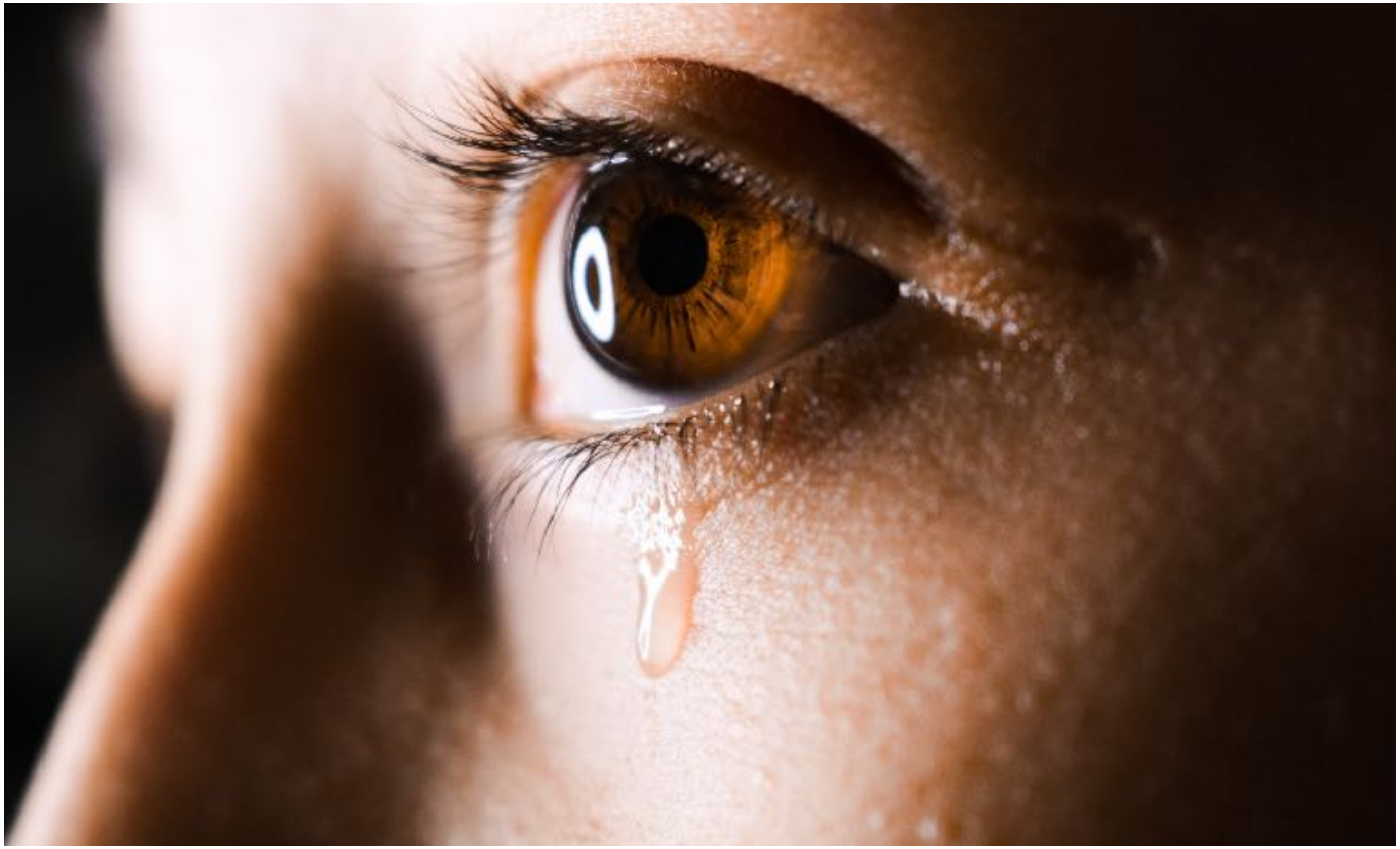


Making Pentesters Sad

Low-hanging Fruit For Enterprise Defenders

Who is this jerk?

