Network Security

Architecture

Antoine Puissant

Enseignant : M. Chapin

2014 - 2015

Résumé

Ceci est le résumé

Table des matières

1 Introduction

Différents scénarios pour un début d'attaque :
- Scan de ports en TCP. C'est bruyant.
- Scan de port en UDP. Sur le DNS, on envoie et on attend une réponse. En UDP, c'est plus long, bruyant, et moins fiable.
- On peut collecter de l'information en continue pour connaître ce qu'on a en face.
- On va alors chercher des vulnérabilités sur cette version ou pousser la machine à la limite de la faute. La recherche de vulnérabilité reste quelque chose de bruyant puisqu'on va communiquer avec la machine.
- La dernière étape est d'utiliser la faille. Cela va pouvoir être de rester dans la machine de manière durable, créer des utilisateurs, ou autre.

Tout cela va, en partie, être arrêté par le pare-feu. Ce dernier est présent sur les couches 3 et 4 du modèle OSI. Sur les autres couches, il sera presque aveugle.

2 Rappels de réseau

Un réseau c'est un ensemble d'objets inter-connecté qui s'échangent des information en utilisant des supports (WIFI, Ethernet, etc...) et des règles communes, les protocoles.
La grande différence entre les supports filaires et d'ondes est que l'on va plus retarder les personnes d'arriver jusqu'au câble. Pour cela, on va mettre de la sécurité physique (alarmes, sécurisation biométriques, etc...). Un attaquant motivé pourra toujours récupérer de l'information que cela soit câblé ou modulaire. Si une personne arrive au support, physiquement, on va considérer que l'attaquant à déjà gagné.
Pour les ondes, si cela « bave » à l'extérieur, il va pouvoir :
- Récupérer des informations, analyser le réseau, les communications, etc...
- Brouiller le signal pour le rendre inopérant. Cela a des fins autres (passer sur un support de secours, empêcher la transmission de messages, etc...).
  Pour se protéger du brouillage, on peut :
  - Théoriquement, mettre en place un système de cage de Faraday
  - Changer de fréquence de transmission
  - Passer sur un système filaire
  - Chercher la source du brouillage pour l'arrêter

Les protocoles sont des règles libres. Tout le monde peut y accéder (contrairement aux règles fermées, propriétaires). C'est un avantage dans la sécurité car il est possible de l'étudier et ainsi de corriger dans certains cas ou de se prémunir des failles. C'est aussi un avantage car l'attaquant va lui aussi connaître le protocole et ses failles.
Ici, nous allons nous concentrer sur l'IPv4. On va alors désactiver l'IPv6 pour ne pas permettre à l'attaquant de rentrer via ce protocole.

2.1 Adresse MAC

Identifiant unique, théoriquement.
Dans une trame Ethernet, on va retrouver l'adresse MAC. Avec dans les 3

premier octets le fabriquant de la carte. Attention, il faut se méfier de ces octets. Ils peuvent être changer et ainsi ne plus être vrais.
A la fin de la trame Ethernet, on va retrouver une signature, le *checksum* qui va nous permettre de connaître l'intégrité de l'information.

2.2 Modèle OSI

ICMP va permettrede faire communiquer entre eux les équipements sur la couche 3. Cela permet aussi de diagnostiquer l'état du réseau. Sur les réseaux militaires, tout ICMP est interdit. Dans certains cas, on va vouloir un filtrage plus fin afin de laisser passer certains ICMP dans un sens et certains autres dans l'autre.
Un pare-feu doit prendre des décisions rapide depuis des règles simple. C'est un fonctionnement assez brutal. On va lui donner des règles sur les couches 3 et 4 :
Si le flux vient de l'entreprise vers un serveur externe valide, on va regarder quel protocole (couche 4) est utilisé. Si c'est du TCP ayant en port de destination le port 80 et en port source un port supérieur à 1024, alors on vient de valider un flux web. Il suffit alors de créer la règle de retour.
Dans la partie application du modèle OSI, on va retrouver plus de failles. Il y a plus d'intelligence, des protocoles plus lisibles (SMTP). Si c'est plus lisible, c'est qu'il y a plus de code, donc plus de chance d'avoir des erreurs dans le code. Un proxy SMTP va avoir besoin de plus de ressource pour plus de finesse.
On va retrouver *iptable* pour faire du filtre d'adresse IP et *ebtable* pour faire des filtres d'adresse MAC.
Un Firewall vendu par un industriel va être un ensemble de proxy et filtres.
L'échange à 3 passes (3 way handshake) est quelque chose que l'on doit connaître pour la mise en place d'un proxy TCP. Il faut que le proxy puisse accepter le SYN du client, le SYN, ACK du serveur, etc...
En cas de RESET du serveur, c'est qu'il n'y a aucune application écoutant sur ce port. Ainsi, il est bon de bloquer le RESET sur le pare-feu afin de ne pas donner de l'information à l'attaquant.
Le mode dynamique d'un protocole n'est pas très simple pour le pare-feu. En effet, en FTP par exemple, le serveur va demander l'ouverture d'un port aléatoire. Un pare-feu bloquant alors les ports lointains, l'accès échouera. Il faut donc que le pare-feu puisse lire les flux FTP afin d'ouvrir un accès temporaire sur le port en question.
Le DNS est une table de correspondance entre le nom de domaine et les adresses IP. Les CNAME [1] sont des alias. Un relais de messagerie MX [2] permet de donner l'adresse du serveur mail.

