National College of Ireland

Configuration Manual

MSc Internship
Cybersecurity

Sarell Lopes
Student ID: x18147241

School of Computing
National College of Ireland

Supervisor: Dr. Muhammad Iqbal

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. SARELL LOPES ……

Student ID: ……x18147241……..……

Programme: MSc Cybersecurity **Year:** 2019

Module: MSc Internship ……..……

Lecturer: ……DR. Muhammad Iqbal ……..…… …

Submission Due Date: ……8 Jan 2020…… ….……

Project Title: …Predicting Attacks on Vulnerabilities using CVSS Impact Score and External Attack Factors ……. ……

Word Count: …… **Page Count:** ……..…….……

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.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: …… ……

Date: …… ……

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

Sarell Lopes
Student ID: x18147241

1 Introduction:

This document serves as a guide to replicate the presented project for predicting attack on discovered vulnerability by using machine learning algorithm random forest. For this proposed research the data is collected from various sources and by using various data analytical tools and techniques the proposed design is being implemented and evaluated for the its outcome and performance based on accuracy, sensitivity and specificity.

2 System Specification

Local machine was used to setup python environment for data cleaning and merging procedure. Also, for browser-based scraping tool.

a) Local Machine

- Operating System: Windows 10 Pro
- Memory (RAM): 16 GB
- HDD: 1024 GB
- Processor: Intel® Core™ i7-7500U CPU @2.90GHz

Google colab is a virtual cloud environment with Jupyter Notebook setup for running python codes. This cloud environment was use to conduct correlation test and processing the machine learning models.

b) Google Colabs

- Operating System: Linux Posix
- Memory (RAM): 13 GB
- HDD: 100 GB
- Processor: Intel(R) Xeon(R) CPU @ 2.20GHz

3 Tools and Technologies

- Python 3.5.9 on local system.
- Python 3.6.9 on google colabs.
- Kate Editor
- Web-Crawling
- Libreoffice
- MSExcel
- Tableau

4 Data Collection

Data is being sourced from the various websites containing Vulnerability data, PoCs and Attack Signatures.

a. National Vulnerability Database for JSON data feed.
b. Datasets (EKITS. SYM-Malware, SYM-Virus) were licensed from the University of Trento
c. Cyberwatch Public DB
d. Syamtec
e. Zeroday website

https://nvd.nist.gov/vuln/data-feeds
http://securitylab.disi.unitn.it/doku.php?id=datasets
https://kb.cyberwatch.fr/vulnerabilities/
https://www.symantec.com/security_response/attacksignatures/
https://www.zero-day.cz/database/

5 Implementation

The script for cleaning and merging the data and running the machine learning code are available on the github at https://github.com/lopessarell/MLVULATTK.

Packages and Libraries used:

1. Pandas
2. numpy
3. seaborn
4. matplolib
5. sklearn
6. imblearn
7. StratifiedKFold
8. SMOTEENN

#CODE ON LOCAL MACHINE

1. Code for reading json files from directory

```
with open(json_filepath, 'r',encoding="utf8") as jsonfile:
    jsondata=jsonfile.read()
```

2. Part of json extraction code

```
cve_data = vul.get("cve")
# print(cve_data["problemtype"]["problemtype_data"][0]["description"])

id=cweid=version3=vectorString3=attackVector3=attackComplexity3=privilegesRequired3=user
availabilityImpact3=base_score3=base_severity3=exploitabilityScore3=impactScore3=version
''
confidentialityImpact2=integrityImpact2=availabilityImpact2=base_metrics_score2=severity
ege2=obtainUserPrivilege2=obtainOtherPrivilege2=userInteractionRequired2=''
id = cve_data["CVE_data_meta"]['ID']
if(cve_data["problemtype"]["problemtype_data"][0]["description"]):
    cweid = cve_data["problemtype"]["problemtype_data"][0]["description"][0]["value"]


if(vul.get("impact")):
    impact_data = vul.get("impact")
```

3. Code functions for binary features:

```
def checkforSYMmal(id,SYMmaldata):

    flag=False
    count = 0
    for record in SYMmaldata:

        if(id.strip() == record[2].strip()):
            count=+1
            flag = True

    return [flag,count]

def checkforexploit(id,exploittdata):

    flag=False
    count = 0
    for record in exploittdata:

        if(id.strip() == record[0].strip()):
            count = record[2]
            flag = True

    return [flag,count]
```

4. Code functions to replace string value with numeric values of CVSS

```
def getACvalues(val):

    val = val.strip()

    if (val == "LOW"):
        val = 0.71

    if(val == "MEDIUM" ):
        val = 0.61

    if(val == "HIGH"):
        val = 0.35

    return val

def getATvalues(val):

    val = val.strip()

    if (val == "MULTIPLE"):
        val = 0.45

    if(val == "SINGLE" ):
        val = 0.56

    if(val == "NONE"):
        val = 0.704

    return val

def getCIAvalues(val):

    val = val.strip()

    if (val == "NONE"):
        val = 0.0

    if(val == "PARTIAL" ):
        val = 0.275

    if(val == "COMPLETE"):
        val = 0.660
```

