Please stop letting me get in

Finn (f3rn0s)

2024-11-14

Volkis

Who am I?

Big nerd. ~~Senile~~ Senior Security Consultant @Volkis.

My interests:

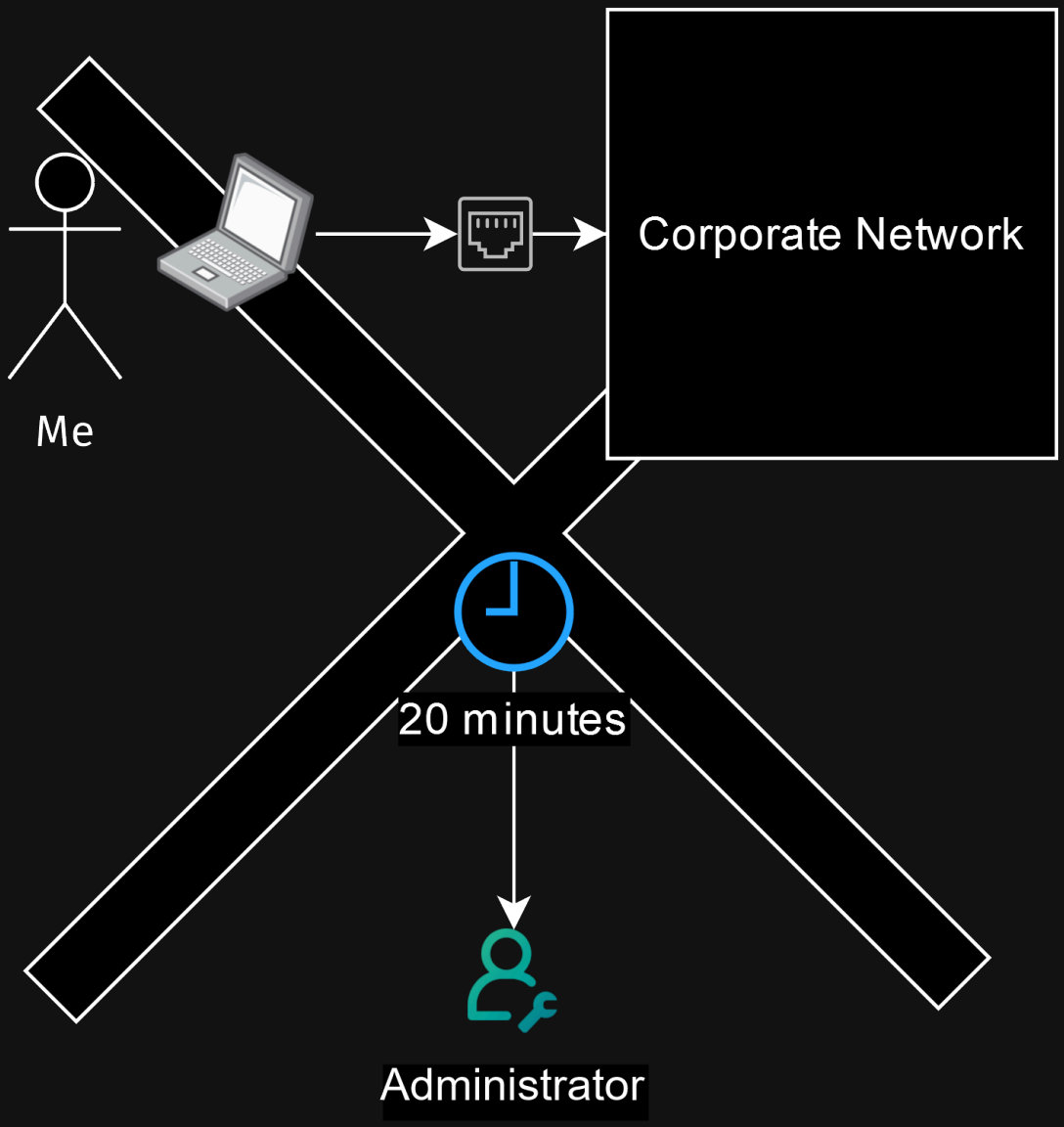
- Active Directory and internal testing.
- Kubernetes.
- Red Teaming
- Finding jank vulnerabilities.

What's this talk about (What do I mean by getting in?)

Corporate networks often have many flaws that allow for:

- An attacker with internal network access to gain credentials.
- An attacker with credentials to escalate privileges.
- An attacker with privileges to gain access to sensitive information.

