CLUB
ETHICAL HACKING

Edition 2019/2020

Séance #2
OneSmile Inc.
Part.1 Pentest

Niveau débutant

27 Nov. 2019

Point de contact

Rémi ALLAIN <rallain@cyberprotect.one>

Daniel DIAZ <ddiaz@cyberprotect.one>

Pré-requis

- Un OS type Kali Linux
  Image VirtualBox: https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

  Sous-système Windows:
  https://www.kali-linux.fr/installation/faire-tourner-kali-linux-en-tant-que-sous-systeme-de-windows-10

- Un logiciel d'analyse de PCAP (Wireshark, Networkminer)
  https://www.wireshark.org/#download

- Metasploit *(déjà installé sur Kali Linux)*
  https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers

- Nmap *(déjà installé sur Kali Linux)*
  https://nmap.org/download.html

Objectifs

La société OneSmile Inc. vous a recruté pour réaliser un pentest sur un addon de leur application la plus populaire. Cet addon est utilisé pour du tracking utilisateur.

Le périmètre de la prestation est **UNIQUEMENT** sur l'addon (sous forme de binaire) et sur les ressources directement associées (api, librairies, etc.)

L'exécutable vous sera délivré par clé USB.

Votre objectif est de tester la sécurité de cet addon et d'évaluer le risque pouvant être porté à OneSmile Inc. en cas d'attaque.

Avant de commencer

Rappel - déroulement d’un pentest:

- Récolte d’informations
- Analyse des menaces
- Analyse des vulnérabilités
- Exploitation
- Post-exploitation
- Reporting

Et après ?

Lors de la prochaine 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:

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

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