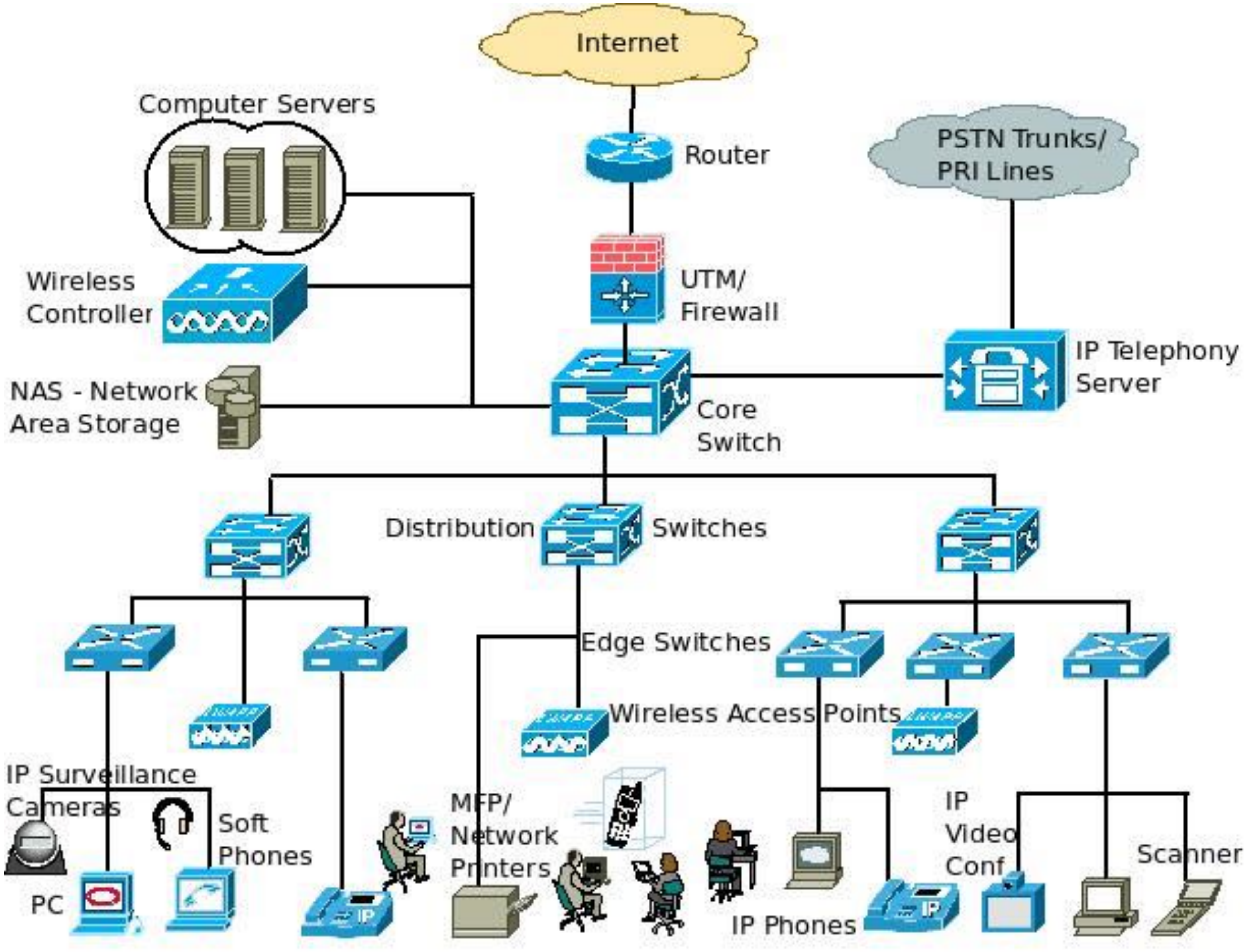
- Mike Loss
- @mikeloss on Twitter
- Pentester at Asterisk in Perth
- Talked about
  - AD Group Policy @ BSidesCBR 2018
  - AD Privesc @ WAHCKON 2017
  - Made a Furby swear @ BSidesCBR 2017
- Has a very bad cold today.

Why is he shouting at us **THIS** time?

