

NIC **REBEL**  
**EDITION**

# GUERRILLA GARDENING



Evgenij Smirnov

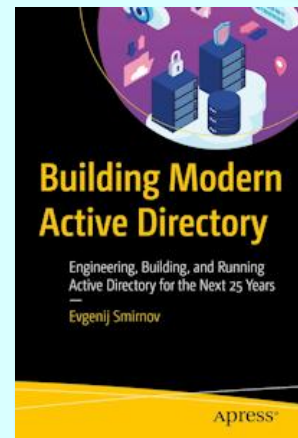
Active Directory (& Co.):  
**How Hard Is Hardening?**

# In this session

- Who's the dude?
- A question for you
- Why the title?
- Hardening examples – **EASY** and **HARD**
- How to **not** break stuff
- Things to take home from this

# Who's the dude?

- Evgenij Smirnov
- Lives in Berlin, Germany | [@it-pro-berlin.de](https://@it-pro-berlin.de)
- Works at Semperis → AD security is my hobby 😊
- MVP since 2020 (PowerShell + Security)
- Published an AD book in 2024 | [@ad2049.com](https://@ad2049.com)
- Gives AD security trainings | [@adgator.org](https://@adgator.org)



# Save The Date

> MISSION: PROTECT YOUR AD  
> WHERE: HANNOVER, GERMANY  
> START: 2026-02-16  
> END: 2026-02-20  
> WILL YOUR COMPANY SURVIVE?  
> THE CLOCK IS TICKING...  
> \_  
> BOOKING: [ADGATOR.ORG/BOOTCAMP](https://adgator.org/bootcamp)



A ? 4 U



As a defender, we have to be perfect every time.  
Attackers only need to find one chink in our armor.

*- Cory Doctorow*



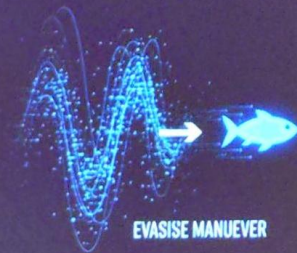


**Your job is not to stop  
the enemy but to  
slow it down...**

Your security controls force the enemy to  
behave abnormally, making it an anomaly, that  
your SOC can detect and stop...



COHESIVE STREAM



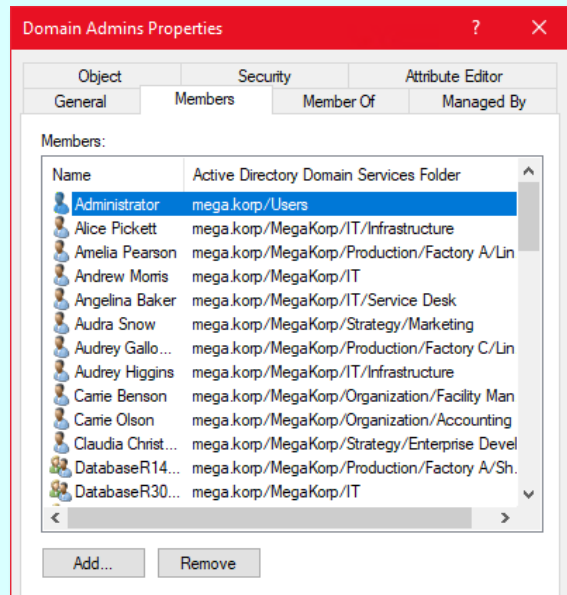
EVASIVE MANUEVER

PATH COMPARISON: GROUP VS. INDIVIDUAL



# Warming up: Easy or hard?

- What if I told you...
- ... that Audra Snow is the Big Boss's wife?
- ...that Carrie Olson is the person who literally pays your salary?
- ...that Audrey Higgins and Alice Pickett \*are\* dedicated AD admin accounts?