5. Code to load all datasets:

```
main_dir = "D:/cvssproj"

with open(main_dir + '/EKITS.csv', newline='') as csvfile:
    EKITSdata = list(csv.reader(csvfile))

with open(main_dir + '/EDB.csv', newline='') as csvfile:
    EDBdata = list(csv.reader(csvfile))

with open(main_dir + '/SYM-malware-threats.csv', newline='') as csvfile:
    SYMmaldata = list(csv.reader(csvfile))

with open(main_dir + '/SYM-network-attacks.csv', newline='') as csvfile:
    SYMnetdata = list(csv.reader(csvfile))

with open(main_dir + '/exploited_vul.csv', newline='') as csvfile:
    exploittdata = list(csv.reader(csvfile))

with open(main_dir + '/cyberwatchdata.csv', newline='') as csvfile:
    cyberwatch = list(csv.reader(csvfile))

with open(main_dir + '/symantec.csv', newline='') as csvfile:
    symantec = list(csv.reader(csvfile))

with open(main_dir + '/zeroday.csv', newline='') as csvfile:
    zeroday = list(csv.reader(csvfile))
```

6. Code to write data in CSV file:

```
vul_data_file.write("%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s\n" %
(year,id,accessVector2,accessComplexity2,authentication2,confidentialityImpact2,integrityImpact2,availabilityImpact2,base_metrics_score2,severit
y2,exploitabilityScore2,impactScore2,obtainAllPrivilege2,obtainUserPrivilege2,userInteractionRequired2,expflag,expcnt,attkflag,attkcnt))
```

#CODE ON COLABS

1. Mounting google drive:

```
[ ]  #code to mount the files from google drive
     from google.colab import drive
     drive.mount('/content/drive')
```

2. Correlation Test:

```
# correlation analysis

corrmat = df.corr()

corrmat.to_csv("/content/VulnDataCorr.csv")

#plotting correlation graph
from matplotlib import pyplot as plt

f, ax = plt.subplots(figsize =(15, 15))
sb.heatmap(corrmat, ax = ax, cmap ="YlGnBu", linewidths = 0.1)
```

3. Splitting data, SMOTE data and Run Random forests

```
#using library for specifying the iteration and split training and test data
cv = StratifiedKFold(n_splits=5)
for train_idx, test_idx, in cv.split(X, y):
    X_train, y_train = X[train_idx], y[train_idx]
    X_test, y_test = X[test_idx], y[test_idx]
    #SMOTE data to resolve imbalance
    X_train, y_train = SMOTEENN().fit_resample(X_train, y_train)
    #Load Random Classifier
    RFCLF = RandomForestClassifier(n_estimators=10000, random_state=0, n_jobs=-1)
    RFCLF.fit(X_train, y_train)
```

4. Performance test for model:

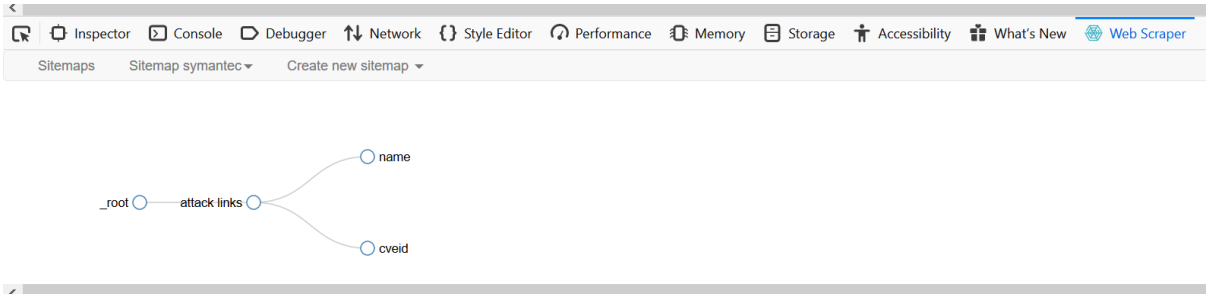
```
#Accuracy
Accuracy_rf = (Avg_tp+Avg_tn)/(Avg_tp+Avg_tn+Avg_fp+Avg_fn)
print("Accuracy {:0.2f}".format(Accuracy_rf))

#Specificity
Specificity_rf = Avg_tn/(Avg_tn+Avg_fp)
print("Specificity {:0.2f}".format(Specificity_rf))

#Recall
Recall_rf = Avg_tp/(Avg_tp+Avg_fn)
print("Recall / Sensitivity {:0.2f}".format(Recall_rf))

#GMean
GM_rf = math.sqrt(Specificity_rf*Recall_rf)
print("Geometric Mean Score {:0.2f}".format(GM_rf))
```

