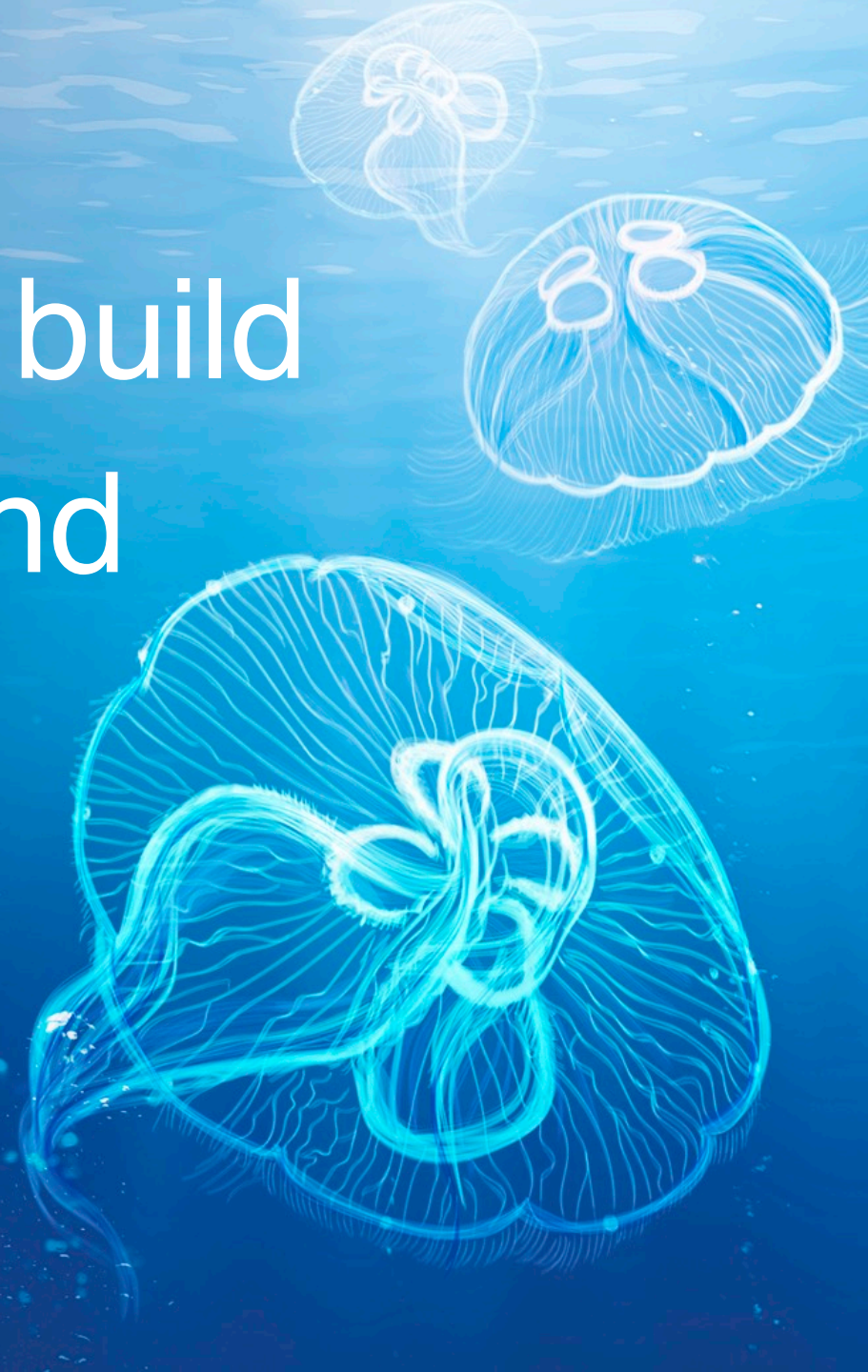
KPMG

You should not build you IAM on Sand



Vienna, 19.02.2020

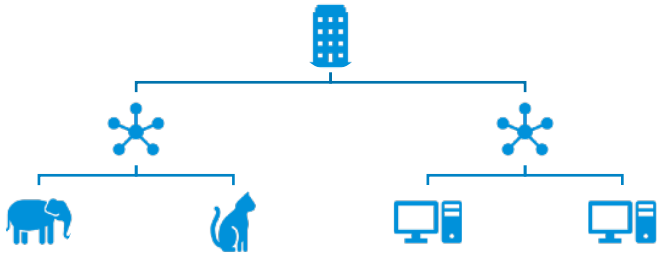
KPMG

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

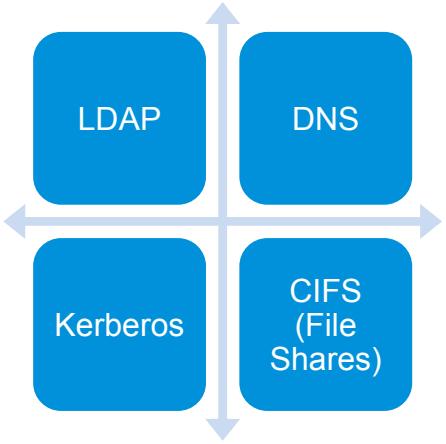
