SOC ALERT ANALYSIS & PHISHING DETECTION

Mini Project Report

Submitted by:
Vidisha Singh

Course: B.Tech (Cyber Security)
College: Lakshmi Narain College of Technology

1.Introduction:

Cyber security plays an important role in protecting systems, networks, and data from cyber threats. Organizations face various attacks such as phishing, malware infections, and unauthorized access attempts.

A Security Operations Center (SOC) continuously monitors alerts, logs, and activities to identify and respond to security incidents. This mini project focuses on understanding basic SOC operations such as phishing detection and log analysis.

2.Problem Statement:

Phishing attacks and unauthorized login attempts are common security challenges faced by organizations. Attackers use fake emails and malicious links to trick users and steal sensitive information.

This project aims to identify phishing indicators and analyse system logs in order to detect suspicious activities and understand the working of a SOC environment.

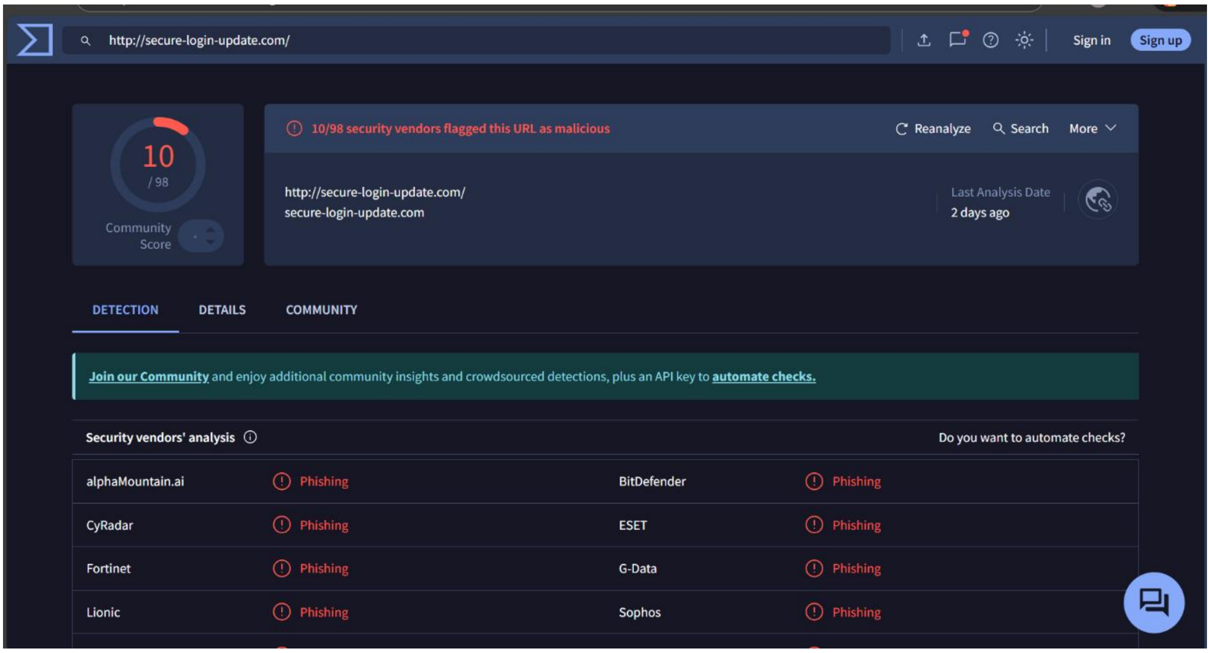
3.Tools Used:

- VirusTotal – Used to analyse suspicious URLs and check whether they are malicious or safe by scanning them with multiple security engines.
- Sample Phishing Emails – Used to understand common phishing patterns such as fake links, urgent messages, and social engineering techniques.
- Sample System Logs – Used to study login attempts and detect suspicious or brute-force activities.
- Google Chrome Web Browser – Used to access online tools such as VirusTotal and to perform research related to phishing detection.
- Microsoft Word – Used to prepare and document the project report.
- Microsoft PowerPoint – Used to create a presentation explaining the project workflow, analysis, and results.

4. Phishing Detection:

Phishing emails are designed to trick users into clicking malicious links or sharing sensitive information such as usernames and passwords. These emails often appear to come from trusted sources.

In this project, a sample phishing email was analyzed. The suspicious URL was checked using the VirusTotal platform. The analysis showed that the link was flagged as malicious or suspicious by multiple security engines, indicating a phishing attempt.



10/98 security vendors flagged this URL as malicious

http://secure-login-update.com/
secure-login-update.com

Last Analysis Date
2 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	BitDefender	Phishing
CyRadar	Phishing	ESET	Phishing
Fortinet	Phishing	G-Data	Phishing
Lionic	Phishing	Sophos	Phishing

The above screenshot shows the analysis of a suspicious URL using VirusTotal.

The URL was detected as malicious by multiple security vendors, indicating a phishing attempt.