6 Scraping using Web Scraper

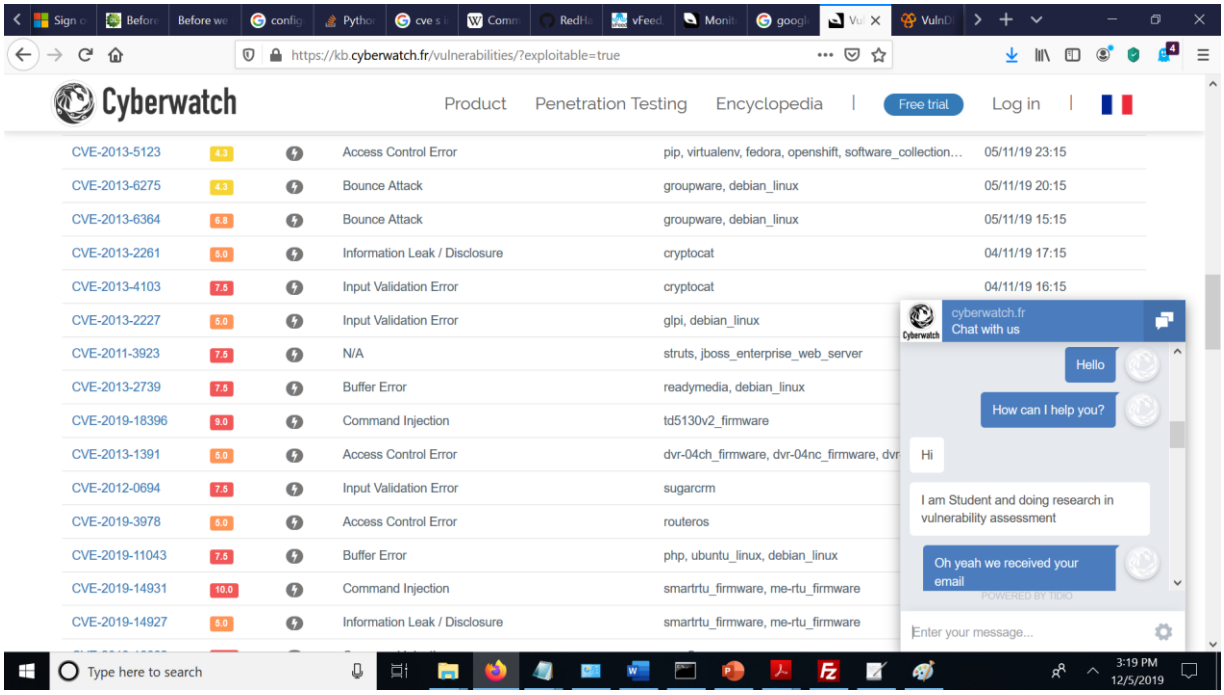
https://webscraper.io/

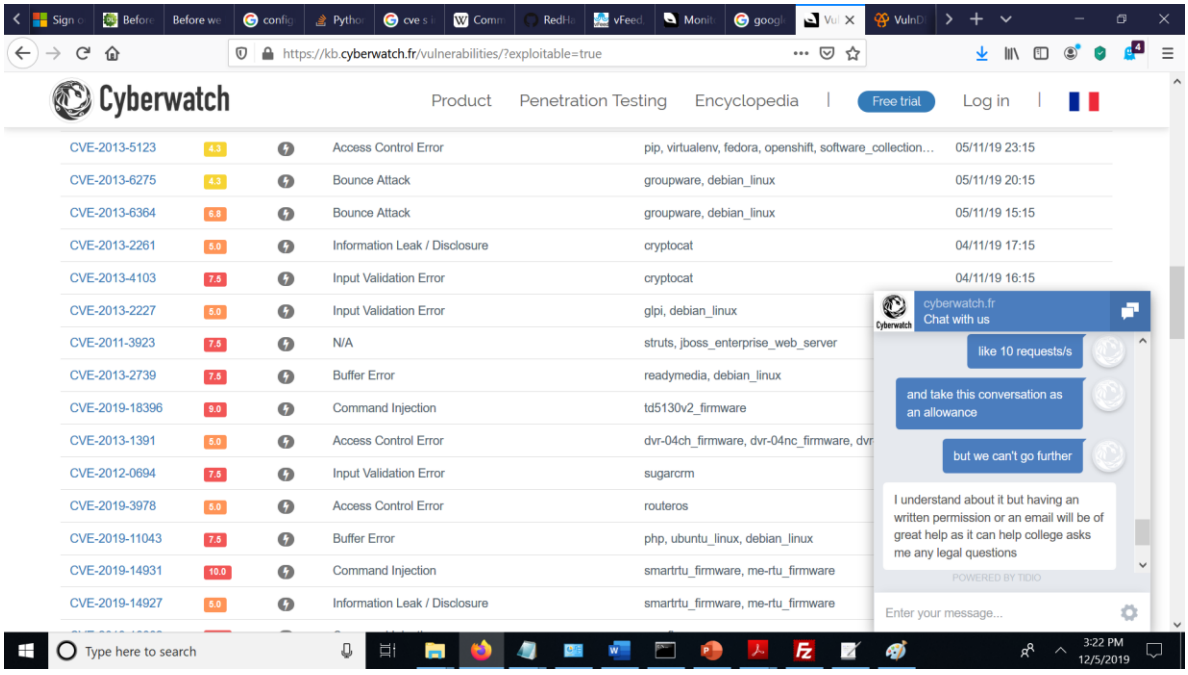
https://www.youtube.com/channel/UCItHuKRAL3w6fspQUQh8Bkw