Vienna, 19.02.2020

What is the Active Directory?

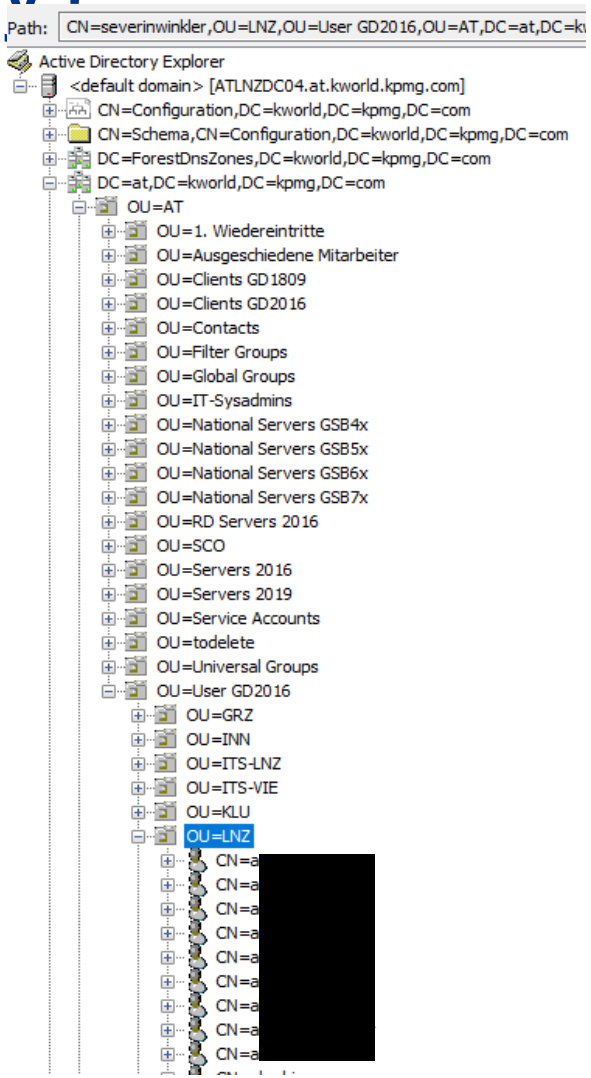
The Model…



The Services…



How does it look?

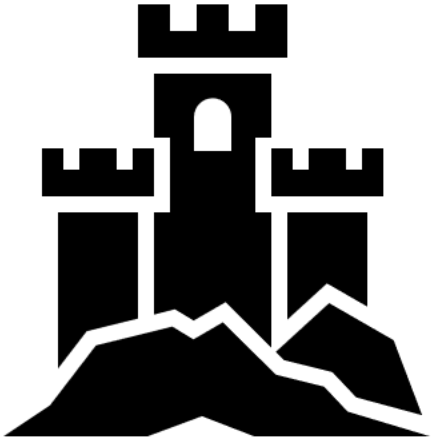


Why care for the Active Directory?

