution?	Yes

Table 8 - Metrics' usability – macro-group Technique TIAR

Macro-group Technique – TIAR - Tools for the Information Aggregation and Reporting			
Metric Name	**Weight**	**Definition**	**Usable in D3.1**
Information structure	20%	Is the post-aggregation report structured in some way? Is data grouped in some nested way with top level data, second level data and so on?	Yes
Adaptability/Flexibility	20%	Is the tool usable with different programming languages and/or has any bindings in scripting languages?	Yes
Efficiency	20%	A measure of how fast the tool is, how thorough the examination is and how understandable are the results.	Yes, only if technical partner is an expert user of the tool
Reporting format	20%	Number of exporting formats available and the ability to deliver them fast and seamlessly	Yes
Data analytic	20%	The ability to explore data and reports in order to extract meaningful insights in the form of charts and graphs.	Yes, only if technical partner is an expert user of the tool

4.2 The evaluation tool

An Excel tool has been developed to allow an automated evaluation of the identified SE tools based on the metrics described in section 4.1. A printout of the Excel tool is available in Appendix 2.
The tool automatically computes the ranking for the different phases and allows the reviewers to add their comments on each section.

4.3 Evaluation of tools

The evaluation of the tool for each SDVA category based on the metrics described in section 4.1 is reported in the following sections. The evaluation ranking is the sum of the ranking received by each tool in the General macro-group and the ranking of the specific SDVA category):

$$R_{total} = R_{General} + R_{SDVA\ phase}$$

It is important to note that, for the sake of readability, only those tools with a ranking above a given threshold (varying for each SDVA category) are reported.
Each table reports:

- The name of the tool.
- The category of the SDVA phase(s) for which it has been designed.
- The ranking (the higher the value the better the tool).
- The notes from the evaluator.
- The nature of the tool: Open Source (OS) in its various forms and licences or Commercial (C).
- The adopted development language(s).

4.3.1 IGAS Evaluation

Table 9 - IGAS Evaluation synthesis

Name of the proposed tool	Category	Ranking	Notes from evaluator	Commercial/ Open Source	Development language(s)
SimplyEmail	IGAS	1,3	Efficient and not resource-hungry. Linux only (Mac OS not fully supported). It seems integrated with theHarvester, not considered in the tool list. See https://github.com/laramies/theHarvester	OS	Python
CreePy	IGAS, TIAR	1,18	Creepy is a geolocation OSINT Tool. No major drawbacks.	OS	Python

Name of the proposed tool	Category	Ranking	Notes from evaluator	Commercial/ Open Source	Development language(s)
Maltego	IGAS	1,15	Look at a lot of different sources. Can be extended with third-party plugins (transforms) such as socialnet by shadowdragon. Not open source.	C	Not applicable
Inteltechniques (API Social Network)	IGAS, TIAR	1,15	It is a website that groups a lot of functionalities useful for OSINT resources. It could be a very useful resource for learning how to interact directly with public available API of lots of different sources.	OS	Web API
FOCA	IGAS, TIAR	1,10	Good performances but source code not available	C	Not applicable
Twoif	IGAS, TAHP, TEAT, TIAR	0,95	Given a list of twitter usernames the script will bring back approximately the last 500 tweets for each user and use those to create the list	OS	Ruby on Linux
Selenium	IGAS, TAHP, TEAT	0,90	Selenium is a suite for automated web functional testing. It could be used as a tool to find bugs and vulnerabilities in web application, both classical (SQL injection, XSS) and high level vulnerabilities (workflow based vulnerabilities, functional privilege escalation). It can be used also to automatically collect relevant information on web sites. API can be leveraged to perform advanced tasks and to integrate the tool capabilities in a complex workflow.	OS	Java, C#, Ruby, Python, JavaScript (Node) on all platforms
FullContact	IGAS, TIAR	0,75	Commercial product. No source code is provided	C	Not applicable

