MI-LXC: Une plateforme pédagogique pour la sécurité réseau

François Lesueur
francois.lesueur@insa-lyon.fr
@FLesueur

https://github.com/flesueur/mi-lxc

SSTIC, 5 juin 2020

INSA Lyon, Département Télécommunications, Services et Usages,
CITI, Équipe DynaMid

MI-LXC

Mini-Internet using LXC ?

- Une infrastructure de référence simulant un *mini-internet*
  - Des services nécessaires : DNS, SMTP, HTTP, ...
  - Un routage par BGP entre AS indépendants
  - Un pré-requis nécessaire pour pratiquer la sécurité sur Internet
- Un *framework* pour construire cette infrastructure virtuelle (et d'autres ?)
  - *Infrastructure-as-code*
  - Conteneurs LXC
  - Maintenable, versionnable, SLOC-scalable, léger
- Quelques exemples d'usages en TP de sécurité
  - 1 TP d'autorité de certification ACME
  - 3 TP de sécurité réseau : intrusion, segmentation, IDS
  - (et bientôt du réseau j'espère)

Une infrastructure de référence simulant un *mini-internet*

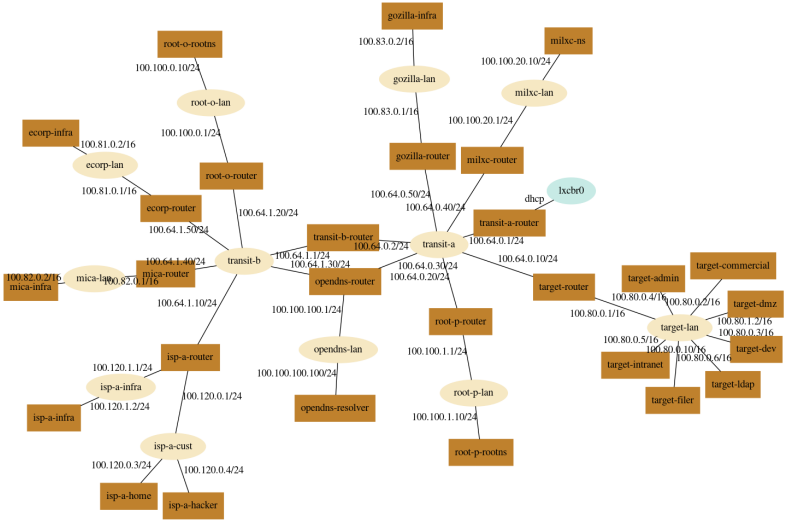
Qu'est-ce qu'on simule ?

Internet, c'est quoi ? *(selon moi...)*

- L'interconnexion de réseaux autonomes ($\approx$ AS)
- À travers du routage multi-tiers (transitaires, BGP)
- Selon des protocoles standards (BGP, HTTP, SMTP, ...)
- Dans une mise en œuvre orchestrée (IANA, ICANN, IETF, ...)

Topologie

- 11 AS (transit + edge)
- Routage BGP
- Racine DNS alternative
- Un TLD .milxc interne
- Zones DNS xyz.milxc
- SMTP, IMAP, HTTP
- Clients mails graphiques
- Suricata, OSSEC, Prelude, SmallStep CA...



Un *framework* pour construire des infrastructures virtuelles

Spécification de la topologie

Spécification de l'infrastructure cible

- Topologie globale dans *global.json*
- Topologie locale d'AS dans un *local.json*
- Provisionning d'hôte par un script bash

Mécanisme de templates

- Templates d'AS
- Templates d'hôtes

Le résultat

Quelques chiffres

- 30 conteneurs, 12 ponts réseau, 6GO HDD, 2GO de RAM
- Moins de 300 lignes de JSON, moins de 1000 lignes de scripts de provisionning

Et donc

- Versionnable
- SLOC-scalable
- Utilisable sur des machines basiques
- Maintenable (à peu près !)

Exemples de TP

HTTPS / CA

Modèle d'attaque

- Connexion HTTP
- Attaque BGP (ou DNS ou MitM)

Déploiement ACME

- Génération CA (Smallstep)
- Obtention certificat
- Déploiement CA chez Gozilla
- MAJ Gozilla

Risque restant

- Attaque durant la certification

Scénario d'intrusion

Objectifs

- Cinématique d'une attaque
- Élévation de privilèges (système, réseau)

- Bruteforce wiki + dépôt
- Mail spoofing
- SE pour faire lancer un rshell
- Lazagne
- Nmap
- Rebond interne
- Profit !

Segmentation réseau

Objectifs

- Appréhender fonctions iptables
- Concevoir une archi segmentée

Contraintes

- LDAP (IMAP, filer, postes)
- SMTP, IMAP, DNS, etc. $\rightarrow$ DMZ
- Des serveurs internes (filer, intranet)
- Des postes de travail, dont admin
- Manque un VPN !

IDS

Objectifs

- Appréhender NIDS/HIDS/Collecte
- On trouve. . . ce que l'on cherche !

- NIDS : Suricata
  - Brute force (par les 403)
  - Le passage d'un #!/bin/sh
  - Nmap interne
- HIDS : OSSEC
  - Brute force (par les logs)
  - Apparition d'un fichier
- Collecte : Prelude/Prewikka
  - Centralisation
  - Corrélation

Et maintenant ?

Ce qui marche bien

- Cette infrastructure et ces 4 sujets
- Assez bien stabilisé grâce à mes nombreux beta-testeurs depuis 2 ans...

Ce qu'on pourrait creuser

- Plus de scénarios ?
- De l'activité bruit de fond dans l'infrastructure ?
- D'autres outils de sécurité (MISP, hunting) ?
- D'autres outils de réseau (netem, dynamips) ?
- D'autres OS (Windows via VM) ?

MI-LXC: Une plateforme pédagogique pour la sécurité réseau

François Lesueur
francois.lesueur@insa-lyon.fr
@FLesueur

https://github.com/flesueur/mi-lxc

SSTIC, 5 juin 2020

INSA Lyon, Département Télécommunications, Services et Usages,
CITI, Équipe DynaMid