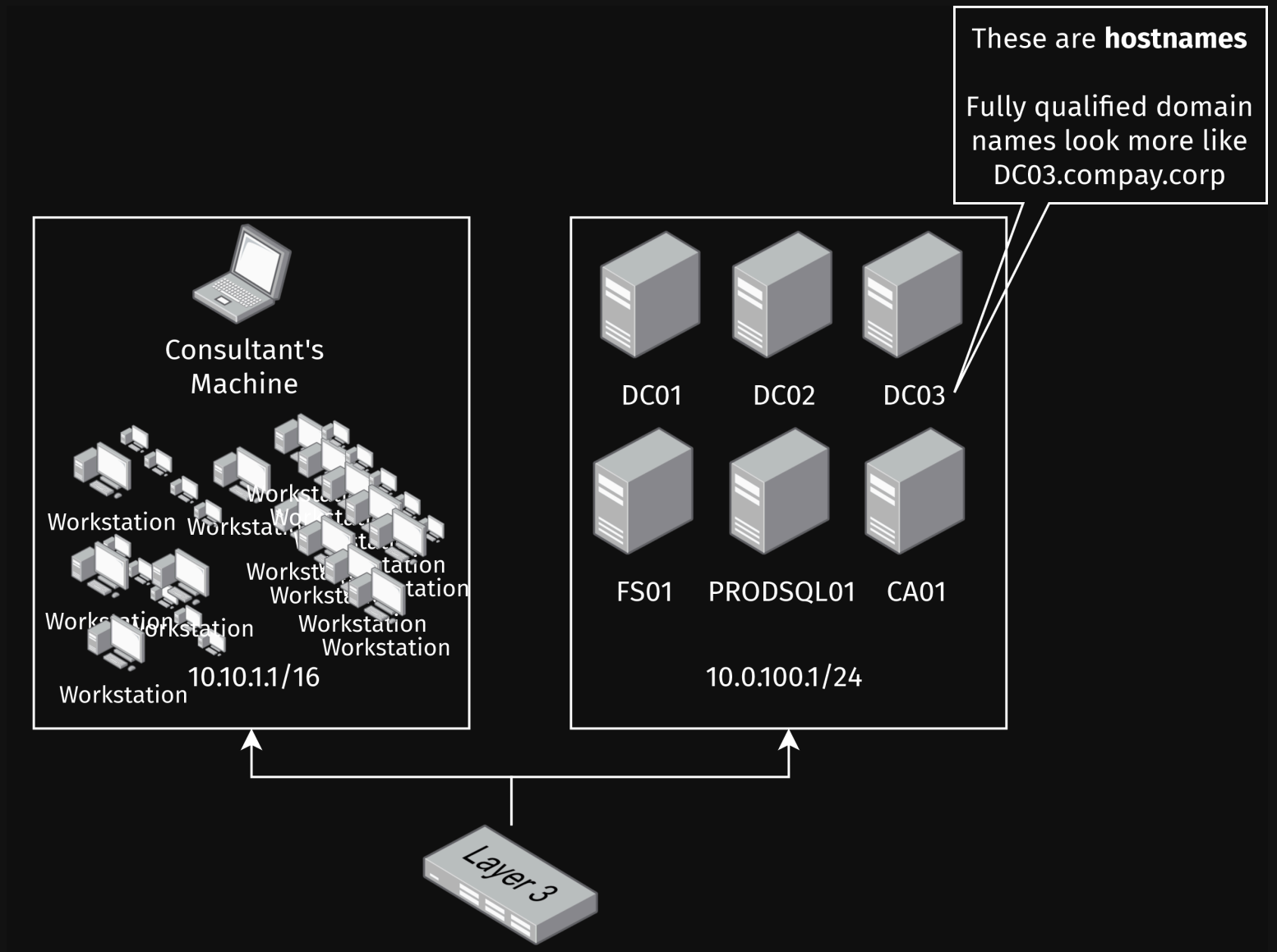
This talk is about the most **common** attacks I've seen over the last ~30 internal penetration tests. By nature, this talk will make a lot of assumptions... not all will apply to every business. i.e. If you don't use Active Directory, you escape a *lot* of these vulnerabilities.



Please stop him

What do most™ corporate networks look like?

- Windows Centric
- Actively use Active Directory
  - Users
  - Groups
  - Access Control Lists
  - File Shares
  - Databases



Average Corporate Network

Why is this a problem?

- Microsoft does *not* provide secure **defaults**.
- Many windows components are very easy to make insecure with very little warnings (i.e. AD CS).
- Most companies trust AD so much, that compromise of it represents compromise of their entire network.
    - Hybrid AD (with trusted-site).
- These attacks all use public tooling, and have public blog posts on them.

Getting initial access

What are our approaches?

- Capture and relay authentication (MiTM)
  - If we capture auth, we can attempt to crack passwords (see Responder)
  - If we capture auth, we can attempt to relay auth to other services (see ntlmrelayx)

What are our approaches?

- Capture and relay authentication (MiTM)
  - If we capture auth, we can attempt to crack passwords (see Responder)
  - If we capture auth, we can attempt to relay auth to other services (see ntlmrelayx)
- Anonymously authenticate
  - Enables a password spray attack
  - Potentially allows shenanigans (Coerced Auth)

What are our approaches?

- Capture and relay authentication (MiTM)
  - If we capture auth, we can attempt to crack passwords (see Responder)
  - If we capture auth, we can attempt to relay auth to other services (see ntlmrelayx)
- Anonymously authenticate
  - Enables a password spray attack
  - Potentially allows shenanigans (Coerced Auth)
- Find a vulnerable service
  - Printer with default admin creds, configured for LDAP
  - VSphere vulns that allow admin access

What are our approaches?

- Capture and relay authentication (MiTM)
  - If we capture auth, we can attempt to crack passwords (see Responder)
  - If we capture auth, we can attempt to relay auth to other services (see ntlmrelayx)
- Anonymously authenticate
  - Enables a password spray attack
  - Potentially allows shenanigans (Coerced Auth)
- Find a vulnerable service
  - Printer with default admin creds, configured for LDAP
  - VSphere vulns that allow admin access

Do a password spray

MiTM

Ideally, you want to man-in-the-middle some request that attempts to authenticate using **NetNTLMv2**.

This could allow you to either **relay** that authentication or perform a password cracking attempt against it.

What is a relay attack

Sometimes message **signing** is not enabled.

Work In Progress

client: session signing		server: session signing						server: EPA				
		SMB1	HTTP	SMB1	SMB2	LDAP	SMB1/2 / LDAP	LDAPS	HTTPS	LDAPS	HTTPS	LDAPS / HTTPS
		"disabled"	*"not supported"*	*"enabled"*	*"not required"*	*"None"*	*"required"*	*"Never"*	*"Off"*	*"When supported"*	*"Accept"*	*"Always / Required"*
SMB1	*"disabled"*	✓	✓	✓	✓🍎	✓💥	✗	✗ *(ntlmrelayx?)*	✓	✓	?	✗
HTTP	*"not supported"*	✓	✓	✓	✓🍎	✓	✗	✓	✓	✓	?	✗
HTTP	*"supported"* (WebDAV and other Microsoft clients)	✓	✓	✓	✓🍎	✓	✗	✓	✓	✗	?	✗
SMB1	*"enabled"*	✓	✓	✓	✓🍎	✓💥	✗	✗ *(ntlmrelayx?)*	✓	✗	?	✗
SMB2	*"not required"*	✓	✓	✓	✓🍎	✓💥	✗	✓💥	✓	✗	?	✗
SMB1	*"required"*	✓	✓	✓	✗ *(ntlmrelayx?)*	✓💥	✗	✗ *(ntlmrelayx?)*	✓	✗	?	✗
SMB2	*"required"*	✓🌿🍎	✓🌿🍎	✓🌿🍎	✓🌿🍎	✓💥🌿🍎	✗	?	✓🌿🍎	✗	?	✗