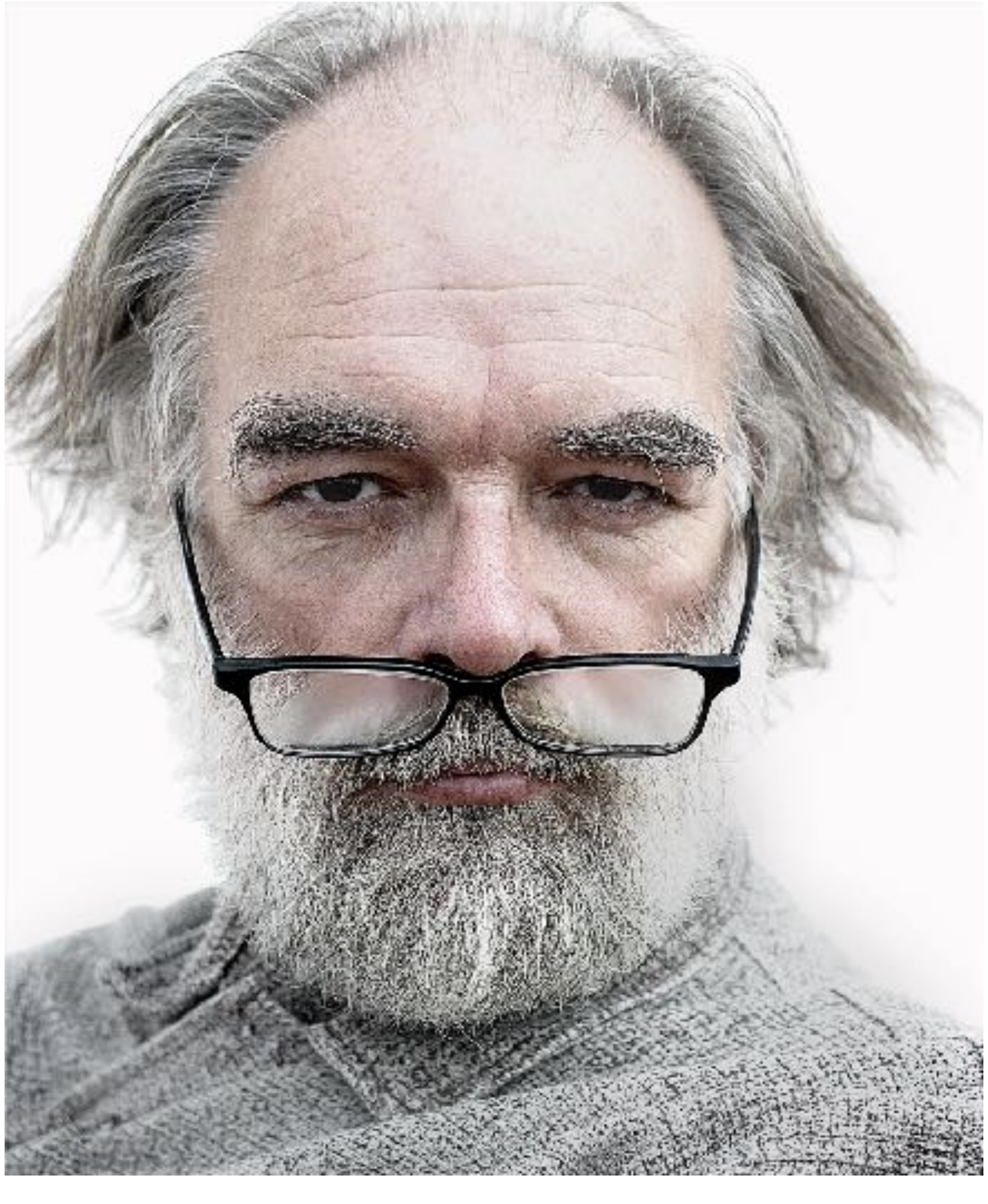
Making Pentesters Be Sad

The Good Ways

All bad networks are basically the same.