# The inconvenient truth about hardening

Whether a particular hardening measure  
is considered easy or hard,

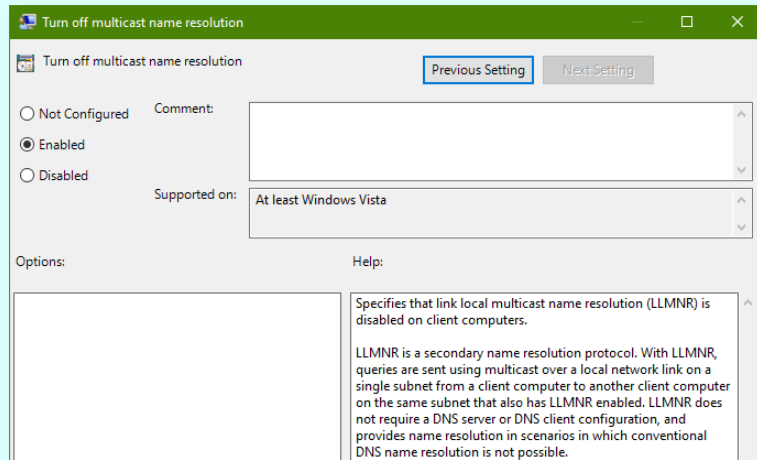
is not a question of complexity or security impact,

but rather of the expected impact on production!

# Extreme Examples

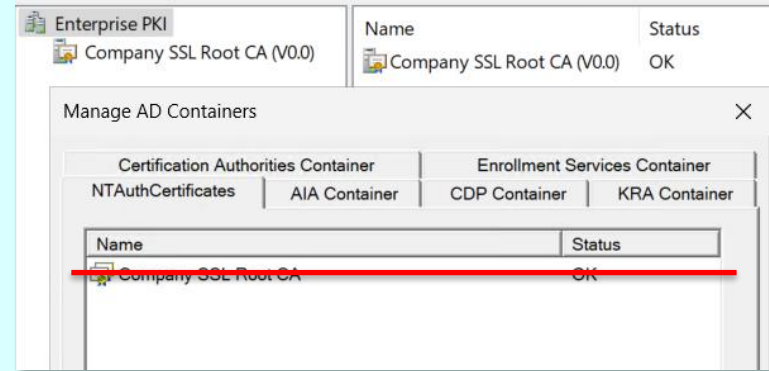
# Extreme examples – EASY 😊

- No one **uses** LLMNR
- Attackers **love** it!
  - Just google „responder“
- On by default on all Windows versions
- Easy to turn off
- Zero impact on production in IT
  - OT? Maybe. Kick them hard if it does.



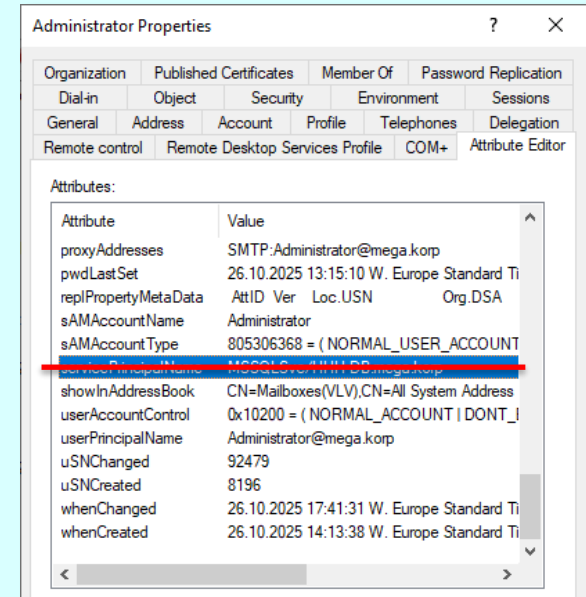
# Extreme examples – EASY 😊

- If a CA is not supposed to issue smart card certificates...
  - ...then it shouldn't be in NTAUTH
- Zero impact on production
- Huge security benefit
- Easy to implement
- Easy to revert if needed



