INSA de Lyon
Département Télécommunications,
Services et Usages

5TC-SRS
TP IDS

Durée : 4h

Ce TP sera réalisé dans l'environnement virtuel "TP-SEC-Infra". Le compte sur toutes les machines est root/root. Pour le démarrer, téléchargez le script `tp-sec-infra.sh` sur Moodle puis exécutez le : `bash tp-sec-infra.sh`

Durant ce TP, vous allez analyser un scénario d'attaque et travailler à sa détection par NIDS, HIDS puis corrélation d'alertes. Les outils utilisés seront Suricata (NIDS), OSSEC (HIDS), Prelude (SIEM et corrélation).

L'architecture réseau et les petits guides de démarrage des outils à manipuler sont à retrouver dans les (nombreuses) annexes (à diagonaliser avant de démarrer, bien sûr) ! Il est recommandé de faire l'ensemble du TP en utilisant la VM Commercial comme poste admin (avec ssh vers Firewall et DMZ) car elle contient une interface graphique mieux intégrée (redimensionnement du bureau par rapport à la taille de la fenêtre virtualbox, possibilité de copier/coller, ...).

1 Analyse de l'attaque

Un script d'attaque `ftp.py` est présent sur la machine du hacker (compte root). Analysez ce que fait ce script. À partir des outils pré-installés sur le SI (ou autre, selon le niveau de difficulté souhaité !), proposez une stratégie de détection mêlant NIDS, HIDS et corrélation. **Faîtes valider cette stratégie par un enseignant !**

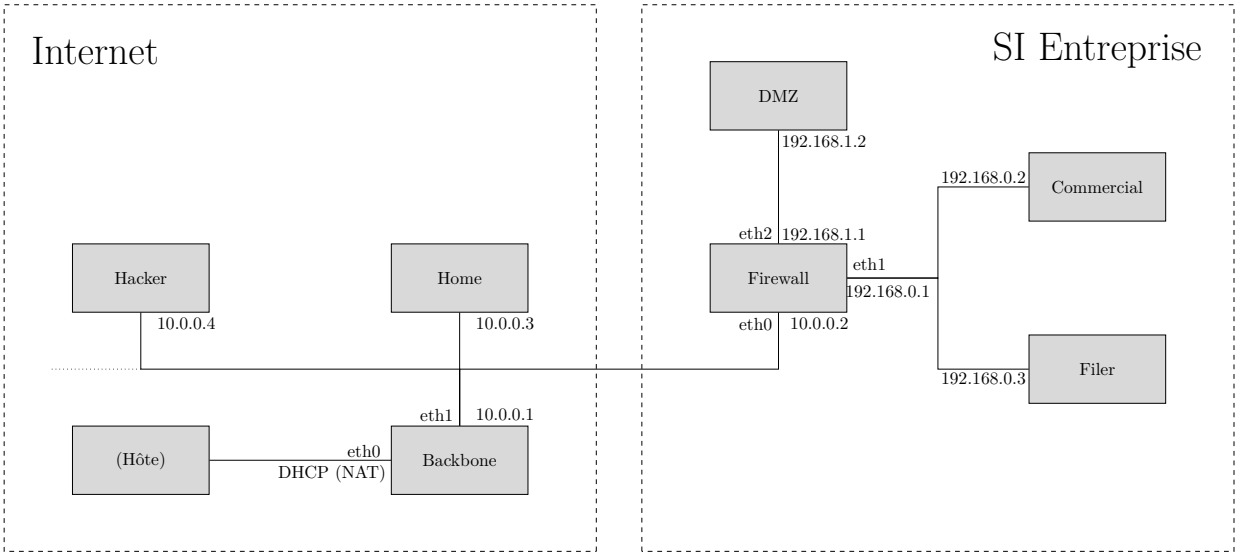
2 Yakafokon

Déployez cette stratégie sur le SI. Les logiciels sont pré-installés mais il faut :
— créer les règles adaptées (règles vides au départ) ;
— connecter les sondes à prelude-manager ;
— créer le script de corrélation adapté.

Une suggestion (forte) est d'écrire et tester les règles de chaque sonde indépendamment (suricata, OSSEC), sans passage par prelude-manager, via leurs fichiers de logs respectifs. Une fois que la sonde fonctionne comme souhaité, elle peut être reliée au manager. Il faut enfin vérifier que les alertes remontent bien.