@_nwodtuhs

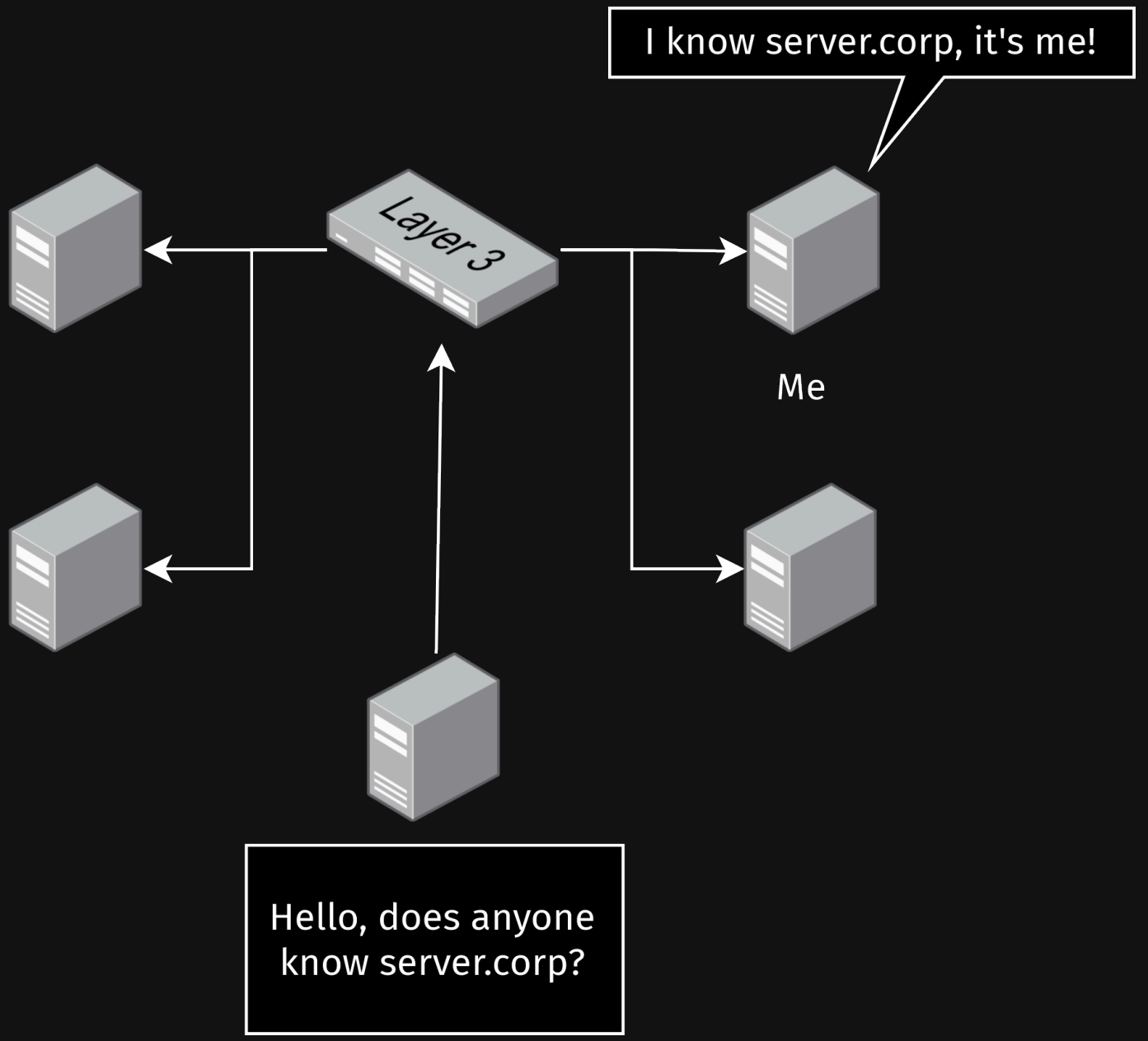
✗	*it doesn't work*
✓	*it works*
🍎	*enabling SMB2 support is needed (`-smb2support`)*
🌿	*disabling multirelay (`--no-multirelay`) is needed (having only one target (`-t`) does that automatically)*
💥	*exploiting CVE-2019-1040 (`--remove-mic`) is needed (for unpatched targets only) or NTLMv1 (doesn't support MIC)*
*	*needs testing and/or confirmation*

✗ *(ntlmrelayx?)* — *ntlmrelayx seemed faulty, needs to be tried again with network analysis*

Credit: The Hacker Recipes - Relay

Name resolution poisoning

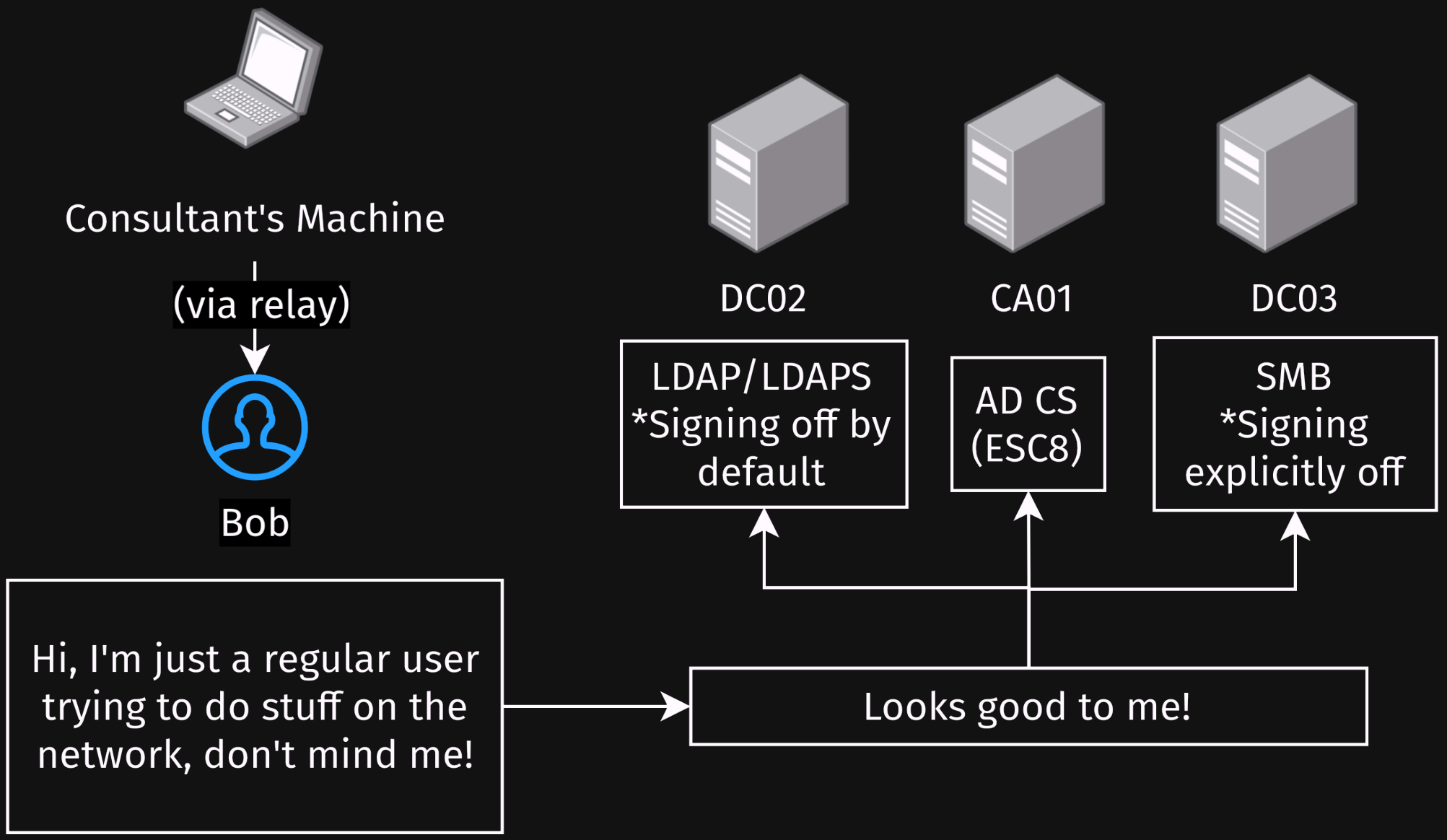
Sometimes windows computers ask computers around them for information about a server.


