LES FAILLES DU WEB

LES 4 ETAPES D'UN HACK

01. Collecter : la première étape est une collecte d'informations (par exemple, noms de réseau et de domaine, serveur de messagerie, fuite de données, OSINT, etc.);

02. Analyser : interpréter des données collectées en phase 1. Analyse des services, ports, adresses, domaines, comportements, employés, etc..;

03. Attaquer : cette étape utilise des attaques applicatives, systèmes, réseau, etc. tels que les "cross-site scripting", "SQL injection", "Buffer Overflow", "Heap Overflow", "SSRF", etc. Tout cela dans le but d'élever ses privilèges;

04. Maintenir : cette dernière étape permet de voir si la vulnérabilité peut être utilisée pour obtenir une présence persistante dans le système exploité;

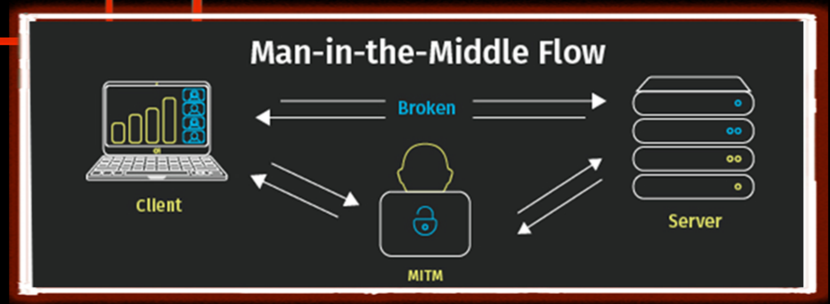
Le but des hackers est forcément l'argent et pour ça il utilisent des "ransomware", des logiciels qui cryptent vos données, puis vous demandent une rançon pour les décrypter, ce type de prise d'otages virtuelles a fait beacoup de bruit lorsque WannaCry, un ransomware, a commencé a se propager, et a fait subir une perte économique de 4 milliards de dollars;

LOG 4 SHELL

est une attaque exploitant une bibliothèque java : Log4J. Bibliothèque java, qui sert a gérer les logs, et une vulnérabilité a été découverte : Log4Shell , la faille permet d'exécuter du code a distance soit le pire cas de figure possible.
Il est possible d'injecter dans un logiciel vulnérable un code malveillant, qui va demander à Log4J d'aller chercher une valeur issue d'une source tierce.
Or, dans ce cas, Log4J ne vérifie pas assez bien les données importées.
Les données importées peuvent alors être du code, qui sera exécuté par Log4J sur le système.

MAN IN THE MIDDLE

est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis.
Si le site est en HTTP, donc non sécurisé (et par conséquent les communications ne sont pas chiffrées), le hacker peut ainsi intercepter les communications entre les parties et donc récupérer des données sensibles tels que les mots de passe ou les cookies de sessions qui servent à l'utilisateur pour se connecter.



Université de Lyon Lyon 1
RAYANE MERLIN
NOAH HERAUD
ANIS BENJEMIA