4.3.2 TAHP Evaluation

Table 10 - TAHP evaluation synthesis

Name of the proposed tool	Category	Ranking	Notes from evaluators	Commercial/ Open source	Development language(s)
gophish	TAHP, TEAT, TIAR	1,35	Attack vector based on email only. Otherwise no major drawbacks.	OS	Go
Lucy	TAHP, TEAT, TIAR	1,20	Commercial tool, Source code not available, multi-platform	C	Not applicable
URLCrazy	IGAS, TAHP, TEAT, TIAR	1,13	Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage. Linux only.	OS	Ruby on Linux
WifiPhisher	TAHP, TEAT	1,08	WifiPhisher is very different than the standard phishing tools that we deal with in DOGANA. Instead of sending emails, messages, posts or other social network communications it uses social engineering to trick a victim into revealing his/her WiFi and/or website. It uses community input and enhancements.	OS	Python
sptoolkit	TAHP, TEAT	0,93	Sptoolkit is designed as an education toolkit referring a user who has clicked on a phishing email to an educational web page regarding phishing. The tool is not designed to do any aggregation nor any reporting.	OS	PHP

Name of the proposed tool	Category	Ranking	Notes from evaluators	Commercial/ Open source	Development language(s)
QuickJack	IGAS, TAHP, TEAT	0,90	Click-jacking, Source code available, maintained by the author	OS	Web-based
Phish5	TAHP, TEAT, TIAR	0,80	Only for educational purposes. Commercial product.	C	Not applicable
PyPhisher	TAHP, TEAT	0,65	Despite the low score of this script it is a very simple basic email phishing script and as such may be useful as part of a more sophisticated phishing software tool.	OS	Python

4.3.3 TEAT Evaluation

Table 11 - TEAT evaluation synthesis

Name of the proposed tool	Category	Ranking	Notes from evaluators	Commercial/ Open source	Development language(s)
Browser Exploitation Framework (BeEF)	TEAT	1,625	Used mostly for recon, social engineering, network discovery and a vector for metasploit modules.	OS	Linux
Pupy	TEAT	1,575	Powerful remote administration tool. Can easily be combined with other tools. Open source.	OS	Python
Lucy	TAHP, TEAT, TIAR	1,50	Commercial tool, Source code not available, multi-platform	C	Not applicable

Name of the proposed tool	Category	Ranking	Notes from evaluators	Commercial/ Open source	Development language(s)
OWASP Zed Attack Proxy Project	TEAT	1,28	Easy to use tool for finding and exploiting classical and advanced web application vulnerabilities. It can be integrated into an attacking workflow both as a standalone application or via API. Highly customizable.	OS	Java - API available in JSON, HTML and XML
gophish	TAHP, TEAT, TIAR	1,23	Attack vector based on email only. Otherwise no major drawbacks.	OS	Go
Social Engineering Toolkit (SET)	TAHP, TEAT	1,00	Open source. Overall an interesting tool with a lot of potential as a hook preparation and execution of attack toolkit.	OS	Python
PyPhisher	TAHP, TEAT	0,90	Despite the low score of this script it is a very simple basic email phishing script and as such may be useful as part of a more sophisticated phishing software tool.	OS	Python
WifiPhisher	TAHP, TEAT	0,85	WifiPhisher is very different than the standard phishing tools that we deal with in DOGANA. Instead of sending emails, messages, posts or other social network communications it uses social engineering to trick a victim into revealing his/her WiFi and/or website. It uses community input and enhancements.	OS	Python
Phish5	TAHP, TEAT, TIAR	0,83	Only for educational purposes. Commercial product.	C	Not applicable

Name of the proposed tool	Category	Ranking	Notes from evaluators	Commercial/ Open source	Development language(s)
SpeedPhishing Framework (SPF)	TAHP, TEAT, TIAR	0,65	Python based tool.	OS	Python

4.3.4 TIAR Evaluation

Table 12 - TIAR evaluation synthesis

Name of the proposed tool	Category	Ranking	Notes from evaluators	Commercial/ Open source	Development language(s)
gophish	TAHP, TEAT, TIAR	1,70	Attack vector based on email only. Otherwise no major drawbacks.	OS	Go
Lucy	TAHP, TEAT, TIAR	1,35	Commercial tool, Source code not available, multi-platform	C	Not applicable
Apache Zeppelin	TIAR	1,125	Nice tools to extract data and represent in several charts formats	OS	Scala (with Apache Spark), SparkSQL, Markdown and Shell.
FullContact	TIAR	1,03	Commercial product. No source code is provided	C	Not applicable
CreePy	IGAS, TIAR	0,73	No major drawbacks.	OS	Python
Phish5	TAHP, TEAT, TIAR	0,63	Only for educational purposes. Commercial product.	C	Not applicable