I know server.corp, it's me!
Layer 3
Me
Hello, does anyone know server.corp?

DHCPv6 poisoning -> Name resolution poisoning

- Windows defaults to the IPv6 DNS server.
- Windows devices are *often* not configured for IPv6.
- Any device on a network can push out DHCPv6 packets.

What's the problem here?


Consultant's Machine
(via relay)
Bob
DC02
CA01
DC03
LDAP/LDAPS
*Signing off by
default
AD CS
(ESC8)
SMB
*Signing
explicitly off
Hi, I'm just a regular user
trying to do stuff on the
network, don't mind me!
Looks good to me!

What do we do with a relay?

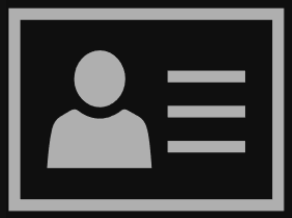
Just because we can relay auth, it doesn't mean we *are* that user.

What do we do with a relay?

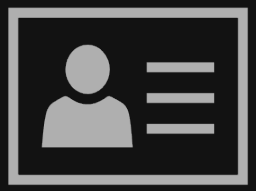
- Relay to SMB
  - Dump domain information such as users and groups.
- Relay to LDAP
  - Dump domain information with more detail.
  - If MAQ is > 0, we can create a macchine with arbitary creds.
  - We can potential create shadowcreds.
- Relay to AD CS
  - Obtain a certificate that can be used to authenticate to LDAP.
  - Potentially exchange that certificate for an NT hash that can be used everywhere.

LDAP descriptions

- In Active Directory user have fields that describe the user, i.e. `Full Name`, `Description`, `sAMAccountName`.
- Anonymous auth, if enabled, allows you to read these descriptions.
- **Any** user can read these descriptions.



Name: Super Admin
SAM: sadmin
Description: Administrator to all our servers!