The Old Crusty

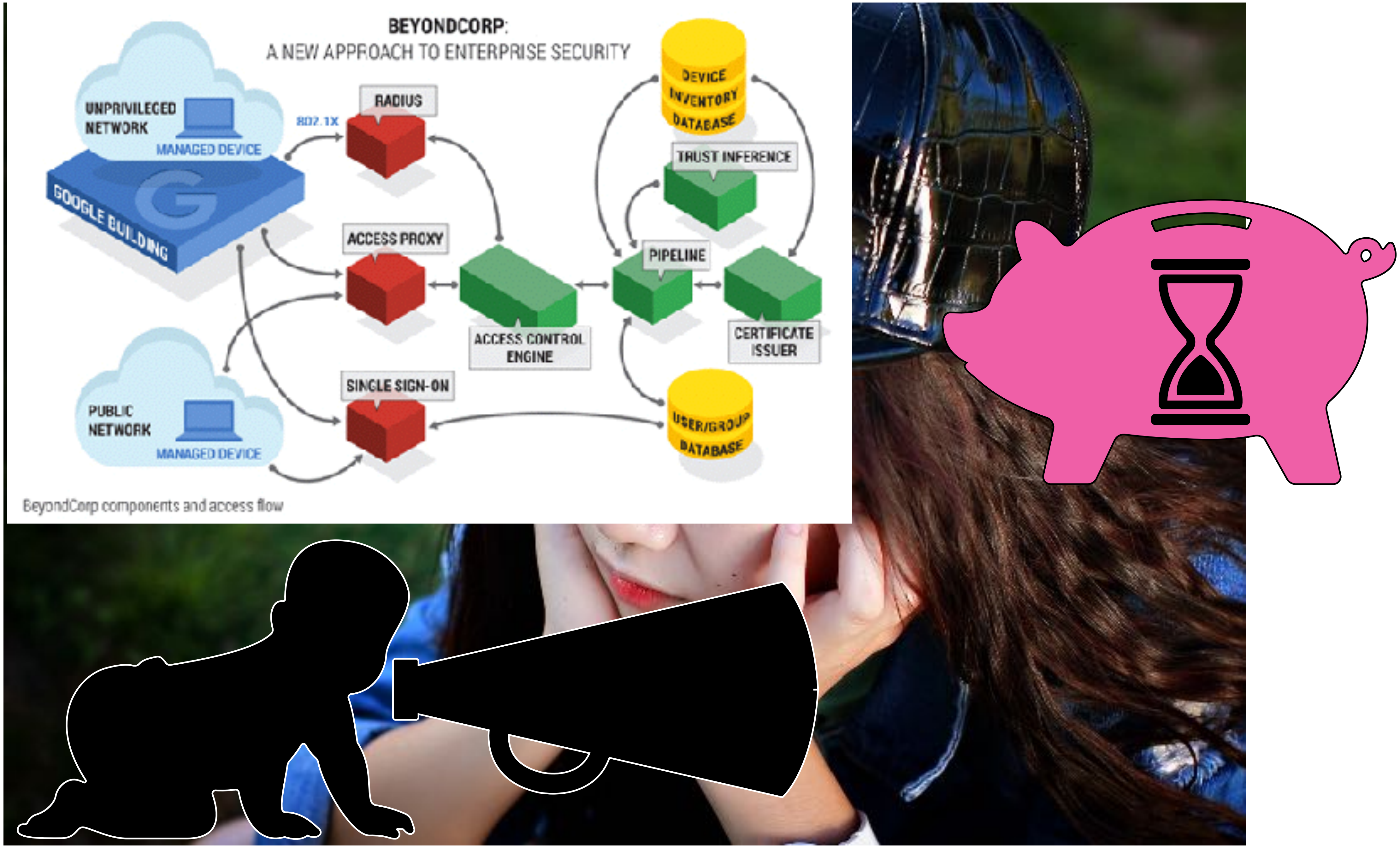


The VBScript Shaman

The "Child Prodigy"

You (maybe?)

You

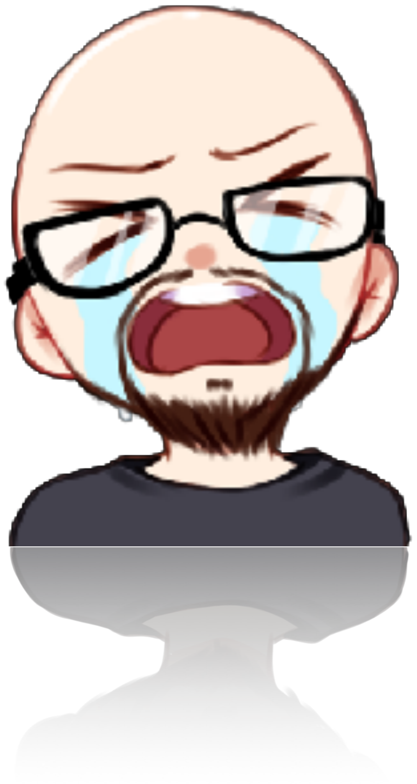


BeyondCorp components and access flow

INITIATE PURPLE CONTENT

Visual Aids

- Jess is a dope sysadmin.
- Mike's a jerk pentester.
- We want Jess to stay cool while making Mike extremely sad.