5 Gaps to be filled

This section presents a high-level gap analysis of the proposed tools that are considered candidates to be integrated in the DOGANA tool-chain. This analysis is based on the expected functionalities of the DOGANA framework, according to the Use Cases (UCs) defined in Deliverable D2.4 "Architectural and design guidelines". Furthermore, it's important to underline that D2.4 is being finalized at the time of writing of this document so some aspects considered in this document may change due to other requirements not yet considered (e.g. the on-going ethical and legal aspects requirements collection).
For each phase of the DOGANA framework, the main functionalities derived from UCs have been identified and the following sections will present the analysis of the gaps and the related proposed actions to be implemented during the next stages of the DOGANA project with the related effort estimation.
A summary of the aspects that have emerged in this analysis is presented here below:

IGAS - **Information Gathering and Analysis Services**

- Identified tools only partially cover the proposed features for information gathering. In particular, there is a lack of tools for passive information gathering from Social Network.
- Due to the above-identified gap, it is suggested to extend the technology scouting on the existing tools, also considering the possibility to include commercial products and to investigate in Task 3.3 "Information gathering analysis services" the costs and benefits between the licencing of commercial products versus developments of missing tools.

TAHP - **Attack and Hook Preparation**

- Some functionalities (e.g. "Create SMS template" and "Create malicious file") are not fully covered by the proposed tools.
- It is probably necessary to increase development/integration effort on Task 3.4 "Tools for the attack and hook preparation" in order to fill this gap.

TEAT - **Attack execution**

- Globally there are sufficient high-quality tools for TEAT, in particular regarding email vector attacks allowing Task 3.5 "Tools for the Execution of the attack" to concentrate mostly on the integration of existing tools.

TIAR – **Information aggregation and reporting**

- The identified tools for this phase do not seem to be adequate for the DOGANA objectives.
- The technology scouting has to be extended to generic data analysis and visualization tools, which may allow to support e.g. the creation of dashboards.

Finally, at the end of this section, a brief analysis on the "documentation and interoperability" will be presented and this is going to be valid for all the above-described phases.

5.1 IGAS - Information Gathering and Analysis Services

The IGAS phase aims at collecting information about the SDVA targets and at analysing the collected data. The information gathering is strictly OSINT oriented and is subject to all legal and ethical limitations regarding data handling and collection. The data analysis aims at executing the loop described in the Social Engineering Attack Framework (i.e. Identify potential sources, gather information from sources, assess gathered information) without violating the "no interpersonal interaction" basic rule.
The following Table 13 highlights the gaps and the actions proposed for the main functionalities identified for this phase, derived from UCs defined in Deliverable D2.4 "Architectural and design guidelines".

Table 13. Gap analysis for IGAS phase

Functionality	Gap Analysis	Actions/Proposals	Effort estimation
Information Gathering	Many tools have been identified but do not fully cover this part of the toolchain. There are few IGAS tool with high rate and able to do a crucial phase like OSINT research on Social Networks (or Passive IG from SN). SN Elicitation and Active IG are not covered by the proposed tools (the related UCs may not be confirmed due other ongoing requirements). Regarding specialization UCs such as "Create list of employees", "Map digital domains" and "Collect company's information", there are tools like *SimpleMail* and *theHarvester*[4] (this one is not present on the list and probably should be) that may support the related features in the toolchain.	Since great attention has to be paid to the Passive IG from SN, it is proposed to both extend the tools scouting and to evaluate the possibility of new developments. Moreover, it is expected to have a substantial integration effort, due to the large variety of required functionalities and the heterogeneity of the development languages of the available tools. Regarding specialisation of features from UCs, such as "Map digital domains", tools like *DNSRecon*[5] and *Fierce*[6] may be considered in further evolution of this deliverable.	Medium/ High

[4] https://github.com/laramies/theHarvester
[5] https://github.com/darkoperator/dnsrecon
[6] https://github.com/mschwager/fierce

Functionality	Gap Analysis	Actions/Proposals	Effort estimation
Data Analysis	Some tools have a data analysis section allowing a minimal data filtering/visualization activity.	At this design stage, it is necessary to accurately define the requirements for the expected functionalities (included in Data Analysis), before evaluating the required actions. There is a high probability that a new development will be required.	Medium
Define information gathering boundaries	Some of the analysed tools provide limited features for boundaries definition, for example the possibility of selecting specific data source for crawling.	It will be necessary to develop an integrated functionality for defining boundaries for all the different tools included in DOGANA framework related to information gathering. Moreover, this function must be implemented with respect to legislation and company policies.	Medium

5.2 TAHP – Attack and Hook Preparation

TAHP phase is aimed at preparing both the attack and the required hook(s). This phase is clearly linked to the "Preparation" described in the Social Engineering Attack Framework and is heavily influenced by the information gathered during the previous phase.