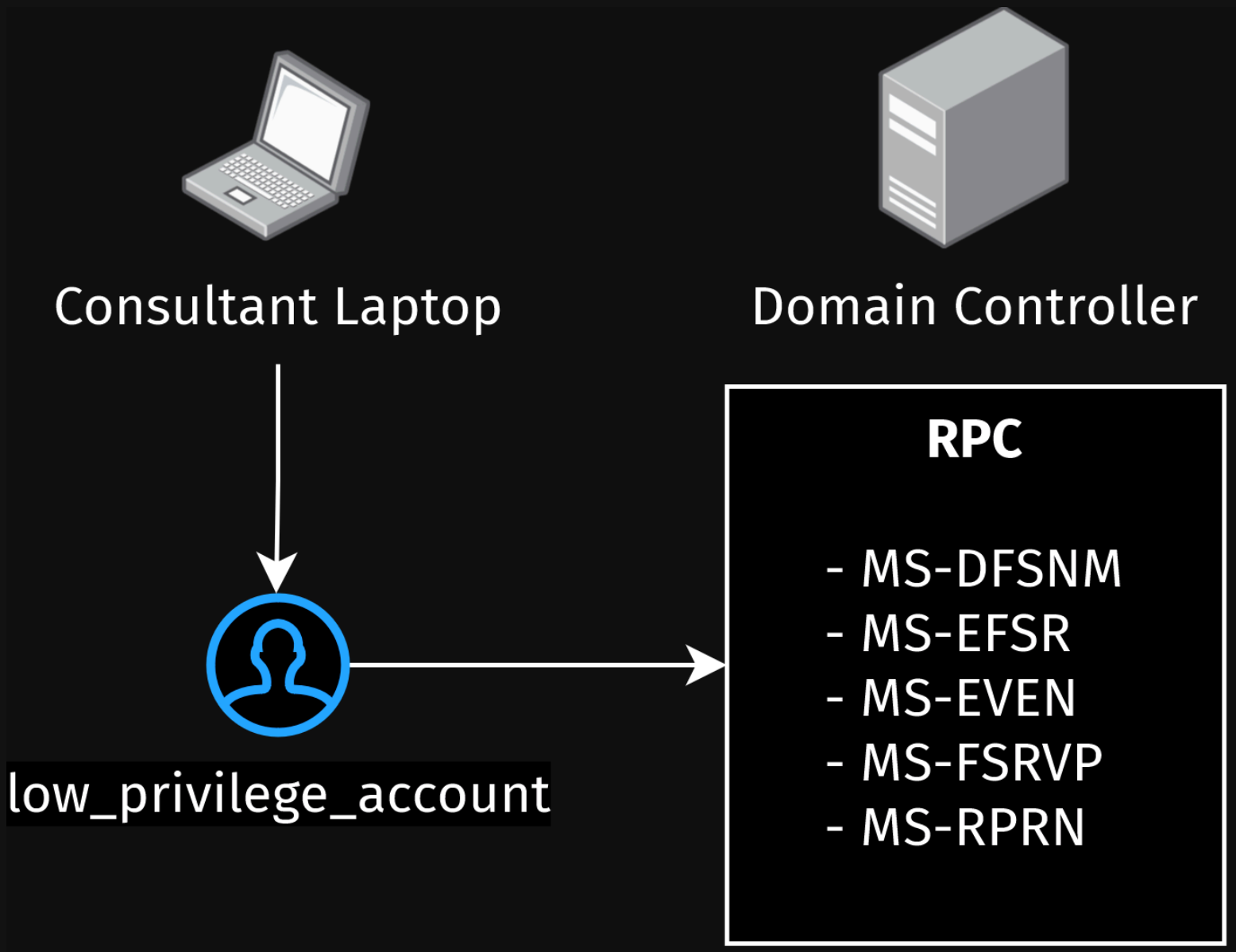


Name: Backup admin
SAM: badmin
Description: Break glass account (pw: B@ckUpAdm1n)

Coerced authentication

The general idea is that a user can *coerce* a machine into authenticating to another machine.