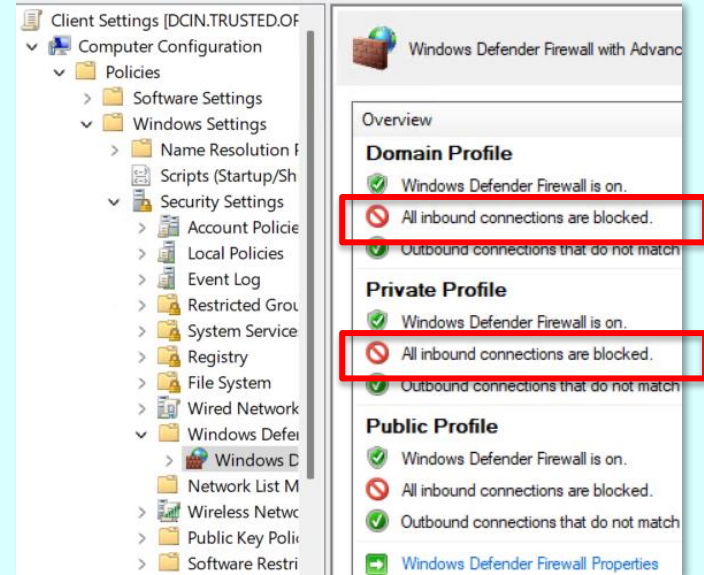
# Extreme examples – EASY 😊

- Kerberoastable RID-500? Really?
  - YES!!!!
- More often than not, the SQL server in question doesn't exist anymore...
  - ...which sometimes makes it worse 😞



# Extreme examples – EASY 😊

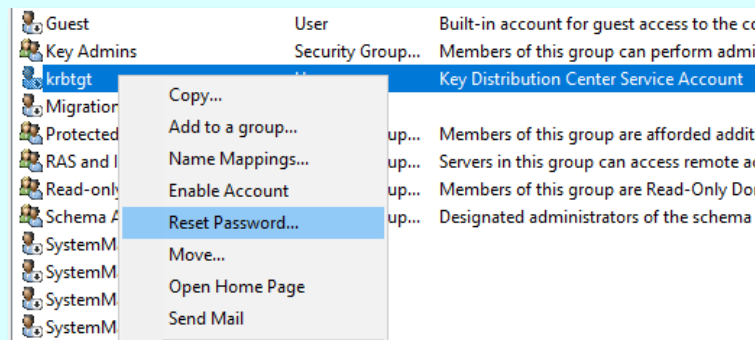
- Thwarts lateral movement between clients like no other measure
- Zero impact in 99% cases
- Highlights the „true value“ of DNS records for clients 😊
- Prepare for never-ending discussions!





# Extreme examples – EASY 😊

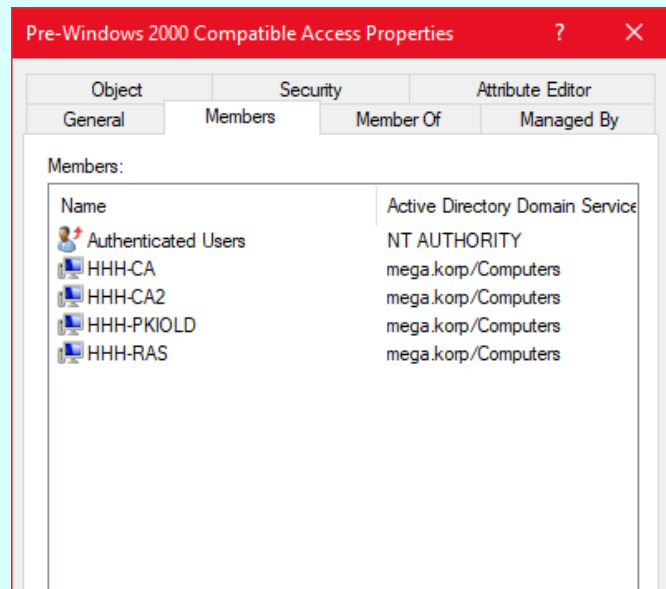
- Restricts usability of Golden Ticket
- Can be automated very easily
- Doesn't break anything if done right
- Don't forget about RODCs!!!
- Don't include Azure Kerberos!!!