- 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

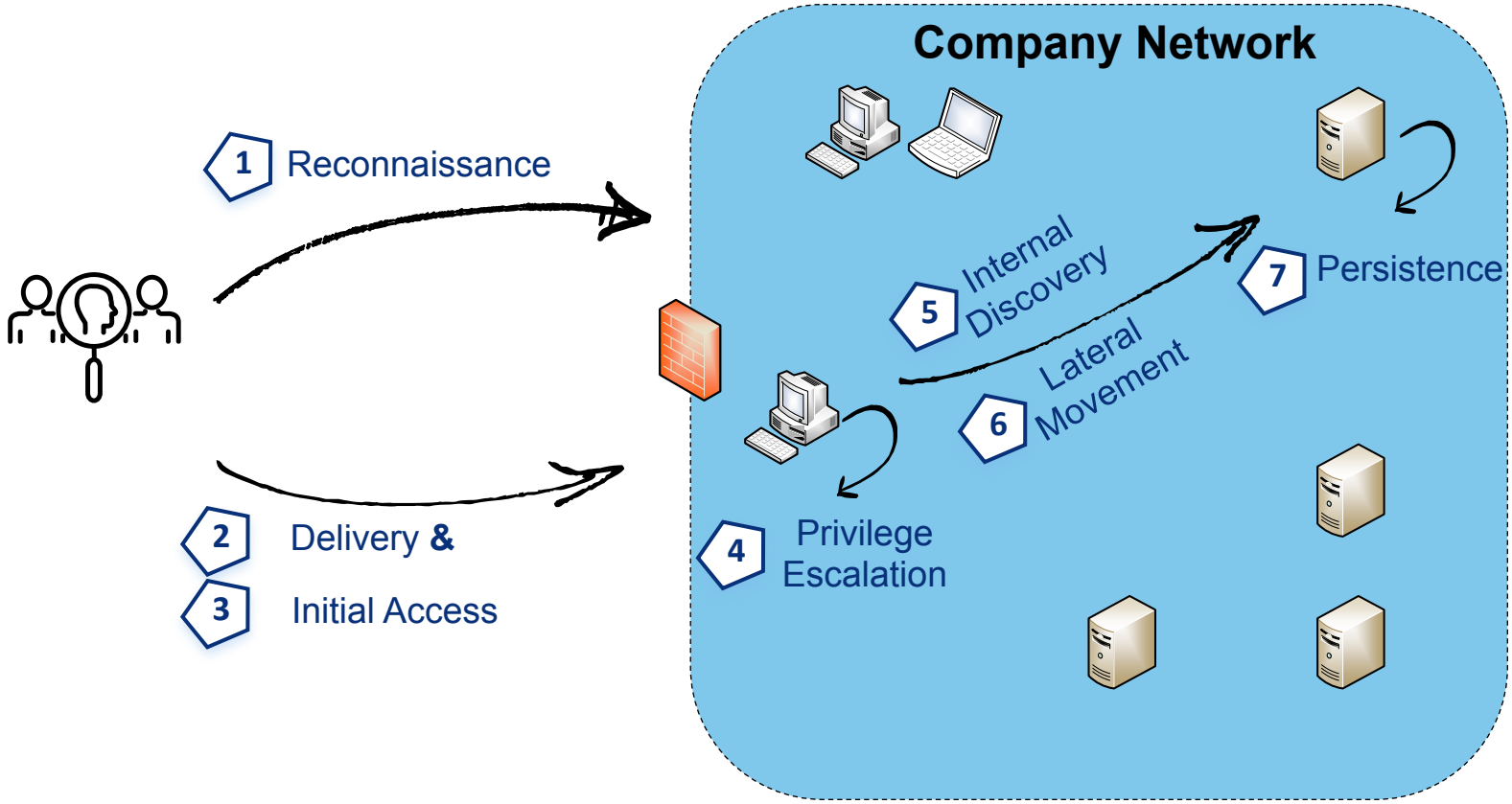
Publiziert am 20. Dezember 2019 von Günter Born

