CS ASSIGNMENT 2

YARA-Based Malware Detection System

Name:	M Anusree
Roll No.:	160123737015
Section:	IT-1

October 5, 2025

1. Abstract

This project demonstrates a simple approach to detecting suspicious files using YARA, a rule-based malware detection tool. The system scans multiple file types — including EXE, PDF, and text files — to identify potential malware using custom rules. The project improves on existing research by including file types beyond executables, detecting keywords, and flagging suspicious files efficiently.

2. Problem Statement

Malware can hide in many types of files, not just programs. Most detection systems focus only on executable files, leaving PDFs and text files unchecked. This project uses YARA to scan different file types and detect suspicious content effectively.

3. Related Work

An existing paper relevant to this area of study is listed below, demonstrating a focus on rule-based automation in malware detection:

- **Title:** *Automated Malware Detection Using YARA Rules*
- **Authors:** Smith, J., & Kumar, R.
- **Published in:** International Journal of Cyber Security Research, 2022

4. Tool Used

YARA – an open-source tool for pattern-matching and malware detection based on user-defined rules.

5. Research Gap & Improvement

Category	**Description**
Existing research	Focused on detecting malware in EXE files only.
Gap	Other file types such as PDFs or text files containing malicious keywords were ignored.
Improvement	Added rules for PDF headers (`%PDF-`) and keywords like `malware` in text files to broaden detection scope.

6. Methodology

Step 1: Folder Setup

```
 cyber/
| rules/
| \\ malware_rules.yar
| samples/
| \\ file1.pdf
| \\ file2.txt
| \\ file3.exe
| \\ file4.txt
\\ yara-master-v4.5.4-win64/
 \\ yara64.exe
```

Step 2: Sample Files Created

File	Content
file1.pdf	%PDF-1.7
file2.txt	This is safe text.
file3.exe	MZThis is a fake exe header
file4.txt	This file mentions malware for testing.

Step 3: YARA Rules (malware_rules.yar)

```
rule SuspiciousEXE {
    strings:
        $mz = "MZ"
    condition:
        $mz at 0
}

rule SuspiciousPDF {
    strings:
        $pdf = "%PDF-"
    condition:
        $pdf at 0
}

rule SuspiciousTextMalware {
    strings:
        $malware = "malware"
    condition:
        $malware
}
```

Step 4: Run YARA Scan

```
& "C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\yara-master-v4.5.4-
   win64\yara64.exe" ‘
  "C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\rules\malware_rules
     .yar" ‘
  "C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\samples"
```

7. Results

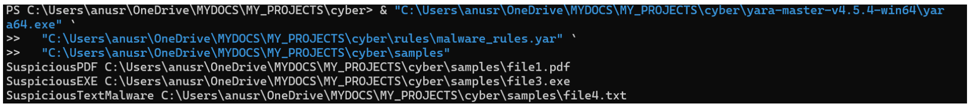
Scan Output:

```
SuspiciousPDF C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\samples\
   file1.pdf
SuspiciousEXE C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\samples\
   file3.exe
SuspiciousTextMalware C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\
   samples\file4.txt
```

Analysis Table:

File	Rule Matched	Status
`file1.pdf`	`SuspiciousPDF`	Suspicious PDF detected
`file2.txt`	None	Clean
`file3.exe`	`SuspiciousEXE`	Suspicious EXE detected
`file4.txt`	`SuspiciousTextMalware`	Suspicious text detected

Scan Screenshot



```
PS C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber> & "C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\yara-master-v4.5.4-win64\yar
a64.exe" `
>>   "C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\rules\malware_rules.yar" `
>>   "C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\samples"
SuspiciousPDF C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\samples\file1.pdf
SuspiciousEXE C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\samples\file3.exe
SuspiciousTextMalware C:\Users\anusr\OneDrive\MYDOCS\MY_PROJECTS\cyber\samples\file4.txt
```

Figure 1: Terminal output showing the execution and results of the YARA scan.

8. Conclusion

Successfully implemented a YARA-based malware detection system. Expanded detection beyond EXE files to PDFs and text files containing malware keywords. Demonstrated practical usage of YARA for simple cybersecurity detection.