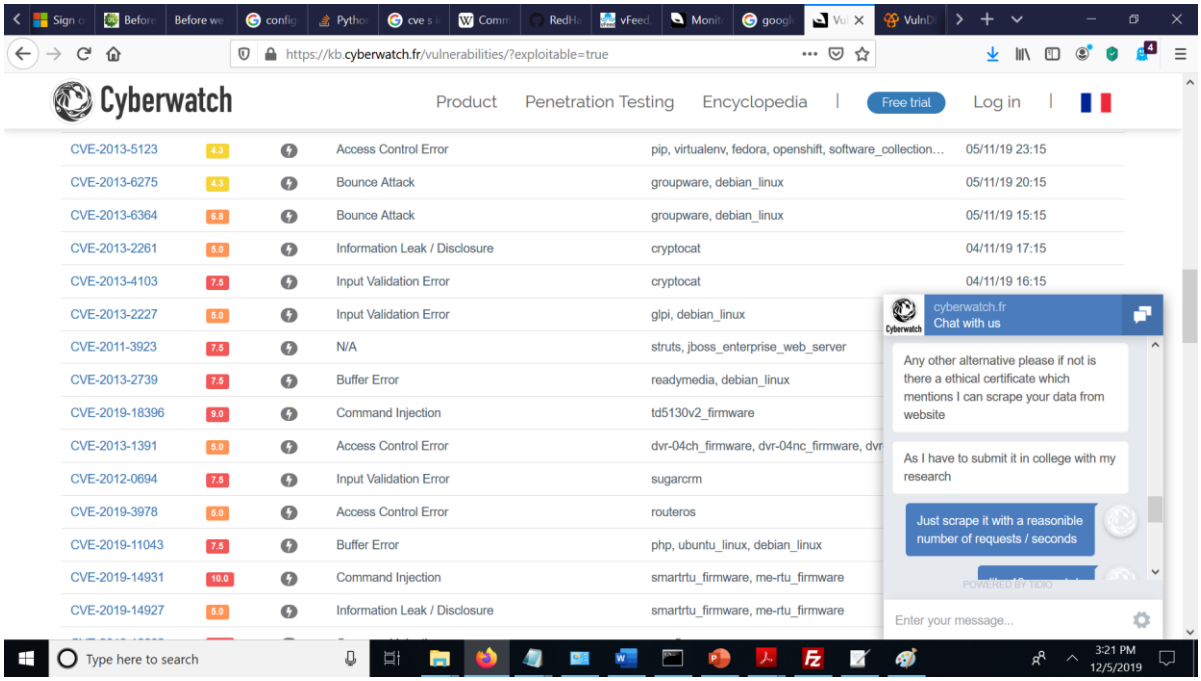
We use this scraper tool to scrape the data from the Symantec attack signatures and zerodaywebsites.

