DarkComet Tracker

Project Management

Bachelor Thesis

Degree programme:	Bachelor of Science in Computer Science
Authors:	Rosalie Truong, Nils Stampfli, Sandro Tiago Carlao
Thesis advisor:	Dr. Endre Bangerter, Reto Inversini
Expert:	Dr. Igor Metz
Date:	16/03/2018

Contents

1 Introduction

In year 2017, the paper "*To Catch a Ratter: Monitoring the Behavior of Amateur Dark Comet RAT Operators in the Wild*", has been published and provides the first reference for the work we are doing today as our Bachelor Thesis.

RATs are the so-called Remote Access Trojans. They allow the people behind them, also called Operators, to remotely access to a victims computer, that has previously been infected. This can then be spied on, manipulated or totally taken over. Several RATs are available for free or at low prices on the Internet. The main topic of our work is the RAT DarkComet.

RATs like DarkComet are mostly used because of their simplicity on doing very bad things. The reason for that is the easy user interface, developed so, that people with no large technical knowledge can use them. Because of that, on one side it has been used by teenagers, "just for fun" and on the other side by intelligences, in a context like the war in Syria. Over all, there is relatively little detailed and systematic knowledge about the use of RATs or the behavior of their Operators.

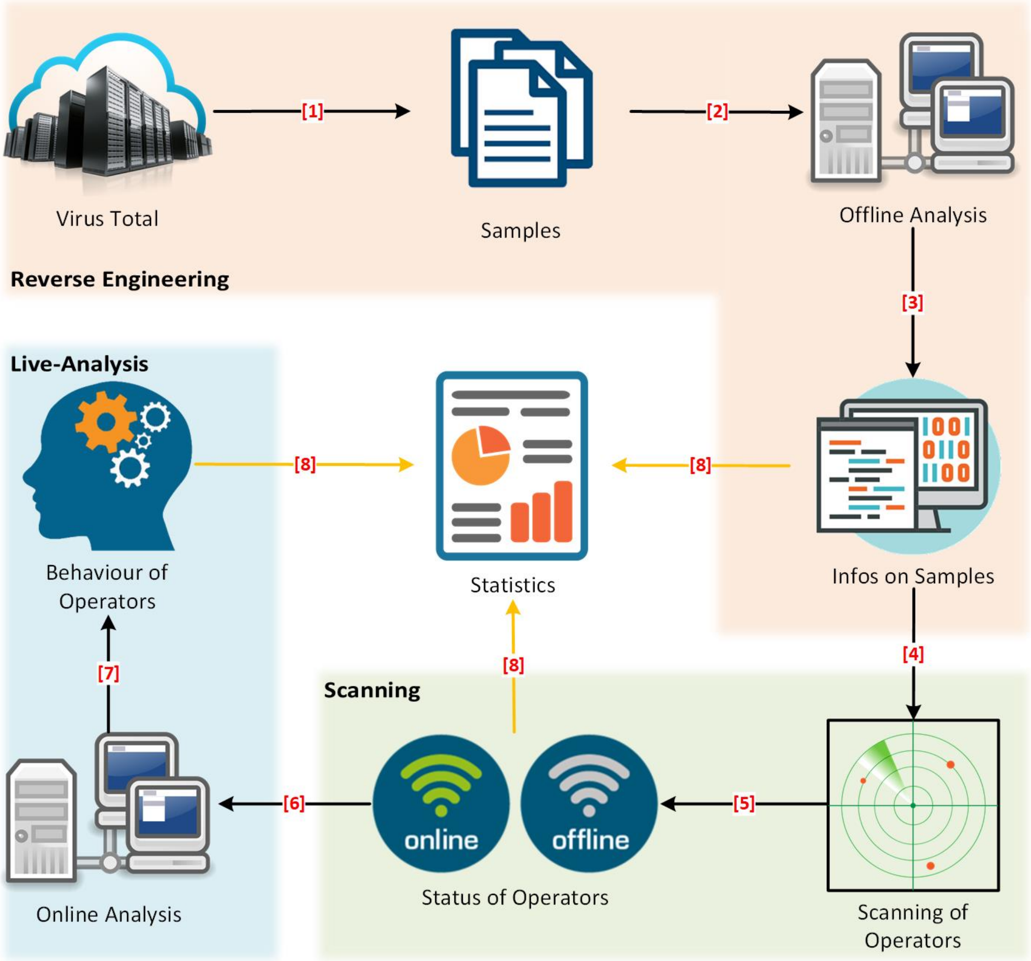
Remote Access Trojans should not be confused with the Remote Administration Tools, like TeamViewer, which represent the legal side of the application possibilities and will not be part of this work.

