UML comme pot à miel

Michaël HERVIEUX
Thomas MEURISSE

Plan

- Introduction et thématique
- Protection du système
- Simulation et topologie réseau
- Logs et traces
- Conclusion

Introduction

- Qu’est ce qu’UML ?
  - User Mode Linux
  - Machine virtuelle (émulation de Linux)
  - Paramétrisation du hardware émulé
  - Toute action sur l’UML reste confinée sur l’UML
- A quoi sert un honeypot ?
  - Etude d’un attaquant
  - Capture de log

Thématique

- UML en tant que pot à miel
  - Avantage : forte interaction
  - Inconvénient : furtivité

Michaël Hervieux – Thomas Meurisse

Protection du système 1 - 4

- Problématique
  - Pourquoi protéger le système ?
    - Différence avec un linux non virtuel
    - Informations traîtres
    - Transparence pour l’attaquant
    - Configuration d’UML

Protection du système 2 - 4

Problèmes de montage

- Montage de la racine

  `/etc/mtab` & création du device associé

- Remontage de la racine

  Les majeurs

- Montage de l'hôte

  Modification du noyau

Michaël Hervieux – Thomas Meurisse

Protection du système 3 - 4

- La partition /proc
  - Eléments étranges et différents

    #more /proc/cmdline

    ubd0=rootfs eth0=tuntap,,fr:fd:0:0:0:1,192.168.210.254 root=/dev/ubd0

  - HoneyPot Proc FileSystem

    Gestion d'accès avec fichier sur l'hôte

Protection du système 4 - 4

- Dmesg

  Le ring buffer du kernel : /proc/kmsg

  La solution dans kernel/printk.c

- Divers indices
  - Taille des disques
  - Mémoire

Simulation 1-1

- une machine sans activité risque d’être inintéressante pour un pirate
- Pour palier à cela :
  - scripts divers simulant des connexions SSH, HTTP ou FTP
  - mise en place de services sur le système UML : FTP, HTTP, serveur IRC, …

Topologie réseau 1-4

- le système hôte sert de passerelle pour l'UML
  - Tout le trafic en direction de l'UML passe donc par l'hôte
  - Toutes les IPs vu de l'UML ont l'adresse MAC de la passerelle

Topologie réseau 2-4

- Simulation de plusieurs connexions associées aux différents scripts
  - Création d'utilisateurs fictifs et utilisation du module owner de iptables :
    - iptables -t nat -A POSTROUTING -m owner --uid-owner id-faux-utilisateur -j SNAT --to ip-fausse-machine

Topologie réseau 3-4

- Réponse à un ping :
  - iptables -t nat -A PREROUTING -p icmp -d ip-fausse-machine -j DNAT --to ip-machine-hote
- Modification du TTL
  - Modification des priorités des tables
  - iptables -t mangle -A POSTROUTING -s ip-fausse-machine -j TTL--ttl-set valeur-ttl

Topologie réseau 4-4

- Divers
  - Mettre en place les différents services au sein du réseau simulé (serveur DNS, …)
  - Spécifier une adresse MAC cohérente pour l'UML en vue d'un fingerprint

Logs et traces 1-3

- Log du trafic réseau

root@hote#tcpdump -i tap0 -s 0 -w fichier

➔Fichier au format pcap exploitable par différents outils

Logs et traces 2-3

- Log de tout ce qui est tapé (log TTY)
  - possibilité offerte par le noyau UML
  - indétectable par l'utilisateur
  - enregistré sur le disque de l'hôte
  - rejouable ultérieurement

Logs et traces 3-3

- Mise en place d’un IDS (prelude) pour détecter les intrusions et faciliter le tri :
  - prelude-manager sur l’hôte
  - prelude-nids sur l’hôte
  - prelude-lml sur le système UML

Conclusion

- Difficile de cacher la virtualité de l’UML
- Récupération de logs indétectable et très complète
- Cloisonnement du système empêchant le pirate de rebondir

Michaël Hervieux – Thomas Meurisse

Pour en savoir plus

- numéro spécial honeypot de MISC (sortie fin juin)
- http://user-mode-linux.sf.net/