Backdoor Linux

Nicolas Sarlin, Matthieu Renard, Ivan Landry et Ibrahima Sory Sow

Plan

- Qu’est-ce qu’un rootkit ?
- Qu’est-ce qu’une backdoor ?
- Notre rootkit :
  - Hijack d’appels systèmes
  - Le keylogger
  - La backdoor
- Démonstration

Un rootkit

- Programme malveillant invisible
- Installé en tant que root (d’où le nom…)
- Intègre souvent une backdoor

Une backdoor

- Elément d’un rootkit
- Sert à communiquer
- Peut envoyer des informations ou recevoir des ordres

Notre rootkit

- Module noyau rendu indétectable
- Hijack des appels systèmes write et getdents64
- Keylogger

Module noyau “invisible”

- Peut être chargé à chaud

- Se supprime de la liste des modules lors de son initialisation
  - Devient invisible (lsmod)
  - Ne peut être déchargé (rmmod)

Hijack d’appels systèmes

- But : ne pas lister un fichier (avec ls)
- Brute-force pour trouver la table des appels systèmes
- Hijack de write : problèmes sur les paramètres que lui passent ls
- Hijack de getdents(64) : mieux, peut tout de même être repéré

La backdoor

- Peut s’insérer à différents niveaux
- Idéalement le plus bas possible pour ne pas être détecté (tcpdump, etc…)
- Repose sur des protocoles souvent autorisés (HTTP, DNS, ICMP…)

Le keylogger

- Ecoute du fichier d’évènement clavier
- Mappage des touches et évènements accessible dans une structure
- Utilisation de plusieurs threads pour trouver le bon fichier

Démonstration

Conclusion

- Modules noyaux très utiles pour faire des rootkits
- Difficile de détecter un rootkit une fois celui-ci installé
- Souvent spécifique à une architecture
- La backdoor est le plus difficile à réaliser