

Configuration Manual

MSc Research Project
MSc Cyber Security

Timofei Milov
Student ID: X22221964

School of Computing
National College of Ireland

Supervisor: Niall Heffernan

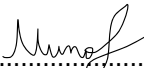
National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Timofei Milov
Student ID: X22221964
Programme: MSc Cyber Security **Year:** 2023/2024
Module: Research Practicum
Lecturer: Niall Heffernan
Submission Due Date: 16/09/2024
Project Title: Analysis of patterns in the source code of malicious npm packages
Word Count: 515 **Page Count:** 4

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 
Date: 13/09/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Timofei Milov
Student ID: X22221964

1. Introduction

This configuration shows how to set an environment, configure virtual machine, prepare dataset, run the GuardDog tool with our analytical system on packages, run weights optimization program, do experiments from the research project. This manual is divided into several sections. Second section is about environment, virtual machine configuration. Third section is about dataset preparation, how to download it. Forth section shows how to run programs and do experiments.

2. Environment

To secure ourselves from malware we need to use isolated environment – virtual machine. We used VMware Fusion hypervisor for the experiments, but you can use VirtualBox or other. We used Ubuntu 24.04 Server, that can be download from Ubuntu official site (Ubuntu, 2024).

Virtual Machine Configuration:

- **Network:** NAT (share with my mac)
- **CPU:** 2 cores
- **Memory:** 4 GB
- **Hard Disk:** 14 GB

Isolation options:

- Disable drag and drop
- Disable copy and paste
- Disable shared folders

Create not root user. For more comfortable work you can configure ssh connection to the virtual machine, but it's not necessary.

3. Dataset preparation

I don't want to send you malware npm samples for security reasons, so you need to download and select them yourself.

Log in to the virtual machine and create directory:

```
mkdir /var/www  
cd /var/www
```

Clone dataset:

git clone <https://github.com/DataDog/malicious-software-packages-dataset>

Create directory for malicious packages:

mkdir npm-malicious-packages

Choose malicious packages:

cd malicious-software-packages-dataset

```
unzip -o -P infected samples/npm/2024-04-17-@mosfe_beam-git-util-v1.0.0.zip -d  
/var/www/npm-malicious-packages/ && tar czvf /var/www/npm-malicious-packages/2024-  
04-17-@mosfe_beam-git-util-v1.0.0.tar.gz /var/www/npm-malicious-packages/2024-04-17-  
@mosfe_beam-git-util-v1.0.0 && rm -rf /var/www/npm-malicious-packages/2024-04-17-  
@mosfe_beam-git-util-v1.0.0
```

Using the command above as example unzip and archive all packages from this list:

1. 2024-04-17-@mosfe_beam-git-util-v1.0.0.zip
2. 2024-04-17-@mosfe_beam-lint-config-v1.0.5.zip
3. 2024-04-17-@mosfe_beam-plugin-s3plus-v0.1.16.zip
4. 2024-04-17-@mosfe_beam-v2.0.0.zip
5. 2024-04-17-@mosfe_owl-config-v1.0.8.zip
6. 2024-04-17-@mosfe_portal-proxy-v1.1.7.zip
7. 2024-04-17-@mosfe_s3plus-v0.1.7.zip
8. 2024-04-17-@mosfe_sso-sdk-v0.0.6.zip
9. 2024-05-03-@sxmp_detector-v0.100.4.zip
10. 2024-05-05-avx-web-build-v1000.0.1.zip
11. 2024-05-29-hello-1st-anni-v4.4.25.zip
12. 2024-05-30-flexfone-reseller-v100.0.3.zip
13. 2024-05-30-flexfone-reseller-v100.0.4.zip
14. 2024-05-30-flexfone-reseller-v100.0.5.zip
15. 2024-05-30-hello-1st-anni-v4.4.30.zip
16. 2024-05-30-hello-1st-anni-v4.4.31.zip
17. 2024-05-30-react-zutils-v1.0.1.zip
18. 2024-06-03-hello-1st-anni-v0.0.1-security.zip
19. 2024-06-07-@atticuss-sra_test-pkg-x4-v3.2.0.zip
20. 2024-06-07-@atticuss-sra_test-pkg-x4-v3.2.1.zip
21. 2024-06-07-@atticuss-sra_test-pkg-x4-v3.2.2.zip
22. 2024-06-07-@atticuss-sra_test-pkg-x4-v3.2.3.zip
23. 2024-06-07-test-pkg-x5-v3.2.0.zip
24. 2024-06-07-test-pkg-x5-v3.2.1.zip
25. 2024-06-07-test-pkg-x5-v3.2.2.zip
26. 2024-06-07-test-pkg-x5-v3.2.3.zip

