EPHEC

Louvain-la-neuve

Sécurité des réseaux informatiques

TP

Projet - Iptables

Rapport d'analyse du groupe 3TL2.4

Groupe 3TL1.4

Herrier Lucie Juckler Christian (Musuvaho Grace) Nyssens Sylvain

13 décembre 2014

1 Introduction

Ce document présente l'analyse que nous avons faite du travail réalisé par le groupe 2TL2.4. Nous avons reçu leur travail, et nous avons par la suite testé leur configuration iptables avec nos scripts et procédures de validation. Nous avons pris leur configuration stockée dans les scripts `config_FW1.sh, config_FW2.sh, config_FW3.sh`. Notons toutefois que leur rapport contient des règles tout autres. Nous n'avons pas testé ces règles, car elles ne devaient pas êtres comprises dans le rapport. Nous expliquons ci-dessous les résultats obtenus lors de nos tests sur les scripts pour chacun des firewalls configurés. Enfin, nous concluons sur la sécurité de la configuration du groupe 2TL2.4.

2 Validation

La plupart des validations décrites ci-dessous ont été réalisée en tapant les commandes à la main. Nous avons également exécuté nos scripts de validations écrits dans le cadre de notre configuration.

2.1 Validation du FW1

Script FW2 sur machine	Résultat espéré	Résultat obtenu avec règles
U1 et U2 : lynx (http et https) vers www.paranoyak.com via la commande `lynx http(s)://192.168.7.10`	OK pour HTTP, pas moyen de tester HTTPS	Ne fonctionne pas
R1 et R2 : test du local dns via la commande `nslookup www.paranoyak.com`. Aussi testé avec un nom de machine via la commande `nslookup SSH`	OK	Ne fonctionne pas
R1 et R2 : lynx (http et https) vers www.paranoyak.com via la commande `lynx http(s)://192.168.7.10`	OK pour HTTP, pas moyen de tester HTTPS	Ne fonctionne pas
R1 et R2 : envoi et réception d'email avec bill sur R1 et steve sur R2, communicant entre eux à l'aide de `mutt`	OK	Ne fonctionne pas
R1 : connexion ssh à processor via la commande `ssh 192.168.4.10`	OK	Ne fonctionne pas
R2 : connexion ssh à processor via la commande `ssh 192.168.4.10`	Not OK	Not OK (coup de chance)
R2 : connexion ssh à SSH via la commande `ssh 192.168.1.10`	OK	Ne fonctionne pas
R1 et R2 : ftp vers FTP via la commande `ftp 192.168.1.11`	OK	Ne fonctionne pas
R1 et R2 : connexion au serveur NFS lors du boot de la machine et échange de fichiers via /home/sharing	OK	Ne fonctionne pas
R1 et R2 : faire un backup de fichier sur rsync. Sur R1, avec login bill et un fichier coucou.txt, on fait la commande `rsync -v test.txt bill@192.168.7.12::backup_ bill`	OK	Ne fonctionne pas

T1 : test du public dns via la commande `nslookup www.paranoyak.com` et les autres noms de domaine	OK	Ne fonctionne pas $->$ suite avec les adresses IP.
T1 : lynx vers www.paranoyak.com via la commande `lynx 192.168.7.10`	OK pour HTTP	Ne fonctionne pas
T1 : envoi réception de mail via `mutt`, loggué en tant que steve sur la machine	OK	Ne fonctionne pas
T1 : connexion à SSH via la commande `ssh 192.168.1.10`, loggué en tant que steve sur la machine	OK	Ne fonctionne pas

Au vu des résultats obtenus ci-dessus avec les commandes entrées à la main, et après lecture de leurs scripts de validation, nous avons jugé qu'il n'était pas nécessaire de tester les connexions avec les scripts.

