Enhance Your Linux DFIR Skills With MasterParser

“Stop wasting time, let MasterParser do the work!”

C:\> whoami /all

EilayYosfan

- Israel
- 6 Years of IT and Security Experience
- PowerShell Developer
- Open Source DFIR Tool Maker
- YouTube Filmmaker
- Black Belt in jujitsu
- Threat Researcher and Incident Responder at “Security JOES”

Workshop Overview

What Will You Learn Today ?

Theoretical

- Linux Logs Fundamentals
- How Linux Logging Works?
- Deep Dive into Authentication Logs
- What is MasterParser?
- How to Use MasterParser?

Workshop Overview

What Will You Learn Today ?

Practical

- Scenario 1 - FTP Brute-Force Attack
- Scenario 2 - The Disgruntled Employee
- Scenario 3 - Why The Server is Unavailable ?
- Scenario 4 - Reconnaissance Activity
- MasterParser Code Dive
- Conclusion and Questions

Linux Logs Fundamentals

(Ubuntu Examples)

What Are Linux Logs?

A Linux log is simply a file that records specific information like events, applications, kernel operations, and much more. When you encounter an issue or even a security risk, these files can prove to be critically important tools for troubleshooting or understanding what is happening on system.

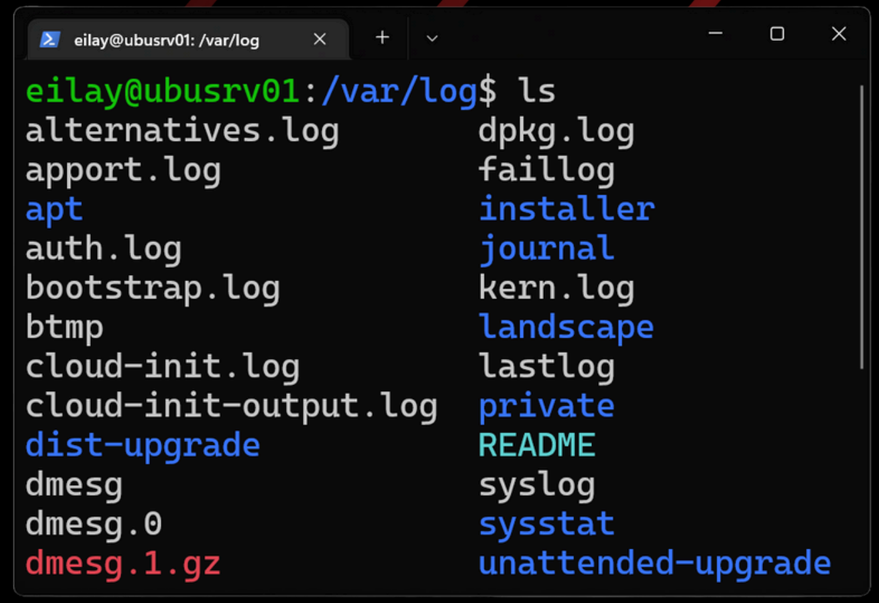
A Linux log can contain information like:

- Kernel Events
- Users Activity's
- Errors and Warnings
- Application Messages
- Authentication Details

Where to Find Linux Logs?

Linux has a special directory for storing logs **“/var/log/“**
This directory contains logs from various sources like the kernel, services, applications running on it, users activity’s on the system, errors, messages and more.

Some applications also write logs in to a proprietary folder inside of the “/var/log/” folder, for example the Apache web server writes logs to the “/var/log/apache2/” directory.