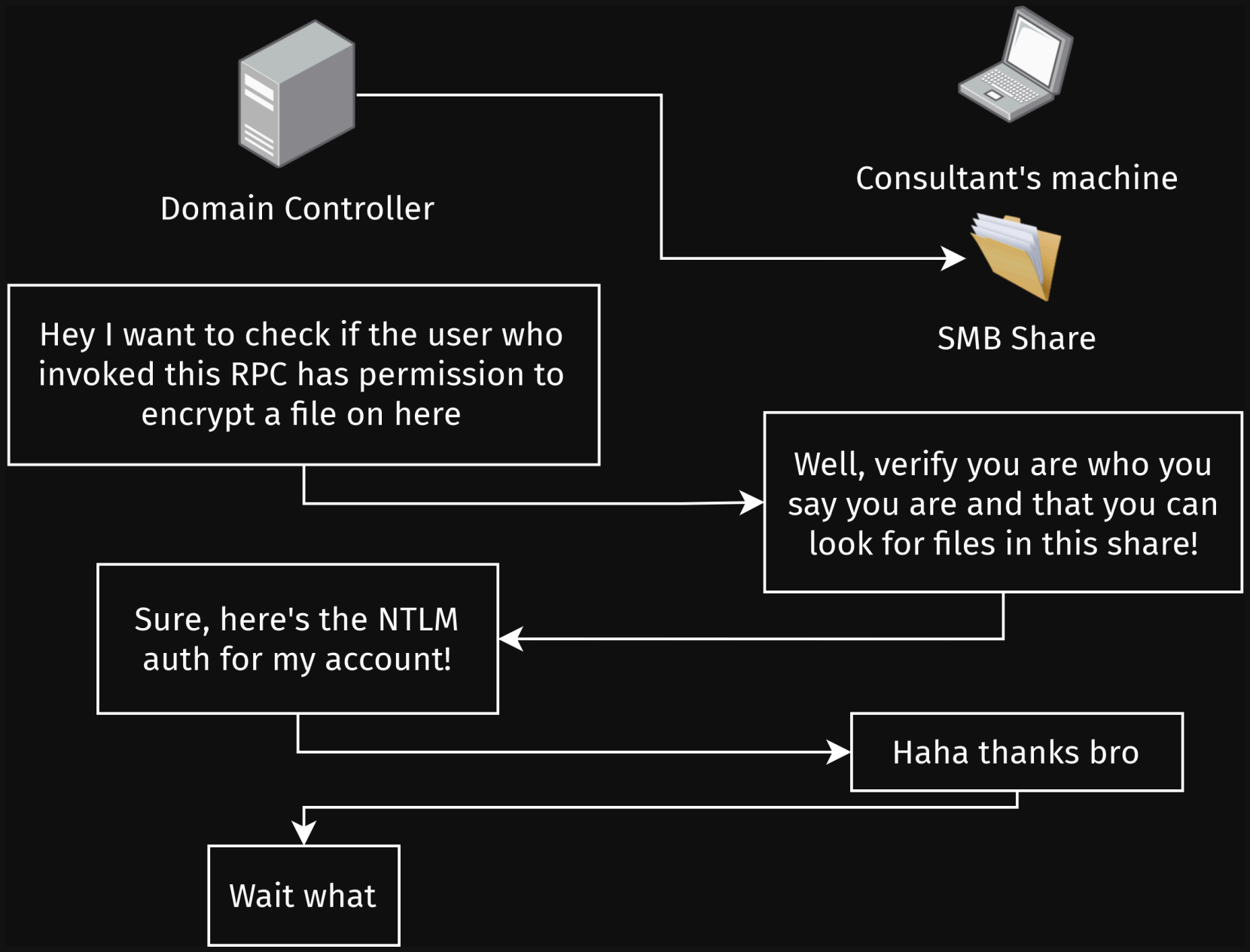
I wonder why this might be useful :p

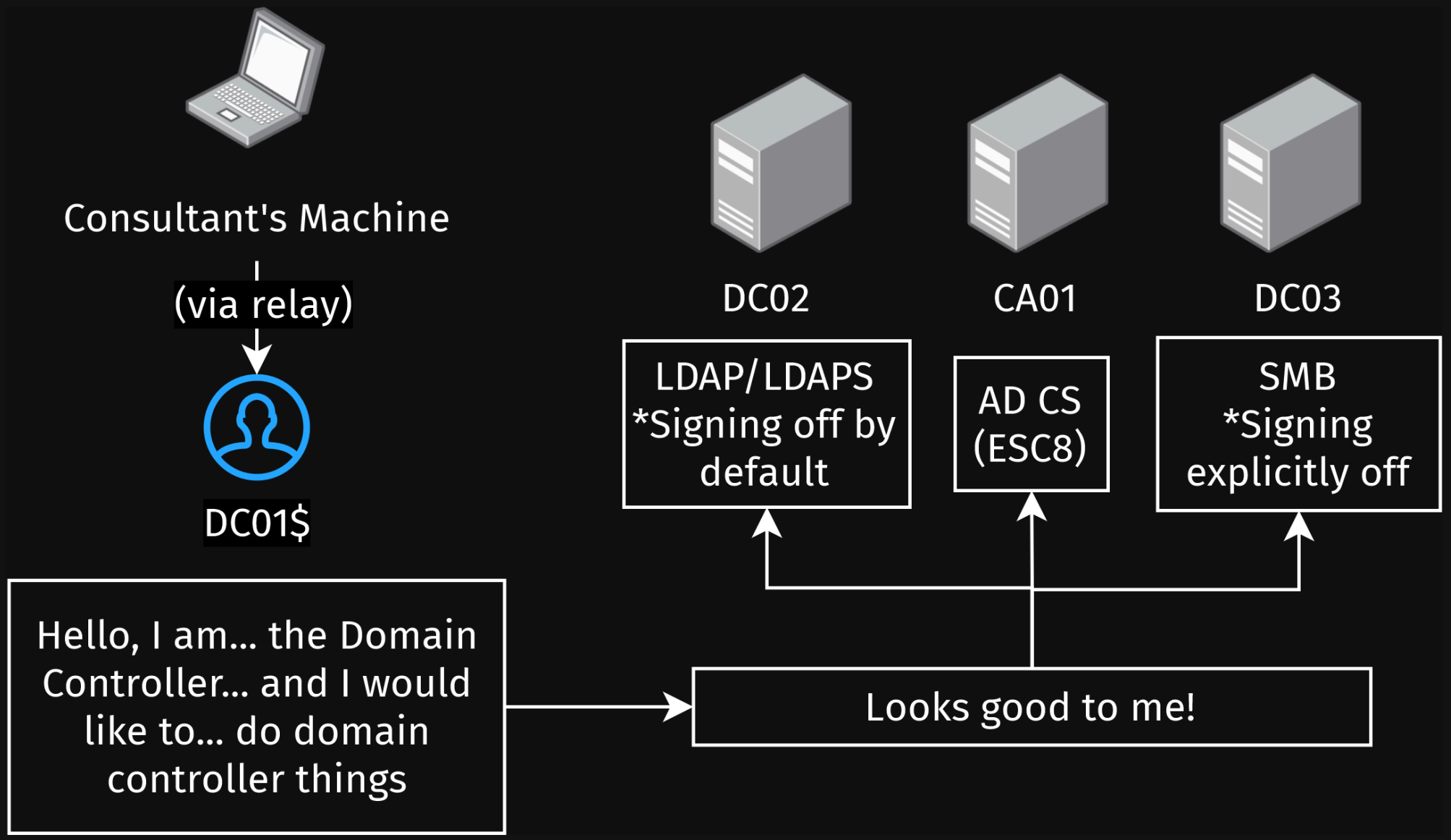

Consultant Laptop
Domain Controller
RPC
- MS-DFSNM
- MS-EFSR
- MS-EVEN
- MS-FSRVP
- MS-RPRN
low_privilege_account

RPC

- MS-DFSNM
- MS-EFSR
- MS-EVEN
- MS-FSRVP
- MS-RPRN

- Thing to do
- Where to do it


Domain Controller
Consultant's machine
SMB Share
Hey I want to check if the user who invoked this RPC has permission to encrypt a file on here
Well, verify you are who you say you are and that you can look for files in this share!
Sure, here's the NTLM auth for my account!
Haha thanks bro
Wait what



There is a small lie here, can you spot it?

Coerced Auth impact

If you give me one service that allows relay, and coerced auth is on, you're probably **screwed**.

- Coerced DC to authenticate to AD CS (ESC8) -> DCSync/LDAP + RBCD
- Coerced DC to authenticate to LDAP -> Shadowcreds -> DCSync

i.e. Very bad

File shares

- Some corporate fileshares have very bad Access Control Lists (ACLs)
- Any Admin can read *any* file on these shares**
- People put *privileged* credentials they shouldn't in all types of places (PowerShell scripts etc.).
- Even if you are already Domain Admin, you might escalate impact from files in a share.

ITADMINSHARE$

passwords.txt

Backup GA and admin creds:

badmin@corporate.microsoftonline.com
WeR3@llyB@ckinUpN0w

DC Sync

Retrieve the password hashes of every user in the domain!

Useful for us since it allows us to perform a cracking attempt and give clients realistiic stats like:

- 90 of 100 employees has passwords that were cracked (90%).
- 15 Services re-use weak passwords such as (C0mp@ny2012).

People still pick passwords that are vulnerable to cracking:

- `Word2222!`
- `C0mpl3x2222!`
- `littlerayofsunshine`

We often see crack rates on engagements of `> 60%`, sometimes as high as `98%`.

If people are legitimately using passwords like `Password01!`, or `Company2024!`, then password spraying **works**.

If we've got weak passwords what's the impact?

My personal enemy... trusted sites.

People **DO NOT** want to do **MFA** in the office.

The solution: trust the devices that connections originate from the office to bypass MFA.

Takeaways

- Look at relay attacks and how to mitigate them. (LDAP/SMB Signing are amazing).
  - Please look at AD CS, it's a privilege escalation nightmare.

Takeaways

- Look at relay attacks and how to mitigate them. (LDAP/SMB Signing are amazing).
  - Please look at AD CS, it's a privilege escalation nightmare.
- Look at your user's passwords (Maybe try to crack your own NTDS and see how bad they are).

Takeaways

- Look at relay attacks and how to mitigate them. (LDAP/SMB Signing are amazing).
  - Please look at AD CS, it's a privilege escalation nightmare.
- Look at your user's passwords (Maybe try to crack your own NTDS and see how bad they are).
- ~~Get a penetration test from someone cool.~~
- Think about how compromise can actually impact you
  - If I crack an employees passwords, does MFA stop me accessing the cloud?

But wait, I have an EDR!

EDRs aren’t magic

- Brittle dections
  - Hashes/identifiers/string matching
- Robust detections
  - Behavioural

EDRs aren’t magic

- Brittle dections
  - Hashes/identifiers/string matching
- Robust detections — Is this perfect?
  - Behavioural

EDR

OMG That has the word 'NTDS' in it, it must be bad!