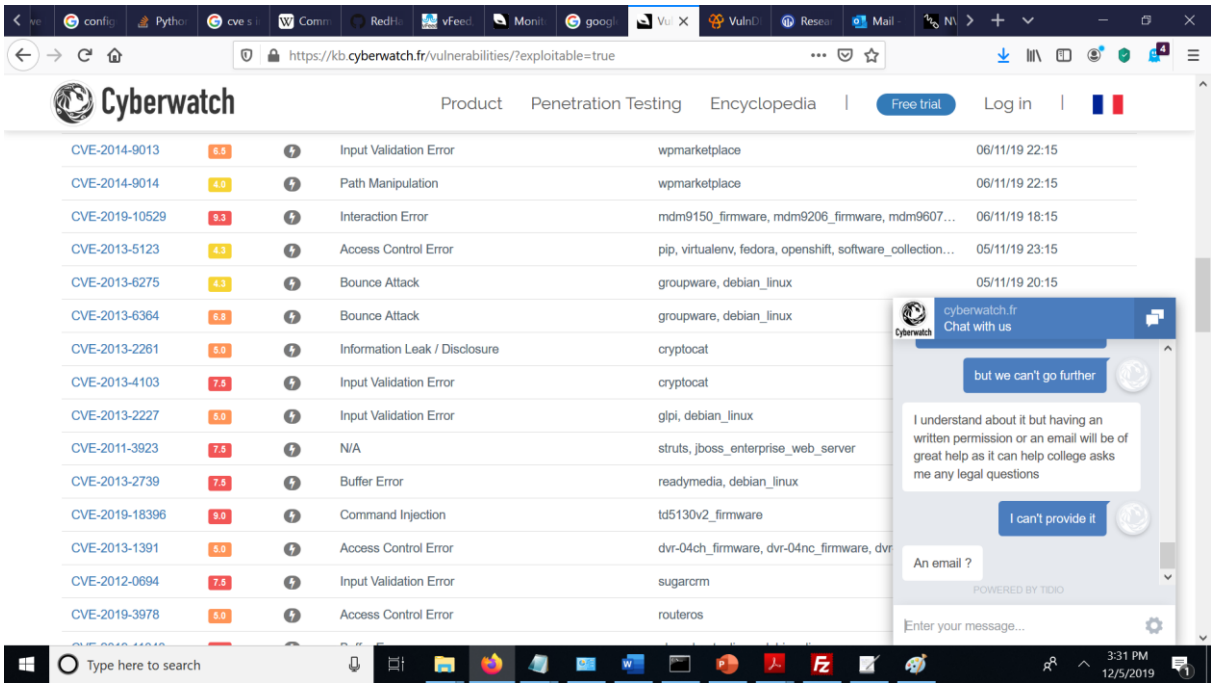


7 Permission from Cyberwatch.com to scrape website









8 Internship and Licensed form are attached below

18. Appendix G – Monthly Internship Activity Report

The Internship Activity Report is a 1 page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and uploaded to Moodle on a monthly basis.

Student Name: SARELL LOPES Student number: 18147241

Company: CRH plc Month Commencing: Sep 19 - Nov 19

Core Task and Activities:

1. Training acquired for SIEM tool Splunk under supervision of Lydia Behan and Heather Roache.
2. Training for ISMS standard ISO 27000 with Lydia Behan and Conor Chaney.
3. Knowledge gained on Qualys tool for Vulnerability assesment and management with Daniel Kennedy and Foad Baghban.
4. Incident Response training by Don and Gary Cantwell.
5. Pentesting lessons learnt from Richard.
6. Guidance provided by Jared and Slawomir on Vulnerability Assessement especially on CVSS
7. Contributed on Cybersecurity awareness program that covered the topics on Online Safety, Home security(IoTs and Home devices), Scams online and Kids Safety.

Employer comments

Sarell had a very positive attitude and was eager to learn new skills. He could benefit from being more proactive to finding tasks. He interacted well with the team in general.

Student Signature: sarellopes Date: 4 Jan 2020

Industry Supervisor Signature: LB - (LYDIA BEHAN) Date: 6/1/20

UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dip. di Ingegneria e Scienze dell'Informazione

Academic License for UNITN DISI Security Databases for Scientific, Non-Profit, Non-Commercial Purposes

The Department of Information Engineering and Computer Science -DISI, University of Trento, Via Sommarive 9, I-38123 Trento, Italy

Hereinafter UNITN by means of

Fabio Massacci (Professor)		Paolo Giorgini (Head of Department)
UNITN PROVIDING SCIENTIST		UNITN REPRESENTATIVE

- Hereby grants a free non-exclusive non-transferable license for the Security Dataset(s)
- NVD-EDB-EKITS-SYM
- FFV-GCV-IEV-ASV
- ESEJ
- to:

  School of Computing,
  National College of Ireland
  Mayor Street
  IFSC
  Dublin 01

Hereinafter RECIPIENT by means of

Name Sarell Lopes (Position) MSc Cybersecurity Student		Name Muhammad Iqbal (Position) Assistant Professor
RECIPIENT SCIENTIST(S)		RECIPIENT REPRESENTATIVE

Under the terms and conditions stated herein:

1. The RECIPIENT asks rights to access the DATASETS mentioned above among the following ones

- **NVD**: is the reference database for the population of vulnerabilities. It collects the data from the *National Vulnerability Database* from NIST.[1]
- **EDB** is the reference database for public (proof-of-concept) exploits. It collects the data from the *Exploit-DB* web site.
  - **EDB-files** contains all actual exploits referenced in EDB, categorized by platform.
- **EKITS** is a database of vulnerabilities and exploits traded in the black markets. We have built an update infrastructure that allows us to keep our database well ahead of any public source on such vulnerabilities publicly available (such as Contagio's Exploit Pack Table).
- **SYM** is a database of vulnerabilities exploited in the wild as reported by Symantec's sensors worldwide. This dataset is a collection of publicly available vulnerability data through Symantec's *Threat Explorer* and Attack Signatures websites.
- **FFV** collects the vulnerabilities of the *Firefox* browser. It is the most comprehensive database. It integrates the Mozilla Foundation Security Advisory (MFSA) bulletin, the Mozilla Bugzilla bugtracker and the NVD.
- **GCV** reports the vulnerabilities of the *Google Chrome* Browser extracted from Chrome Issue Tracker, integrated with the NVD to reconstruct affected versions and checked for consistency with the code distribution. It does not include all vulnerabilities of the browser as some of the third party software such as WebKit are only partly included.
- **IEV** lists the vulnerabilities for *Internet Explorer* extracted from the Microsoft Security Bulletin and integrated with the NVD to reconstruct affected versions.
- **ASV** Vulnerabilities of the Apple Safari Web Browser extracted from the Apple Knowledge Base and integrated with the NVD to reconstruct affected versions.
- **ESEJ** is the list of vulnerabilities in Google Chrome and Mozilla Firefox along with ranges of major versions affected by each vulnerability. For each vulnerability, the dataset contains two affected version ranges: (1) vulnerable versions according to the NVD; (2) vulnerable versions based on the vulnerable code evidence (identified by our algorithm).