Attack and Hook are "human-oriented", Human Attack Vector (HAV) creation is based on Victim Communication Stack (VCS) and the desired templates (for more information see Deliverable D4.1 "Human Attack Vectors in SE 2.0").

The following Table 14 describes the gap analysis.

Table 14. Gap analysis for TAHP phase

Functionality	Gap Analysis	Actions/Proposals	Effort estimation
Define attack boundaries	The analysed tools provide some basic features for defining attack boundaries.	This feature is important because it allows to define the scope of the attack simulation. Given the current landscape of tools It may be necessary to either improve current features of existing tools or to develop a new tool.	Medium
Prepare hook	This phase is almost fully covered by the tools provided at least for what concerns the email attack vector. Actions like **"**Create email template" and "Create and publish website" are properly implemented in tools like *goPhish* and *Phish5* with a complete GUI. Functionalities for creating other kind of attacks like "Create SMS template" and "Create malicious file" are partially included with tool like *SET* with a more basic interaction (i.e. command-line tool). "Create SN message/post template" is not covered by the analysed tools. Moreover, at this stage is not sure that this functionality will be confirmed or not.	Functionalities related to some specialised UCs ("Create emails", "Create SMS template", etc..) must be uniformed and better integrated into each other. Functionalities that are not totally covered (e.g. "Create SMS template", "Create malicious file") will probably need more development effort (if they will be confirmed). The SET tool doesn't emerge in the tools evaluation's process due its low ranking (only 0,53). However, the tool offers some great functionalities that may be important to consider for the next steps of DOGANA framework.	Medium

Functionality	Gap Analysis	Actions/Proposals	Effort estimation
Prepare attack automation or scenario	Automation of this phase (e.g. if a target does not open an email, the tool automatically tries to sends an SMS to his phone number) is not performed by the identified tools	The automation of attack intended for the DOGANA framework is a particular feature, that will probably be fully implemented from scratch.	High

5.3 TEAT – Attack execution

The TEAT phase is aimed at performing the attack. This phase is clearly linked to several parts of the Social Engineering Attack Framework: “Develop relationship”, “Exploit relationship” and “Debrief”. Attack Execution includes baiting the target, selecting an attack vector, launching and monitoring an attack. An attack can be either “single” or “composite”.
The following Table 15 describes the gap analysis for this phase

Table 15. Gap analysis for TEAT phase

Functionality	Gap Analysis	Actions/Proposals	Effort estimation
Select attack vector	All tools (e.g. *SET*) providing different attack vectors have the possibility to choose how to attack a target.	It is important to choose the different attack vectors and integrate them in DOGANA. The required functionality can be either obtained by integrating and improving the existing tools or developed from scratch using, as examples, those available in the existing tools.	Medium
Bait the target	This UC is well covered by the proposed tools.	Despite the fact that some tools already provide this feature, it will probably be necessary to integrate functionalities for each specific attack vector, as defined in specialized UCs (“Launch phishing attack”, “Launch SMS attack” and “Launch website attack”).	Low/ Medium
Attack monitoring	Some tools like *goPhish* provide the live monitoring functionality.	Starting from the existing tools, this UC needs to be further implemented to cover the missing aspects before being integrated in the DOGANA framework.	Medium

5.4 TIAR – Information aggregation and reporting

The TIAR phase is aimed at collecting and organising the results of the attack, by creating reports and statistics. This phase focuses on result's handling with typical functionalities like: data aggregation, import/export, statistics generation, query result, data filtering.

The following Table 16 describes the gap analysis.

