PROJET 2 : Analyse des logs sur un server compromis

Objectifs : identifier la cause de la compromission via l'analyse de logs

PLAN MIS À JOUR

I. Introduction

1. Présentation du contexte
2. Symptômes observés
3. Objectifs de l'investigation

II. Préparation de l'environnement

1. **Téléchargement d'Ubuntu Server (22.04 ou 24.04 LTS)**
2. Installation sur :
    a. VM (VirtualBox / VMware)
    b. ou machine dédiée
3. Configuration de base :
    a. mise à jour du système
    b. installation d'OpenSSH
    c. création d'un utilisateur administrateur
4. Installation des outils nécessaires :
    a. Apache2
    b. outils de gestion des logs
    c. packages requis par ELK

✓ télécharger Ubuntu
✓ configurer la machine virtuelle
✓ installer Apache
✓ installer ELK pas à pas
✓ lancer des analyses de logs
✓ compléter ton rapport

III. Collecte des données

1. Identification des logs :
    a. Apache (access.log, error.log)
    b. SSH (auth.log)
    c. Syslog
2. Exportation et centralisation des logs
3. Préparation des fichiers pour Logstash

Analyse des logs Apache

- Requêtes suspectes
- Erreurs HTTP
- Probe/scans

Analyse des logs SSH

- Tentatives de brute-force
- Connexions étrangères

Analyse des logs Syslog

- Processus suspects;[2]
- Alertes système

IV. Mise en place de l'ELK Stack

1. Installation d'Elasticsearch
2. Installation de Logstash
3. Installation de Kibana
4. Architecture de la chaîne de collecte (log → Logstash → Elasticsearch → Kibana)

V. Configuration de l'ELK Stack

1. Configuration de Logstash :
    a. Inputs
    b. Filters (grok, geoip, date)
    c. Outputs
2. Paramétrage d'Elasticsearch
3. Configuration de Kibana :
    a. Index Patterns
    b. Dashboards

VI. Analyse des logs

1. Analyse des logs Apache
2. Analyse des logs SSH
3. Analyse des logs Syslog

VII. Visualisation avec Kibana

1. Création des dashboards
2. Visualisation des anomalies
3. Analyse des pics de charge, IP suspectes, brute-force SSH

VIII. Reconstitution de la chronologie de l'attaque

1. Phase de reconnaissance
2. Phase d'exploitation
3. Phase d'installation/persistance
4. Phase d'exécution malveillante
5. Phase post-compromission

IX. Détermination de la cause de la compromission

1. Vulnérabilité exploitée
2. Étendue de l'attaque
3. Impact sur le serveur

X. Contre-mesures

1. Sécurisation système
2. Sécurisation applicative
3. Sécurisation réseau

4. Mise en place d’un IDS/IPS
5. Durcissement SSH

XI. Politique de journalisation améliorée

1. Centralisation
2. Rotation et conservation des logs
3. Horodatage synchronisé
4. LogLevel optimisé

XII. Conclusion

1. Résumé de l’analyse
2. Résultat de la reconstitution
3. Recommandations finales