2.2 Validation du FW2

Script FW2 sur machine	Résultat espéré	Résultat obtenu avec règles
U1 et U2 : test du local dns via la commande `nslookup www.paranoyak.com`. Aussi testé avec un nom de machine via la commande `nslookup SSH`	OK	Ne fonctionne pas
U1 : lynx (http et https) vers www.paranoyak.com via la commande `lynx http(s)://www.paranoyak.com`	OK pour HTTP, pas moyen de tester HTTPS	Ne fonctionne pas
U2 : lynx (http et https) vers www.paranoyak.com via la commande `lynx http(s):/www.paranoyak.com`	OK pour HTTP, pas moyen de tester HTTPS	Ne fonctionne pas
U1 : envoi de mail de Bill à Steve via `mutt`, loggué en tant que bill sur la machine	OK	Ne fonctionne pas
U2 : réception de mail de Steve à Bill via `mutt`, loggué en tant que steve sur la machine	OK	Ne fonctionne pas

Au vu des résultats obtenus ci-dessus avec les commandes entrées à la main, et après lecture de leurs scripts de validation, nous avons jugé qu'il n'était pas nécessaire de tester les connexions avec les scripts.

2.3 Validation du FW3

Script FW3 sur machine	Résultat espéré	Résultat obtenu avec règles
processor : résolution de noms à l'aide du LDNS `nslookup SSH`	OK	Ne fonctionne pas -¿ suite des commandes avec les adresses IP.
R1 : connexion ssh à processor via la commande `ssh 192.168.4.10`	OK	Ne fonctionne pas.
R2 : connexion ssh à processor via la commande `ssh 192.168.4.10`	Not OK	Not OK (coup de chance)

SSH : connexion ssh à processor via la commande `ssh 192.168.4.10`	OK	Ne fonctionne pas
processor : ftp vers FTP via la commande `ftp FTP`	OK	Ne fonctionne pas
processor : lynx vers www.paranoyak.com via la commande `lynx www.paranoyak.com`	Not OK	Not OK (coup de chance)

Au vu des résultats obtenus ci-dessus avec les commandes entrées à la main, et après lecture de leurs scripts de validation, nous avons jugé qu'il n'était pas nécessaire de tester les connexions avec les scripts.

3 Remarques

1. Nous avons eu du mal à pouvoir démarrer leur labo. En effet, les fichiers de configuration étaient mal encodés pour certains caractères. Ceci fait que nous avons du les modifier avant de pouvoir les exécuter. Par ailleurs, nous avons du supprimer les lignes de commentaires, celles-ci contenant des accents ne passant pas lors du démarrage du labo netkit.
2. Lors du démarrage du FW1, celui-ci a affiché des erreurs de type `Bad argument` et `Can't use -i with OUTPUT`.
3. Nous avons constaté ce qui semble être une erreur au niveau de la configuration de l'OUTPUT du FW3, qu'ils ont mis par défaut en ACCEPT, et pour lequel le groupe 3TL2.4 à défini par la suite d'autres règles ACCEPT.
4. Lors du démarrage du FW3, celui-ci a affiché une erreur de type `No chain/target/match by that name`.

4 Conclusion

Au terme de cette analyse nous pouvons conclure que le labo netkit, sur base des scripts `config_FW1.sh, config_FW2.sh, config_FW3.sh`, ne fonctionne pas. Nous pensons toutefois que la configuration figurant dans le rapport du groupe 3TL2.4 aurait pu fonctionner. Nous ne l'avons cependant pas testée, ce n'est pas dans le contrat. Les scripts de validations qu'ils ont réalisés étaient prévu notamment pour être exécutés sur les firewalls, ce qui les a probablement induit en erreur.

En ce qui concerne la sécurité de leur réseau, rien ne peut passer, mis à part un trafic directement vers ou depuis les différents firewalls. Des règles en FORWARD auraient résolu ce problème. Nous ne pouvons pas vraiment statuer sur la sécurité de leur configuration. Au stade où nous l'avons testé, il était trop sécurisé. Certes, ce qui doit être évité comme connexion l'est comme demandé. Les règles étant mal implémentée, nous ne pouvons pas plus nous prononcer sur le sujet. Notons que la policy par défaut des OUPUTS était en ACCEPT, ceci est contraire à une bonne pratique de sécurité. Surtout que la policy de ACCEPT et FORWARD étaient en DROP.