TP KALI AVANCE

Tede, Sacha

Mr. Jacquemin

Introduction :

La sécurité des systèmes d'information est aujourd'hui une priorité pour toutes les organisations, face à des menaces en constante évolution. Pour comprendre et anticiper ces risques, il est essentiel d'adopter une approche proactive : apprendre à penser comme un attaquant pour mieux se défendre.

Dans ce TP nous allons explorer Kali Linux (système d'exploitation spécialement conçu pour les tests de sécurité et l'audit réseau) un peu plus en détails.

Nous allons tester différents d'outils comme GoldenEye, T50 ou encore Legion. Nous allons simuler des attaques et voir quelles seront leurs impacts sur la cible. De plus, nous verrons comment se protéger de ces attaques.

L'objectif de ce TP est double :

- Découvrir les vulnérabilités exploitées par des attaquants.
- Apprendre à renforcer la sécurité des systèmes en prenant conscience des outils et techniques utilisés par les pirates.

Pour ce TP, nous aurons besoin de différents outils pour mener à bien les attaques :

- Une machine avec Kali sous Linus
- Une machine cible (dans mon cas ce sera le PC Client de mon contexte)
- GoldenEye
- T50
- Legion

Pour mener à bien les simulations, j'ai volontairement enlevé la sécurité de ma machine cible.

1) La machine répond-elle encore correctement après avoir exécuté le programme ? (GoldenEye)

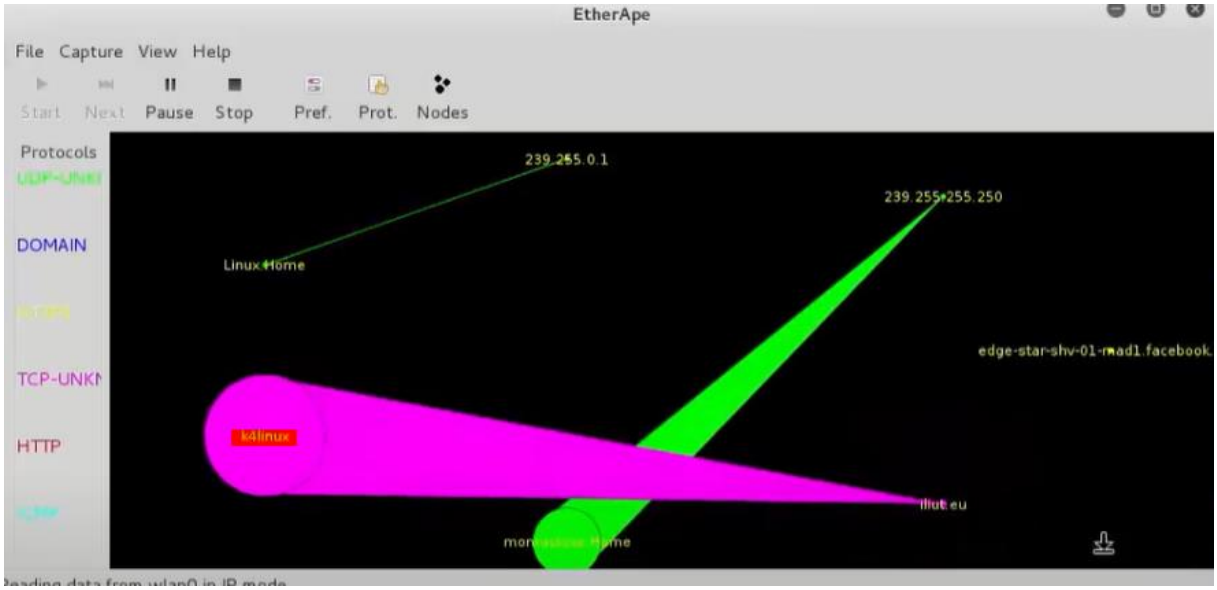
GoldenEye : GoldenEye est un outil de test de pénétration utilisé principalement pour effectuer des attaques de type Denial of Service (DoS) et Distributed Denial of Service (DDoS). Il est conçu pour tester la résistance d'un serveur Web ou d'une application aux attaques par inondation HTTP (HTTP Flood).

