LogHound User Manual

Table of Contents

---

1. Introduction

LogHound is a powerful forensic tool designed to analyze Windows Event Logs (EVTX) for potential security threats. It can detect:

- **Failed login attempts**
- **Privilege escalation events**
- **Account modifications**
- **Persistence techniques**
- **Suspicious service creations**
- **PowerShell activity**

The tool can export its findings into CSV or PDF reports for further investigation.

---

2. Installation

Prerequisites:

- **Python 3.x**
- **Required Python libraries:**

```
Unset
```

- `pip install pandas argparse reportlab xmltodict Evtx`

- **Administrative privileges (recommended for full access to system logs)**

---

3. Running LogHound

Note: The code should be run in PowerShell, and PowerShell must be run as an administrator

Basic Usage

Run the tool with the following command:

```
Unset
```

- `python loghound.py`

Available Command-Line Arguments

Unset

- `python loghound.py --logpath <LOG_DIRECTORY> --outputformat <csv|pdf> --outputpath <OUTPUT_DIRECTORY> --days <NUMBER_OF_DAYS>`

Argument	Description	Default Value
--logpath	Path to event log files	System logs
--outputformat	Report format: `csv` or `pdf`	csv
--outputpath	Directory where reports will be saved	User Documents/LogHound
--days	Number of days of logs to analyze	7

Example:

Unset

- `python loghound.py --outputformat pdf --days 30`

---

4. Features & Capabilities

Security Log Analysis:

- **Detects failed login attempts (Event ID 4625)**
- **Identifies privilege escalation (Event ID 4672)**
- **Monitors account modifications (Event IDs 4720, 4738, 4732)**

System Log Analysis:

- **Detects suspicious service creation (Event ID 7045)**

PowerShell Log Analysis:

- **Flags suspicious command execution (Event ID 4104)**
- **Looks for common attack patterns (e.g., Invoke-Mimikatz, Base64 encoded commands)**

---

5. Understanding the Output

After execution, LogHound provides a summary of findings and generates detailed reports in the specified format.

Example Output Summary:

```
Unset

- Windows Event Log Forensics Summary:
- ==================================
- Analysis Period: 2024-03-01 to 2024-03-07
- Output Directory: C:/Users/User/Documents/LogHound
- Output Format: csv
-
- Findings:
-   FailedLogins: 5 events
-   PrivilegeEscalation: 2 events
-   AccountModifications: 3 events
```

```
    ServiceCreation: 1 event
    PowerShellActivity: 7 events

Check the output directory for detailed reports.
```

---

6. Exporting Results

CSV Report:

Each category of findings is stored in separate CSV files. Example:

```
Unset
FailedLogins_20240307_123456.csv
PrivilegeEscalation_20240307_123456.csv
...
```

PDF Report:

If `--outputformat pdf` is selected, a professionally formatted PDF report is generated.

Example:

```
Unset
LogHound_Report_20240307_123456.pdf
```

---

7. Troubleshooting

1. Script does not detect logs

- **Ensure the tool is run with Administrator privileges.**

- **Check the log path (`C:/Windows/System32/winevt/Logs`).**

2. PDF export not working

- **Install ReportLab: `pip install reportlab`**

3. No suspicious activities detected

- **Increase the `--days` parameter to analyze a longer period.**

---

8. Frequently Asked Questions (FAQ)

Q: Can I run LogHound on a non-administrator account?

A: Yes, but some logs may be inaccessible without admin privileges.

Q: Where are the reports stored by default?

A: Reports are saved in `C:/Users/<YourUser>/Documents/LogHound/`.

Q: How do I analyze logs from a remote system?

A: Copy the EVTX logs from the remote system to a local directory and run LogHound with `--logpath <path_to_logs>`.

End of User Manual