Network Forensics & Log Analysis

Modul mendalam tentang investigasi forensik jaringan dan analisis log untuk profesional keamanan siber

Agenda Pembelajaran

01

Pengantar Network Forensics

Konsep dasar dan ruang lingkup investigasi jaringan

02

Dasar-Dasar Packet Capture

Teknik pengumpulan dan jenis data jaringan

03

Analisis dengan Wireshark

Investigasi mendalam menggunakan tools profesional

04

Analisis Log & Korelasi

Menggabungkan berbagai sumber data untuk insight

05

Praktik Lab Hands-on

Simulasi investigasi kasus data exfiltration

Tujuan Pembelajaran

Setelah menyelesaikan modul ini, Anda akan mampu melakukan investigasi forensik jaringan secara komprehensif dan profesional.

- Memahami konsep dasar **forensik jaringan** dan pentingnya analisis log dalam investigasi keamanan siber
- Melakukan **packet capture** dan analisis trafik menggunakan **Wireshark** untuk mengidentifikasi aktivitas mencurigakan
- Mengidentifikasi tanda-tanda **data exfiltration** atau **command & control (C2)** activity dalam jaringan
- Melakukan korelasi antara berbagai sumber log (firewall, proxy, IDS, SIEM) untuk membangun timeline serangan
- Menyusun laporan analisis jaringan berbasis bukti yang dapat digunakan untuk tindakan hukum

Apa Itu Network Forensics?

Network forensics adalah cabang dari digital forensics yang berfokus pada pemantauan, pencatatan, dan analisis aktivitas jaringan komputer untuk tujuan investigasi keamanan, deteksi intrusi, dan pengumpulan bukti digital.

Definisi & Ruang Lingkup

Forensik jaringan mencakup proses sistematis untuk menangkap, merekam, dan menganalisis event jaringan guna menemukan sumber serangan, melacak aktivitas mencurigakan, dan mengidentifikasi kebocoran data.

Tujuan Utama

- Menemukan aktivitas mencurigakan dalam trafik jaringan
- Tracing pelaku serangan siber
- Memverifikasi kebocoran data (data breach)
- Mengumpulkan bukti digital untuk proses hukum

Karakteristik Bukti Jaringan

Volatile

Data jaringan bersifat sementara dan mudah hilang jika tidak segera ditangkap. Bukti dapat menguap dalam hitungan detik atau menit.

Cepat Berubah

Trafik jaringan terus berjalan dan berubah setiap saat. Window of opportunity untuk menangkap bukti sangat terbatas.

Dokumentasi Presisi

Membutuhkan pencatatan yang sangat detail termasuk timestamp, metadata, dan chain of custody untuk validitas hukum.

Penting: Karena sifatnya yang volatile, respons cepat dan prosedur capture yang tepat sangat krusial dalam forensik jaringan. Keterlambatan beberapa menit saja dapat menyebabkan hilangnya bukti penting.

Etika & Legalitas dalam Network Forensics

Pengumpulan data jaringan harus mematuhi regulasi hukum dan standar etika profesional. Pelanggaran dapat membatalkan bukti dan menimbulkan konsekuensi hukum.

Consent & Authorization

Pastikan Anda memiliki izin yang sah untuk melakukan monitoring dan packet capture. Dalam konteks perusahaan, biasanya tercakup dalam kebijakan IT dan kontrak kerja karyawan.

Warrant & Legal Basis

Untuk investigasi kriminal, warrant atau surat perintah dari otoritas yang berwenang mungkin diperlukan. Pahami yurisdiksi dan regulasi lokal yang berlaku.

Chain of Custody

Dokumentasikan setiap langkah pengumpulan, penyimpanan, dan analisis bukti. Maintain integritas bukti dengan hash verification dan access logging untuk keperluan legal.

Dasar-Dasar Packet Capture

Jenis Data Jaringan

Packet

Data mentah level terendah yang berisi header dan payload lengkap dari setiap frame jaringan.

Flow

Agregasi dari packets yang terkait dalam satu sesi komunikasi, lebih ringkas untuk analisis volume tinggi.

Log

Catatan event yang dihasilkan oleh perangkat jaringan seperti firewall, IDS, atau proxy server.