Table 16. Gap analysis for TIAR phase

Functionality	Gap Description	Actions/Proposals	Effort estimation
Information aggregation and reporting	This phase is partially covered because the identified tools for this stage do not seem to be adequate for the whole purpose of DOGANA. Anyways some tools, like *goPhish,* have the possibility to view the result of a specific phishing campaign already done.	In order to obtain a complete functionality for information aggregation and reporting, it will be probably necessary to develop a specific interface. For this purpose, it is conceivable to use specific tools for data visualization and analysis like: - *Tableau*[7] - *QlikView*[8] - *Microsoft Power BI*[9]	Medium/High

5.5 Documentation and interoperability of tools

As one may expect, some tools are better documented than others and this could impact the effort estimation during a deeper testing of a particular offered feature. Furthermore, it is expected to deal with different categories of tools (scripting, web-based, etc.) also developed with different programming languages (Python, Ruby, etc.).
The following Table 17 describes the gap analysis for documentation and interoperability.

[7] http://www.tableau.com/
[8] http://www.qlik.com/
[9] https://powerbi.microsoft.com/

Table 17. Gap analysis for documentation and interoperability

Functionality	Gap Description	Actions/Proposals	Effort estimation
Documentation	As expected, some tools are better documented than other.	This different level of documentation could impact the effort necessary to evaluate the tools, e.g. a deeper test of a particular feature.	Low
Interoperability	There are different categories of tools (scripting, web-based, etc.) also developed with different programming languages (Python, Ruby, etc.).	The difference between tools analysed which may be included in the toolchain raises an important requirement for the architecture design. It is important to design a "tools-independent" architecture that provides interfaces able to interact with different categories of tools, possibly developed with different programming languages.	Medium

6 Conclusions

This document offers an interesting landscape of candidate tools for all the phases of a SDVA. From the analysis of the gaps the following points emerge:

- The available tools in the open source (or similar) domain are sufficient only for the attack preparation (TAHP) and execution (TEAT) phases.
- The information gathering (IGAS) phase lacks tools for both the information gathering and data analysis functionalities.
    - For what concerns the information gathering functionality, the major gap is the absence of a performant tool to passively extract information from social networks. This gap is to be filled either by the adoption of commercial tools or by the development of the required tools within DOGANA. The decision will be taken in Task 3.3 “Information gathering analysis services” with the continuous support of Task 3.1 in scouting possible new tools.
    - For what concerns the data analysis functionality, it is necessary to perform a more detailed analysis of the requirements in Task 3.3 before defining the exact tool to be developed.
- The information aggregation and reporting (TIAR) phase shows a lack of efficient and complete tools. Here the recommendation is to consider generic tools available in the public domain for data analytics.
- In the TAHP phase there is the need to consider the SET tool despite its low ranking (only 0,53) since the tool offers some great functionalities that may be important to consider for the next steps of DOGANA framework.

Finally, it is worth mentioning that it is planned to provide an update of the tools’ landscape and to revise the gap in the Deliverable D3.1b “Revised report on existing tools, their evaluation and the gap to be filled by DOGANA development” due at M22. This update will allow to monitor the evolution of the tools and, if necessary, to take into considerations possible evolutions of the SDVA scenarios both from the technical and the ethical point of view.

7 Ethical and privacy compliance checklist

	Risk (as described in D1.3 Section 3)	Requirement	Argumentation
Stage 1. Preliminary measures	The research results may have a severe negative impact on the human rights of individuals or groups (e.g. privacy, discrimination, stigmatization)	Risk mitigation, such as • a human rights impact assessment • the involvement of human rights experts in the research • training of personnel and/or technological safeguards Risk-assessment • details on how the research could affect human rights • details on the measures taken to prevent abuse	As this deliverable includes a critical review of existing software tools, it does not have an immediate legal and ethical impact. On the contrary the review may highlight tools having potential privacy or ethical impacts. The self-assessment in D3.1 will be conducted in line with and limited to the metrics described in D2.2. Since D2.2 has no ethical metric, D3.1 includes a brief analysis of the ethical and privacy impacts of the tools (see section 3.2).
	The research has the potential to be abused or misused	Risk-assessment • details on the measures taken to prevent abuse • if applicable, copies of personnel security clearances	See above.