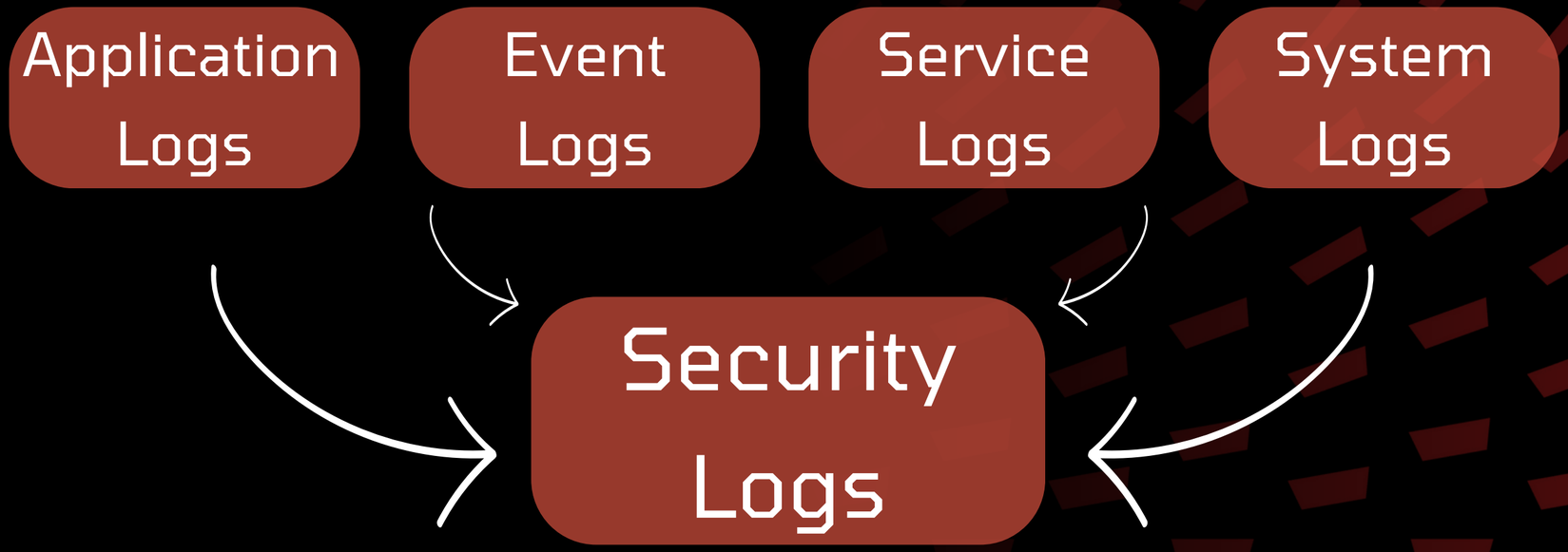
Common Categories of Linux Logs

Linux logs can be classified into different types based on their source or purpose. Most Linux log directories can be grouped into four main categories:

- Application Logs
- Event Logs
- Service Logs
- System Logs

Common Categories of Linux Logs

Linux logs can be classified into different types based on their source or purpose. Most Linux log directories can be grouped into four main categories:



How Linux Logging Works?

(Ubuntu Examples)

Which is Easier to Read and Understand?

2024-05-05T11:40:00 Accepted password for eilay from 192.168.2.10 port 65107 ssh2
Failed password for eilay at Fri, 06 May 2024 11:40:00 GMT from 192.168.2.10 port 64853 ssh2
changed user 'Kevin' information at May 06, 2024 11:40:00
05/06/2024 11:40:00 pam_unix(passwd:chauthtok): password changed for Max
change user 'Max' password at 06/05/2024 11:40:00

Dec 22 14:24:49 eilay-desktop sshd[1074]: Accepted password for eilay from 192.168.2.10 port 65107 ssh2
Dec 23 19:24:44 eilay-desktop sshd[1094]: Failed password for eilay from 192.168.2.10 port 64853 ssh2
Dec 24 19:35:34 eilay-desktop chfn[2374]: changed user 'Kevin' information
Dec 25 10:25:58 eilay-desktop passwd[2639]: pam_unix(passwd:chauthtok): password changed for Max
Dec 26 16:26:10 eilay-desktop usermod[2248]: change user 'Max' password

What is syslog?

Syslog is a protocol that computer systems use to send event data logs to a central location for storage. Logs can then be accessed by analysis and reporting software to perform audits, monitoring, troubleshooting, and other essential IT or Security operational tasks.

The go-to logging method since the 1980s, the syslog protocol has maintained its popularity through its ease of use, making it simple and straightforward to transport event log messages.

The syslog History

Syslog was developed in the 1980s by Eric Allman as part of the “Sendmail” project. and has since become the standard logging solution on Unix-like systems.

But there was a problem

Syslog originally functioned as a de facto standard, without any authoritative published specification, and many implementations existed, some of which were incompatible. Although it has been popular for decades, syslog hasn’t always been easy to define, due to lack of standardization.

The Solution

Due to incompatibilities and a lack of standardization, the IETF created two Request for Comments (RFC) documents to standardize the event log format issue and establish a standard for how event logs should appear.

RFC 3164 & RFC 5424

RFC 3164 - created in August 2001 as the initial guide on how the event log format should appear, was also known as the 'old syslog' or 'BSD syslog'. This RFC is not considered a standard.

