Handleiding: Threat `CVE-2024-6387` Uittesten

Deze handleiding beschrijft hoe je de kwetsbaarheid `CVE-2024-6387` kunt uittesten in een kritieke Debian-omgeving (versie 10 Bullseye), die wordt aangevallen vanaf een Kali Linux-machine. Beide virtuele machines (VM's) worden opgestart via `VBoxManage`, en de benodigde scripts worden automatisch geïnstalleerd via PowerShell-scripts.

---

0. Voor het stappenplan

1. Clone de github-repo op: `https://github.com/JoranVanGoethem/NPE-Cybersecurity`
2. Voer in deze repository het stappenplan uit, hierin vind u ook de nieuwste handleiding en extra informatie over de aanval. Daarnaast staan hier ook de meest recente scripts in voor het testen van deze aanval.

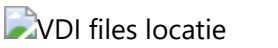
1. Stappenplan

1.1 VM's Aanmaken

1. **Download de benodigde VDI-bestanden**:
   - **Kali Linux**: Kali.vdi
   - **Debian 11 Bullseye**: Debian.vdi

   
   Sourceforge locatie

2. **extract de zip files**
   - extract Kali in de locatie: `/vdi-files/Kali`
   - het pad noemt: `/vdi-files/64bit/64bit/Kali Linux 2024.4 (64bit).vdi`
   - extract Debian in de locatie: `/vdi-files/Debian`
   - het pad noemt: `/vdi-files/32bit/32bit/Debian 11 (32bit).vdi`

   
   VDI files locatie

3. **Pas de `Build-VM.sh` aan INDIEN vorige stap niet gevolgd**:
   - Vervang `DEBIAN_VDI_PATH=""` met:

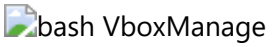
     ```
     DEBIAN_VDI_PATH="/jouw/pad/naar/Debian.vdi"
     ```

   - Vervang `KALI_VDI_PATH=""` met:

     ```
     KALI_VDI_PATH="/jouw/pad/naar/Kali.vdi"
     ```


Sourceforge locatie

4. **Voeg VBoxManage toe aan de terminal**
    - voer het commando: `export PATH=$PATH:"/c/Program Files/Oracle/VirtualBox"` uit

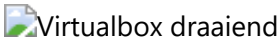

bash VboxManage

5. **Voer het script `Build-VM.sh` uit.**
    - open een git bash terminal in de map `/src/VM-Scripts/`
    - Voer dit commando uit om kali & Debian aan te maken: `./Build-VM.sh`
    - De virtuele machines worden aangemaakt in VirtualBox.


bash script runnen

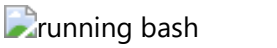

virtualbox VM's

6. **start de VM's**
    - open virtualbox en start beide VM's


Virtualbox draaiend

7. **Controleer of de VM's correct zijn opgestart** via de VirtualBox GUI of via:

```
VBoxManage list runningvms
```


running bash

8. **Log in op de VM's**
    - Log in met het wachtwoord: `osboxes.org` op de kali VM
    - Log in met het wachtwoord: `osboxes.org` op de Debian VM


VM schermen

1.2 Installatie van OpenSSH 8.5p1 op Debian

1. SSH-verbinding met Debian VM:

```
ssh -p 2222 osboxes@127.0.0.1

# wachtwoord = osboxes.org
```

```
C:\Users\camma>ssh -p 2222 osboxes@127.0.0.1
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:enbsCjQvNP3vJ60tiKuLsj1gmmv9TPkJ6GozRs3Exbg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:2222' (ED25519) to the list of known hosts.
osboxes@127.0.0.1's password:
Linux osboxes 5.10.0-8-686 #1 SMP Debian 5.10.46-4 (2021-08-03) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 16 09:47:03 2025
osboxes@osboxes:~$
```

2. Maak het script aan:

```
nano install_openssh_8.5p1.sh
```

```
osboxes@osboxes:~$
osboxes@osboxes:~$ sudo ./install_openssh_8.5p1.sh
```

3. Maak het script uitvoerbaar en voer het uit:

```
chmod +x install_openssh_8.5p1.sh
sudo ./install_openssh_8.5p1.sh
```

Na het uitvoeren moet je onderstaande afbeelding verkrijgen. Ook kun je controleren of de juiste versie van OpenSSH is geïnstalleerd.

```
✅ Stap 4: Configuratie aanpassen...
✅ Stap 5: sshd starten...
🚀 Installatie voltooid. Controleer met: ssh -V
osboxes@osboxes:~$ ssh -V
OpenSSH_8.5p1, OpenSSL 1.1.1w  11 Sep 2023
osboxes@osboxes:~$
```

Sluit hier de SSH-verbinding met Debian zodat poort 22 niet bezet is tijdens de aanval.