Tools Umum

- **Wireshark** — GUI-based packet analyzer paling populer
- **tcpdump** — Command-line packet capture untuk Unix/Linux
- **Tshark** — Versi CLI dari Wireshark
- **NetworkMiner** — Network forensics analysis tool
- **Zeek (Bro)** — Network security monitoring framework
- **Moloch (Arkime)** — Full packet capture dan indexing system

File Format & Teknik Capture

File Format Utama

.pcap (Packet Capture) — Format standar untuk menyimpan packet capture data, kompatibel dengan hampir semua tools analisis.

.pcapng (Packet Capture Next Generation) — Format lebih modern yang mendukung metadata tambahan, multiple interface capture, dan enhanced timestamps.

Inline Capture

Penempatan capture point pada **gateway, IDS, atau span port switch** untuk monitoring trafik yang melewati chokepoint jaringan. Ideal untuk menangkap trafik keluar-masuk jaringan organisasi.

Host-Based Capture

Capture dilakukan langsung pada **endpoint atau workstation** untuk memonitor trafik lokal spesifik. Berguna untuk investigasi targeted pada host yang dicurigai terinfeksi malware.

Praktik terbaik: lakukan pengumpulan data jaringan tanpa mengganggu operasional sistem. Gunakan dedicated capture interface dan pastikan storage capacity mencukupi untuk high-volume traffic.

Analisis dengan Wireshark

Wireshark adalah tools packet analyzer paling populer yang menyediakan kemampuan inspeksi mendalam terhadap ratusan protokol jaringan dengan interface yang user-friendly.

Navigasi & Filter Dasar Wireshark

Display Filters Esensial

```
ip.addr == 192.168.1.100
tcp.port == 443
http contains "password"
dns.qry.name contains "malicious"
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

Display filters memungkinkan Anda menyaring tampilan packet tanpa mengubah file capture asli. Sangat powerful untuk fokus pada subset data yang relevan.

Capture Filters