A description of the tables and entries in of the DATASETS is provided as ANNEX A.

2. The RECIPENT intends to use the dataset for the following scientific, non-profit, non-commercial purposes

As master student at NCI, my research topic is on vulnerability assessment and its effects on the businesses in which I'll be focusing on the CVSS, where I'll primary focus on prioritizing the vulnerabilities with help of CVSS and other internal and external factors in organization and argue that direct relying on CVSS is not fruitful to manage and patch the vulnerabilities in IT infrastructure. I'll be analyzing the data of vulnerabilities that are discovered and that have been actually exploited or the exploit is present in wild and I'll also consider the vulnerabilities in legacy and unsupported systems that are still in use. I found the research paper by Prof Fabio Massacci very helpful and aligned with my research topic. The rich database develop by the scientist at your reputed university will help me design the machine learning model that will help prioritizing the vulnerabilities discovered in organization.

The RECIPENT agrees that such purposes, the name of the RECIPIENT's scientist(s)

and affiliation, and any publications by the RECIPIENT that uses the DATASETS will be listed by UNITN on the web site http://security-data.disi.unitn.it.

3. "MODIFICATIONS" of DATASETS is software or database tables or database columns created by RECIPIENT which contains/incorporates DATASETS or a part thereof or SQL code and data table values of DATASETS or a part thereof.

4. The RECIPIENT is free to make MODIFICATIONS of DATASETS by making in-house copies of tables and to modify copied tables, for example by the addition of columns and changing of data. The RECIPIENT is free to use the database in-house as he/she wishes and to create logical objects containing original and/or derived data so long as such use does not violate terms specified in this agreement.

5. The license is free of charge so long as DATASETS, or any component of DATASETS, or any derivative work that includes or depends on DATASETS in whole or in part, is used for scientific, non-profit, non-commercial use only. Any other use of DATASETS and use of MODIFICATIONS of DATASETS for other purposes, alone or integrated into other databases or software, requires prior written consent by UNITN.

6. RECIPIENT shall have the right to publish its findings and results related to DATASETS, provided that UNITN researchers are cited as the source of DATASETS and the references below are cited in the publication. The published references for DATASETS are listed below:
    a. **NVD, EDB, EKITS, SYM:**
        i. **Luca Allodi and Fabio Massacci. 2014. Comparing Vulnerability Severity and Exploits Using Case-Control Studies. *ACM Transactions on Information and System Security*. 17(1), 20pp, 2014. DOI=10.1145/2630069**
        ii. Its preliminary version whenever historical attribution is important:
            1. Luca Allodi and Fabio Massacci. 2012. A preliminary analysis of vulnerability scores for attacks in wild: the ekits and sym datasets. In *Proc. of the 2012 ACM Workshop* BADGERS '12. DOI=10.1145/2382416.2382427
    b. **FFV, IEV, ASV, GCV:**
        i. **Fabio Massacci and Viet Hung Nguyen. An Empirical Methodology to Evaluate Vulnerability Discovery Models. *IEEE Transactions on Software Engineering* 40(12):1147-1162, 2014. DOI=10.1109/TSE.2014.2354037**
        ii. Its preliminary versions whenever historical attribution is important:
            1. Fabio Massacci, Stephan Neuhaus, Viet Hung Nguyen. After-Life Vulnerabilities: A Study on Firefox Evolution, its Vulnerabilities and Fixes. In *Proc. of the 3rd Int. Symp. on Engineering Secure Software and Systems (ESSoS'11)*, 2011. Springer Verlag. DOI=10.1007/9783642191251.
            2. Viet Hung Nguyen, Fabio Massacci. An Independent Validation of Vulnerability Discovery Models. In *Proc. of the 7th ACM Symp. ASIACCS'12,* 2012. DOI=10.1145/2414456.2414458.

c. **ESEJ:**
   i. **Viet Hung Nguyen, Stanislav Dashevskyi, Fabio Massacci. 2015. An Automatic Method for Assessing the Versions Affected by a Vulnerability. In *Empirical Software Engineering* (to appear). DOI=10.1007/s10664-015-9408-2**
   ii. Its preliminary version whenever historical attribution is important:
      1. Viet Hung Nguyen, Fabio Massacci. The (Un)Reliability of Vulnerable Version Data of NVD: an Empirical Experiment on Chrome Vulnerabilities. In *Proc. of the 8th ACM Symp. ASIACCS'13*, 2013. DOI=10.1145/2484313.2484315.

The RECIPIENT undertakes to notify UNITN of the existence of the publication by email at security-data@disi.unitn.it.

7. It is the responsibility of the RECIPIENT to read the articles mentioned in Article 6 in order to understand the scientific limitations of the DATASETS.