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/

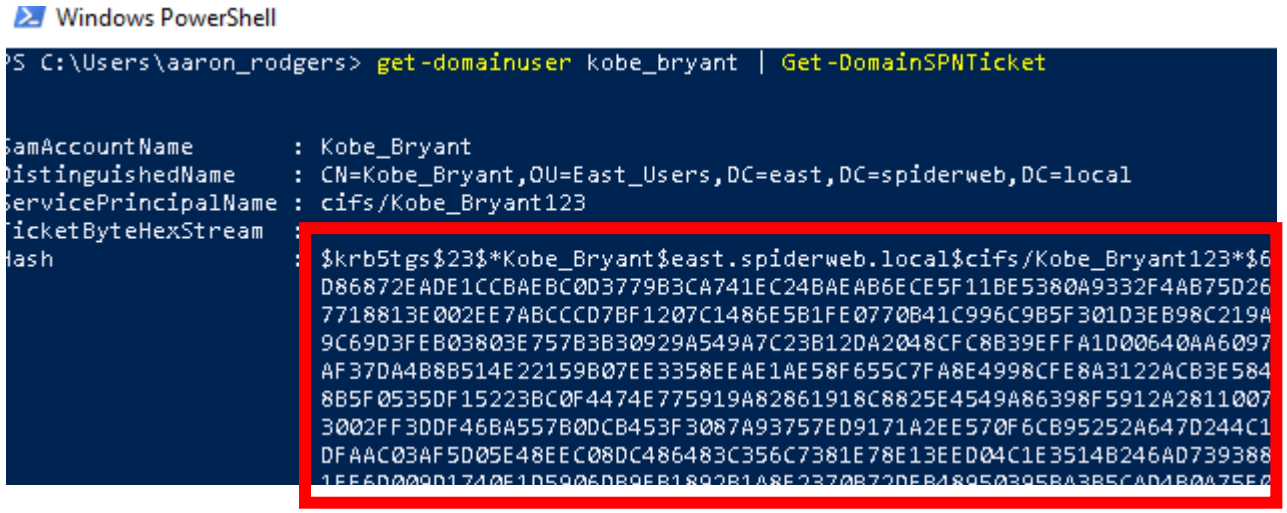
Authentication and Passwords in Active Directory

	Name	PWs stored …	Main Risks..	Situation
PW storage „*protocols*“	**LM Hash**	• Local SAM db • ntds.dit on DC	• PWs very easy to crack	Deactivated per default since Server 2008
	NT Hash (aka NTLM Hash)	• Local SAM db • ntds.dit on DC	• Pass-the-Hash	Default PW storage mechanism on DCs
Authentication Protocols	**NTLMv1** (aka Net-NTLMv1)	• Used in Challenge/ Response between server+client	• Crack Response • Relay Attacks	
	NTLMv2 (aka Net-NTLMv2)	• Like NTLMv1 but better.	• Crack Response • Relay Attacks	
	Kerberos	• In DC, never on network or clients, but.. • TGTs, Caches, ST,…	• Silver Ticket • Golden Ticket • Kerberroasting	Default since Windows 2003

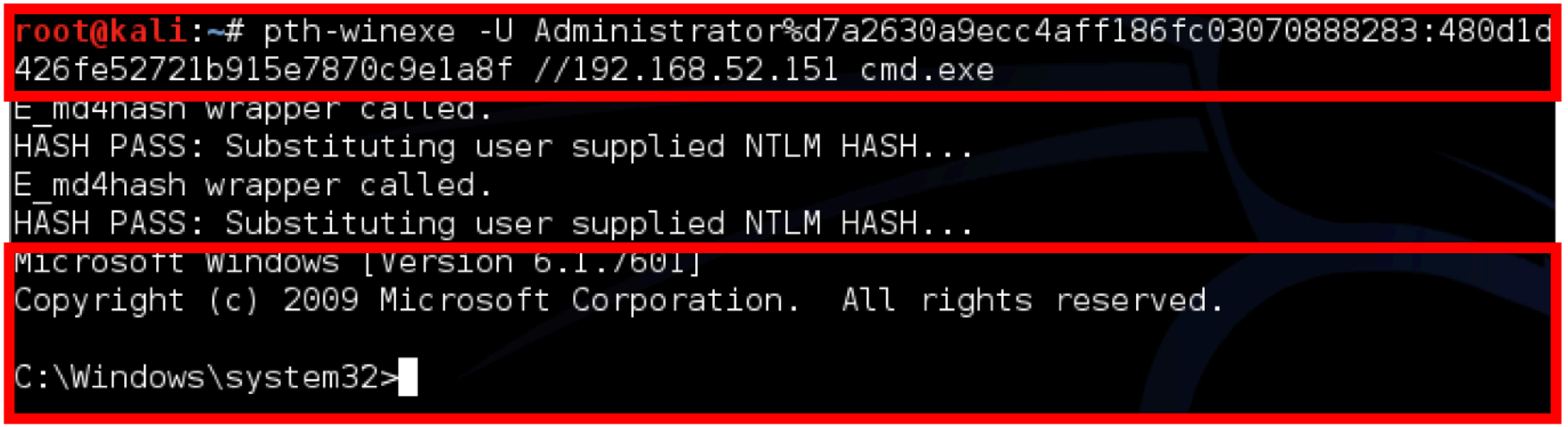
Common Attacks: Mimikatz (read secrets from LSASS process)

```
  .#####.   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
        tspkg :
         * Username : user
         * Domain   : test-PC-x64
         * Password : t3stus3r
...
```