1.1 Main Goals & Motivation

The main goal of this project is the reproduction of the environment for the DarkComet-tracker, described in the paper "To Catch a Ratter". Where possible we like to improve the basic system and ideas. Using this tracker, we try to catch and understand the RAT DarkComet and so their operators.

The first part of the tracker consists of the reverse-engineering. With proper scripts and analysis, we extract information from a RAT-sample.
The second part is about the scanning-environment. With proper tools we track and monitor the operators of these RAT-samples.
The third part is about the analysis-environment. With an analysis-environment, we catch the operators online and live, to analyse their behaviour.
Finally, over all the obtained data, we do statistical analysis and categorization.

2 Data flow



[1] DarkComet samples are downloaded from Virus Total.
[2] Using the analysis-environment Cuckoo and with additional scripts, the samples are analysed offline.
[3] Base-information (at least IP and port) about the sample and the operator of the RAT are extracted.
[4] To catch the active operators we scan them, or more precisely we scan their IP-address.
[5] We try to get as much information about operators as we can, like geographical or activity information.
[6] If we know at least that an operator is active, we can begin an online analysis. But if we get a feeling of his behaviour, it is a lot easier to really catch him. For the online analysis we infect a Windows machine with the sample in a Cuckoo-environment.
[7] The actions of the operators are caught in order to analyse the behaviour of the operator.
[8] The results from each part (reverse engineering, scanning and live-analysis) are used to make some statistics and draw conclusions about the operators.