8. No property rights with respect to DATASETS shall transfer to RECIPIENT through this agreement. UNITN may demand compensation for uses other than those granted in this license according to article 15.

9. The RECIPIENT, the user and any research assistants, co-workers or other workers who may use DATASETS agree to not give the data to third parties or grant licenses which include DATASETS, alone or integrated into other databases, to third parties without prior consent of UNITN.
   RECIPIENT may not place DATASETS on public servers unless prior agreement is given by UNITN.
   UNITN may demand compensation from RECIPIENT for transfer of information and licenses granted to third parties by RECIPIENT.

10. The RECIPIENT undertakes to refer any requests by third parties for the provision of DATASETS to UNITN at security-data@disi.unitn.it

11. Where the research involving DATASETS results in an invention or patentable MODIFICATION of DATASETS, RECIPIENT and its Researcher/s shall promptly disclose this development to UNITN. RECIPIENT and UNITN shall decide in common about the inventorship, taking due consideration UNITN's contribution to the invention through DATASETS. Decisions about further proceedings, such as filing of a patent application or exploitation, shall be made after inventorship is determined.

12. DATASETS is not guaranteed as suitable for use with any application. UNITN gives no warranty express or implied of any kind with regard to the distribution, content or operation of DATASETS, in particular but not limited to any warranty of suitability or fitness for any purpose. UNITN will not assume liability for damages occurred through the use of DATASETS.

13. UNITN will disclose any known rights of third parties to DATASETS to the best of its

knowledge. However, UNITN does not warrant for any possible infringement of rights. RECIPIENT has to acquire on his own all necessary licenses for supporting DATASETS if not otherwise agreed in writing.

14. This license covers usage of DATASETS only, and does not of itself entitle the RECIPIENT to any support from UNITN in the installation, maintenance or use of DATASETS. Distributions of DATASETS and updates to it will be accompanied by a document clarifying issues related to support. RECIPIENT will inform UNITN of any defects found in DATASETS by email at security-data@disi.unitn.it.

15. In case the DATASETS is or will be under the control of RECIPIENT before this agreement is signed UNITN gives consent to use of DATASETS under the condition of RECIPIENT'S prior consent to this agreement.

16. This agreement may be terminated by either party with two months notice.

17. Disputes and requests for compensation related to this license will be adjudicated by the International Court of Arbitration of the International Chamber of Commerce (ICC). Both parties agree to consider ICC arbitration final and agree to abide by its ruling and pay its awards without further appeals.

Fabio Massacci (Professor)		Paolo Giorgini (Head of Department)
UNITN PROVIDING SCIENTIST		UNITN REPRESENTATIVE
	UNIVERSITY OF TRENTO - Italy Department of Information Engineering and Computer Science	5 DIC 2019
Date and signature	Stamp of the Organization	Date and signature

Name Sarell Lopes (Positions) MSc Cyber Security Student		Name Muhammad Iqbal (Position) Assistant Lecturer
RECIPIENT SCIENTIST(S)		RECIPIENT REPRESENTATIVE
4 DEC 2019	IFSC Mayor Street Dublin 1 National College of Ireland Student Services	04/12/2019
Date and signature	Stamp of the Organization	Date and signature

ANNEX A – DATASETS TABLES AND ATTRIBUTES

1. **NVD** Note that each entry in the NVD dataset **does not correspond to a vulnerability**. A vulnerability ID can be associated with more than one software or vendor. The same ID can be reported in different tuples.

a. **CVE_ID:** Id of the vulnerability.
b. **Pub_date:** First publication date of the vulnerability
c. **Mod_date:** Date of last update to the entry
d. **CVSS_score:** CVSS v2.0 Risk Score of the vulnerability
e. **CVSS_Imp:** CVSS v2.0 Impact score of the vulnerability
f. **CVSS_Expl:** CVSS v2.0 Exploitability score of the vulnerability
g. **CVSS_AV:** CVSS Exploitability assessment: Access Vector
h. **CVSS_AC:** CVSS Exploitability assessment: Access Complexity
i. **CVSS_Au:** CVSS Exploitability assessment: Authentication
j. **CVSS_Conf:** CVSS Impact assessment: Confidentiality
k. **CVSS_Integ:** CVSS Impact assessment: Integrity
l. **CVSS_Avail:** CVSS Impact assessment: Availability
m. **Aff_Sw:** Software affected by the vulnerability
n. **Vendor:** Vendor of the software
o. **Description:** English description of vulnerability

2. EDB
(*) in EDB-files only

a. **E-id:** Exploit-DB record ID
b. **Cve-id:** CVE_ID of vulnerability to which the exploit refers
c. **Date:** date of emission of exploit
d. **Osvb-id:** ID to third-party vulnerability database: OSVDB
e. **(*) File:** Path to the exploit
f. **Description:** Description of exploit
g. **Author:** name of the researcher who published the exploit
h. **Platform:** operating system of the vulnerability/exploit
i. **Type:** type of exploit (e.g. remote, webapp, denial-of-service)
j. **Port:** remote access port to the vulnerability as reached by the exploit (iff *type==remote*)