Le but de cette attaque est de surchargée la machine cible de requête http uniquement. En fonction des performances et de la quantité de requêtes http envoyé par l'attaquant, la machine cible peut soit être indisponible un petit moment, elle peut

être très lente et la qualité du service proposé peut être dégradée ou dans le pire des cas la machine attaquée peut devenir inaccessible.

Pour ma part, ma machine cliente n'a pas forcément été inaccessible, néanmoins, lorsque j'ai essayé d'aller sur un navigateur web, c'était très lent, la qualité d'image était légèrement dégradée.

C'est une arme redoutable notamment contre les personnes qui vivent du streaming car cela peut rendre la machine du streamer indisponible et ainsi couper leur live.



Sur cette capture d'écran, on voit bien que l'activité principale détectée par EtherApe (logiciel qui permet de surveiller un réseau informatique. Ce logiciel est muni d'une interface graphique qui permet de visualiser ce qui se passe sur un réseau) est majoritairement causé par des requêtes venant de Kali Linux.

2) Quels sont les enjeux / dangers possibles avec une telle application ?

- Saturation des ressources : L'attaquant envoie énormément de demandes au serveur, ce qui peut le rendre temporairement hors service ou l'empêcher de fonctionner correctement, l'enjeu par exemple est pour les gros sites (Amazon, Nike) qui sont énormément sollicités.

- Dos ou DDos : C'est une attaque vers une machine cible qui consiste a submergé la machine avec beaucoup de requêtes, ce qui va faire dégrader la qualité de service de la cible ou encore de la rendre indisponible.

- Impact sur l'infrastructure réseau : L'attaque peut non seulement ralentir ou bloquer la machine ciblée, mais aussi remplir la connexion Internet, ce qui peut affecter d'autres services qui utilisent le même réseau

- Légalité et éthique : Utiliser cet outil pour attaquer un système sans autorisation est illégal. Il est impératif même lors de test d'avoir le consentement de la cible sous peine de sanctions.

3) Comment s'en protéger ?

Pour se protéger contre une attaque réalisée avec GoldenEye, plusieurs solutions peuvent être mises en place :

- Pare-feu : Il permet de détecter et de bloquer les requêtes malveillantes avant qu'elles n'atteignent le serveur, notamment celles issues des outils de type DoS ou DDoS.

- Limitation des connexions : L'activation de limites sur le nombre de connexions simultanées par adresse IP peut réduire l'impact d'une attaque HTTP Flood.

- IPS et IDS : La mise en place de systèmes de détection d'intrusions (IDS) et protection (IPS) permettent la surveillance du réseau et de repérer des comportements suspects avant qu'ils ne deviennent graves.

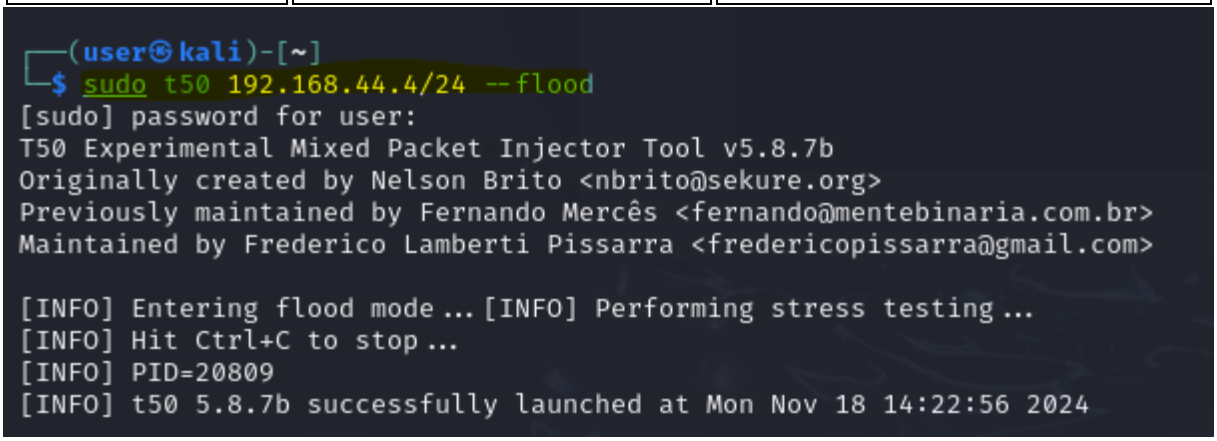
4) L'application T50 fait-elle la même chose que l'application GoldenEye ?