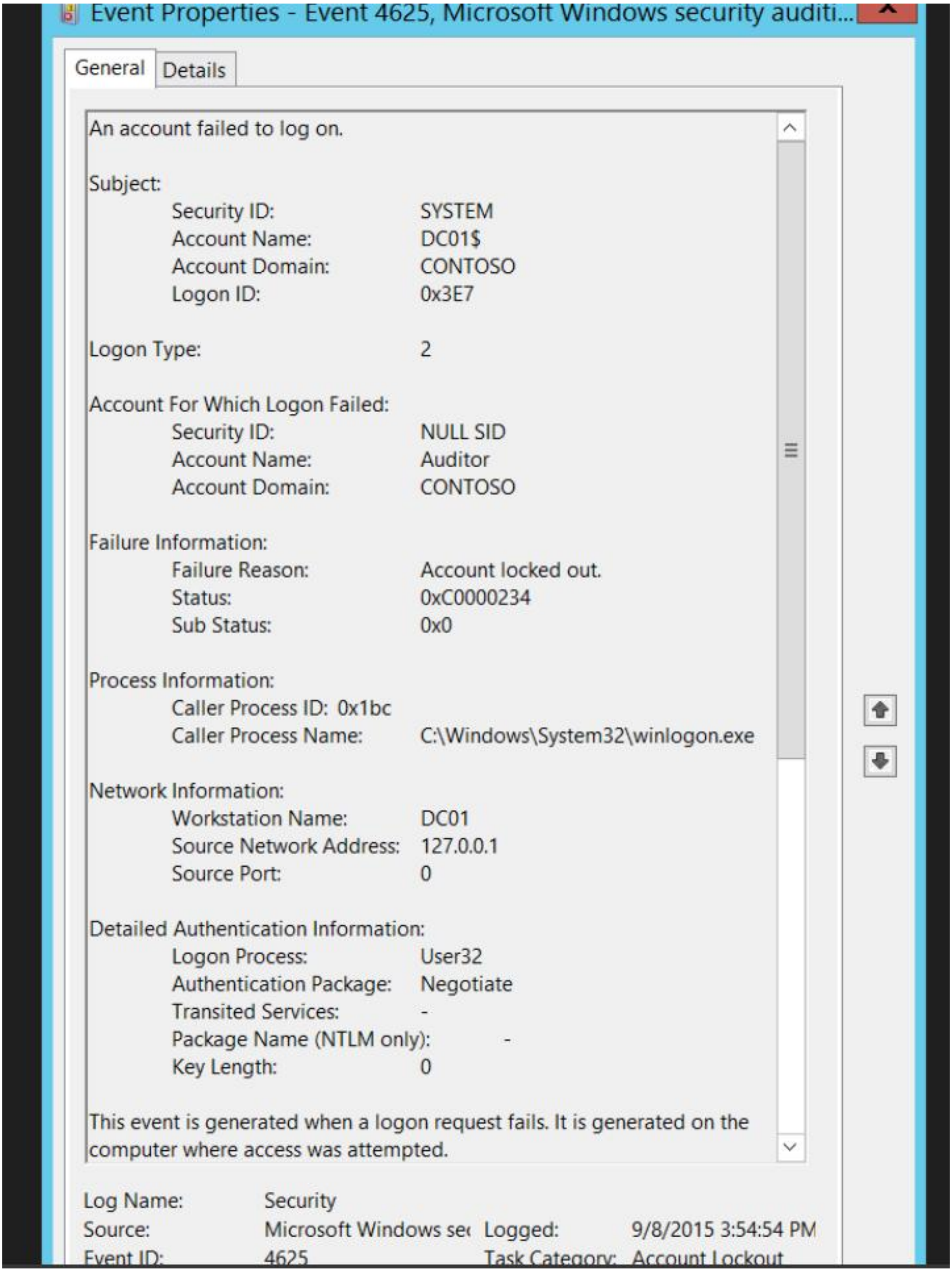
Such phishing links are commonly used to trick users into entering sensitive information like usernames and passwords.

SOC analysts use tools like VirusTotal to quickly identify and block malicious URLs.

5. Log Analysis:

System logs were analyzed to identify abnormal login behavior. One common indicator of an attack is multiple failed login attempts from the same user or source.

The analyzed log shows Event ID 4625, which represents a failed logon attempt. Such events may indicate brute-force attacks or unauthorized access attempts. Log analysis helps SOC analysts detect and respond to suspicious activities.


Event Properties - Event 4625, Microsoft Windows security auditi...
General
Details

```
An account failed to log on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DC01$
        Account Domain:         CONTOSO
        Logon ID:               0x3E7

Logon Type:                     2

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           Auditor
        Account Domain:         CONTOSO

Failure Information:
        Failure Reason:         Account locked out.
        Status:                 0xC0000234
        Sub Status:             0x0

Process Information:
        Caller Process ID: 0x1bc
        Caller Process Name:    C:\Windows\System32\winlogon.exe

Network Information:
        Workstation Name:       DC01
        Source Network Address: 127.0.0.1
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the
computer where access was attempted.
```

```
Log Name:    Security
Source:      Microsoft Windows sec  Logged:          9/8/2015 3:54:54 PM
Event ID:    4625                   Task Category:   Account Lockout
```

6.Incident Response Process

The incident response process followed in this project includes the following steps:

1. Identification – Detecting suspicious activity through logs or alerts.
2. Analysis – Analyzing phishing links and login failures.
3. Containment – Blocking malicious IPs or preventing further access.
4. Eradication – Removing threats from the system.
5. Recovery – Restoring normal system operations.
6. Lessons Learned – Improving security measures to prevent future incidents.

7.Result:

This project successfully demonstrated the basic functioning of a Security Operations Center (SOC).

It helped in understanding phishing detection, log analysis, and incident handling techniques used in real-world cybersecurity environments.

8. Conclusion:

This mini project provided practical knowledge about SOC operations and cybersecurity monitoring.

It improved understanding of phishing attacks, system log analysis, and incident response processes.

Such knowledge is essential for working in cybersecurity and SOC analyst roles.