```
host 10.0.0.5
port 80 or port 443
net 192.168.0.0/24
not broadcast and not multicast
```

Capture filters diterapkan saat proses capture untuk mengurangi volume data yang disimpan. Menggunakan syntax BPF (Berkeley Packet Filter).

Tips: Gunakan capture filters untuk mengurangi noise pada saat capture, dan display filters untuk eksplorasi analisis detail setelah capture selesai.

Identifikasi Protokol & Pola Anomali

Unusual DNS Queries

Query DNS dengan panjang domain abnormal, format hex encoding, atau query ke domain generation algorithm (DGA) mengindikasikan komunikasi malware dengan C2 server. Perhatikan high-frequency queries ke domain baru.

Large Outbound Transfer

Volume data keluar yang tidak biasa, terutama ke IP eksternal yang tidak dikenal atau pada jam-jam tidak normal, dapat mengindikasikan data exfiltration atau pencurian informasi sensitif.

Repeated Failed Connections

Koneksi berulang yang gagal ke berbagai port mengindikasikan port scanning atau brute force attack. Perhatikan pola SYN packets tanpa handshake completion.

Protokol umum untuk dianalisis: **HTTP/HTTPS** (web traffic), **DNS** (name resolution), **FTP** (file transfer), **SSH** (remote access), **ICMP** (ping/traceroute), **SMB** (file sharing).

Ekstraksi File & Payload dari PCAP

Identifikasi Stream

Gunakan "Follow TCP Stream" atau "Follow HTTP Stream" untuk melihat komunikasi lengkap antara dua host.

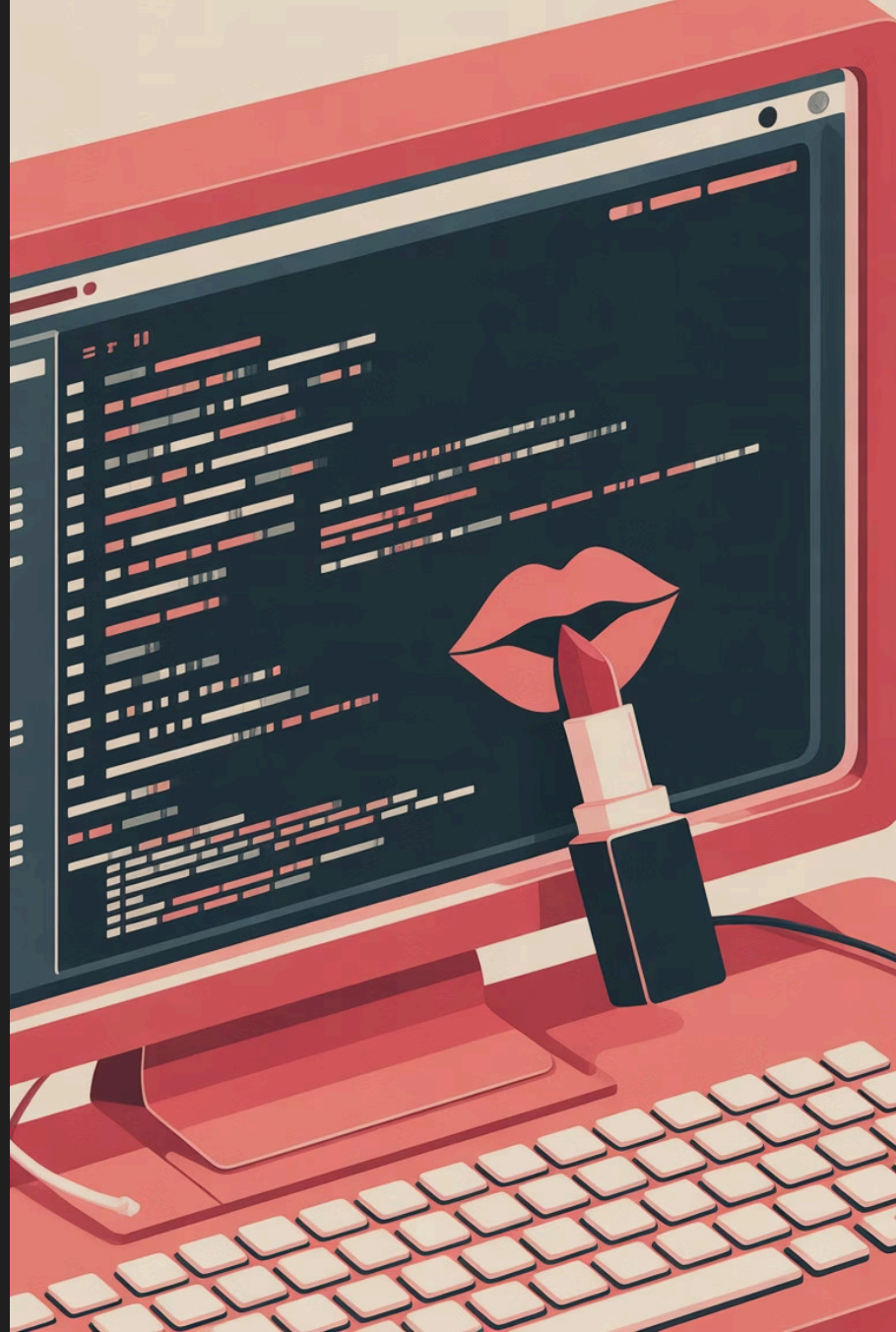
Filter Objek

Wireshark dapat secara otomatis mengekstrak objek HTTP, SMB, TFTP, dan protokol lainnya dari capture file.

Export & Verify

Export file untuk pemeriksaan lanjutan dengan antivirus, sandbox, atau static analysis tools. Hitung hash untuk chain of custody.

Menu: **File → Export Objects → HTTP/SMB/TFTP**. Pastikan untuk men-quarantine file yang diekstrak dalam environment terisolasi sebelum analisis untuk menghindari infeksi.



Analisis Log & Korelasi Data

Analisis log adalah proses sistematis untuk memeriksa, menggabungkan, dan mengkorelasikan catatan event dari berbagai sumber untuk mendapatkan gambaran komprehensif tentang insiden keamanan.

Korelasi data dari multiple sources sangat penting karena single log source jarang memberikan complete picture dari sebuah serangan. Threat actor sophisticated sering menggunakan multiple vectors dan techniques.

Jenis Log Utama dalam Network Forensics

1

Firewall Logs

Mencatat setiap koneksi yang diblokir atau diizinkan, termasuk source/destination IP, port, protokol, dan action yang diambil. Sangat berguna untuk mengidentifikasi anomali port dan unauthorized access attempts.

