5. Network Forensic

La **scienza forense** si occupa dell'applicazione di metodi scientifici per supportare indagini in ambito sia criminale che civile. Con l'evoluzione tecnologica, questo campo si è ampliato, includendo discipline specializzate che analizzano diverse tipologie di evidenze, come l'esame delle impronte digitali, le analisi tossicologiche e molti altri ambiti.

Tra queste, l'**analisi forense digitale** è una branca specifica della scienza forense che si focalizza sull'individuazione, raccolta, analisi e conservazione di prove presenti su dispositivi digitali, come computer, smartphone o hard disk.

Per garantire che le analisi forensi digitali siano efficaci e valide, vengono seguiti cinque principi fondamentali:

1. **Integrità dei dati**: I dati raccolti devono rimanere intatti e non essere alterati durante il processo di analisi.
2. **Tracciabilità e verificabilità**: Tutte le operazioni eseguite devono essere registrate in modo chiaro e riproducibile, così che un'entità terza possa confermare gli stessi risultati ripetendo il processo.
3. **Supporto specialistico**: Gli specialisti devono essere coinvolti per gestire situazioni complesse o tecnicamente avanzate.
4. **Formazione adeguata**: Anche in assenza di specialisti, il personale operativo deve essere preparato ad applicare le procedure di base per evitare errori o contaminazioni delle prove.
5. **Legalità**: Ogni azione deve essere svolta rispettando le leggi, le linee guida e i protocolli forensi stabiliti, per garantire che le prove siano ammissibili in sede legale.

Network Forensics

La **network forensics** è una branca della **digital forensics** che si focalizza sull'analisi e l'interpretazione dei dati provenienti dal traffico di rete di un sistema o infrastruttura sottoposta a osservazione. Questo tipo di indagine si concentra sul monitoraggio, sulla raccolta e sull'analisi delle comunicazioni in rete per individuare attività sospette o illecite.

L'analisi di **network forensics** ha diversi obiettivi fondamentali:

- **Collezionare informazioni** utili per comprendere eventi o attività svolte sulla rete.
- **Ottenere evidenze legali**, garantendo che le informazioni raccolte possano essere utilizzate come prova in sede giudiziaria.

- **Individuare e analizzare il comportamento di malware** o altre attività malevole, come tentativi di intrusione o compromissioni.
- Tracciare e attribuire azioni a specifici utenti o dispositivi coinvolti.

Come detto nel contesto della **digital forensics**, anche nel mondo della rete:

"*Anche le persone più attente lasciano tracce o artefatti dietro di sé*"

Questo principio è particolarmente vero in un ambiente connesso, dove ogni operazione, sia essa legittima o malevola, genera tracce sotto forma di pacchetti di rete, log o altre evidenze digitali che possono essere recuperate e analizzate.

Artefatti lato Host

La comunicazione digitale, sia essa tramite rete o tra dispositivi connessi, **inizia e termina su dispositivi fisici**, come computer, smartphone o tablet. Ogni volta che avviene una comunicazione, vengono generati e lasciati **artefatti digitali**, ovvero tracce che rappresentano l'attività svolta.

L'**analisi forense** ha il compito di identificare questi artefatti digitali all'interno della vasta mole di dati presenti sui dispositivi, separando ciò che è rilevante per l'indagine da ciò che è irrilevante. Gli artefatti lato host possono essere fondamentali per ricostruire azioni, eventi e connessioni, e spesso rappresentano la chiave per individuare le responsabilità o comprendere la dinamica di un attacco.

OSCAR

La **network forensics**, così come la **digital forensics**, segue una metodologia standard conosciuta come **OSCAR**, che garantisce un approccio strutturato e coerente nell'indagine. Questa metodologia si articola in cinque fasi principali:

Obtain

La prima fase consiste nell'**identificazione delle informazioni** relative all'incidente e all'ambiente in cui si è verificato. L'obiettivo è raccogliere una visione d'insieme dell'evento, considerando elementi come:

- **Timestamp** degli eventi per costruire una timeline precisa.
- **Endpoint coinvolti**, come dispositivi, server o sistemi interessati dall'incidente.

- **Contesto generale** dell’accaduto, utile per formulare ipotesi iniziali.

Questa fase è cruciale per preparare il terreno all’investigazione, assicurandosi che le informazioni essenziali siano ben definite fin dall’inizio.

Strategize

La **pianificazione dell’indagine** è fondamentale per massimizzare l’efficacia delle operazioni. In questa fase si definiscono:

- **Obiettivi** dell’investigazione, come identificare le cause dell’incidente o raccogliere prove per azioni legali.
- **Priorità operative**, identificando quali dati acquisire per primi e quali evidenze sono più rilevanti.
- **Fonti di dati** da analizzare, ad esempio log di rete, traffico catturato o registri dei dispositivi.
  La strategia deve includere anche una valutazione del **costo e valore delle fonti di evidenza** e un piano per aggiornare il team o il cliente sui progressi.