A Architecture réseau

L'infrastructure réseau est la suivante :



Les logiciels suivants sont pré-installés :
— Suricata (VM Firewall)
— Prelude-manager (VM Firewall)
— Prelude-correlator (VM Firewall)
— Prewikka (VM Firewall)
— OSSEC (VM DMZ)
— serveur FTP (VM DMZ)

B Suricata (NIDS)

Suricata est un IDPS réseau qui utilise le même format de règles que Snort. Il est installé dans la VM Firewall. Sa configuration est dans `/etc/suricata/suricata-debian.yaml` et nous allons utiliser le fichier de règles `/etc/suricata/rules/local.rules` et vous pourrez visualiser le fichier de log `/var/log/suricata/fast.log`.

La règle Snort
`alert tcp 10.0.0.1 80 -> 192.168.1.0/24 111 (content:"Waldo"; msg:"Waldo's here";sid:1001)`
signifie par exemple que :
— On étudie les paquets TCP allant de `10.0.0.1:80` vers le sous-réseau `192.168.1.0/24:111`
— Contenant la chaîne "Waldo"
— Le log affichera "Waldo's here" s'il y a une correspondance

— alert peut être remplacé par drop pour jeter le paquet au lieu de le journaliser
— Le *sid* est un identifiant de règle, il doit être unique
— Les règles peuvent être composées de nombreux éléments (contenu, taille, expressions régulières, etc. Tout est ici : `http://manual.snort.org/node32.html`)

Lisez les règles présentes dans le fichier `local.rules`. Déclenchez la règle "COMMUNITY WEB-MISC Test Script Access" en accédant au serveur web de la DMZ. La requête est-elle exécutée avec succès ?

Analysez ensuite la signature de CodeRed (un ver se propageant via une faille des serveurs web Microsoft IIS). Arrivez-vous à déclencher cette alerte ? Peut-on vraiment parler d'intrusion ? Comment qualifier cette alerte ?

Lorsque vous modifiez les règles, il faut recharger le fichier avec `service suricata restart`.

Dans la configuration préinstallée, Suricata est en écoute seulement (pas IPS). D'autres configurations de Suricata permettent de le mettre en interception, par exemple en activant `nfqueue` dans `/etc/default/suricata`. Pour activer ensuite le passage par Suricata dans la configuration installée, il faut ajouter une décision NFQUEUE au lieu des décision ACCEPT dans les règles IPTables. Par exemple, pour faire passer par Suricata tout le trafic forwardé : `iptables -A FORWARD -j NFQUEUE` (attention, suricata prend des décisions définitives, le reste des règles n'est pas appelé ensuite !)

C OSSEC (HIDS)

OSSEC est un HIDS installé sur la machine DMZ. Il permet notamment de surveiller les logs et les fichiers présents sur la machine. Sa configuration se trouve dans `/var/ossec/etc/ossec.conf`. La partie `syscheck` est responsable de surveiller les fichiers présents (`https://ossec.github.io/docs/manual/syscheck/index.html`), il est aussi possible d'analyser les logs (`https://ossec.github.io/docs/manual/monitoring/index.html`). Attention pour syscheck, la surveillance d'apparition de nouveaux fichiers (non présente par défaut, il faut ajouter une option et une règle, tout est détaillé sur la page de doc) nécessite de désactiver `realtime`.

Pour utiliser syscheck, il faut attendre que la surveillance soit prête (cela prend un certain temps au démarrage), à surveiller dans `/var/ossec/logs/ossec.log`. Les alertes sont ensuite dans `/var/ossec/logs/alerts/alerts.log`.

D Prelude-manager (concentrateur)

Prelude-manager est un concentrateur d'alertes. Il utilise le format d'alerte IDMEF et Suricata et OSSEC savent lui remonter leurs alertes. Le jumelage entre le manager et les sondes est réalisé via un échange TLS SRP [1] géré par `prelude-admin`.

Lors du jumelage, chaque sonde conserve un *profil* local (`/etc/preludes/profiles/<profile>/` contenant sa configuration et son matériel cryptographique (certificat, clés). Le manager, lui, a signé le certificat (avec sa clé privée...) mais ne conserve pas de liste des sondes enregistrées. `prelude-admin list -l` permet de lister les profils actuellement configurés sur la machine locale.