Implement LAPS

- Microsoft Local Admin Password Solution (LAPS)
- Sets, stores, and rotates passwords for local accounts securely.
- Makes Mike extremely sad.

https://adsecurity.org/?p=1790
https://www.microsoft.com/en-au/download/details.aspx?id=46899

Disable the local RID 500 "Administrator" account.

- BUILT-IN\Administrator can do stuff other "Administrators" can't.
- Disable it to make Mike sad.
- Booting in safe mode will re-enable it in a pinch.

Remove passwords from GPOs

- Heaps of ways to store passwords in Group Policy Objects, all are terrible.

- Find most of them with these two commands:

```
IEX (new-object net.webclient).downloadstring(”https://raw.githubusercontent.com/
PowerShellMafia/PowerSploit/master/Exfiltration/Get-GPPPassword.ps1”); Get-GPPPassword
```

```
IEX (new-object net.webclient).downloadstring(https://raw.githubusercontent.com/
PowerShellMafia/PowerSploit/master/Exfiltration/Get-GPPAutologon.ps1”); Get-GPPAutologon
```

Implement a custom AD password filter

- Nobody will let you change the password policy.
- Telling them to choose better passwords won't help.
- Instead, make it outright impossible to choose most terrible passwords.
- `https://github.com/jephthai/OpenPasswordFilter`
- Block list should include:
  - `password`
  - `welcome`
  - `letmein`
  - `hello`
  - **Days of week**
  - **Months**
  - **Seasons**
  - **Company Name**
  - **Anything you can think of.**

https://docs.microsoft.com/en-us/windows/desktop/secmgmt/installing-and-registering-a-password-filter-dll

Deal with default passwords

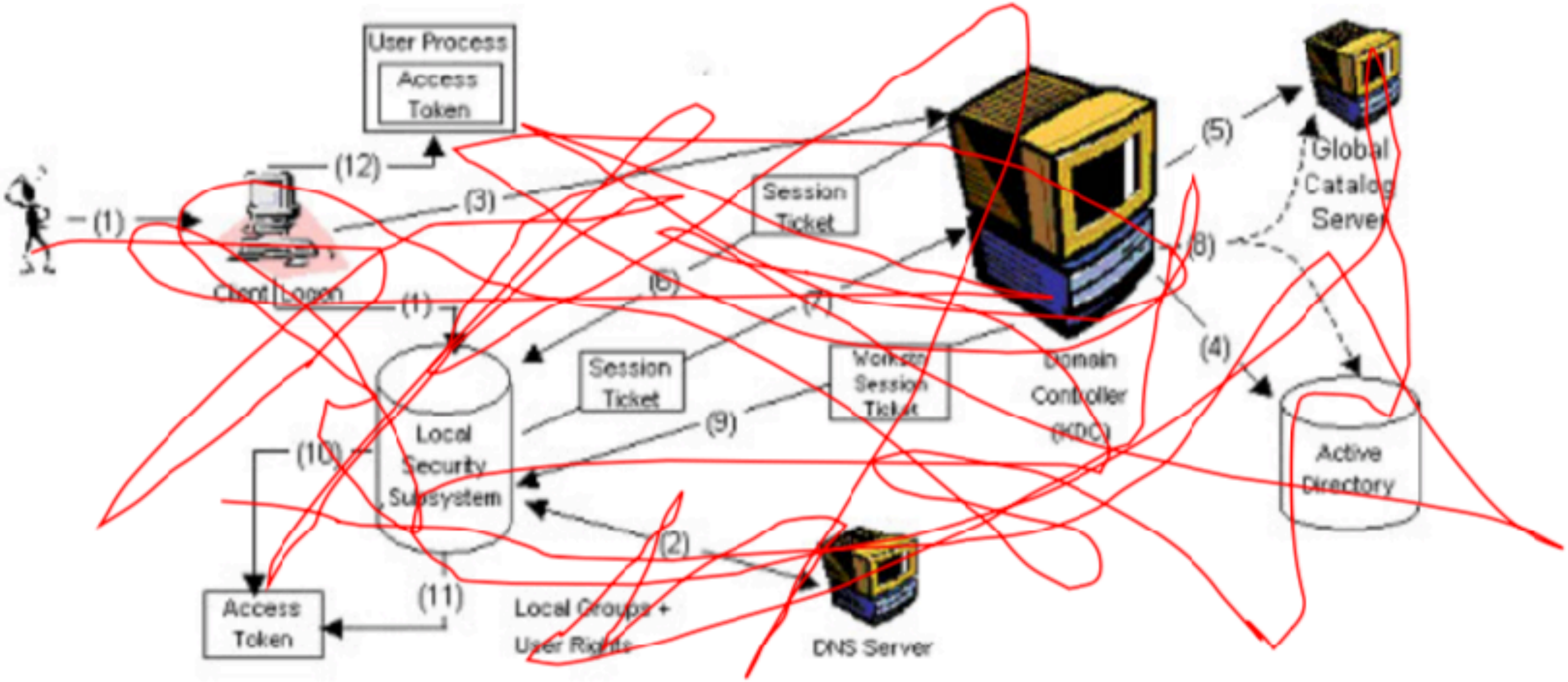
- Find them with nmap, it's what I'd do.