Stage 2. Research considerations	The research may have a negative impact on human rights	Research methods for correct interpretation of the research results should be provided	See above.
	Confidential DOGANA internal information could be disclosed through the research	Caution when publishing or otherwise disseminating those results. Compliance with non-disclosure agreements and other (internal) contracts in relation to the research data Compliance with the technical partner couples relationships	D2.3 is a confidential document and the proposed methodology will be used, within the project, only on partners' information and data. Consequently, there is no risk of disclosing confidential information outside DOGANA.
Stage 3. Post measures	Data loss	Detailed measures on the storage-assessment (including access control) Assessment by the end-users according to WP7 and considering the three different sharing levels	The information included in the deliverable and the concerning related activities are neither personal data nor critical data for partners. Therefore, there is no need to define additional countermeasures to avoid data loss, others than the ones already in place for the storage of the DOGANA deliverables.
	The research may have a negative impact on human rights	Caution when publishing or otherwise disseminating those results Statement that no data other than the results of the project (software and documentation) will be exported to non-EU Member States	

8 References

[1] Daries, J.P., Reich, J., Waldo, J., Young, E.M., Whittinghill, J., Ho, A.D., Seaton, D.T. and Chuang, I. (2014) 'Privacy, anonymity, and big data in the social sciences', *Communications of the ACM*, 57(9), pp. 56–63. doi: 10.1145/2643132.

[2] Narayanan, A., Huey, J. and Felten, E.W. (2016) *A precautionary approach to big data privacy*. Springer Science + Business Media.

[3] Sedayao, J., Bhardwaj, R. and Gorade, N. (2014) 'Making big data, privacy, and Anonymization work together in the enterprise: Experiences and issues', *2014 IEEE International Congress on Big Data*. doi: 10.1109/bigdata.congress.2014.92.

[4] U.S. Office for Civil Rights (OCR) (2012) *Guidance on de-identification of protected health information guidance regarding methods for de-identification of protected health information in accordance with the health insurance portability and accountability act (HIPAA) privacy rule*.

[5] Garfinkel, S.L. (2015) *De-identification of personal information*. National Institute of Standards and Technology (NIST).

Appendix 1 – The on-line survey template

DOGANA Tools Survey

Task 3,1 - Evaluation of the landscape and Gap Analysis

*Required

1. **Your Name and Surname** *

2. **Your Organisation** *

3. **Name of the proposed tool** *

4. **Official web site of the proposed tool** *

5. **Which category do you think the proposed tool belongs to?** *

Please select one or more options below
Tick all that apply.

- [ ] Information gathering services
- [ ] Attack and hook preparation tools
- [ ] Attack execution tools
- [ ] Information aggregation and reporting tools
- [ ] System integration, testing and maintaining tools
- [ ] Other: _____

6. **Short description of the proposed tool**

7. **Have you previously used the proposed tool?** *
Mark only one oval.

- ◯ Yes *Skip to question 8.*
- ◯ No *Skip to question 11.*

Experience with the proposed tool

8. **What's your personal experience with the proposed tool?** *
Mark only one oval.

- ◯ Just installed it
- ◯ Installed and tested to briefly verify its functionalities and performances
- ◯ Used it for a short period of time: e.g. tested for a simple applications, tried some tutorials, etc.
- ◯ Used it several times in an academic context, to run some tests for research purposes
- ◯ Used it for a long time and fully tested for advanced tasks either in academic or professional context, I am expert with it and/or I know it very well.

9. **How would you rate the proposed tool performances on a scale from 1 to 5 (5 being the better score) ?** *
Mark only one oval.

- ◯ 5 – Very high
- ◯ 4 – High
- ◯ 3 – Average
- ◯ 2 – Low
- ◯ 1 – Very low

10. **Do you have any additional information about the proposed tool? (e.g. OS which it has been tested on, known bugs, strengths and weaknesses, opinions regarding the category it belongs too, etc.).**

Optional questions on the proposed tool

This part of the questionnaire is optional - so please fill it if it is easy for you to collect the required information

General information

11. **Author**

12. **Direct link to the proposed tool**

13. **Current version of the proposed tool**

14. **Supported OS / Platform (e.g, Linux, Windows, etc,)**

15. **Supported Languages (e.g, C++, Python, Perl, etc,)**

16. **Exporting options and formats**

Other technical information

Appendix 2 – The Excel-based evaluation tool

DOGANA Tools' Evaluation Tool

			Scoring criteria
Tool name			+1,0 - Fully satisfies the basic requirements
Tool web-site			+0,5 - Fully satisfies basic requirements but needs minimal adaptation effort
Evaluator's name			0 - Satisfies basic requirements but needs some modification
Evaluator's organisation			-0,5 - Partially dissatisfies the basic requirements.
DOGANA phase			-1,0 - Fully dissatisfies the basic requirements.
Overall score	0,00		

