Analisis Sistem Operasi Linux & macOS: Log, Artefak, dan Persistensi

Memahami jejak digital dalam investigasi keamanan siber

Author: Edy Susanto

Pentingnya Analisis Log dan Artefak dalam Forensik Digital

Log Sistem

Log sistem seperti syslog dan bash_history menyimpan jejak aktivitas pengguna dan sistem secara komprehensif, memberikan timeline kejadian penting.

Artefak macOS

macOS memiliki artefak unik seperti plists, Spotlight, dan Unified Logs yang kaya informasi untuk investigasi mendalam.

Deteksi Ancaman

Praktik analisis log membantu menemukan indikator persistensi dan aktivitas mencurigakan dalam sistem operasi.

Author: Edy Susanto

Log Penting di Linux: syslog dan bash_history

Syslog

Menyimpan catatan sistem dan aplikasi secara terpusat.

- Lokasi: /var/log/syslog atau /var/log/messages
- Mencatat event sistem, error, dan warning
- Format timestamp dan severity level

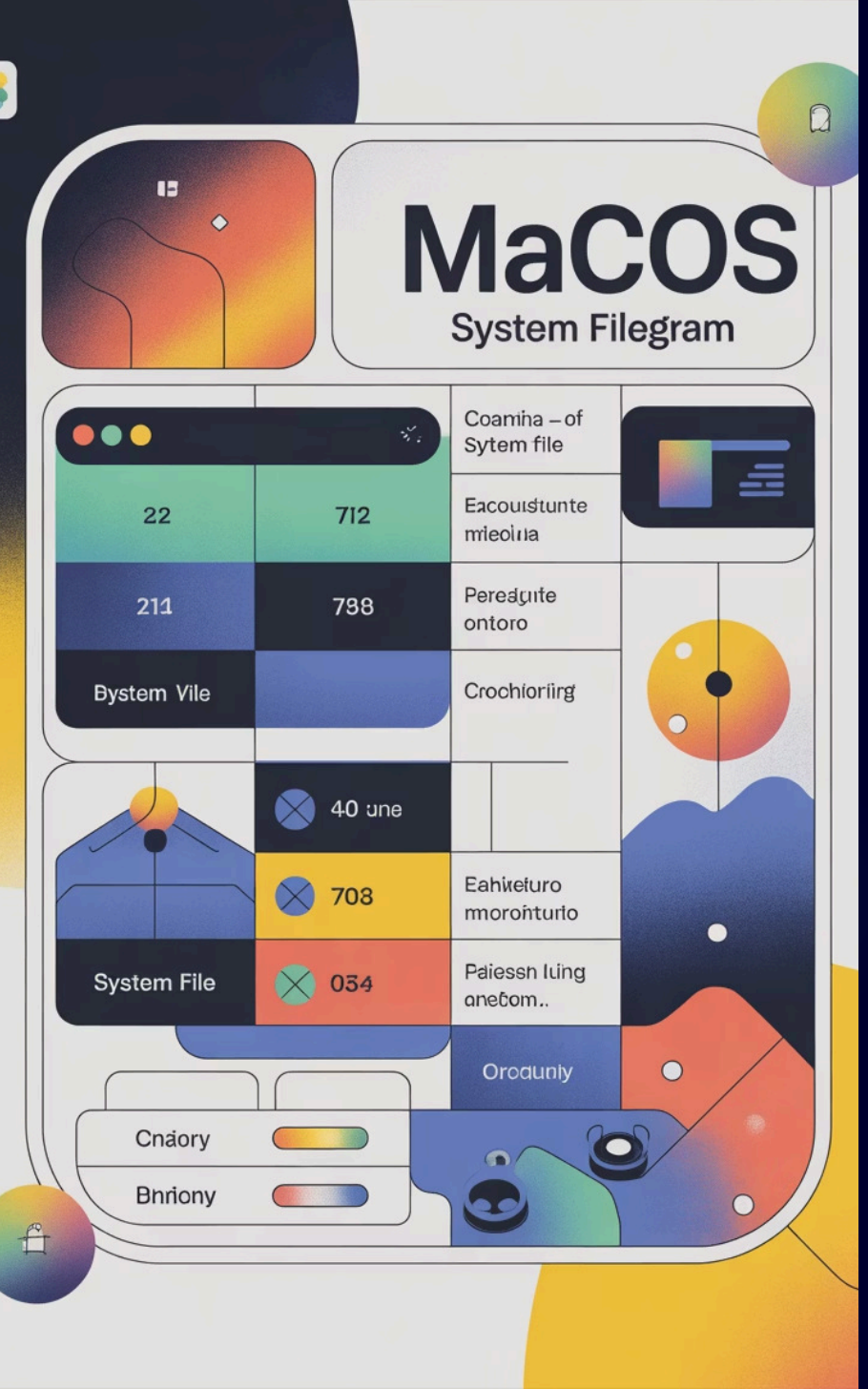
Bash History

Riwayat perintah shell pengguna yang detail.

- File: ~/.bash_history
- Jejak aktivitas user di command line
- Dapat mengungkap perintah mencurigakan

Contoh temuan: perintah mencurigakan, akses root tidak terdokumentasi, atau eksekusi skrip otomatis yang tidak dikenal.

Author: Edy Susanto



Artefak Khas macOS: Plists, Spotlight, dan Unified Logs

01

Property Lists (Plists)

File konfigurasi .plist mengatur startup dan preferensi sistem, termasuk LaunchAgents dan LaunchDaemons yang mengontrol proses background.

02

Spotlight Index

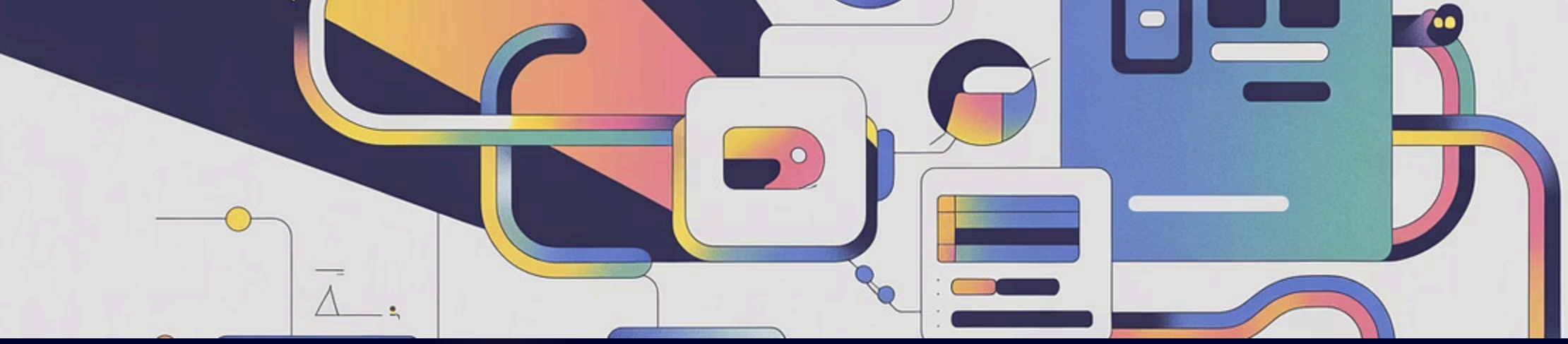
Sistem indeks pencarian yang menyimpan metadata file dan aktivitas pengguna, memberikan wawasan tentang file yang diakses dan dibuat.

03

Unified Logs

Sistem logging terpusat macOS yang menyimpan event sistem dan aplikasi secara detail dengan timestamp presisi tinggi.

