Fondements de la sécurité : TD5 - Pare-feux et IDS

Exercice 1 : Vulnérabilités d'un pare-feu sans état

Sujet

Le pare-feu sans état d'une université qui relie son réseau à Internet (via une ligne de 40 Gbps) a été configuré de la manière suivante :

- Seules les connexions entrantes (initiées depuis l'extérieur de l'université) sur les ports `22`, `80` et `443` sont permises ;
- Toutes les connexions sortantes (initiées depuis l'intérieur de l'université) sont permises.

1. Rappelez les services correspondant aux numéros de ports indiqués.
2. S'agissant de la gestion du trafic entrant, quelle(s) règle(s) de filtrage permettraient de mettre en oeuvre la politique de sécurité définie ici ?
3. Pour quelle raison l'université a-t-elle pu choisir un pare-feu sans état ?
4. Expliquer comment un adversaire ne disposant pas d'un accès interne au réseau cette université pourrait "cartogra- phier" ce dernier en le scannant depuis l'extérieur.
5. Que faudrait-il changer pour améliorer la situation ?

Résolution

Question 1

- 22 : **SSH/TCP**
- 80 : **HTTP/TCP**
- 443 : **HTTPS/TCP**

Question 2

@IP src	port src	@IP dst	port dst	Protocole	Drapeaux	Action
*	*	local	`80`	tcp	SYN, ACK, FIN, RST	ACCEPT
*	*	local	`443`	tcp	SYN, ACK, FIN, RST	ACCEPT
*	*	local	`22`	tcp	SYN, ACK, FIN, RST	ACCEPT

@IP src	port src	@IP dst	port dst	Protocole	Drapeaux	Action
*	*	*	*	*	*	DROP, LOG

Question 3

Question 4

Avec des outils qui scannent des ports (*Nmap* par exemple), l'attaquant peut également cartographier le réseau en envoyant des paquets tcp SYN-ACK à toutes les adresses IP du réseau sur les ports `80`, `443` et `22`. Les pare-feux sans état répondront à ces paquets avec un paquet tcp RST. L'attaquant peut ainsi cartographier le réseau en analysant les réponses.

Question 5

Il faudrait utiliser un pare-feu avec état. En effet, un pare-feu avec état va garder en mémoire les connexions établies et les paquets échangés.

Exercice 2 : Pare-feu sans état

Sujet

On considère un pare-feu sans état dont le critère de filtrage repose sur les paquets SYN (paquets dont le drapeau SYN est 1, et le drapeau ACK est 0). On souhaite que le serveur de messagerie (`128.178.1.1`) sur le réseau interne puisse recevoir et envoyer des messages de et vers Internet.

Service SMTP / tcp : port `25`.

1. Quelles règles proposeriez-vous et dans quel ordre ?

Résolution

Question 1

@IP src	port src	@IP dst	port dst	Protocole	Drapeaux	Action
*	*	`128.178.1.1`	`25`	tcp	SYN = 1 et ACK = 0	ACCEPT
*	*	`128.178.1.1`	`25`	tcp	SYN = 0 et ACK = 1	ACCEPT

@IP src	port src	@IP dst	port dst	Protocole	Drapeaux	Action
`128.178.1.1`	`25`	*	*	tcp	SYN = 1 et ACK = 0	ACCEPT
`128.178.1.1`	*	*	`25`	tcp	*	ACCEPT
*	`25`	`128.178.1.1`	*	tcp	*	ACCEPT
*	*	*	*	*	*	DROP, LOG

Exercice 3 : Pare-feu sans état (2)

Sujet

On considère un pare-feu sans état qui abrite la machine `203.167.75.1` et dont le critère de filtrage repose sur les paquets SYN (paquets dont le drapeau SYN est 1, et le drapeau ACK est 0). L'utilisateur de cette machine souhaite naviguer sur le Web, recevoir des connexions telnet provenant de l'extérieur du réseau interne, ainsi que recevoir et initier des connexions SSH de et vers Internet. Les serveurs HTTP, telnet et SSH utilisent respectivement les ports `80`, `23` et `22`.

1. Quelles règles proposeriez-vous et dans quel ordre ?

Résolution

Question 1

Exercice 4 : Pare-feu avec état

Sujet

Soit l'architecture illustrée en *figure 1*. On suppose que l'adresse du serveur Web est `10.0.0.2` et que les proxys SMTP, HTTP et DNS possèdent respectivement les adresses `10.0.0.25`, `10.0.0.80` et `10.0.0.53`. Les trois proxys sont utilisés en mode direct (donc vers Internet) et inverse (donc depuis Internet). Le serveur Web doit aussi être accessible depuis le réseau interne. On désigne par `dmz_proxy` toutes les adresses de la zone des proxys et par `dmz_web` toutes les adresses de la zone du serveur web.