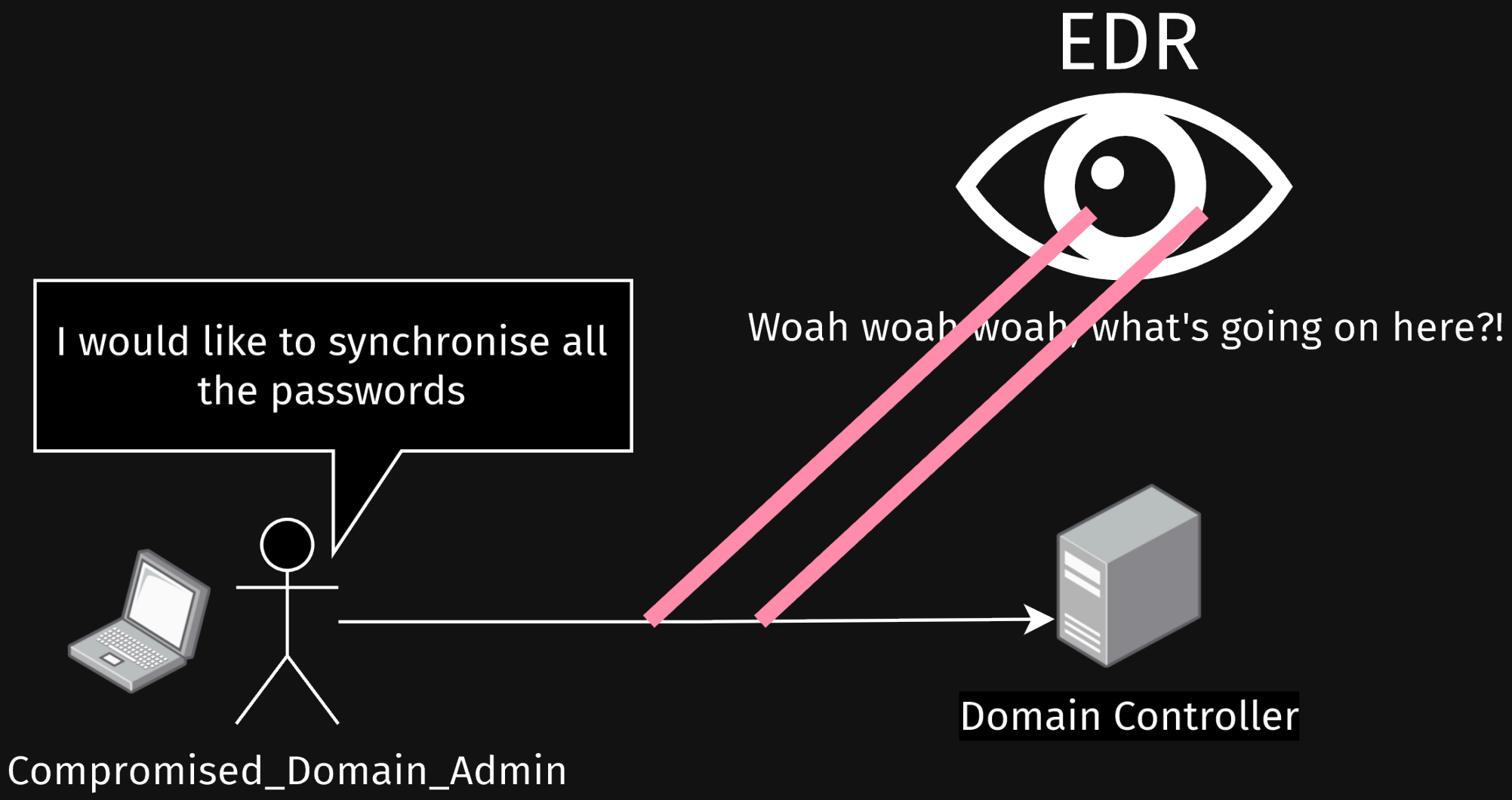
```
$ copy C:\temp\shadow\Windows\NTDS\ntds.dit  .\ntds.dit

$ copy C:\temp\shadow\Windows\NT*\*.dit  .\cool_normal_file.dit
```

Brittle Detections

Can often be bypassed by obfuscation:

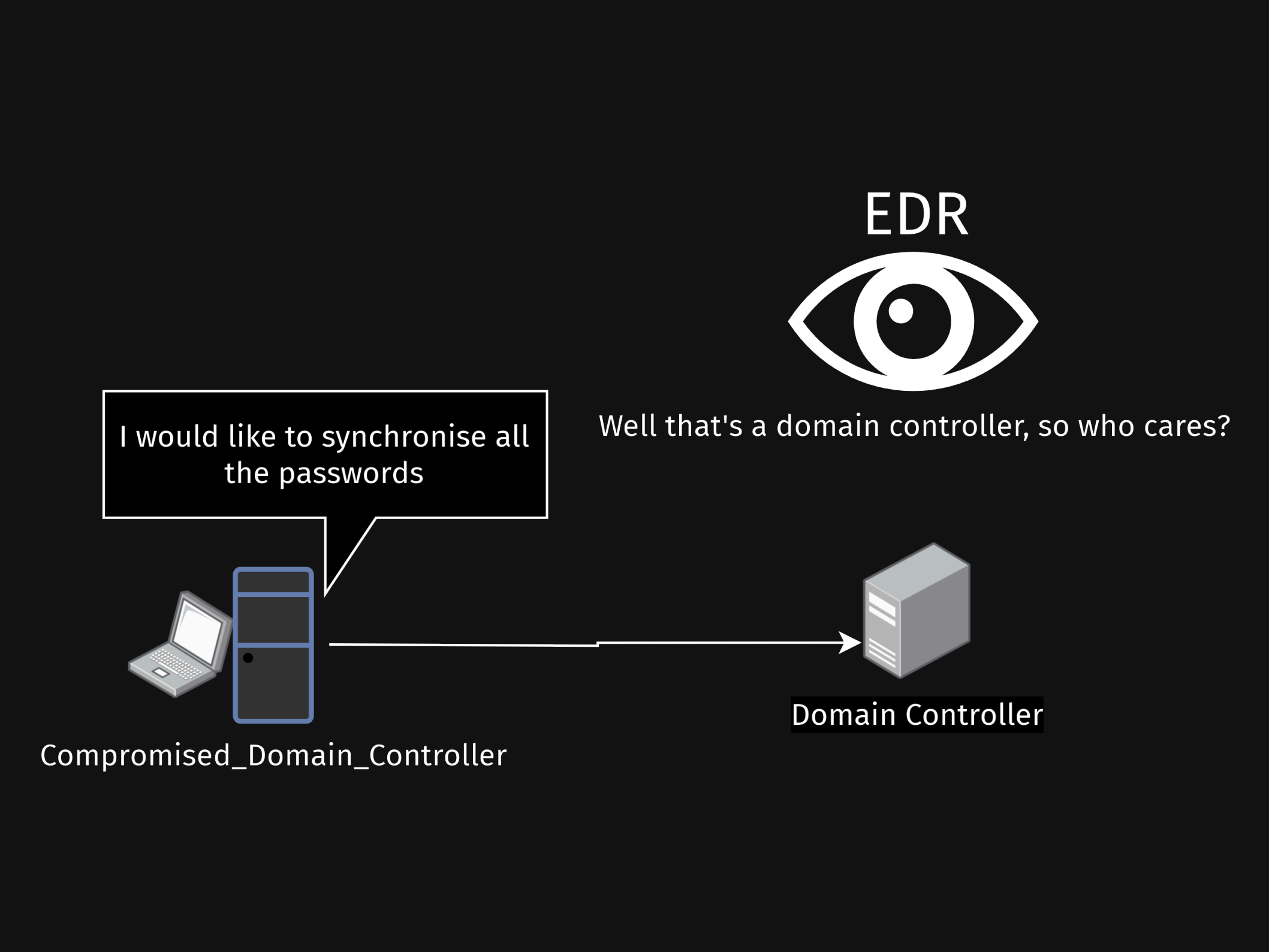
- Changing strings
- Recompiling files with garbage
- All the normal AV bypass stuff you see.