- A better way: <https://github.com/zjorz/Public-AD-Scripts>

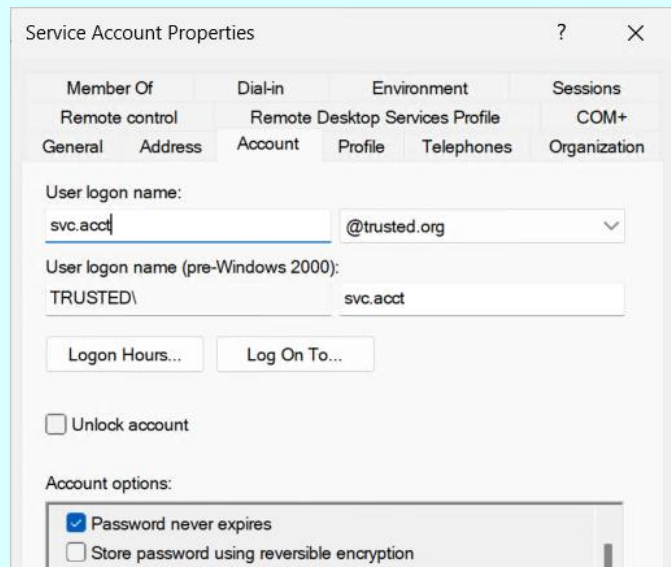
# Extreme examples – HARD ☹️

- Very easy to implement...
  - ...but might – *will?* – break things!
- Very hard to predict impact on prod
- Perceived security improvement = low
  - „it's just for reconnaissance“
- Should **definitely** be possible for privileged objects



# Extreme examples – HARD ☹️

- Knowing where the account is **actually** being used is the hardest part
- Does the service **really** not support a gMSA?
- Can it still be rotated automatically?



The screenshot shows the 'Service Account Properties' dialog box. The 'General' tab is selected. The 'User logon name' field contains 'svc.acct' and the domain dropdown is set to '@trusted.org'. The 'User logon name (pre-Windows 2000):' field shows 'TRUSTED\' and 'svc.acct'. There are buttons for 'Logon Hours...' and 'Log On To...'. An 'Unlock account' checkbox is present and unchecked. Under 'Account options', the 'Password never expires' checkbox is checked, and 'Store password using reversible encryption' is unchecked.

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop	Services Profile	COM+
General	Address	Account	Profile
		Telephones	Organization

User logon name:  
svc.acct @trusted.org

User logon name (pre-Windows 2000):  
TRUSTED\ svc.acct

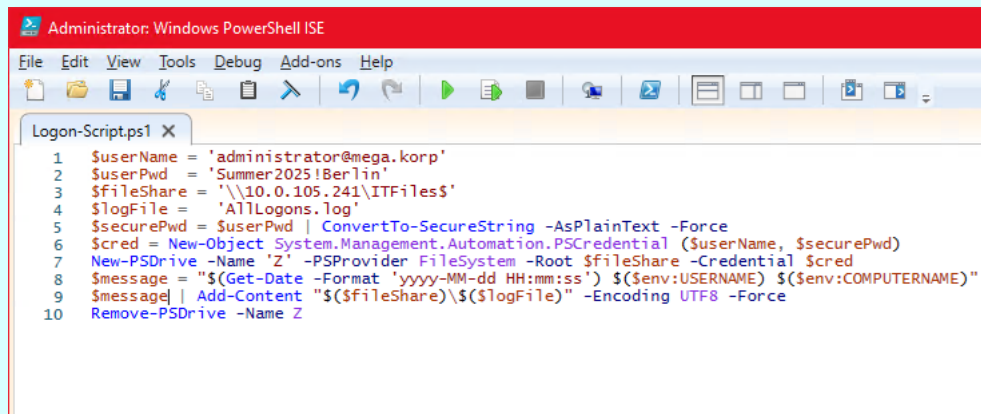
Logon Hours... Log On To...

