Firewall

Jean-François Berdjugin
IUT 1 Dept SRC
L'Isle d'Abeau

Problème

Les protocoles d'Internet sont conçus pour réaliser un transport robuste et non une sécurité robuste

=>

Mise en œuvre de solutions de sécurité et parmi elles les firewalls ou pare-feu.

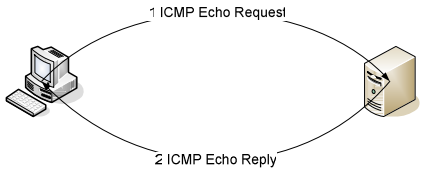
Méthodes d'attaques
Intrusion

Exemple :

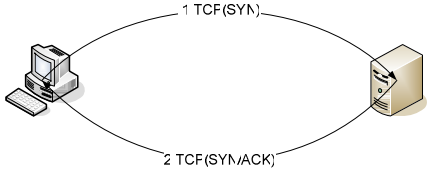
- Sondage : Ping en diffusion ou TCP SYN/ACK ou SYN/FIN (RST) sur des ports bien connus.
- Balayage de port.
- Caractérisation des versions.
- Intrusion (Outils Exploit, ou détournement de session).
- Après utilisation de logiciels de prise de contact (rootkit).

Sondage

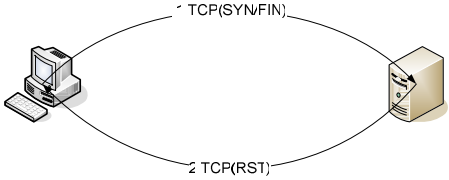
- Ping : ICMP echo request => ICMP echo reply (niveau 3)



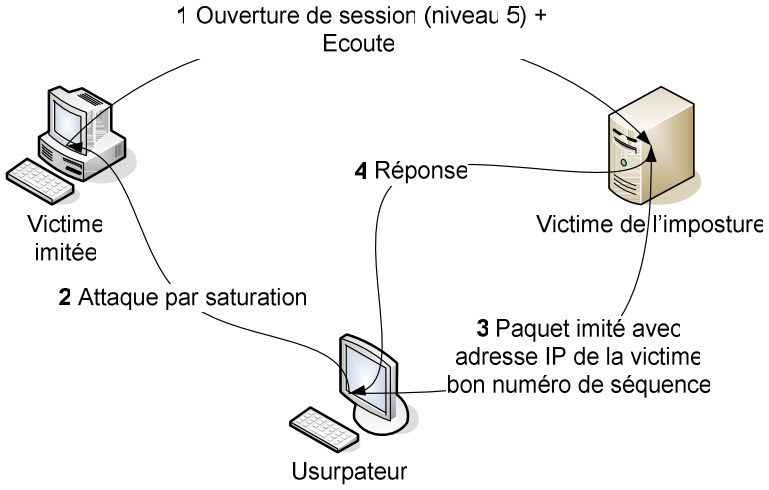
- SYN/ACK (niveau 4)



- SYN/FIN (niveau 4)



Détournement de session

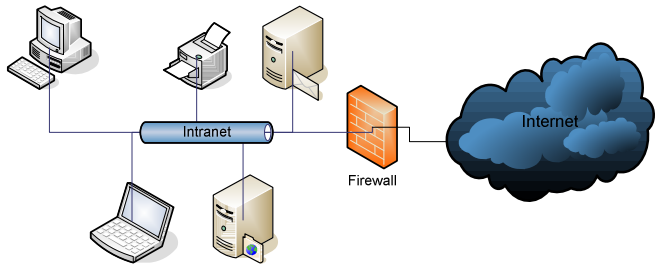


Méthodes d'attaques déni de service

- Message défectueux (plantage)
- Stricto sensu (rafale de SYN – effort asymétrique -)
- Bête et méchante (ping en diffusion avec comme adresse source celle de la victime)
- Distribuée (utilisation d'autres ordinateurs infectés)

Firewall

Définition : machine sure et fiable faisant interface entre un réseau public et un réseau privé.



Services

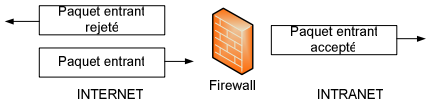
- **Filtrage IP (et Transport)**
- NAT /PAT (Network Address Translation / Port Address Translation)
- Relais Applicatifs (Proxy)

- Authentification, VPN (Virtual Private Network), …

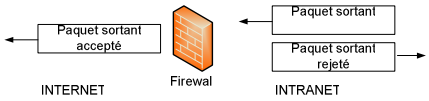
Firewall

Deux Flux:

1. En entrée (Internet vers Intranet)



2. En sortie (Intranet vers Internet)



Inspection des paquets

Niveau 4

Entête TCP	Corps TCP
Entête UDP	Corps UDP

Niveau 3

Entête ICMP	Corps ICMP
Entête IP	Corps IP

=> Filtrage sur le Type de message (TCP,UDP, ICMP), les ports (pour UDP et TCP) et les adresses IP => des règles (Access Control List).

