TP6 – Digital Forensics & Incident Response

Groupe : HAMAD, TONNERRE, CHAFAI, FAUVART, DELANGHUE

Encadrant : Sébastien Mériot (@smeriot)

Durée : 4 heures

# Introduction

Dans ce rapport, nous allons détailler l’analyse forensique réalisée dans le cadre du TP6 portant sur la détection et la réponse à un incident de cybersécurité sur le réseau de l’entreprise fictive CandyRiver. Nous avons utilisé Wireshark pour analyser les flux contenus dans un fichier `pcap`, identifié un comportement malveillant, et déroulé une investigation complète jusqu’à l’exfiltration de données sensibles.

# Warm-Up Question

Notre supérieur nous a transmis une pièce jointe chiffrée (MeetingNotes.pdf.asc) et un mot de passe via Signal. Nous avons utilisé GnuPG pour déchiffrer le fichier avec la commande suivante :

gpg --decrypt MeetingNotes.pdf.asc

Cette pièce contient des informations critiques sur la situation et sur les discussions avec le CISO de CandyRiver.

# Rôles attribués dans l'équipe

- Coordinateur : Mehdi – responsable de la communication avec l'encadrant et de la gestion de l’équipe

- Report Manager : Tonnerre – responsable de la rédaction du présent rapport

- Security Experts : Chafai, Fauvart, Delanghue – responsables de l’analyse des paquets réseau

# Définitions rapides

- NIDS (Network Intrusion Detection System) : système de détection des intrusions sur le réseau. Il capture et inspecte les paquets réseau pour détecter des activités suspectes.

- SIEM (Security Information and Event Management) : outil de centralisation et de corrélation des logs de sécurité.

# Analyse de la règle NIDS

Cette règle détecte l’usage de la fonction system($\_GET[...]) dans un corps de requête HTTP POST, souvent utilisée dans des webshells ou attaques RCE (Remote Code Execution).

alert tcp any any -> any any (msg: "Suspicious HTTP POST request"; flow:to\_server; content:"POST"; http\_method; content:"system($\_"; http\_client\_body; classtype:web-application-attack; sid:283; rev:3;)

# Position du NIDS

Le NIDS est déployé sur un switch SPAN connecté à la DMZ, ce qui permet de surveiller le trafic entrant et sortant sans être intrusif. C’est une bonne pratique si correctement configurée.

# Analyse du fichier PCAP – Étapes clés

Voir les pages suivantes pour une analyse détaillée des paquets.