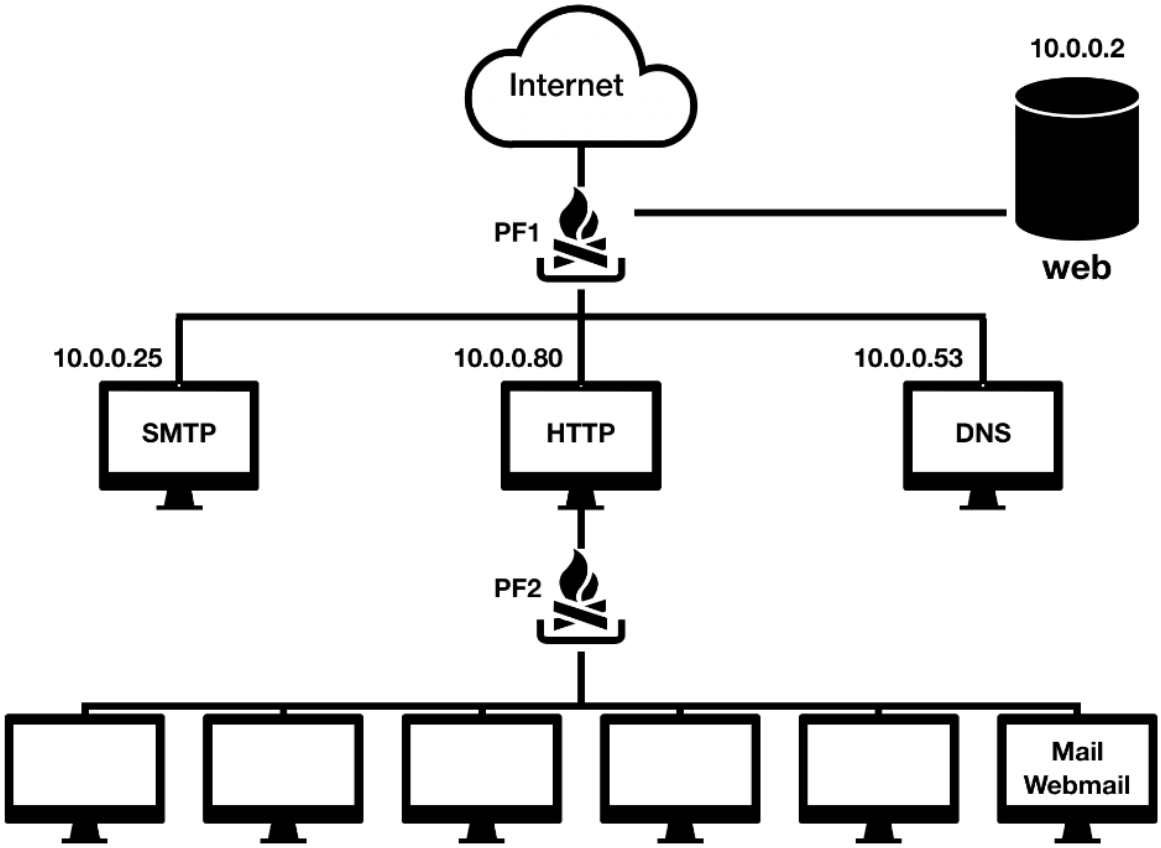

FIGURE 1 – Architecture en sandwich.

1. Ecrire les règles de filtrage pour le pare-feu externe à état (PF1).

Résolution

Question 1

Pour dresser le tableau des règles, nous cloisonnons par secteur (d'abord `dmz_proxy` puis `dmz_web`) en droppant les paquets qui ne sont pas destinés à ces secteurs petit à petit.

@IP src	port src	@IP dst	port dst	Protocole	Action
*	*	`10.0.0.25`	`25`	tcp	ACCEPT
*	*	`10.0.0.80`	`80`	tcp	ACCEPT
*	*	`10.0.0.53`	`53`	udp	ACCEPT
*	*	`dmz_proxy`	*	*	DROP, LOG
`10.0.0.25`	`25`	*	*	tcp	ACCEPT
`10.0.0.80`	`80`	*	*	tcp	ACCEPT
`10.0.0.53`	`53`	*	*	udp	ACCEPT
`dmz_proxy`	*	*	*	*	DROP, LOG
*	*	`10.0.0.2`	`80`	tcp	ACCEPT

@IP src	port src	@IP dst	port dst	Protocole	Action
*	*	dmz_web	*	*	DROP, LOG
dmz_web	*	*	*	*	DROP, LOG
*	*	*	*	*	DROP, LOG