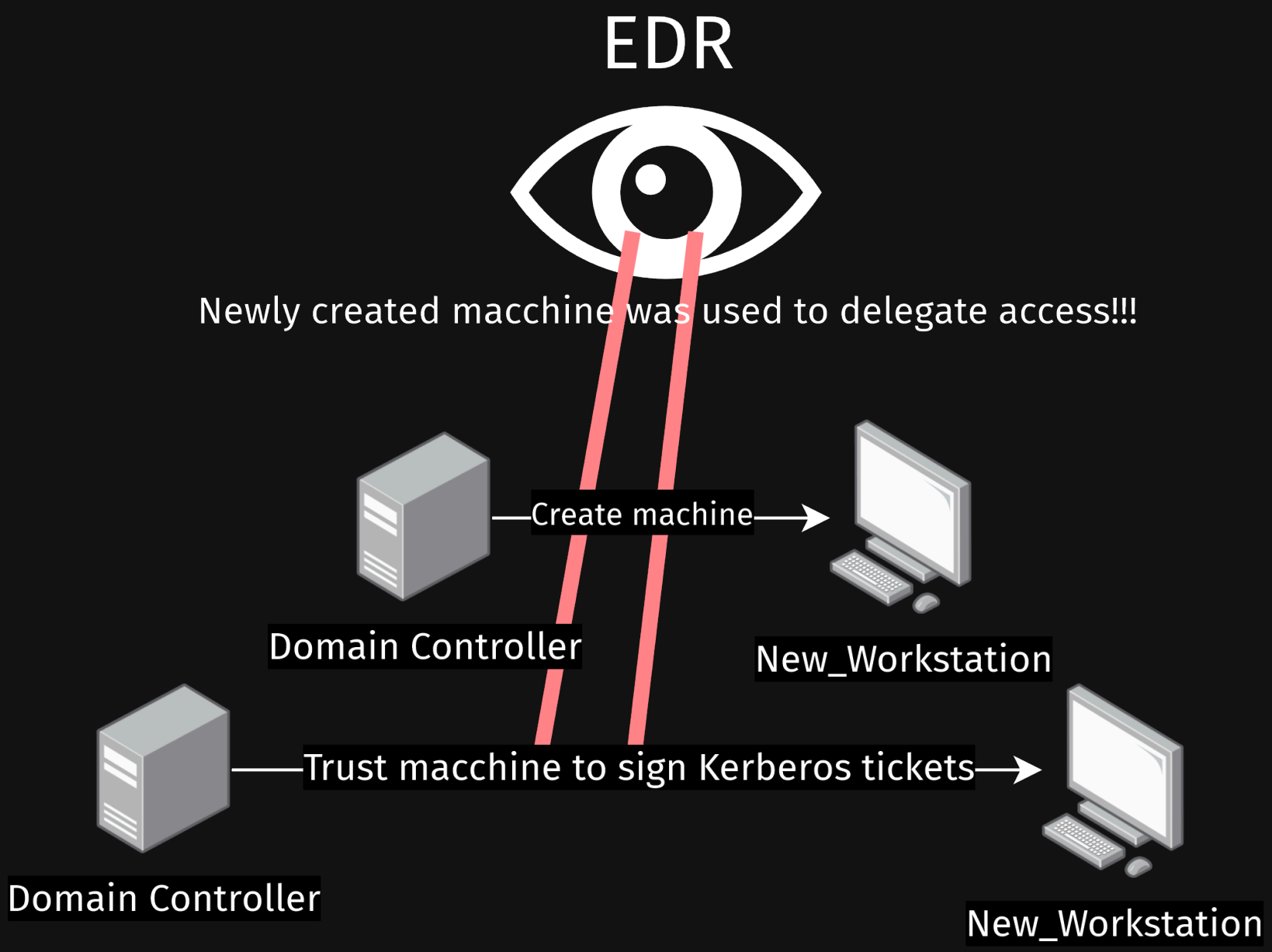

EDR
I would like to synchronise all the passwords
Woah woah woah, what's going on here?!
Compromised_Domain_Admin
Domain Controller

Robust detections

These are **harder** to bypass, but it's not impossible.

- Make traffic seem like it's normal (i.e. using windows tools such as PsExec).
- Look at each singular step in the detection and think about how you could break it.


EDR
I would like to synchronise all the passwords
Well that's a domain controller, so who cares?
Domain Controller
Compromised_Domain_Controller


EDR
Newly created macchine was used to delegate access!!!
Create machine
Domain Controller
New_Workstation
Trust macchine to sign Kerberos tickets
Domain Controller
New_Workstation

EDRs aren’t a silver bullet

Might **seem** obvious to security professionals, but it’s not as intuitive as it seems.

Q/A