Collect

La fase di **raccolta delle evidenze** è quella operativa, in cui si procede secondo il piano stabilito. Durante questa fase:

- Si acquisiscono i dati dai sistemi coinvolti, come pacchetti di rete, log di firewall, router, o altri dispositivi.
- **Documentare ogni azione** è essenziale, registrando dettagli come:
  - Sistemi a cui è stato effettuato l’accesso.
  - Azioni eseguite e metodi utilizzati per l’acquisizione.
  - Tempi e persone coinvolte.
- Si utilizzano strumenti professionali per catturare e salvare i dati (ad esempio, cattura di pacchetti, imaging di dischi o raccolta di log).
- **Copia delle evidenze**: Le evidenze raccolte devono essere clonate per garantire che i dati originali non vengano alterati. Per ogni copia, si genera un **codice hash** (come MD5 o SHA-256) che ne attesta l’integrità e la verificabilità.

Nota importante. Tutte le operazioni devono essere eseguite **solo sulle copie** delle evidenze, mai sui dati originali, per preservarne l’integrità in caso di utilizzo legale.

Analyze

La fase di **analisi** è il cuore dell'intero processo di network forensics, dove i dati raccolti vengono esaminati per estrarre informazioni significative e ricostruire gli eventi. Durante questa fase:

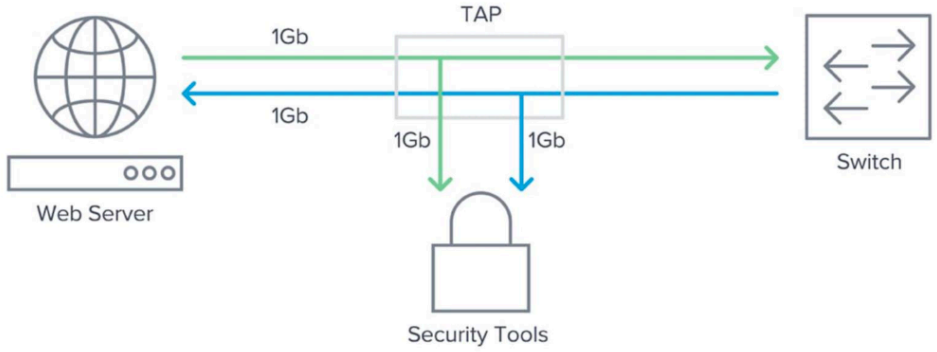
- Si utilizzano **tecniche manuali e automatizzate**, sfruttando una varietà di strumenti per analizzare i dati provenienti da diverse fonti, come log, pacchetti di rete o file acquisiti.
- Si procede a **correlare le informazioni** raccolte, collegando i dati tra loro per identificare pattern o relazioni che potrebbero essere rilevanti per l'indagine.
- Si costruisce una **timeline degli eventi**, organizzando cronologicamente i dati per comprendere l'ordine e la sequenza delle attività svolte.
- Si eliminano i **falsi positivi**, ovvero risultati che non rappresentano reali minacce o anomalie, al fine di concentrare l'attenzione solo sui dati effettivamente utili.
- Si sviluppano **teorie di lavoro** basate sulle prove raccolte, che aiutano a spiegare il comportamento degli attori coinvolti o la causa degli eventi.

Infine c'è la fase di **Report**, dove bisogna redigere un report sulle operazioni svolte.

Network evidence

Le fonti di **network evidence** possono essere diverse, tra cui:

- **Traffic snooping**: Permette di raccogliere informazioni nella rete mediante **network taps** inseriti fisicamente tra i cavi che inoltrano il contenuto del traffico ad una determinata porta per analizzarli. Se l'utilizzo dei dispositivi fisici **taps** non è possibile si può ricorrere alle **SPAN port** ("Tap where you can, SPAN where you must"), software da applicare a determinate porte di un sistema per la replicazione dei dati.



- **Network switch**: I **network switch** utilizzano tabelle di memoria, spesso chiamate **CAM tables** (Content-Addressable Memory), per mappare i **MAC address** dei dispositivi alle rispettive porte fisiche.
- **Tabelle di routing**: Le tabelle di routing nei **router** indicano le reti a cui il dispositivo si connette e i percorsi attraverso cui il traffico viene inoltrato.

- **DHCP Logs**: Quando viene assegnato dinamicamente un IP ad un MAC address, vengono creati nuovi log (e.g., Uno strumento utile è ARP Watch)
- **DNS Server Logs**: Servono a capire la relazione IP-Hostname
- **syslog**: file che contiene il log dei tentativi di accesso ad un sistema.
- **IDS/IPS logs**: I log dei sistemi **IDS/IPS** (Intrusion Detection System/Intrusion Prevention System) offrono una visione dettagliata di potenziali minacce.
- **Firewall Logs**: Tracciano le connessioni consentite e bloccate.
- **Proxy server logs**: I log dei **proxy server** offrono una panoramica del traffico web generato dagli utenti.