3 Définitions

Pare-feu Un pare-feu est un élément ou un ensemble d'éléments placé(s) entre deux réseaux et suivant les règles suivantes :
— Tous les flux réseaux passent par là.

1. Cannonical Name
2. Mail eXchanger

- Seuls les flux autorisés par une politique locale peuvent passer. Cela correspond à :
  - J'interdis tout sauf certains flux (whitelist).
  - J'autorise tout sauf certains protocoles (blacklist).
- Le système en lui même doit-être résistant aux attaques(c.f. GRSecurity). Pour cela, on va pouvoir :
  - On va bloquer tout ce qui vient directement sur la machine.
  - On va bloquer tout ce qui permet de contrôler la machine (SSH)
  - On peut mentir sur la machine en elle-même. Cependant, il faut faire très attention et le faire partout pour être crédible.
  - On enlève toutes les applications inutiles (interface graphique, gestion de l'IPv6, etc...). On enlève le maximum de chose jusqu'à la recompilation du noyau.

Un bastion Un bastion est un pare-feu très sécurisé car il est le premier à faire face à l'extérieur, l'inconnu. Il ne faut pas que ça compromission compromette les autres pare-feux.

Principe de moindre privilège cela consiste à ne donner que les droits nécessaire à notre utilisateur.

Principe de défense en profondeur On ne fait pas confiance qu'à une seule ligne de défense. Il faut multpliser les défense. On peut aussi mettre en place des IDS, etc...

Un goulet d'étranglement Cela va permettre d'analyser tout ce qui passe car tous les flux passent par la. On peu en avoir plusieurs pour ne pas avoir des ≪ bouchons ≫.

Le maillon faible C'est l'élément qui met le plus en danger le système. Par exemple, l'humain est le plus grand maillon faible. Chez l'humain, un administrateur pensant savoir est une grande faille.

La panne sans danger Cela va être le cas permettant de savoir si le système fonctionnel fonctionne toujours suite à une coupure de courant ou autre.

Diversité des défenses On va mettre un second pare-feu, mais de famille différente pour ne pas subir une faille deux fois.

KISS [3] On garde le système simple. Il ne faut pas empiler les structures.

Régulièrement, il faut réévaluer la politique de sécurité et réaliser des audits de la sécurité en place. Il faut aussi documenter la solution pour pouvoir évaluer le produit.
Quand quelque chose traverse la machine (la passerelle), on utilise le Forward. INPUT et OUTPUT c'est le pare-feu lui-même.

-i carte par laquelle ça rentrer

-o carte par laquelle ça sort

-s adresse IP source

-d adresse de destination

-p protocole

–**sport** port source

–**dport** port de destination

-m module

Afin de changer la politique d'INPUT ou OUTPUT ou FORWARD, il faut utiliser la commande :

```
iptables –P INPUT DROP
```

Pour administrer notre pare-feu, on peut passer par le SSH. Pour cela, on doit :

— Installer le service sshd serveur
— Le configurer sur un port de notre choix (ici, port 1313)
— On va ensuite autoriser le SSH à passer sur le firewall

Pour visualiser les log, il faut taper (sous Mageia) journalctl -u ssh -f

4 NAT

Le SNAT c'est quand on change l'IP source. Les adresses IP du réseau local sont alors remplacées par l'adresse du routeur.
Sur le client, on marque :

```
iptables -t NAT -A POSROUTING -o externe -j SNAT --source
```

A partir du moment que ça sort par la carte externe, on fait le NAT. L'option MASQUERADE permet de faire du SNAT quand on n'a pas d'IP fixe dans le réseau local. Ainsi, on n'a pas à mettre des règles pour les clients.

5 Proxy

Les qutres fonctions du proxy sont :

L'accélération Pour cela, on va avoir un système de cache commun. Pour les pages statique c'est très performant puisque les pages ne seront pas unique pour chaque utilisateur.

Vérification de la conformité On vérifie si le protocole est bon. Pour cela, on vérifie par rapport à la RFC. Il peut alors savoir si le paquet se disant d'un protocole est bien fait en fonction de ce que la RFC définie. Dans le cas de non conformité, on peut droper le paquet. Cependant, l'utilisateur ne saura pas pourquoi il ne peut pas avoir sa requête. On peut aussi corriger le paquet à la volée. Le proxy étant en coupure, et ayant l'intelligence de décoder le paquet pour le comparer à la RFC, il peut réencoder le paquet correctement.

Anonymisation C'est naturellement le cas puisque le client envoie sa requête au proxy, puis le proxy relie la requête. Le client est alors caché, inexistant pour les personnes externes.

Filtre Il pourra filtrer grâce à ses connaissances de la RFC, sur des URL (avec des whitelists et des blacklists).

Le proxy-cache est, généralement dans une DMZ.
Si on souhaite que le proxy soit transparent pour l'utilisateur, il faut faire une règle de DNAT sur le pare-feu. Ainsi, quand une requête de l'utilisateur veut aller sur Internet, le pare-feu envoie la requête sur le proxy. Ce dernier va alors analyser la trame puis la renvoyer au proxy.

5.1 Reverse proxy

Le reverse proxy est au proxy ce que le DNAT est au NAT.
Le principe est le même que pour un proxy, mais à l'inverse : de l'extérieur à l'intérieur.

Références

[1] GRSecurity. *GRSecurity*. GRSecurity. 2015. URL : `https://grsecurity.net/` (visité le 06/10/2015).