2

Proxy Logs

Merekam aktivitas browsing pengguna termasuk URL yang diakses, user agent, response code, dan byte transferred. Essential untuk mendeteksi akses ke website berbahaya atau phishing.

3

IDS/IPS Logs

Berisi signature-based alerts tentang potensi serangan, exploit attempts, atau aktivitas mencurigakan. Timestamp yang akurat sangat penting untuk korelasi dengan sumber log lainnya.

4

SIEM Data

Security Information and Event Management system mengagregasi dan mengkorelasikan log dari berbagai sumber secara otomatis. Menyediakan alerting, dashboard, dan correlation rules yang sophisticated.

Teknik Korelasi Manual

1

Match IP Addresses

Identifikasi IP source dan destination yang sama di berbagai log sources untuk melacak pergerakan attacker atau malware communication.

2

Synchronize Timestamps

Pastikan semua log sources menggunakan NTP yang sama. Konversi ke UTC jika diperlukan untuk menghindari timezone confusion dalam timeline.

3

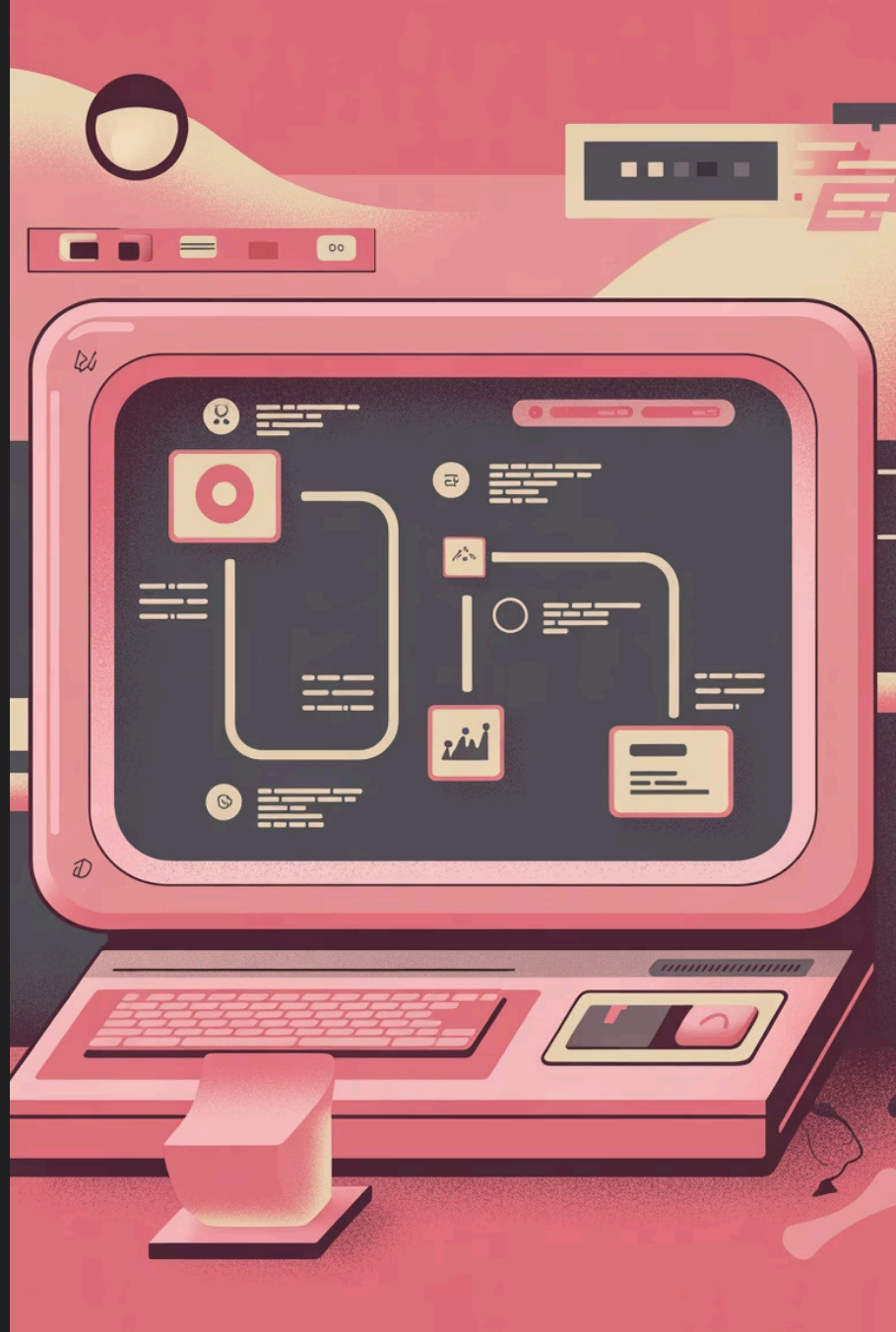
Correlate Event Types

Hubungkan event yang berbeda namun related, misalnya: firewall block → IDS alert → endpoint antivirus detection untuk membangun attack chain.

4

Build Attack Timeline

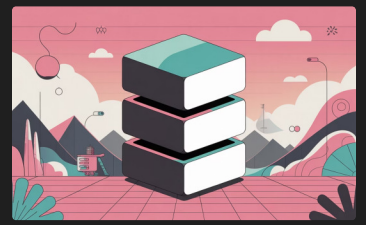
Susun kronologi lengkap dari initial compromise hingga exfiltration untuk memahami tactics, techniques, and procedures (TTPs) attacker.



Tools untuk Analisis & Korelasi Log

Splunk

Platform SIEM terkemuka dengan kemampuan search, monitoring, dan analisis data machine-generated yang powerful. Mendukung custom dashboards dan correlation rules yang kompleks.



ELK Stack

Kombinasi **Elasticsearch** (search engine), **Logstash** (log aggregation), dan **Kibana** (visualization). Open-source solution yang scalable untuk log management.

Graylog

Open-source log management platform dengan real-time search, alerting, dan dashboarding capabilities. Cocok untuk organizations dengan tight budget.

Praktik Lab: Analisis Data Exfiltration

Skenario: Anda adalah forensic analyst yang diminta menganalisis file `exfiltration.pcap` setelah security team mendeteksi aktivitas mencurigakan dari workstation karyawan. Tugas Anda adalah mengidentifikasi apakah terjadi data theft dan menentukan scope dari insiden tersebut.

Langkah-Langkah Investigasi Lab

Filter Outbound Traffic

Buka file di Wireshark dan aplikasikan filter: `ip.src == <internal_ip> && tcp.port == 443` untuk melihat trafik keluar yang suspicious, terutama komunikasi encrypted yang mencurigakan.

Detect C2 Communication