T50 et GoldenEye sont plus ou moins similaires sans l'être.

GoldenEye est un outil qui se concentre uniquement sur les attaques de type HTTP, donc c'est un outil qui cible plus les serveur web en général.

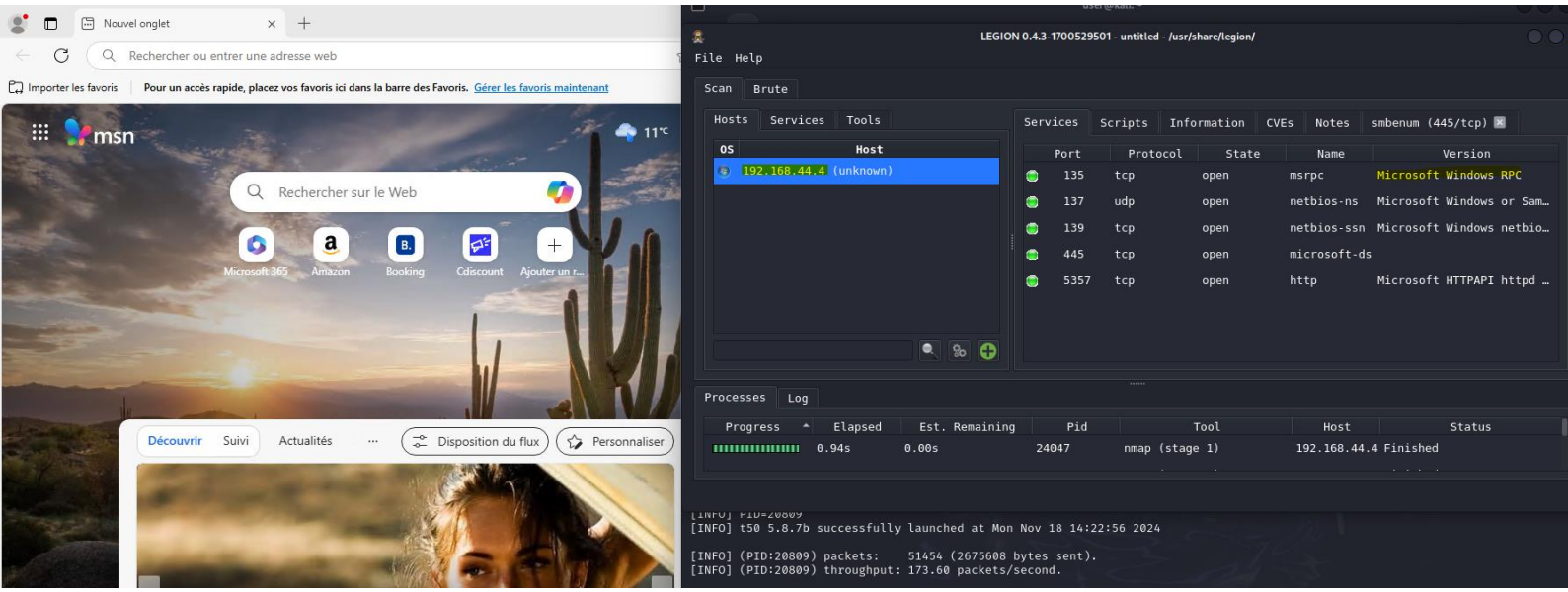
T50 peut cibler différents types de protocoles réseau comme TCP, UDP, ICMP et http, il permet d'avoir une large possibilité d'attaque.