RFC 5424 - created in March 2009, is considered a standard. This format provides more structured and standardized data for syslog messages than RFC 3164.

Understand RFC 3164 Format

Disclaimer - as of today, the default syslog software in Debian is rsyslog, and rsyslog default format is RFC 3164. Therefore, for this workshop, we will only analyze examples in RFC 3164 format (ISO 8601).

RFC 3164 Explained:

MMM DD hh:mm:ss HOSTNAME TAG: MESSAGE

- MMM DD hh:mm:ss — ISO 8601, Log timestamp.
- HOSTNAME — From what device this log came from.
- TAG — Mostly process name with process ID.
- MESSAGE — The description of the event log, what is the event all about.

RFC 3164 Real Event Log Example:

Dec 22 16:54:10 eilay-desktop usermod[2248]: change user 'Max' password

How Linux Logging Works

Learning Path

How Linux Logging Works

Learning Path

What is rsyslog?

The **r**ocket-fast **sys**tem for **log** processing

Rsyslog is an open-source software utility used on Unix-like computer systems for forwarding log messages. rsyslog uses the standard BSD syslog protocol, specified in RFC 3164.

rsyslog offers high-performance, great security features and a modular design. While it started as a regular syslogd, rsyslog has evolved into a kind of swiss army knife of logging.

Later on, we'll have a cool scenario on how to detect if an attacker has stopped the rsyslog services.

Deep Dive Into Auth.Log

What is Auth.Log?

The auth.log is a system log file that records authentication-related events. It contains information about user logins, logouts, authentication failures, and other security-related events.

Monitoring auth.log can help system administrators and security teams track user activity, identify potential security threats, and troubleshoot authentication issues. It's an essential component of system security and auditing in Linux environments

```
Jan 22 09:57:37 UBUSRV01 systemd-logind[662]: New seat seat0.
Jan 22 09:57:37 UBUSRV01 systemd-logind[662]: Watching system button
Jan 22 09:57:37 UBUSRV01 systemd-logind[662]: Watching system button
Jan 22 09:57:37 UBUSRV01 systemd-logind[662]: Watching system button
Jan 22 09:57:38 UBUSRV01 sshd[747]: Server listening on 0.0.0.0 port
Jan 22 09:57:38 UBUSRV01 sshd[747]: Server listening on :: port 22.
Jan 22 09:58:24 UBUSRV01 login[679]: pam_unix(login:session): sessio
Jan 22 09:58:24 UBUSRV01 systemd-logind[662]: New session 1 of user
Jan 22 09:58:25 UBUSRV01 systemd: pam_unix(systemd-user:session): se
Jan 22 09:59:37 UBUSRV01 systemd-logind[662]: New seat seat0.
Jan 22 09:59:37 UBUSRV01 systemd-logind[662]: Watching system button
Jan 22 09:59:37 UBUSRV01 systemd-logind[662]: Watching system button
Jan 22 09:59:37 UBUSRV01 systemd-logind[662]: Watching system button
Jan 22 09:59:39 UBUSRV01 sshd[810]: Server listening on 0.0.0.0 port
Jan 22 09:59:39 UBUSRV01 sshd[810]: Server listening on :: port 22.
Jan 22 10:03:39 UBUSRV01 login[686]: pam_unix(login:auth): authentic
Jan 22 10:03:43 UBUSRV01 login[686]: FAILED LOGIN (1) on '/dev/tty1'
```

Auth.Log ID

Full Name: Authentication Log.
Log Location: “/var/log/Auth.Log”
Log Format: RFC 3164
Availability: Included by default in Ubuntu.
Read & Write: The user “syslog” or “root”.
Read Only: Member of “adm” group.
Logrotate: Active.

```
"auth.log*"
      9545 May  5 09:30 auth.log
   2345826 Mar 21 11:20 auth.log.1
    250263 Mar 21 11:21 auth.log.2.gz
    220031 Mar 21 11:21 auth.log.3.gz
    185754 Mar 21 11:21 auth.log.4.gz
```

```
eilay@ubusrv01: /var/log
eilay@ubusrv01:/var/log$ ls -l /var/log/auth.log
-rw-r----- 1 syslog adm 21719 May  5 08:45 /var/log/auth.log
```

Auth.Log - Treasure for IR Cases

What can you find in Auth.Log?

