Fiche de cours : Introduction à la Forensique Réseau

I. Définition de la Forensique Réseau

A. Domaine spécifique de la Forensique

- Sous-domaine de la Forensique
- Concentration sur l'investigation du trafic réseau
- Objectif : Accéder aux informations transmises, analyser le trafic en direct ou enregistré, rassembler des preuves/artefacts, comprendre les problèmes potentiels

B. Processus d'investigation

- Enregistrement des paquets de trafic réseau
- Création de sources investigables
- Analyse des causes fondamentales d'un événement
- Objectif final : Fournir suffisamment d'informations pour détecter des activités malveillantes, des violations de sécurité, la conformité aux politiques/réglementations, la santé du système et le comportement utilisateur

C. Les 5W de l'investigation

- Who (Source IP et port)
- What (Données/payload)
- Where (Destination IP et port)
- When (Heure et date)
- Why (Comment/Qu'est-ce qui s'est passé)

D. Cas d'utilisation de la Forensique Réseau

Découverte du réseau
Réassemblage des paquets
Détection des fuites de données
Détection d'activités malveillantes et d'anomalies

Contrôle de la conformité aux politiques/réglementations

II. Avantages de la Forensique Réseau

A. Avantages généraux

Disponibilité d'une preuve basée sur le réseau dans la nature
Facilité de collecte de données/évidence sans créer de bruit
Difficulté de détruire les preuves réseau

B. Avantages spécifiques

Disponibilité de sources de journaux
Possibilité de recueillir des preuves pour des activités malveillantes non résidentes

III. Défis de la Forensique Réseau

A. Défis généraux

Prise de décision
Collecte adéquate de données/évidence sur le réseau
Capture de données courte
Indisponibilité de captures complètes de paquets sur des événements suspects
Trafic chiffré
Préoccupations liées à la confidentialité et au GDPR dans l'enregistrement du trafic
Utilisation de ports non standard
Problèmes de fuseau horaire
Manque de journaux

IV. Sources d'évidence en Forensique Réseau

- TAPS
- Appareils en ligne

- Ports SPAN
- Concentrateurs (Hubs)
- Commutateurs (Switches)
- Routeurs
- Serveurs DHCP
- Serveurs de noms (Name Servers)
- Serveurs d'authentification
- pare-feu (Firewalls)
- Serveurs proxy Web
- Serveurs de journaux centraux
- Journaux (IDS/IPS, Application, OS, Périphérique)

V. Objectifs Principaux de la Forensique Réseau

Opérations de sécurité (SOC)

- Surveillance quotidienne de la performance et de la santé du système, du comportement utilisateur et des problèmes de sécurité.

Gestion des incidents/Réponse et chasse aux menaces

- Activités d'investigation pendant/après un incident pour comprendre la raison de l'incident, détecter des activités malveillantes et suspectes, et examiner le contenu du flux de données.

VI. Types de données investiguées en Forensique Réseau

Trafic en direct
Captures de trafic (captures de paquets complètes et flux réseau)
Fichiers journaux

VII. Outils pour l'investigation en Forensique Réseau

NetworkMiner

- Axé sur l'analyse du flux global/état du trafic limité

Wireshark

- Analyse approfondie du trafic et des paquets

Tcpdump

- Prochainement disponible

Tshark

- Prochainement disponible