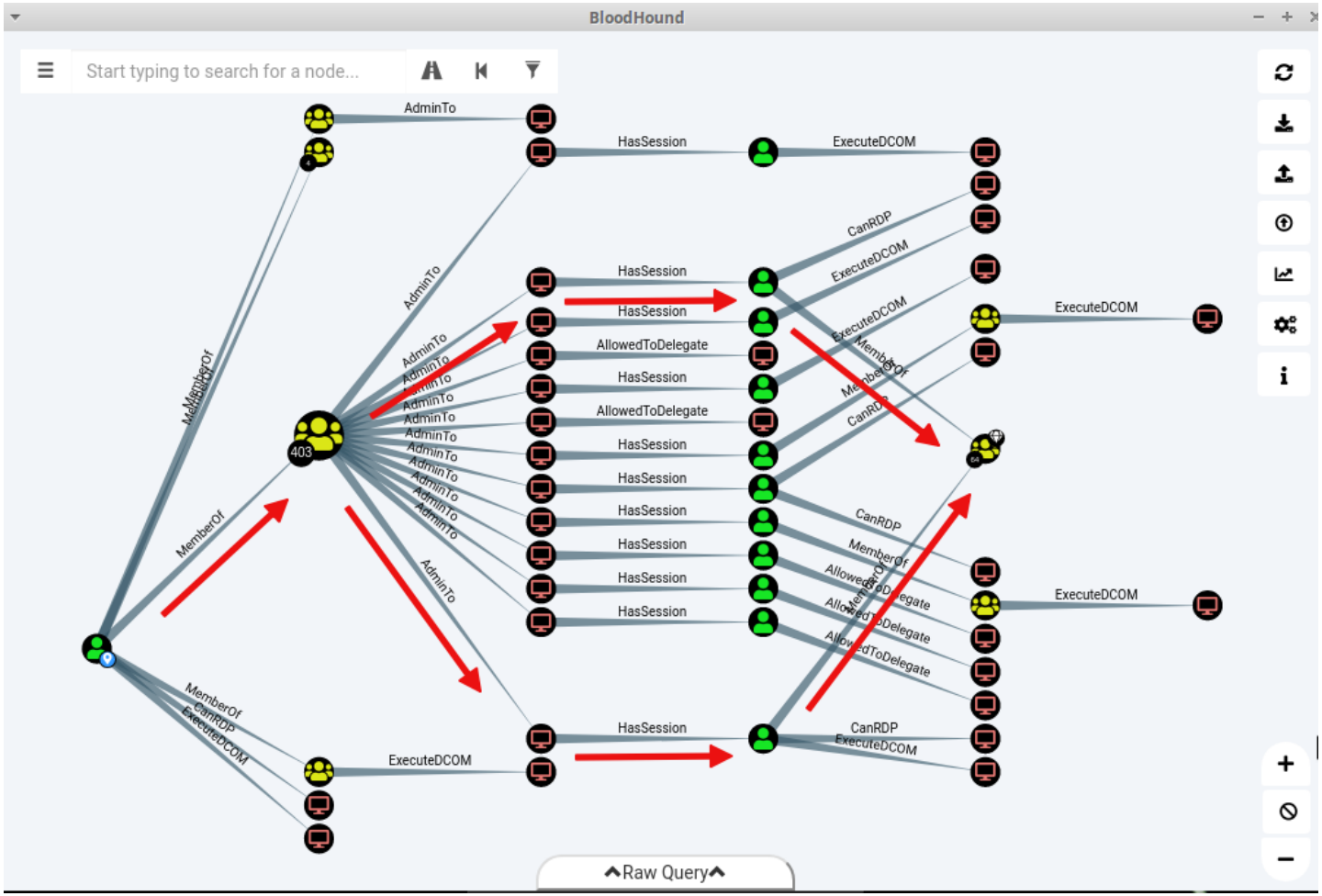
Common Attacks: Kerberroasting



Common Attacks: Pass-the-Hash



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	Countermeaures *)
DCSync	Extract password data into a malicous DC	• PWs reset for all users • KRBTG 2x
DCShadow	Use malicious DC to add new (bad) objects into existing AD Extremely stealthy	• Monitor for suspicious AD configuration changes
Dump and Crack ntds.dit	Typicall gives 20-80% of passwords of all users.	• PWs reset for all users • Reset KRBTG 2x
Skeleton Key	Sets an DC in-memory master password that can be used with any user	• Reboot DCs (but auto-deployment might be configured)
Golden Ticket	Create a kerberos ticket that allows subsequent access to all AD resources	• 2x pw reset for the KRBTGT account
Unknown unknowns	? ?	? ?