1.3 Aanval Uitvoeren vanuit Kali op de Debian VM

1. Test de verbinding tussen Kali en Debian

```
ping 192.168.56.101
```

```
┌──(osboxes㉿osboxes)-[~]
└─$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=3.16 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.945 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=2.77 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.76 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.29 ms
^C
── 192.168.56.101 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4023ms
rtt min/avg/max/mdev = 0.945/1.984/3.161/0.850 ms
```

2. Start sshd in debugmodus (voor live logging tijdens aanval):

```
sudo /usr/sbin/sshd -ddd
```

```
osboxes@osboxes:~$ sudo /usr/sbin/sshd
```

Als je een fout zou krijgen zoals: `Bind to port 22 failed: Address already in use` Stop dan de actieve SSH-service:

```
sudo systemctl stop ssh
sudo systemctl disable ssh
```

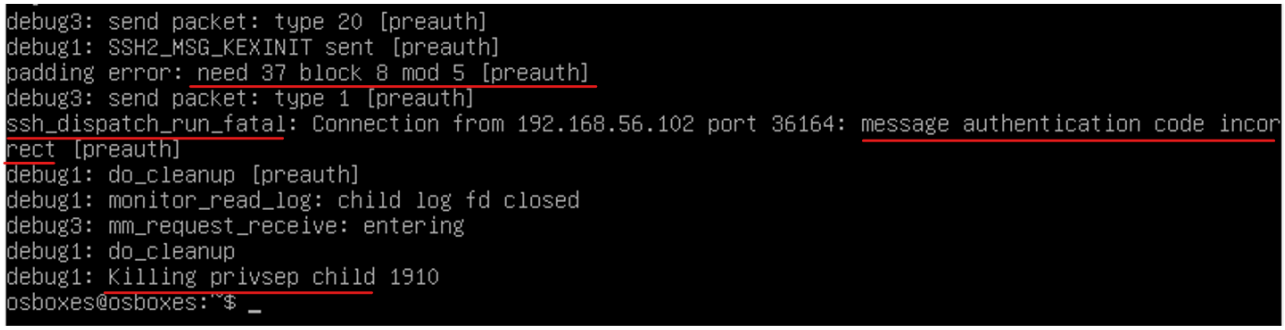
Na het uitvoeren van deze commando's zou alles correct moeten verlopen.

3. Voer de exploit uit op de doelmachine via netwerkinterface eth1, met 200 gelijktijdige verbindingen om de race condition te triggeren.

```
python3 CVE-2024-6387.py exploit -T 192.168.56.101 -p 22 -n eth1 -s 200
```

```
File  Actions  Edit  View  Help
┌──(osboxes㉿osboxes)-[~/Downloads]
└─$ python3 CVE-2024-6387.py exploit -T 192.168.56.101 -p 22 -n eth1 -s 200 -t 3
```

4. Monitor ondertussen de debug-output in Debian: Let op onderstaande signalen in de debug-output, die wijzen op succesvolle exploitatie.
    - `padding error`
    - `ssh_dispatch_run_fatal`
    - `message authentication code incorrect`
    - `killing privsep child`



---

2. Cheatsheet

Handige commando's en referenties:

Commando	Omschrijving
`ssh -p 2222 osboxes@127.0.0.1`	Maakt verbinding met de Debian VM via poort 2222 (port forwarding)
`nano install_openssh_8.5p1.sh`	Opent een nieuw scriptbestand om OpenSSH 8.5p1 te installeren
`chmod +x install_openssh_8.5p1.sh`	Maakt het script uitvoerbaar
`sudo ./install_openssh_8.5p1.sh`	Voert het installatiescript uit als root
`sudo /usr/sbin/sshd -ddd`	Start sshd in debugmodus voor live monitoring van de aanval
`sudo systemctl stop ssh && sudo systemctl disable ssh`	Stopt en schakelt de standaard SSH-service uit om conflicten te vermijden
`ping 192.168.56.101`	Test de netwerkverbinding vanaf Kali naar Debian
`python3 CVE-2024-6387.py exploit -T 192.168.56.101 -p 22 -n eth1 -s 200`	Voert de exploit uit vanaf Kali met 200 gelijktijdige verbindingen

---

3. Samenvatting

Aanval Uitvoeren op de Debian VM

1. **Plaats het exploit-script** `CVE-2024-6387.py` op de Kali VM (via shared folder of `scp`).
2. **Voer het script uit op de Kali VM**:

```
python3 CVE-2024-6387.py <doel-ip>
```

3. Monitor het gedrag van de Debian VM om te controleren of deze crasht of een shell terugstuurt.

Verifiëren van de Aanval

1. Open een terminal op je hostmachine.
2. Controleer in VirtualBox welke poort wordt doorgestuurd naar de SSH-poort van de Debian VM.
3. Maak verbinding via SSH met de Debian VM:

```
ssh -p <poortnummer> gebruiker@127.0.0.1
```

4. Controleer of de verbinding faalt of is overgenomen:
    - Indien de verbinding is gekraakt of overgenomen, is de aanval geslaagd en is de SSH-verbinding niet meer veilig.

---

4. Opmerkingen

- Zorg ervoor dat je **netwerkadapter** in VirtualBox correct is ingesteld (bijv. **NAT met poort-forwarding**).
- Gebruik **een afgesloten testomgeving**, los van productie- of persoonlijke systemen.
- **Update en patch kwetsbare systemen** na het testen.
- Deze handleiding is bedoeld **voor educatieve doeleinden** en mag **niet** worden gebruikt voor ongeautoriseerde aanvallen.

---

5. Makers van het Project

Deze handleiding is gebaseerd op de resources en scripts die beschikbaar zijn op de GitHub-pagina van het project:

- GitHub Repository: NPE-Cybersecurity
- Auteurs: Joran Van Goethem, Leander Counye en Vincent Cammaert

6. Bron van het Python-script

Het Python-script CVE-2024-6387.py is geïnspireerd door de repository van de volgende auteur:

- GitHub Repository: CVE-2024-6387 Exploit
- Auteur: Karmakstylez