cd /var/www

```
mkdir npm-benign-packages  
cd /var/www/npm-benign-packages  
npm pack async@3.2.5
```

Download all benign packages using the command above:

1. `async@3.2.5`
2. `axios@1.7.2`
3. `chalk@5.3.0`
4. `date-fns@3.6.0`
5. `day@0.0.2`
6. `express@4.19.2`
7. `grunt@1.6.1`
8. `html-entities@2.5.2`
9. `jest@29.7.0`
10. `js-yaml@4.1.0`
11. `karma@6.4.3`
12. `lodash@4.17.21`
13. `mocha@10.6.0`
14. `moment@2.30.1`
15. `mongoose@8.5.1`
16. `mysql@2.18.1`
17. `passport@0.7.0`
18. `path@0.12.7`
19. `pm2@5.4.2`
20. `sentry@0.1.2`
21. `socket@0.0.1`
22. `ts-node@10.9.2`
23. `vue@3.4.32`
24. `vue-router@4.4.0`
25. `web3@4.11.0`
26. `webpack@5.93.0`

```
mkdir /var/www/experiments  
cp /var/www/npm-malicious-packages/2024-04-17-@mosfe_beam-git-util-v1.0.0.tar.gz  
/var/www/experiments/  
cp /var/www/npm-malicious-packages/2024-05-30-flexfone-reseller-v100.0.4.tar.gz  
/var/www/experiments/  
cp /var/www/npm-malicious-packages/2024-05-30-hello-1st-anni-v4.4.31.tar.gz  
/var/www/experiments/  
  
cp /var/www/npm-benign-packages/day-0.0.2.tgz /var/www/experiments/  
cp /var/www/npm-benign-packages/passport-0.7.0.tgz /var/www/experiments/  
cp /var/www/npm-benign-packages/sentry-0.1.2.tgz /var/www/experiments/
```

4. How to run programs

To run programs, you need to clone them from GitHub:

```
cd /var/www  
git clone https://github.com/Timofey21/guarddog-research-testing
```

Create Python virtual environment:

```
cd guarddog-research-testing  
python3 -m venv venv  
source venv/bin/activate
```

Now you can scan packages:

```
python -m guarddog npm scan /var/www/npm-malicious-packages/2024-04-17-  
@mosfe_beam-git-util-v1.0.0.tar.gz
```

To run weights optimization program:

```
cd /var/www  
git clone https://github.com/Timofey21/weights\_optimization
```

```
cd weights_optimization  
python3 -m venv venv  
source venv/bin/activate
```

To do experiments, you need to change weights back in **guarddog-research-testing**:

```
cd /var/www/guarddog-research-testing  
cd guarddog  
cp confidence_weights_backup.json confidence_weights.json  
cp severity_weights_backup.json severity_weights.json
```

And now you can start an experiment:

```
cd /var/www/weights_optimization  
python3 -m venv venv  
source venv/bin/activate
```

```
python main.py
```

References

Ubuntu (2024) *Get Ubuntu Server | Download, Ubuntu*. Available at: <https://ubuntu.com/download/server> (Accessed: 8 August 2024).