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


Discussion

KPMG
Severin Winkler

Senior Manager
Cyber Security

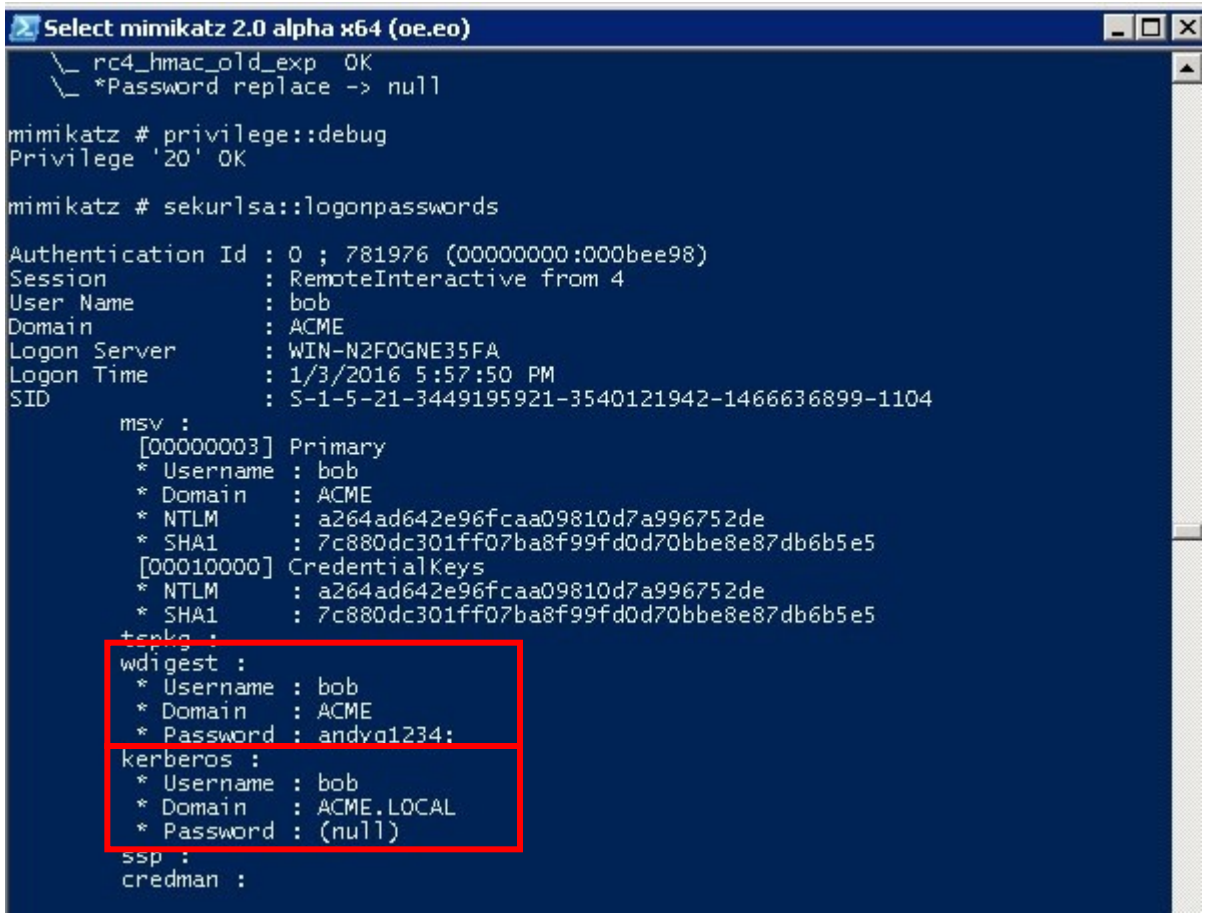
KPMG Advisory GmbH
Kudlichstraße 41-43
4020 Linz

M +43 664 820 24 24
E severinwinkler@kpmg.at
W 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



Enabling credential caching again:

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