General

Metric Name	Weight	Definition	Score	Comment
Understandability	20%	How easy is it to understand and learn how to use the software and its functions?		
Documentation	15%	Is user documentation comprehensive, appropriate, and well-structured?		
Installability	10%	How straightforward is it to build and/or install on a supported system?		
Identity	5%	Is Project/software identity clear and unique? Is it easy to understand who owns the project/software?		
Support	10%	How easy is to understand how the project is run and the development of the software managed? Is there evidence of current/future community and developer support? Is there any evidence of current/future development?		
Portability	5%	Is the software usable on multiple platforms?		
Changeability	15%	How easy is it to understand and test at the source level? Is it easy to modify?		
Interoperability	20%	Is it interoperable with other required/related software?		
		Total score for General section	0,00	

Page 1 of 3

DOGANA Tools' Evaluation Tool

IGAS – Information Gathering Analysis Services				
Metric Name	Weight	Definition	Score	Comment
Number of sources	5%	Number of information sources like social media, documents, public web sites, blogs that the tool is capable to search for.		
Performance	15%	A measure of software performance including minimum specific system requirements (the less the better) and time spent for information retrieval, processing and output (the less the better).		
Correlation capability	20%	Is there any information correlation functionality? If the answer is yes, how many of them and what is the relevance of the gathered information?		
Output quality	40%	How relevant is the retrieved information with provided search criteria?		
Information filtering	20%	Is there any information filtering functionality?		
		Total score for IGAS section	0,00	

TAHP – Tools for the attack and hook preparation				
Metric Name	Weight	Definition	Score	Comment
Automation	20%	What is the level of automation in its functions? For example, in identifying potential targets, bypassing security challenges, interacting with a "chat environment".		
Templating	25%	When it comes to create fake identities, fake profiles or custom made fake web pages, what is the available level of customization? Is it possible to provide different templates or is there only a limited set of premade resources?		
Impact	20%	Are the most famous social networks and communities included among the exploitable ones? Are there premade versions of famous web sites and/or logos?		
Level of variety of the target	10%	How many target social networks, communities and web sites can be targeted/exploited? Do the targets belong to just one category (e.g. only social networks, only chats, etc.) or multiple ones?		
Properties of the fake entity that has been created	25%	How good is the tool in emulating human behavior (e.g. chat skills, fake profile creation, etc.) or web pages (e.g. cloning a web site, writing fake emails, etc.).		
		Total score for TAHP section	0,00	

Page 2 of 3

DOGANA Tools' Evaluation Tool

TEAT – Tools for the Execution of the ATtack

Metric Name	Weight	Definition	Score	Comment
Multi-attack availability and combination	30%	What is the range of attack vectors and strategies offered by the tool? Is it possible to combine different kind of attacks together? Is it possible to create sequences of attacks?		
Automation	30%	Is it possible to automatize the attacking process, either as a whole or single steps of it?		
Mass attack level	5%	Is there any functionality regarding the handling of mass attack campaigns? If the answer is "yes", how many different targets can be attacked in an hour time?		
Attacker's identity concealment and or spoofing	30%	Is it possible to hide attacker's identity or assume a fake one? How good are the spoofing/hiding capabilities of the software?		
Persistence	5%	Is the tool able to provide some form of persistent access to the target after a successful attack execution?		
		Total score for TEAT section	**0,00**	

TIAR - Tools for the Information Aggregation and Reporting

Metric Name	Weight	Definition	Score	Comment
Information structure	20%	Is the post-aggregation report structured in some way? Is data grouped in some nested way with top level data, second level data and so on?		
Adaptability/ Flexibility	20%	Is the tool usable with different programming languages and/or has any bindings in scripting languages?		
Efficiency	20%	A measure of how fast is the tool, how thorough is the examination and how understandable are the results.		
Reporting format	20%	Number of exporting formats available and ability in deliver them fast and without technical problems.		
Data analytic	20%	The ability of exploring data and reports in order to extract meaningful insights in the form of charts and graphs.		
		Total score for TIAR section	**0,00**	

Further comments.

Page 3 of 3