Author: Edy Susanto



Teknik Persistensi di macOS: LaunchAgents & LaunchDaemons

1	2	3
Mekanisme Persistensi Malware sering menggunakan file .plist di direktori ~/Library/LaunchAgents atau /Library/LaunchDaemons untuk memastikan auto-start saat sistem boot.	**Studi Kasus: Silver Sparrow** Malware Silver Sparrow (2021) menggunakan LaunchDaemons untuk bertahan di Mac M1, menginfeksi ribuan perangkat sebelum terdeteksi.	**Metode Deteksi** Periksa plist mencurigakan dengan perintah `launchctl list` dan `find` pada direktori plist untuk identifikasi anomali.

```
find ~/Library/LaunchAgents -type f -name "*.plist"
launchctl list | grep -v "com.apple"
```

Author: Edy Susanto

Teknik Persistensi di Linux: Cron Jobs dan Skrip Otomatis

Lokasi Kritis

- /etc/crontab
- /etc/cron.d/
- /var/spool/cron/
- User crontab (crontab -e)

Vektor Serangan

Cron jobs memungkinkan penjadwalan tugas berulang yang dapat disalahgunakan oleh attacker untuk persistensi.

> Malware dapat menambahkan cron job untuk menjalankan payload secara periodik tanpa interaksi user, mempertahankan akses jangka panjang.

Deteksi Efektif

Audit crontab dengan `crontab -l` dan periksa file cron di /etc/cron.* untuk entry mencurigakan atau tidak dikenal.

Author: Edy Susanto

Praktik: Menemukan Indikator Persistensi dan Aktivitas User

Audit File Plist

Cari file plist baru atau dimodifikasi di macOS dengan `find ~/Library/LaunchAgents -mtime -7` untuk mendeteksi perubahan dalam 7 hari terakhir.

Periksa Cron & History

Audit cron jobs dan bash_history di Linux untuk perintah atau jadwal mencurigakan yang mengindikasikan aktivitas malicious.

Query dengan Osquery

Gunakan tools seperti osquery untuk query log dan aktivitas proses secara terstruktur, memudahkan analisis forensik mendalam.

Author: Edy Susanto

Studi Kasus: Analisis Persistensi Malware macOS dengan Osquery

Kekuatan Osquery dalam Forensik

Osquery mengubah sistem operasi menjadi database SQL relasional, memudahkan audit file, proses, network connection, dan konfigurasi sistem secara real-time.

Aktivasi Audit

Enable audit event di /etc/security/audit_control untuk capture detail eksekusi proses dan system call.

Query Proses

Jalankan query SQL untuk mendeteksi proses mencurigakan dan analisis hubungan parent-child process tree.

Identifikasi Anomali

Temukan pola abnormal seperti proses tanpa parent, koneksi network ke IP asing, atau file binary tersembunyi.

```
SELECT pid, name, path, parent FROM processes
WHERE path NOT LIKE '/System/%'
AND path NOT LIKE '/usr/%';
```

Author: Edy Susanto

Tips Hardening dan Mitigasi Persistensi

Strategi Perlindungan Proaktif

System Integrity Protection

Batasi hak tulis pada direktori LaunchDaemons dengan SIP (System Integrity Protection) di macOS untuk mencegah modifikasi unauthorized.

Audit Rutin

Nonaktifkan cron job yang tidak dikenal dan periksa login items di macOS System Preferences secara berkala.

Monitoring Tools

Gunakan monitoring tools seperti KnockKnock dan Jamf Protect untuk deteksi dini persistensi mechanism dan anomali sistem.

Author: Edy Susanto

Kesimpulan & Langkah Selanjutnya

Kunci Investigasi

Analisis log dan artefak adalah kunci mengungkap aktivitas tersembunyi dan mekanisme persistensi dalam sistem operasi modern.

Pendekatan Holistik

Kombinasi teknik analisis Linux dan macOS memperkuat kemampuan forensik digital dan threat hunting yang komprehensif.

Praktik Berkelanjutan

Praktikkan audit rutin dan gunakan tools otomatis untuk menjaga keamanan sistem serta deteksi ancaman lebih awal.

Rekomendasi: Lanjutkan pembelajaran dengan hands-on lab, ikuti threat intelligence feeds, dan bergabung dengan komunitas forensik digital untuk terus update teknik terbaru.

Author: Edy Susanto