

Group 7

Step 6: Mitigation

Team Members:-

1. Vamshi Krishna Bukka - 11693102 - vamshikrishnabukka@my.unt.edu
2. Sivabhavana Nelluri - 11702191 - sivabhavananelluri@my.unt.edu
3. Nithish Kumar Boggula - 11559328 - nithishKumarBoggula@my.unt.edu
4. Revanth Boddupalli - 11718089 - revanthBoddupalli@my.unt.edu
5. Vikram Reddy Allam - 11697684 - vikramallam@my.unt.edu

Memo: Implementation of the Ransomware Mitigation Component

Objective:

The design and implementation of a ransomware mitigation component that is activated by detections from our monitoring system are described in this component. When suspected ransomware activity is detected, the component uses a number of countermeasures to reduce harm and quickly restore system integrity.

System Overview:

When the monitor.py file from the monitoring component script detects odd file system actions, such the creation of files with extension like .enc, it generates mail to the admin that the ransomware mitigation component responds to.

Mitigation Strategy:

1. Immediate Response:

Alerting: System administrators receive an automated alert as soon as suspicious activity that detects ransomware.

Process Termination: In order to prevent the ransomware from encrypting or corrupting more files, all processes connected to the suspicious activity are immediately stopped concurrently.

2. Network Isolation:

Prevent Spread: The ransomware is isolated from the targeted network segments in order to stop it from contacting any command and control servers or spreading to more computers.

Traffic Control: To reduce the chance of data theft and additional malware downloads, firewall rules are used to restrict or block both incoming and outgoing network traffic.

3. Backup and Recovery:

Restoration: Backups are used to restore systems to their most recent, reliable configuration.

4. Preventive Measures:

Updates and Patching: To fix vulnerabilities that future ransomware attacks potentially exploit, all software and firmware should be updated continuously.

User Training: In order to stop future breaches, all users should receive regular instruction on the newest cybersecurity procedures and how to spot phishing attacks.

5. Defense in Depth:

Layered Security: It is the application of several security layers, such as intrusion detection, antivirus, and anti-malware software, among others, to offer all-around security.

Redundancy and Failover: Systems are built with redundancy and failover features to ensure availability even in the event of an attack.

Continuous Monitoring: Improvements to the system to better identify abnormalities and react to them.

Conclusion:

The mitigation component for ransomware is made to be both proactive and reactive, enhancing the entire security posture to prevent future events while resolving current threats. Our goal in putting these measures into practice is to make sure that our systems are resilient and dependable against advanced ransomware attacks.

Screenshots:

Firstly running mitigation and monitor code

```
sn1318@sn1318-virtualbox: ~/Desktop/compu... x sn1318@sn1318-virtualbox: ~/Desktop/compu... x sn1318@sn1318-virtualbox: ~/Desktop/compu... x
sn1318@sn1318-virtualbox:~/Desktop/computersecurity/monitoring$ python3 mitigation.py
Ransomware mitigation system initiated.
```

```
sn1318@sn1318-virtualbox: ~/Desktop/compu... x sn1318@sn1318-virtualbox: ~/Desktop/compu... x sn1318@sn1318-virtualbox: ~/Desktop/compu... x
sn1318@sn1318-virtualbox:~/Desktop/computersecurity/monitoring$ python3 monitor.py
Monitoring...
```


Now running the ransom script

```
sn1318@sn1318-virtualbox: ~/Desktop/compu... x sn1318@sn1318-virtualbox: ~/Desktop/compu... x sn1318@sn1318-virtualbox: ~/Desktop/compu... x
sn1318@sn1318-virtualbox:~/Desktop/computersecurity$ python3 script.py
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/Updated - Ransomware Project-1.pdf' encrypted successfully.
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/lab1/Lab1a_Network_Scanning.pdf' encrypted successfully.
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/lab2/Lab1b_Packet_Sniffing.pdf' encrypted successfully.
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/lab3/Lab2_Firewalls_IDS.pdf' encrypted successfully.
sn1318@sn1318-virtualbox:~/Desktop/computersecurity$
```

The detection component detects ransom, an alert is sent to admin, and it restores the data from backup.

```
sn1318@sn1318-virtualbox:~/Desktop/computersecurity/monitoring$
sn1318@sn1318-virtualbox:~/Desktop/computersecurity/monitoring$ python3 mitigation.py
Ransomware mitigation system initiated.
ALERT: Potential ransomware activity detected.
Alert sent to admin.
ACTION: Scanning for and terminating suspicious processes.
ACTION: Restoring data from backups using rsync.
Data successfully restored from ../critical-backup to ../critical.
```

Email:



untsegroup@gmail.com

to me ▾

7:59 PM (2 minutes ago) ☆ 😊 ↩ ⋮

The ransomware process has been identified and stopped. starting the process of recovery.