Gunakan filter: `dns && dns.qry.name contains "strange-domain"` untuk menemukan query DNS ke domain yang tidak biasa atau menggunakan DGA patterns yang umum pada malware.

Identify Periodic Patterns

Analisis komunikasi periodik antar host yang mengindikasikan beacon behavior dari malware. Perhatikan interval yang teratur atau komunikasi ke IP eksternal yang repeated.

Cross-Check Logs

Validasi temuan dengan memeriksa firewall dan proxy logs. Cari domain atau IP address yang sama untuk konfirmasi dan additional context tentang aktivitas tersebut.

Build Attack Timeline

Susun kronologi lengkap: **initial connection → C2 communication → data exfiltration**. Dokumentasikan setiap tahap dengan timestamp, volume data, dan protokol yang digunakan.

Komponen Laporan Analisis Forensik

IP Internal & Eksternal Terlibat

Dokumentasikan semua IP addresses yang terlibat dalam insiden, termasuk geo-location IP eksternal, ASN information, dan reputation check dari threat intelligence feeds.

Protokol & Port Digunakan

Identifikasi semua protokol dan port numbers yang digunakan dalam komunikasi mencurigakan. Perhatikan penggunaan non-standard ports atau protocol tunneling attempts.

Volume & Arah Trafik

Hitung total bytes transferred, duration of communication, dan direction (inbound/outbound). Volume besar keluar mengindikasikan data exfiltration yang perlu investigasi lebih lanjut.

Indikasi Data Theft atau Malware

Berikan assessment apakah terdapat indikasi data theft berdasarkan volume, timing, destination, dan file types yang ditransfer. Include IOCs (Indicators of Compromise) untuk threat hunting.

Laporan harus bersifat objektif, faktual, dan didukung dengan bukti konkret dari analisis. Sertakan screenshots, packet captures yang relevan, dan hash values untuk referencing.

Key Takeaways

Network forensics membutuhkan respons cepat

Bukti jaringan bersifat volatile dan cepat hilang. Implementasikan continuous packet capture dan log retention policy yang memadai untuk mendukung investigasi.

Korelasi multi-source adalah kunci

Single log source jarang memberikan complete picture. Gabungkan data dari firewall, IDS, proxy, dan SIEM untuk mendapatkan comprehensive understanding of incidents.

Tools hanya alat bantu

Wireshark, Splunk, dan tools lainnya powerful, namun efektivitas investigasi tetap bergantung pada skill, experience, dan critical thinking dari analyst.

Dokumentasi adalah segalanya

Maintain chain of custody, dokumentasikan setiap langkah analisis, dan preserve evidence integrity untuk keperluan legal dan post-incident review.