Pour jumeler une sonde au manager, il faut :
— côté manager (VM Firewall) : `prelude-admin registration-server prelude-manager`

1. `https://en.wikipedia.org/wiki/TLS-SRP`

— côté sonde : `prelude-admin register <profile> "idmef:w" <IP manager> --uid <UID> --gid <GID>` avec
  — `<profile>` : nom du profil, `suricata` pour Suricata et `OSSEC-DMZ` pour OSSEC (pour être cohérent avec la pré-configuration)
  — `<IP manager>` : l'IP du manager
  — `<UID>/<GID>` : l'uid et le gid de la sonde qui va remonter les alertes (ici 1003/1003 pour suricata, 1005/1005 pour OSSEC), utilisé pour poser les droits sur le matériel cryptographique généré lors du jumelage

E Prewikka (interface web de visualisation)

Prewikka est une application web permettant la visualisation de l'état des sondes enregistrées ainsi que des alertes. Il est installé sur la machine Firewall, accessible depuis le navigateur de la machine Commercial à l'URL `http://192.168.0.1`. Le compte est admin/admin (bien sûr, la première étape dans un vrai déploiement est de changer cela...).

Si prelude-manager apparaît *offline*, il faut le relancer (sur la VM Firewall) :

`service prelude-manager restart` (il y a un message d'erreur mais en fait, ça marche [au moins en partie]).

Par défaut, la liste des agents (les sondes) est vide. Il faut ajouter Suricata (activer prelude dans la configuration suricata `/etc/suricata/suricata-debian.yaml` puis `service suricata restart`) puis OSSEC (activer prelude dans la configuration OSSEC `/var/ossec/etc/ossec.conf` puis `service ossec restart`).

Vous pouvez ensuite visualiser des événements. Si tout n'apparaît pas, quelques restarts de services peuvent faire tomber en marche !

F Prelude-correlator (corrélation)

Jumelage avec le manager : `prelude-admin register prelude-correlator "idmef:rw" 127.0.0.1 --uid prelude-correlator --gid prelude-correlator` (accès read/write cette fois-ci car la corrélation nécessite la lecture des alertes remontées et l'écriture de nouvelles alertes). Puis relancer le service prelude-correlator.

Une règle de corrélation est en fait un script python. Vous trouverez un exemple dans `/usr/share/doc/prelude-correlator/examples`. Pour l'installer, tapez :

— `python setup.py build`
— `python setup.py install`

Puis dans `/etc/prelude-correlator/prelude-correlator.conf`, ajoutez :

```
[MyPlugin]
disable=false
```

Enfin, relancez prelude-correlator. Une documentation plus complète est disponible ici : `https://www.prelude-siem.org/projects/prelude/wiki/PreludeCorrelator`. YOLO !

G Shorewall

Vous avez pu vous rendre compte de la complexité du réglage manuel du pare-feu. En particulier, la lecture des règles existantes ou la vérification de leur cohérence peut présenter des problèmes. La maintenance d'une telle solution est donc complexe dans un environnement de production : les règles changent souvent et demandent une inspection régulière.

De nombreuses solutions ont été développées pour faciliter la gestion des règles iptables. Nous allons ici utiliser shorewall. Shorewall n'est pas un démon et repose entièrement sur iptables. Il consiste en une série de scripts permettant de simplifier la configuration. Installez shorewall avec la commande `apt-get install shorewall`

Les documentations sont disponibles dans `/usr/share/doc/shorewall` et des exemples de configuration dans le sous-dossier `examples`. La configuration doit être placée dans `/etc/shorewall`. Les fichiers de configuration sont tous documentés, comme vous pourrez le remarquer :

- zones : définit des zones (pour donner des noms logiques aux interfaces utilisées, par exemple Internet, dmz...)
- interfaces : correspondance interface / zone
- rules : contient la liste des exceptions
- policy : politiques par défaut pour certaines interfaces
- masq : traduction d'adresses pour un réseau entier

La DMZ fournit les services suivants : DNS (UDP 53), IMAP (TCP 143), SMTP (TCP 25) et HTTP (TCP 80).

Implémentez avec Shorewall sur la machine Firewall une politique de sécurité simple pour le SI complet.