Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 02 janvier 2017
N° CERTFR-2017-ACT-001

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-001

1 - Outils et recommandations pour la création de traces réseau au format PCAP

La capture de paquets au format PCAP est une pratique répandue dans le cadre d'opérations d'investigation numérique. Elle permet d'observer les communications réseau entre les postes compromis et les serveurs de commandes et de contrôle et ainsi d'obtenir une vision du périmètre de la compromission, mais également l'identification des informations exfiltrées.

Différents logiciels libres peuvent être utilisés pour enregistrer des traces réseau au format PCAP. Les choix d'architecture, et plus particulièrement les méthodes utilisées pour lire les paquets sur l'interface de capture, peuvent varier d'un logiciel à un autre. Cela peut avoir des impacts sur leurs performances. Ce bulletin d'actualité présente la technologie *PF_RING* puis les outils de capture open-source *tcpdump* et *netsniff-ng*. Enfin, quelques recommandations relatives à la création de traces réseau sont présentées.

PF_RING

PF_RING est une technologie développée par la société *Ntop*, dans le but de fournir une méthode dédiée à la capture de paquets à haut débit. Pour cela, cette technologie utilise un nouveau type de socket, exposé via le module noyau *pf_ring.ko*.

PF_RING s'utilise avec l'un des deux modes suivant:

- PF_RING (Mode standard)
- PF_RING ZC (Zero Copy)

L'API de la librairie *libpfring* permet d'interagir avec le module *pf_ring.ko* afin de capturer les paquets sur l'interface réseau. Les fonctions de l'API diffèrent selon le mode utilisé (*pfring_open()* en mode standard / *pfring_zc_open_device()* en mode ZC). Le mode *PF_RING ZC* permet d'outrepasser le noyau lors de la lecture des paquets et permet ainsi d'obtenir des performances optimales. Cependant, ce mode nécessite une carte réseau compatible ainsi que la recompilation du module noyau de la carte. En mode d'utilisation standard, *PF_RING* est compatible avec tout type de carte.

tcpdump

tcpdump est l'outil le plus communément répandu pour effectuer des captures réseau. Il s'appuie sur la librairie *libpcap* pour lire les paquets sur l'interface réseau. *Ntop* fournit une version modifiée de *tcpdump* et de la librairie *libpcap* afin d'ajouter le support de la technologie PF_RING. Les modifications sont principalement portées sur le code de la librairie *libpcap* qui utilise l'API de la librairie *libpfring* pour lire les paquets sur l'interface. Cependant, les fonctions de l'API utilisées ne sont pas les fonctions ZC. Par conséquent, cette version de *tcpdump* peut-être utilisée avec un module noyau *PF_RING* sans le support ZC, mais ne permettra pas d'obtenir des performances optimales lors de la capture des paquets.

netsniff-ng

netsniff-ng est un outil libre dédié à la capture de paquets à haut débit, conçu pour obtenir des performances optimales. La capture des paquets est effectuée via un mécanisme basé sur le type de socket *RX_RING* et l'appel système *mmap()*, qui permet la réception de paquets dans un buffer circulaire, partagé entre l'espace noyau et l'espace utilisateur. Ce mécanisme permet à *netsniff-ng* d'obtenir des performances similaires à la technologie *PF_RING*, utilisée en mode standard (non ZC). L'avantage de cet outil est qu'il fonctionne avec tout type de carte réseau, et qu'il ne nécessite pas le chargement d'un module noyau complémentaire.

Pour atteindre des résultats optimaux avec *netsniff-ng*, il est recommandé d'utiliser les options suivantes:

- *--bind-cpu*: définit l'affinité du thread vers un CPU spécifique
- *--prio-high*: définit la priorité du thread à la valeur maximale supporté par le système d'exploitation

Évaluation des performances

Les outils *netsniff-ng* et *tcpdump* (avec *PF_RING* en mode standard) peuvent consommer sans perte les paquets jusqu'à 10 Gb/s avec un processeur de nouvelle génération (sans écriture du fichier PCAP). Un nombre de coeurs élevé n'est pas strictement nécessaire puisque les 2 outils utilisent un seul fil d'exécution (thread).

Les problématiques liées à la perte de paquets se produisent lors de l'écriture d'un fichier PCAP, si le débit est supérieur à la vitesse maximale d'écriture du disque. Les accès disques étant le facteur limitant, l'utilisation de filtres BPF (*Berkeley Packets Filters*) sera recommandée pour limiter l'enregistrement des paquets à un sous-ensemble d'hôtes ou à un protocole particulier. En outre, l'utilisation d'un système de fichier de type *ramfs* peut permettre l'écriture d'un fichier PCAP à haut-débit, mais de taille restreinte (limitation liée à la quantité de mémoire volatile disponible).

Recommandations

Il est très fortement recommandé de ne pas installer et exécuter le logiciel de capture sur un poste potentiellement compromis. En effet, un code malveillant pourrait détecter l'utilisation de celui-ci et modifier son comportement en adéquation (fermeture des connexions réseau, suppression des traces et terminaison du processus, ...). Par conséquent il est recommandé d'utiliser une machine dédiée à cette tâche. La carte réseau utilisée lors de la capture doit être en mode *promiscuous* afin de capturer tous les paquets, même ceux qui ne sont pas destinés à la machine locale. Cette opération s'effectue avec l'utilitaire *ip* :

```
sudo ip link set eth0 promisc on
```

Enfin, pour limiter les risques liés à une éventuelle élévation de privilèges, il est recommandé d'octroyer la capacité *CAP_NET_RAW* (man 7 capabilites) au fichier exécutable choisi pour effectuer la capture, et ainsi d'exécuter le processus avec un utilisateur dédié, possédant des droits restreints. La commande *setcap* peut-être utilisée pour ajouter cette capacité:

```
sudo setcap cap_net_raw+ep /usr/sbin/tcpdump
```

2 - Rappel des avis émis

Dans la période du 26 décembre 2016 au 01 janvier 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-430 : Vulnérabilité dans les routeurs Netgear
- CERTFR-2016-AVI-431 : Multiples vulnérabilités dans Mozilla Thunderbird

Gestion détaillée du document

02 janvier 2017 version initiale.