



**BHASKARACHARYA NATIONAL INSTITUTE FOR SPACE
APPLICATIONS AND GEO-INFORMATICS**

WEEKLY PROGRESS REPORT (13/02/2023 – 19/02/2023)

WEEK 4

PROJECT NAME

MALWARE DETECTION USING ML

PROJECT DESCRIPTION :

**DESIGN AND IMPLEMENT ML MODEL TO
DETECT MALWARE IN SYSTEM**

GROUP MEMBER :

**Pratham Patel, Shubham Patel, Shashank Sharma,
Yash Soni**

GROUP ID :

12

GROUP GUIDE :

HARSH KIRATSATA

GROUP COORDINATOR :

SIDHDHARTH PATEL

COLLEGE GUIDE NAME :

**MAYANK PATEL, RITIKA LADHA, KINJAL
CHAUDHARI**

COLLEGE GUIDE No. :

+91 9033280445, 8866438698, 9723173567

COLLEGE GUIDE EMAIL :

**mayank.patel@adaniuni.ac.in,
ritika.ladha@adaniuni.ac.in,
kinjal.chaudhari@adaniuni.ac.in**

COLLEGE NAME :

**ADANI INSTITUTE OF INFRASTRUCTURE AND
ENGINEERING**

13/02/2023 TILL 19/02/2023 (7 DAYS)

Learning Basic malware definition and brainstorming

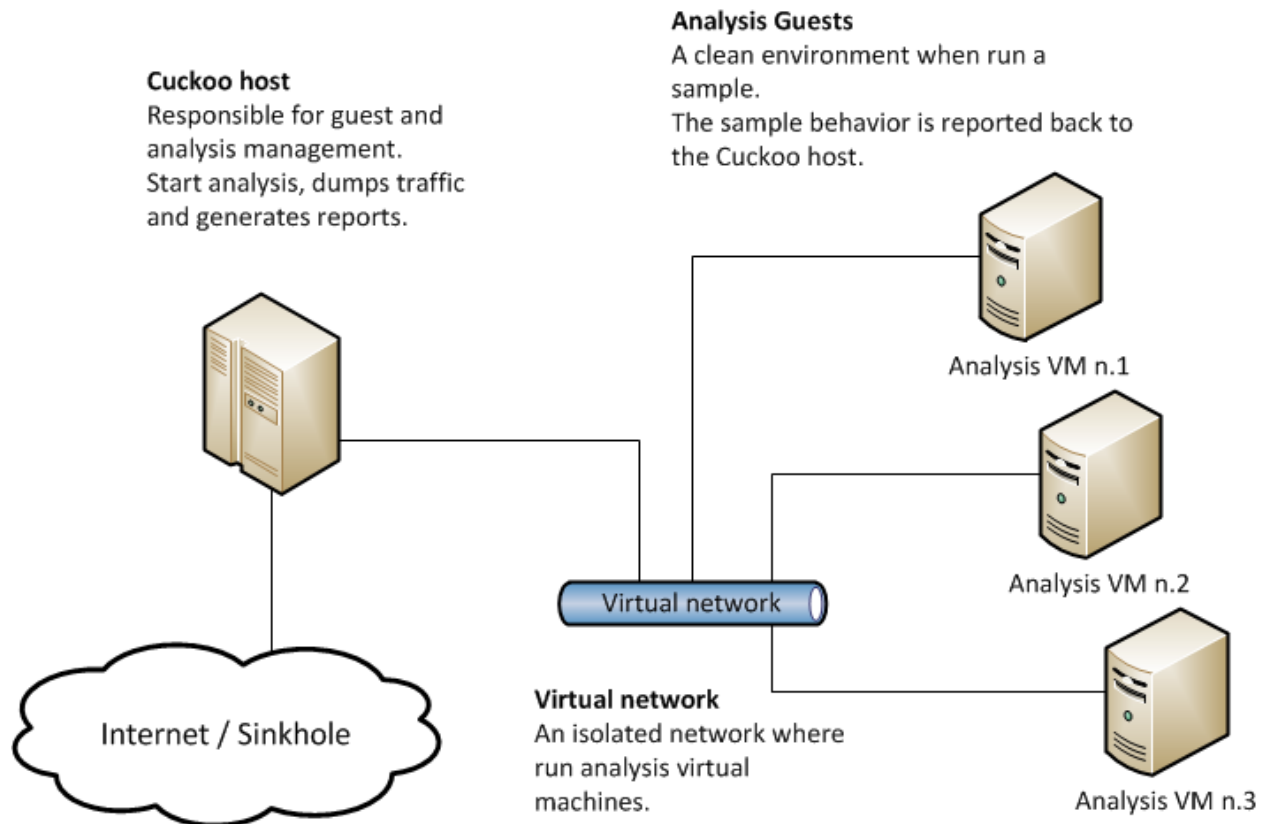
13/02/2023	Explored about Malwares in different os (Windows, Kali, Mac).
14/02/2023	Learned about various ongoing malware detection system.
15/02/2023	Started Exploring about cuckoo malware detection.
16/02/2023	Learned about various use cases and file types of cuckoo.
17/02/2023	Took a brief view of cuckoo functionalities and dashboard.
18/02/2023	Holiday (Maha Shivratri).
19/02/2023	Holiday (Sunday).

WEEK 5(PLAN)	In the next week we are planning to prepare raw data using cuckoo in order to detect malware using ml.
---------------------	---

REFERENCE :

- <https://youtu.be/fn33V4iX5G4>
- <https://github.com/Vatshayan/Android-Malware-Detection-Using-Machine-Learning>
- <https://www.varonis.com/blog/cuckoo-sandboxhttps://github.com/Vatshayan/MALWARE-DETECTION-FINAL-YEAR-PROJECT>
- https://www.youtube.com/watch?v=HMWuIRpPpuA&list=PLonIF40eS6nzc7TqDshRo7k-mTM1Tu_j4
- <https://cuckoosandbox.org/>
- <https://cuckoo.readthedocs.io/en/latest/usage/feedback/>

Screen Shots :



Dashboard

Recent

Pending

Search

Submit

Summary

Static Analysis

Behavioral Analysis1

Network Analysis

Dropped Files6

Dropped Buffers

Process Memory1

Compare Analysis

Export Analysis

Reboot Analysis

Options

Feedback

Unlock sidebar

Summary

File CVE-2011-2462.pdf_

Download

Size	269.2KB
Type	PDF document, version 1.7
MD5	721fda5df552f4130218ad9bd2a4ab78
SHA1	5d89644214f2783b99491ebad61b4c5a8844f7e3
SHA256	036e049c625a2c3fc5f434d0784a2a215fbde7a90c561db730c
SHA512	Show SHA512
CRC32	286348D3
ssdeep	None
Yara	None matched

Score