☐ Unlock account

Account options:  
☒ Password never expires  
☐ Store password using reversible encryption

# Extreme examples – HARD ☹️

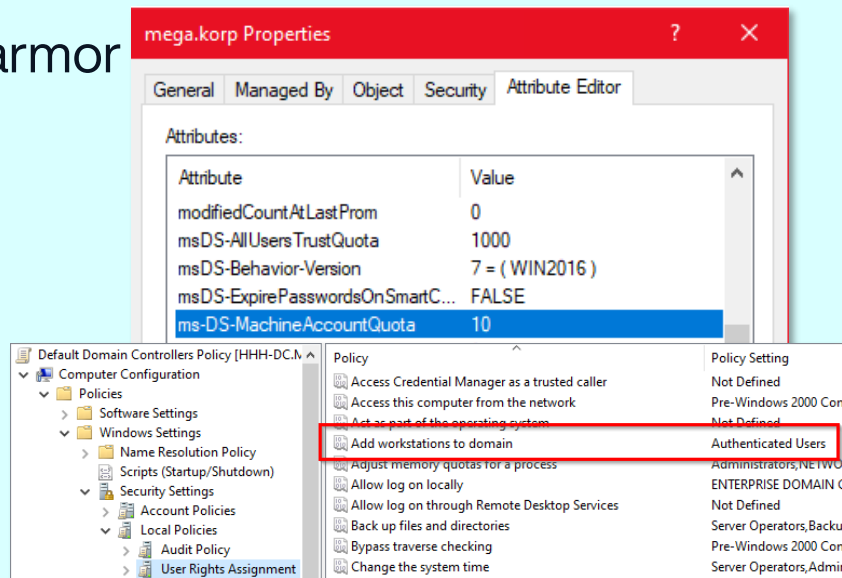
- The hardest part is finding them all
  - → 80/20 applies here!
- The second hardest part is giving fellow admins something they can use
- But sooo worth it...
- ...really!



```
1 $userName = 'administrator@mega.korp'
2 $userPwd = 'Summer2025!Berlin'
3 $fileShare = '\\10.0.105.241\ITFiles$'
4 $logFile = 'AllLogons.log'
5 $securePwd = $userPwd | ConvertTo-SecureString -AsPlainText -Force
6 $cred = New-Object System.Management.Automation.PSCredential ($userName, $securePwd)
7 New-PSDrive -Name 'Z' -PSProvider FileSystem -Root $fileShare -Credential $cred
8 $message = "$(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') $($env:USERNAME) $($env:COMPUTERNAME)"
9 $message | Add-Content "$($fileShare)\$($logFile)" -Encoding UTF8 -Force
10 Remove-PSDrive -Name Z
```

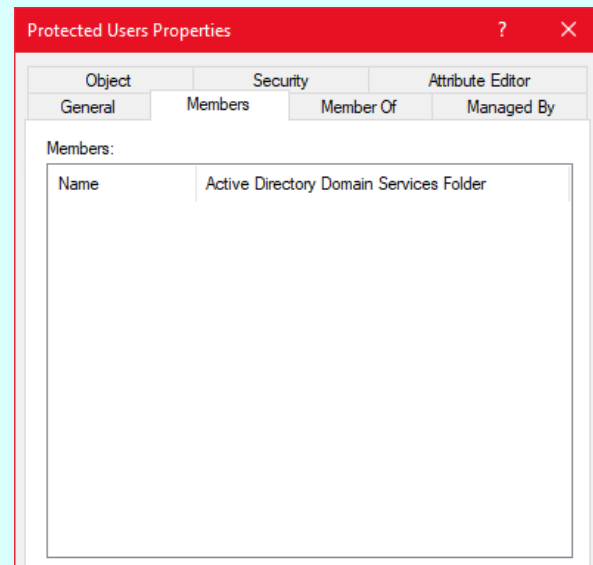
# Extreme examples – HARD ☹️

- Domain Join is a huge chink in the armor
- Hardening it requires revisiting all workstation and server lifecycle
- But → can be done in layers 😊
- Until then the chink remains...