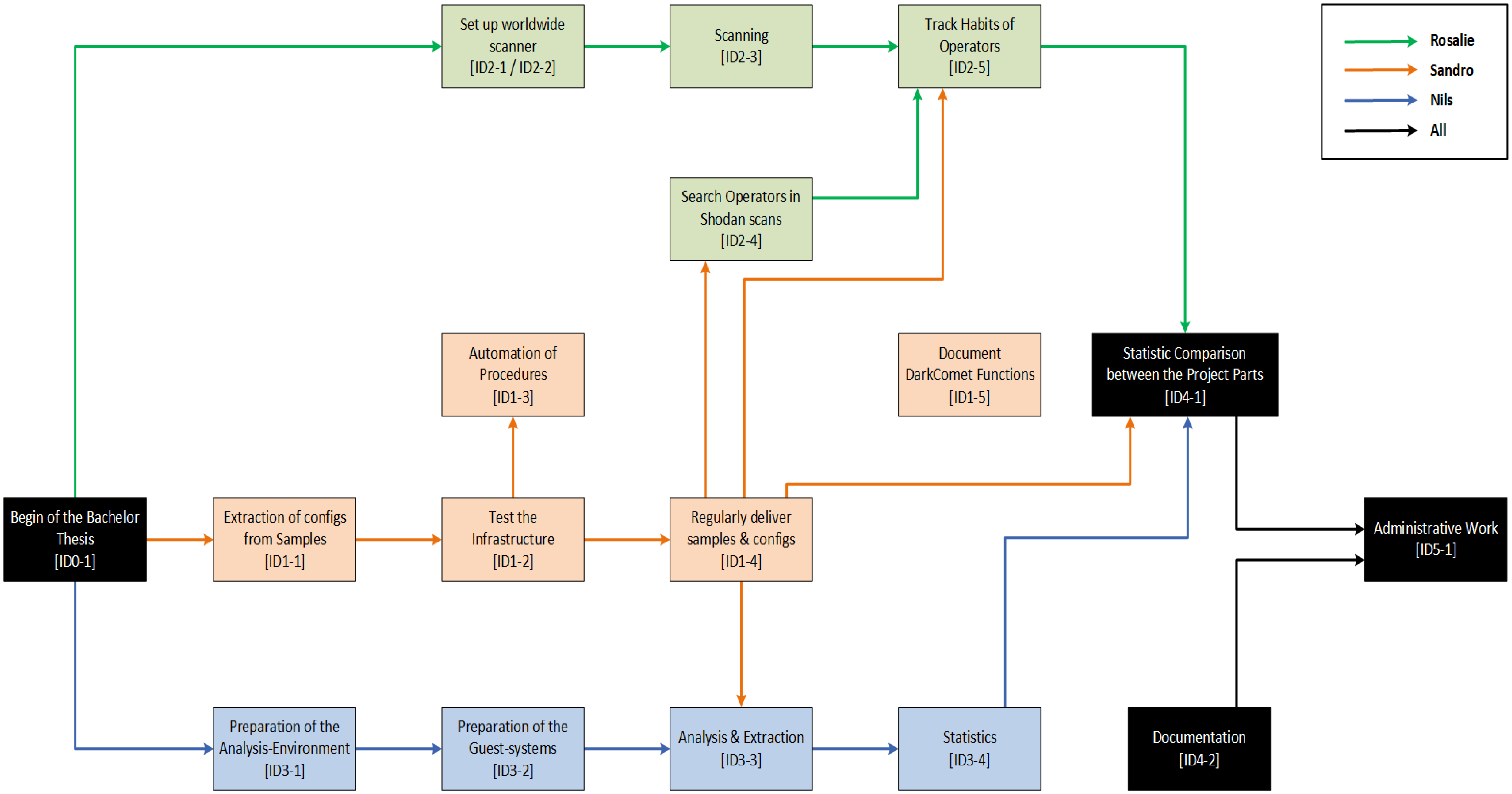
3 Work Packages

In the next table we define the Work Packages we intend to study and implement in the coming weeks. For each entry there is a unique ID number that is, per its definition, unique in the whole project. Moreover, each entry has a Task Title, a description and a field that defines if it necessary doing to accomplish that Task to accomplish the whole project. The colors in the table, as in the whole project, are there to indicate who is doing the Task in a more visual form than just writing the names: black stands for all (Rosalie, Sandro and Nils), orange stands for Sandro, green stands for Rosalie and blue stands for Nils.

ID-Nr.	Task Title	Description	Comment
ID0-1	Begin of the Bachelor thesis	Write and draw Project Management documents such as Data flow, goals and tasks description, Gannt chart	must
Reverse engineering			
ID1-1	Extraction of Config from Samples	Write a script for Cuckoo which uses volatility to recognize if a sample is a DarkComet and extract at least ip/hostname, port and password from the config.	Must
ID1-2	Test the Infrastructure	Do tests of cuckoo analyses with different types of samples (packed, unpacked, …), improve the stability and performance of the volatility script	Must
ID1-2.1	Yara Rules Quality Enhancement	Enhance the quality of Yara Rules, especially for DarkComet version 5 and newer. For a better quality search in Virtus Total.	Optional
ID1-3	Automation and Optimization of Procedures	Write a new script to automate the execution of cuckoo analyses, DarkComet Configuration extraction and statistics over password, port, and ip	Optional
ID1-3.1	Data Storage and Correlation	Automatically compare and correlate result data from analysis to find similarities and therefore enhance live analysis results quality.	Optional
ID1-4	Regularly deliver Samples & Configs	Regularly perform analyses with cuckoo on Samples downloaded from VirusTotal. Extract the config (ip, password, …) and pass them to my teammates	Must
ID1-5	Documentation of DarkComet Functions	For each function of DarkComet, capture the network flow to understand the commands, and draw a sequence diagram of the communication.	Must
Scanning			
ID2-1	Set up Scanner	Set up a scanner which can recognize DarkComet operators (NMap)	Must
ID2-2	Set up worldwide Scanner	Set up a scanner which as the capacity to scan the whole world in a reasonable time (Masscan, ZMap/ZGrab, or …)	Optional
ID2-3	Scanning	Perform scanning to find operators. The operators will be listed for further tasks.	Must

