CLUB
ETHICAL HACKING

Edition 2019/2020

Niveau débutant

Séance #3
OneSmile Inc.
Part.2 Forensic

8 Janvier 2020

Point de contact

Rémi ALLAIN <rallain@cyberprotect.one>

Daniel DIAZ <ddiaz@cyberprotect.one>

Déroulé de la séance

Partie exercice:

- Analyses des logs récoltés pendant le pentest
  - Comprendre les schémas d'attaques et les assets
  - Identifier les attaquants (nombres, heures, portées, etc.)
  - Identifier les vulnérabilités exploitées
- Travail sur la remédiation

Partie réflexion / débat:

- Etude de l'architecture initiale
- Réflexions sur le traitement des logs *(journaliser, c'est bien, être alerté c'est mieux.)*
- Recommendations

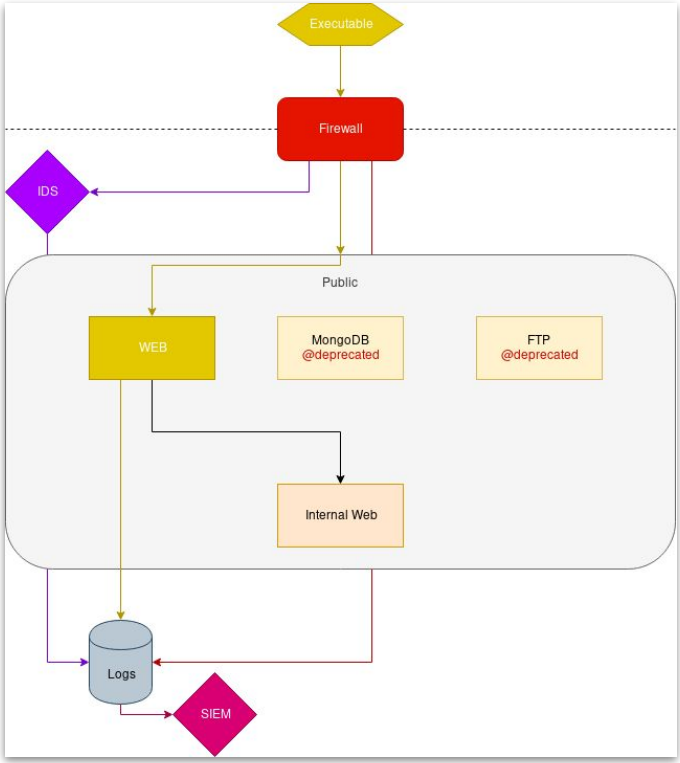
Forensic - Exercice

Sur **Kibana**, choisissez la période allant de **2019-11-27 6am** à **2019-11-27 2pm**
Les deux indices à analyser sont ***`web-logs`*** *et* ***`web-logs-full`***

- À quelle période, un pic de connexion a-t-il été enregistré ? (à 5 minutes près)
- Combien de personnes distinctes se sont connectées au serveur ?
    - Comment les avez-vous identifiées ?
- Quel est le top 10 des comportements suspects ? (les attaques / scans qui reviennent le plus souvent)
- Quelle est l'attaque qui a été la plus visible ? (la moins discrète)
- Identifier les tentatives de brute-forcing
- Identifier les processus de crawling

Réflexion / Débat

Architecture théorique



Journaliser, c'est bien

Être alerté c'est mieux.

Des questions ? → **rallain@cyberprotect.one**