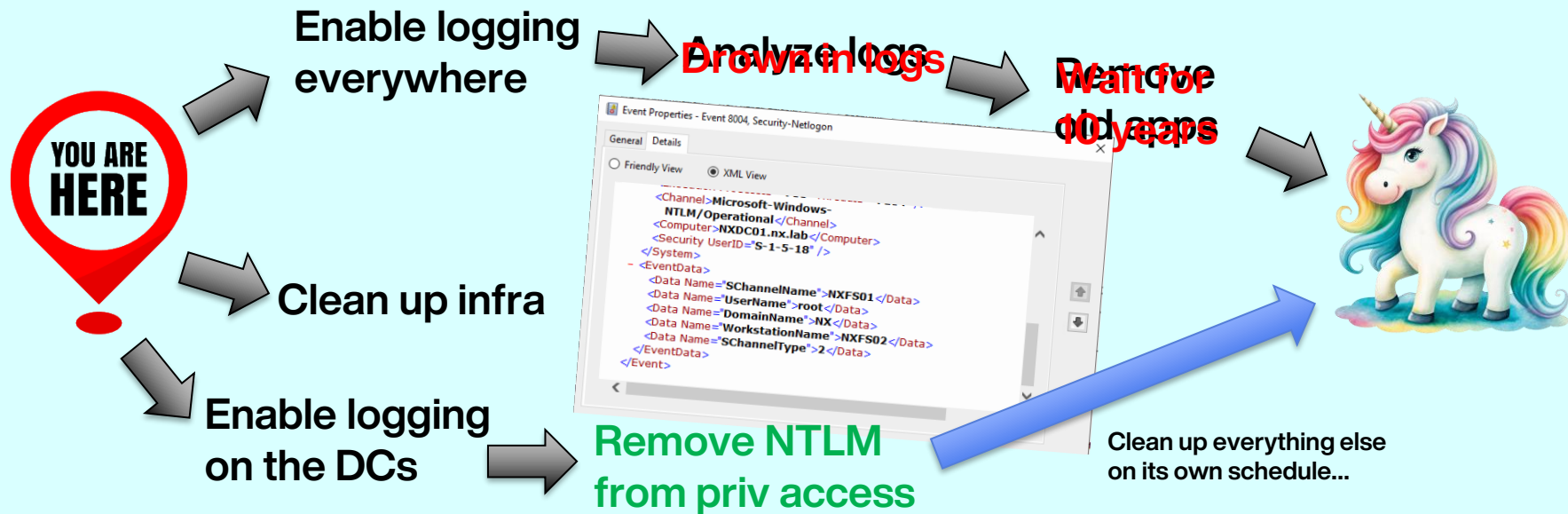


# Extreme examples – HARD ☹️

- Easy to implement → breaks stuff
- Easy to roll back → that's what happens
- Hard to predict impact
  - PowerPUG by Jake Hildreth helps...
  - ...to an extent.
- Ties in with NTLM disablement



# How (**not**) to do it – NTLM disablement



# Things to take home

- For the love of all that is holy, stop using RID-500 **now!**
- Button down things that have no impact on production → tomorrow 😊
- When starting something, make sure that at least priv access is handled
- Do not chase the grand vision at the cost of plugging holes in the hull
- Make PKI your priority – or get rid of it altogether, if you can
- Attackers love name spoofing, make it your other priority
- Domain Join is a prime factor und must get your love and attention!
- Any assessment tool will help → look at the findings, not at the score!
- Exceptions are to-do lists, not „accepted risk“ lists!



# References & Resources

- PowerPUG: <https://github.com/jakehildreth/PowerPUG>
- Locksmith: <https://github.com/jakehildreth/Locksmith>
- Tame My Certs: <https://docs.tamemycerts.com/>
- PingCastle: <https://netwrix.com/en/products/pingcastle/>
- Purple Knight: <https://www.semperis.com/purple-knight>
- GPOZaurr: <https://github.com/EvotecIT/GPOZaurr>
- AD Bootcamp: <https://adgator.org/bootcamp>

A ? 4 ME ?

@it-pro-berlin.de

@ad2049.com

@adgator.org