Problème la fragmentation IP (où sont les ports) :

Entête IP	Entête TCP	Corps TCP

Entête IP	Corps TCP

⇒Filtrage statique (chaque paquet est examiné indépendamment des autres) ou Filtrage dynamique (chaque paquet est évalué en fonction des autres).

Statique vs Dynamique

Statique simple mais que faire des paquets ne transportant pas d'entête TCP, les laisser passer => un trafic indésirable peut entrer.

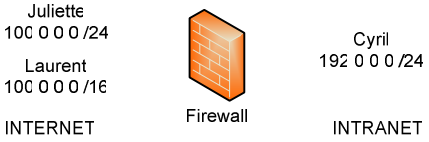
Dynamique plus sûr mais gourment en ressources, gestion d'une table des connexions (Type, Adresse IP interne, Numéro de port interne, Adresse IP externe, Numéro de port externe, état), plus intelligence (ex : FTP, port de données choisi par le serveur).

Exemple ACL factice

Cyril est responsable du réseau 192.0.0.0 /24, il travail avec Laurent qui est sur le réseau 100.0.0.0/16, il ne souhaite pas autoriser son réseau à Juliette qui est sur le réseau 100.0.0.0 /24 et ceux pour tous les services (on ne regarde pas les ports).

Règle pour le trafic entrant	@ origine	@ destination	Action	Commentaires
R1	100.0.0.0 /16	192.0.0.0 /24	Accepter	Laurent entrant
R2	100.0.0.0 /24	192.0.0.0 /16	Refuser	Juliette entrant
R3	0.0.0.0 /0	0.0.0.0 /0	Refuser	Refuser tout le reste

Exemple ACL factice



Règle pour le trafic entrant	@ origine	@ destination	Action	Commentaires
R1	100.0.0.0 /16	192.0.0.0 /24	Accepter	Laurent entrant
R2	100.0.0.0 /24	192.0.0.0 /16	Refuser	Juliette entrant
R3	0.0.0.0 /0	0.0.0.0 /0	Refuser	Refuser tout le reste

P1 de Juliette vers Cyril si R1 alors Problème (séquentiel)
si R2 alors Ok (préfix réseau)
=> Importance de l'ordre et difficultés d'écriture

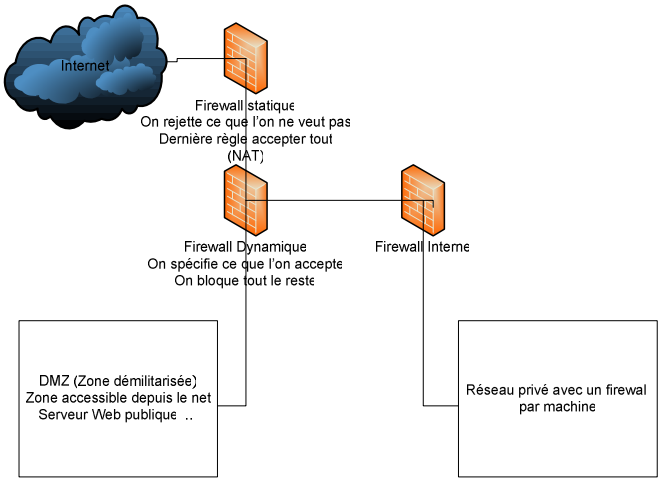
Exemple ACL réel

Exemple iptables sous Linux :
#Si aucune règle spécifique n'est acceptée, on bloque tout
#Ici trois chaînes : FORWARD traversée, INPUT vers un processus local, OUTPUT depuis un processus local.
Iptables –P INPUT DROP
Iptables –P OUTPUT DROP
Iptables –P FORWARD DROP

#On accepte tout ce qui passe sur le réseau local (192.0.0.0 /24)
Iptables –A INPUT –s 192.0.0.0/24 –j accept
Iptables –A OUTPUT –d 192.0.0.0/24 –j accept
Iptables –A FORWARD –s 192.0.0.0/24 –j accept

#On autorise ensuite les différents services
…

Architecture paranoïde



Conclusion

Des outils indispensables faisant partie d'une politique de sécurité qui ne peuvent en aucun cas être une solution unique.

Maintenant utilisés conjointement avec des loggers (surveillance) et une évolution vers des firewalls actifs (qui modifies dynamiquement les règles).