ID2-4	Search Operators in Shodan Scans	Search new operators through Shodan. The operators will be listed for further tasks. Search operators who use: • Default passwords • Common passwords	Must
ID2-5	Track Habits of Operators	Track the habits of the operators to respond on the question: When are they active? A list of the connection times will be created.	Must
Live-Analysis			
ID3-1	Preparation of the Analysis-Environment	• Prepare the Cuckoo-infrastructure, where a RAT-sample can be analysed • Configure an ip-table rule-set to allow online-analysis • Install & connect the environment to a BFH-separated network	Must
ID3-1.1	Additional Security Layer	Implement Suricata IDPS as additional security level for the whole environment and network.	Optional
ID3-2	Preparation of the Guest-System	Prepare a virtual Windows-7 guest, that is looking as real as possible, to cozen the operators during the analysis	Must
ID3-2.1	Additional Services	Prepare fake-webcam service, to cozen the operators even more	Optional
ID3-3	Analysis & Extraction	Do the analysis & extract information about the operator and their behavior, from the obtained data and the cuckoo-report automatically	Must
ID3-4	Statistics	Do statistical analysis of these extracted information about the operator and create a statistic overview → categorization	Must
ID4-1	Statistic Comparison between the Project-Parts	Analyse the relation between the statistical data of the live-analysis and the statistical data from the scanning-results and if possible, including the research-engineering	Must
ID4-2	Documentation	Main documentation of the project	Must
ID5-1	Administrative Work	Administrative tasks, presentations, Final Day, Film	Must

In the following diagram we draw the dependencies of the Tasks in the work packages. The colors simplify the overview of a complex process, in more sub processes necessary to accomplish the main goals. Each time an arrow is drawn from a task A to a task B, it means that the task B needs the task A to be accomplished to be able to start.


Rosalie
Sandro
Nils
All
Set up worldwide scanner [ID2-1 / ID2-2]
Scanning [ID2-3]
Track Habits of Operators [ID2-5]
Search Operators in Shodan scans [ID2-4]
Automation of Procedures [ID1-3]
Document DarkComet Functions [ID1-5]
Statistic Comparison between the Project Parts [ID4-1]
Begin of the Bachelor Thesis [ID0-1]
Extraction of configs from Samples [ID1-1]
Test the Infrastructure [ID1-2]
Regularly deliver samples & configs [ID1-4]
Administrative Work [ID5-1]
Preparation of the Analysis-Environment [ID3-1]
Preparation of the Guest-systems [ID3-2]
Analysis & Extraction [ID3-3]
Statistics [ID3-4]
Documentation [ID4-2]

4 Planning

For each work package, we define the tasks, duration, dates and amount of work per person. On the next page you find the graphical representation of this table. A more complete and complex version is available and can be asked by the Expert and the Advisers.

ID-Nr.	Work	Duration	Begin	End	Hours per Person	Total
ID0-1	Begin of the Bachelor thesis	1 week	19.02.2018	22.02.2018	24	72
1	**Reverse engineering**	**9 weeks**	**26.02.2018**	**03.05.2018**	**216**	**216**
ID1-1	Extraction of config from Samples	1 weeks	26.02.2018	01.03.2018	24	24
ID1-2	Test the Infrastructure	1 weeks	05.03.2018	08.03.2018	24	24
ID1-3	Automation of procedures	7 weeks	12.03.2018	03.05.2018	39	39
ID1-4	Regularly deliver samples & configs	7 weeks	12.03.2018	03.05.2018	39	39
ID1-5	Document DarkComet functions	4 weeks	03.04.2018	26.04.2018	90	90
2	**Scanning**	**9 weeks**	**26.02.2018**	**03.05.2018**	**216**	**216**
ID2-1 ID2-2	Set up worldwide scanner	3 weeks	26.02.2018	15.03.2018	60	60
ID2-3	Scanning	4 weeks	19.03.2018	19.04.2018	70	70
ID2-4	Search operators in Shodan scans	9 weeks	26.02.2018	03.05.2018	36	36
ID2-5	Track habits of operators	7 weeks	12.03.2018	03.05.2018	50	50
3	**Live-Analysis**	**9 weeks**	**26.02.2018**	**03.05.2018**	**216**	**216**
ID3-1	Preparation of the Analysis-Environment	3 weeks	26.02.2018	16.03.2018	54	54
ID3-2	Preparation of the Guest-System	2 weeks	05.03.2018	16.03.2018	24	24
ID3-3	Analysis & Extraction	5 weeks	19.03.2018	26.04.2018	114	114
ID3-4	Statistics	1 weeks	30.04.2018	03.05.2018	24	24
ID4-2	Statistic Comparison between the Project Parts	5 weeks	07.05.2018	08.06.2018	12	36
ID4-2	Documentation - Final report - Page for the Book - Poster - Film	5 weeks	07.05.2018	08.06.2018	108	324
ID5-1	Administrative work, Presentation, “Finaltag”	1 week	11.06.2018	15.06.2018	24	72
	Total				384	1152

