Sécurité des Réseaux - TP6

Snort

Monroe Samuel

30 décembre 2015

1 Préambule

Ce tp est réalisé avec CentOS Security virtualisé de l'EPHEC avec VMWare.

2 Règles Snort

alert tcp 10.1.0.2 any -¿ 10.2.0.2 any
(flags : SA ; msg : "SYNACK détecté entre Serveur web et PCin" ; sid : 1000002 ;)

alert tcp 10.1.0.2 80 -¿ any any
(content : "Content-type : text/html" ; msg : "Message HTML détecté" ; sid : 1000003 ;)

alert icmp 10.1.0.1 any ¡¿ 10.1.0.3
(msg : "Messages ICMP détectés entre FW1 et FW3 !" ; sid : 1000004 ;)

alert tcp any any -¿ any any
(msg : "Full XMAS Scan Détecté" ; flags : SRAFPU ; sid : 9000004 ;)

3 Validation des règles

Après avoir entré ces règles dans le fichier local.rules, je fais tourner SNORT en mode IDS via **snort -dev -l ./log -h 10.1.0.0/24 -c /etc/snort/snort.conf**

Premièrement, pour valider les trois premières règles, j'imagine qu'un accès Web depuis PCin avec Links va probablement générer une alerte sur les deux premières puisque une connexion Web est aussi une connexion TCP avec les classiques SYN/SYNACK/ACK.
Ensuite, je tente un ping depuis FW1 vers FW2 pour vérifier la troisième.

Dans le dossier précisé .log, on retrouve des fichiers dont un nommé **alert**, qui contient les alertes générées.
Je retrouve les alertes concernant le SYNACK et les messages ICMP mais pas celui WEB. Une réinspection de mes règles me fera découvrir que c'était une erreur de syntaxe, cela devait être **Content-Type** et pas **Content-type**.

Enfin, pour le scan XMAS, je tente un **nmap -sX 10.1.0.0/24** mais cela ne génère rien du tout au niveau des alertes.
La documentation NMAP parle des flags FIN, PSH, URG que j'ai pourtant bien relevé dans ma règle, j'essaie donc en ne laissant que ceux-ci (FPU), ce qui se révelera concluant et remplira bien mon fichier d'alertes de SCANS XMAS.

Après correction, mes règles sont les suivantes :

alert tcp 10.1.0.2 any -¿ 10.2.0.2 any
(flags : SA ; msg : "SYNACK détecté entre Serveur web et PCin" ; sid : 1000002 ;)

alert tcp 10.1.0.2 80 -¿ any any
(content : "Content-Type : text/html" ; msg : "Message HTML détecté" ; sid : 1000003 ;)

alert icmp 10.1.0.1 any ¡¿ 10.1.0.3 any
(msg : "Messages ICMP détectés entre FW1 et FW2 !" ; sid : 1000004 ;)

alert tcp any any -¿ any any
(msg : "Full XMAS Scan Détecté" ; flags : FPU ; sid : 1000005 ;)