Caractéristique	GoldenEye	T50
Type d'attaque	Attaque HTTP Flood pour surcharger un serveur web.	Attaques réseau multi-protocole (ICMP, TCP, UDP, HTTP, etc.).
Niveau d'action	Niveau application (couche HTTP).	Niveau réseau (protocole IP).
Protocoles ciblés	Exclusivement HTTP (simulateur de requêtes web).	Plusieurs protocoles : TCP, UDP, ICMP, HTTP, etc.
Objectif principal	Tester la résilience d'un serveur web.	Tester les performances d'un réseau ou d'un équipement réseau.
Complexité de l'utilisation	Facile à configurer (simple flood HTTP).	Polyvalent mais demande des connaissances réseau.
Portée des dégâts	Spécifique à un service web (port HTTP/HTTPS).	Peut affecter des routeurs, pare-feu, ou plusieurs équipements.



5) Quels sont les enjeux / dangers possibles avec une telle application ?

Legion est un outil d’audit et de reconnaissance qui permet de scanner des réseaux à la recherche de vulnérabilités et de services ouverts. Bien qu'il soit utile pour effectuer des tests de sécurité et des analyses de vulnérabilités, son utilisation présente plusieurs enjeux et dangers.



Les enjeux / dangers concernant cette application sont les suivants (Legion) :

- Enjeux légaux : Comme pour GoldenEye et T50, il faut avoir des autorisations pour pratiquer sur une cible (consentement), sous peine de sanctions juridiques si cela venait à ne pas être respecté

- Exploitation des failles : Legion peut trouver des failles dans les systèmes (comme des services non sécurisés ou mal configurés). Si ces failles sont utilisées par des attaquants, cela peut entraîner des fuites de données, des intrusions ou des compromissions graves de sécurité

- Risques pour les systèmes scannés : Un scan mal configuré ou trop agressif peut provoquer des interruptions de service ou des problèmes imprévus sur la machine cible

- Exposition des données personnelles : L’application Legion peut collecter des informations détaillées sur les services, les ports ouverts et les systèmes.

Comment se protéger contre Legion :

- Pare-feu : Mettre en place des pares-feux pour limiter l'accès aux systèmes non autorisés

- Outils de surveillance (IPS/IDS) : Utiliser des outils pour détecter les tentatives de scans et les comportements suspects sur le réseau

- Mise à jour et correction des services : Mettre à jour régulièrement les services de la machine afin de réduire les risques de failles

Conclusion :

Ce TP nous a permis de comprendre pourquoi il est crucial de bien sécuriser nos machines, en expérimentant avec des outils comme GoldenEye, T50 et Legion.

L'objectif était de voir comment un attaquant pourrait exploiter des failles de sécurité et, à partir de là, comprendre comment mieux protéger nos systèmes.

En testant GoldenEye et T50, on a vu comment ces outils peuvent saturer une machine cible avec des requêtes.

On a aussi exploré Legion, un outil qui permet de scanner un réseau et de repérer des vulnérabilités. Cela rappelle également à quel point il est important de mettre à jour régulièrement la qualité de la sécurité d'une machine.

Ce TP nous a aussi rappelé que l'utilisation de ces outils doit être éthique et légale. Il est crucial d'avoir l'autorisation de tester un système. De plus, on a vu que les vulnérabilités découvertes peuvent être utilisées pour voler des données, causer des pannes, ou même pirater un réseau.

Enfin, on a appris comment se protéger contre ces attaques. En se mettant dans la peau d'un attaquant, on comprend mieux les failles à corriger et les protections à mettre en place.

Pour finir, ce TP nous a bien montré l'importance de sécuriser nos systèmes et comment, en simulant des attaques, on peut se préparer à mieux les défendre.

L'objectif du TP est donc atteint : on sait maintenant comment se protéger, mais aussi pourquoi c'est essentiel.