- Group Activity
  - User Add To Group
  - User Removed From a Group
  - Group Creation
  - Group Deletion
  - Group Renaming
  - Group Permission Change
- Elevated Activity
  - Elevated Command Executions
  - Sudo execution timeline
  - Non sudoers activity
- Device Control
  - Detect What Device Connected to Host
  - When Host Turn On\Off
- SSH / FTP
  - Logins / Logouts
  - Valid / Nonvalid Login
  - Timelines
  - Brute-Force Detection
- CRON
  - Scheduled Task Execution Record
- User Activity
  - User Creation
  - User Deletion
  - System Login / Logout
  - User Password Resets
  - User Information Change

MasterParser

"Stop wasting time, let MasterParser do the work!"

What is MasterParser?

MasterParser stands as a robust Digital Forensics and Incident Response tool meticulously crafted for the analysis of Linux logs within the var/log directory.

Specifically designed to expedite the investigative process for security incidents on Linux systems, MasterParser adeptly scans supported logs, such as auth.log for example, extract critical details like SSH logins, user creations, event names, IP addresses and much more. The tool's generated summary presents this information in a clear and concise format, enhancing efficiency and accessibility for Incident Responders.

How to Use MasterParser?

Open GitHub and follow my instructions
We will do the first scenario together

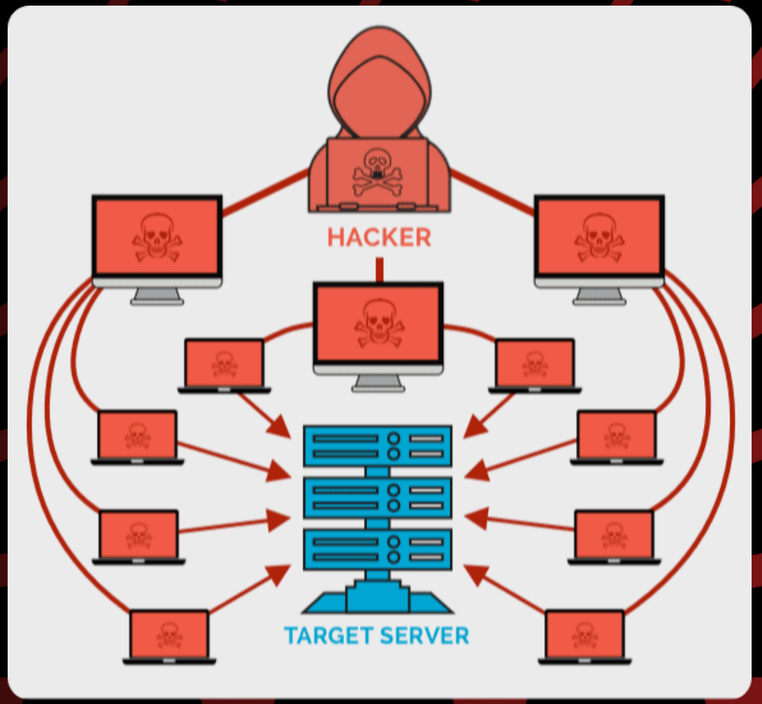
Exercises and Scenarios

Scenario 2 - The Disgruntled Employee

- Analysis Time: 15 Minutes
- Try both manual and automatic analysis
- Understand what happened
- Write a report about it

Scenario 3 - Why The Server is Unavailable?

- Analysis Time: 20 Minutes
- Try both manual and automatic analysis
- Understand what happened
- Write a report about it



Scenario 4 - Reconnaissance Activity

- Analysis Time: 15 Minutes
- Try both manual and automatic analysis
- Understand what happened
- Write a report about it

MasterParser Code Dive

Conclusion and Questions

What Did You Learn Today?

- Linux Log Fundamentals
  - What are Linux logs
  - Where you can find them
  - What is the content of Linux logs
- How Linux Logging Works
  - Log Protocols
  - Log Formats
  - syslog Software
- Deep Dive Into Auth.Log
  - What is Auth.Log
  - Why it is so important
  - What is the content of auth.log
- MasterParser
  - What is MasterParser
  - How to use MasterParser
- Exercises and Scenarios
  - 01 - FTP Brute-Force Attack
  - 02 - The Disgruntled Employee
  - 03 - Why The Server is Unavailable
  - 04 - Reconnaissance Activity
- MasterParser Code Dive
  - Take part in the making of it !

Stay in Touch !

EilayYosfan

Visit Security Joes Website

Detect & Respond to security incidents anywhere, anytime. Remotely.