4.1 Gannt Chart

Grapahical representation of the planning, over the 16 weeks of the bachelor thesis.

<table>
<tr><th>Week</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th></tr>
<tr><td>Start Date</td><td>19.02.18</td><td>26.02.18</td><td>05.03.18</td><td>12.03.18</td><td>19.03.18</td><td>02.04.18</td><td>09.04.18</td><td>16.04.18</td><td>23.04.18</td><td>30.04.18</td><td>07.05.18</td><td>14.05.18</td><td>21.05.18</td><td>28.05.18</td><td>04.06.18</td><td>11.06.18</td></tr>
<tr><td colspan="17"></td></tr>
<tr><td>Begin of the Bachelor thesis</td><td>ID0-1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Extraction of config from Samples</td><td></td><td>ID1-1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Test the Infrastructure</td><td></td><td></td><td>ID1-2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Automation of procedures</td><td></td><td></td><td></td><td colspan="7">ID1-3</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Regularly deliver samples &amp; configs</td><td></td><td></td><td></td><td colspan="7">ID1-4</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Document DarkComet function</td><td></td><td></td><td></td><td></td><td></td><td colspan="4">ID1-5</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Set up worldwide scanner</td><td></td><td colspan="3">ID2-1 / 2-2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Scanning</td><td></td><td></td><td></td><td></td><td colspan="4">ID2-3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Search operators in Shodan scans</td><td></td><td colspan="9">ID2-4</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Track habits of operators</td><td></td><td></td><td></td><td colspan="7">ID2-5</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Preparation of the Analysis-Environment</td><td></td><td colspan="3">ID3-1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Preparation of the Guest-System</td><td></td><td></td><td colspan="2">ID3-2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Analysis &amp; Extraction</td><td></td><td></td><td></td><td></td><td colspan="5">ID3-3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Statistics</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>ID3-4</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Statistic comparison between the project parts</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="5">ID4-1</td><td></td></tr>
<tr><td>Documentation</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="5">ID4-2</td><td></td></tr>
<tr><td>End of Bachelor thesis</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>ID5-1</td></tr>
</table>

5 Ethical & Judicial Questions

It is important that a scan should be seen as such and not perceived as an attack. Furthermore, persons need the possibility to go out of the scan range. We must also pay attention to the used resources (in some cases it could lead to DOS attacks!) and not be too intrusive with our scans. At least it is important to monitor a scan to react if an error occurs.

We took the following measures to satisfy the requirements:
Before we perform a scan, we define the IP range and the ports that will be scanned. The IPs will also be scanned randomly and not incremental. In our scans we send a link to our website: https://bfhthesisnoscan.wixsite.com/noscan. On the website an e-mail address is given to revoke the scan, there are as well more information about us and our project.

Also for the live-analysis and the creation of the guest-system, there have to be set some boundaries. The guest-system will be configured and prepared as real as possible. And so, a lot of specific and pseudo-personal user-data. Such as personal data like photos, videos are questionable. We don't want to attack someone’s privacy and abuse their online data.