3. EKITS

a. **Ek_id:** Id of exploit kit
b. **E_name:** exploit kit name
c. **Version:** version of exploit kit
d. **Date:** date of release of exploit kit on the black markets (month)
e. **Price:** advertised price
f. **Per:** license duration (year,month,week)
g. **Service1:** Services sold alongside the product (not available for all ekits)
h. **Service2:** Services sold alongside the product (not available for all ekits)
i. **Service3:** Services sold alongside the product (not available for all ekits)

j. **Cve_id:** CVE_ID of vulnerability exploited by the kit
k. **P_source:** primary source of information
l. **S_source:** secondary source
m. **Notes:** english notes on the ekit/advertisement/services

4. SYM (malware + network attacks)

a. **attack_ID:** ID of attack referenced by Symantec (network attacks table)
b. **threat_ID:** ID of malware referenced by Symantec (malware table)
c. **Type:** where in the text the vulnerability is mentioned (i.e. description of attack or references)
d. **CVE:** CVE_ID of vulnerability
e. **String:** name of to the attack on Symantec's website

5. FFV

a. **bugID:** the identifier of a bug responsible for this vulnerability.
b. **cve:** the identifier of an CVE entry referring to this vulnerability.
c. **mfsa:** the identifier of an MFSA entry referring to this vulnerability.
d. **bugDate:** the date when the corresponding bug is filed to Bugzilla.
e. **cveDate:** the date that the corresponding CVE is filed to NVD.
f. **minVersion:** the earliest major version that this vulnerability affects to.
g. **maxVersion:** the latest major version that this vulnerability affects to.

6. GCV

a. **bugID:** the identifier of a bug responsible for this vulnerability.
b. **cve:** the identifier of an CVE entry referring to this vulnerability.
c. **bugDate:** the date when the corresponding bug is filed to ChromeIssueTracker.
d. **cveDate:** the date that the corresponding CVE is filed to NVD.
e. **minVersion:** the earliest major version that this vulnerability affects to.
f. **maxVersion:** the latest major version that this vulnerability affects to.
g. **codeMinVersion:** the earliest major version where the vulnerable code footprint is found.
h. **codeMaxVersion:** the latest major version where the vulnerable code footprint is found.

7. IEV

a. **cve:** the identifier of an CVE entry referring to this vulnerability.
b. **mssb:** the identifier of an MS Security Bulletin entry referring to this vulnerability.
c. **cveDate:** the date that the corresponding CVE is filed to NVD.
d. **minVersion:** the earliest major version that this vulnerability affects to.
e. **maxVersion:** the latest major version that this vulnerability affects to.

8. ASV

a. **cve:** the identifier of an CVE entry referring to this vulnerability.
b. **akb:** the identifier of an Apple Knowledge Base entry referring to this vulnerability.

c. **cveDate:** the date that the corresponding CVE is filed to NVD.
d. **minVersion:** the earliest major version that this vulnerability affects to.
e. **maxVersion:** the latest major version that this vulnerability affects to.

8. ESEJ

a. cve: the identifier of a CVE entry refferring to this vulnerability.
b. bugID: the identifier of a bug responsible for this vulnerability (Bugzilla or Chrome issue tracker).
c. cveDate: the date that the corresponding CVE is filed to the NVD.
d. minVer: the earliest major version that this vulnerability affects.
e. maxVer: the latest major version that this vulnerability affects.
f. bugFix: the bug fix commit that was successfully located.
g. esminVer: the earliest major version that this vulnerability affects, according to the code evidence identified by our algorithm.
h. esmaxVer: the latest major version that this vulnerability affects, according to the code evidence identified by our algorithm.

UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dip. di Ingegneria e Scienze dell'Informazione

This is the human readable summary of your rights and obligations. It is provided for your convenience only. The formal text of the agreement is the only binding document.

- You can
  1. share these datasets in whatever format with any member of your institution—faculty, administration, students, research associates in the case of universities, and employees in the case of government ministries and research organizations;
  2. use these datasets in creative ways for scientific, not-profit, non-commercial use including publications under the terms of the agreement.

- You cannot
  1. post any of these datasets on your website such that it becomes available to non-members of your institution, or make copies that circulate outside of your institution;
  2. use it for profit or commercial purposes unless agreed in writing.

- You agree to
  1. cite the appropriate reference work in all your publications that make use of the datasets or its derivatives;
  2. provide us the information on the publication where you used the data by email to **security-data @disi.unitn.it** for the purposes of posting it on our web site **http://security-data.disi.unitn.it** with your name and affiliation**;**
  3. refer to us any person or organization outside your institution who would like to use the data.

- You are aware that
  1. other parties may have rights or set licensing obligations in some of the data contained in the datasets and it is up to you to obtain permissions from these parties if needed;
  2. the datasets may contains errors or may be unfit for your purposes and we bear no liability for any problem you might encounter.