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.

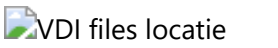
1. Stappenplan

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

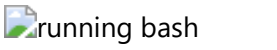

virtualbox VM's

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

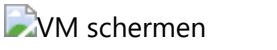

Virtualbox draaiend

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 PowerShell-script Uitvoeren

1.3 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.

1.4 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.

---

2. Cheatsheet

> Handige commando's en referenties:

Commando	Omschrijving
`ssh -p <poort> gebruiker@127.0.0.1`	Verbinding maken met de VM via poortforwarding
`scp bestand gebruiker@127.0.0.1:/pad`	Bestand kopiëren naar de VM via SCP
`VBoxManage startvm "VM-Naam"`	VM opstarten via CLI
`VBoxManage showvminfo "VM-Naam"`	Informatie tonen over een specifieke VM
`VBoxManage list runningvms`	Lijst van draaiende VM's tonen
`VBoxManage controlvm "VM-Naam" poweroff`	VM geforceerd afsluiten via CLI

---

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