- An extremely good list of app fingerprints and default creds can be found at: https://github.com/nnposter/nndefaccts

```
nmap --script http-default-accounts --script-args http-default-accounts.fingerprintfile=~/http-default-accounts-fingerprints-nndefaccts.lua 192.168.1.0/24 --open -sV -vv -oA output
```

Just un-fuck the password on anything with an SPN…

- Fuck you, I'm not explaining Kerberos and you can't make me.



Kick stale RDP sessions

- Can't steal creds if nobody's logged on...
- Group Policy settings:

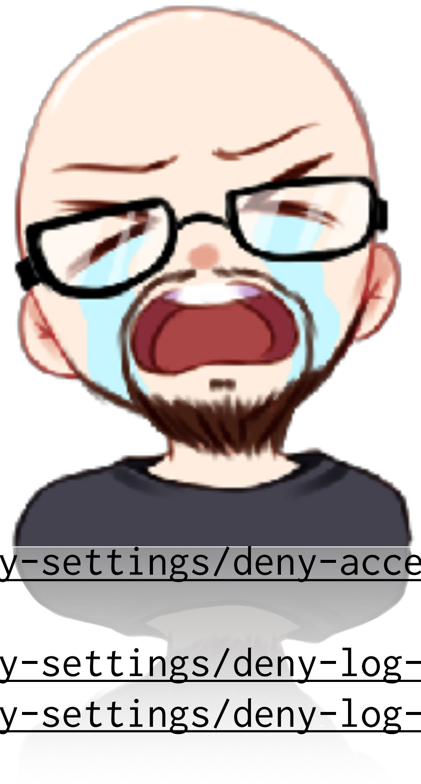
```
Windows Server 2003: Computer Configuration\Administrative Templates\Windows
Components\Terminal Services\Sessions

Windows Server 2008: Computer Configuration\Administrative Templates\Windows
Components\Terminal Services\Terminal Server\Session Time Limits

Windows Server 2008 R2: Computer Configuration\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Session Time
limits
```

Get crazy with logon type restrictions.

- Deny any logon types that aren't required.
- 'Local', 'remote interactive', and 'from the network'.
- Awesome for overriding complex nested group memberships.
- Find them in Group Policy:
  `Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment`



https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-through-remote-desktop-services

Turn your host-based firewalls back on

- I know you disabled the Windows Firewall.
- You don't think it does anything.
- Trust me, it can be a pain in my ass.

https://channel9.msdn.com/Events/Ignite/New-Zealand-2016/M377

Set SMB signing to "Required"

- There's a whole world of bullshit tricks we like to pull with NTLM authentication.
- By doing this you kill like 80% of them.

https://blogs.technet.microsoft.com/josebda/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2/

Not-so-low hanging

But so worth it.

Segmentation and segregation

- Apply principle of "least privilege" to network comms.
- Only permit traffic on a given port between machines where actually needed.
- Yes it will take ages to get done.
- Just start eating the elephant.

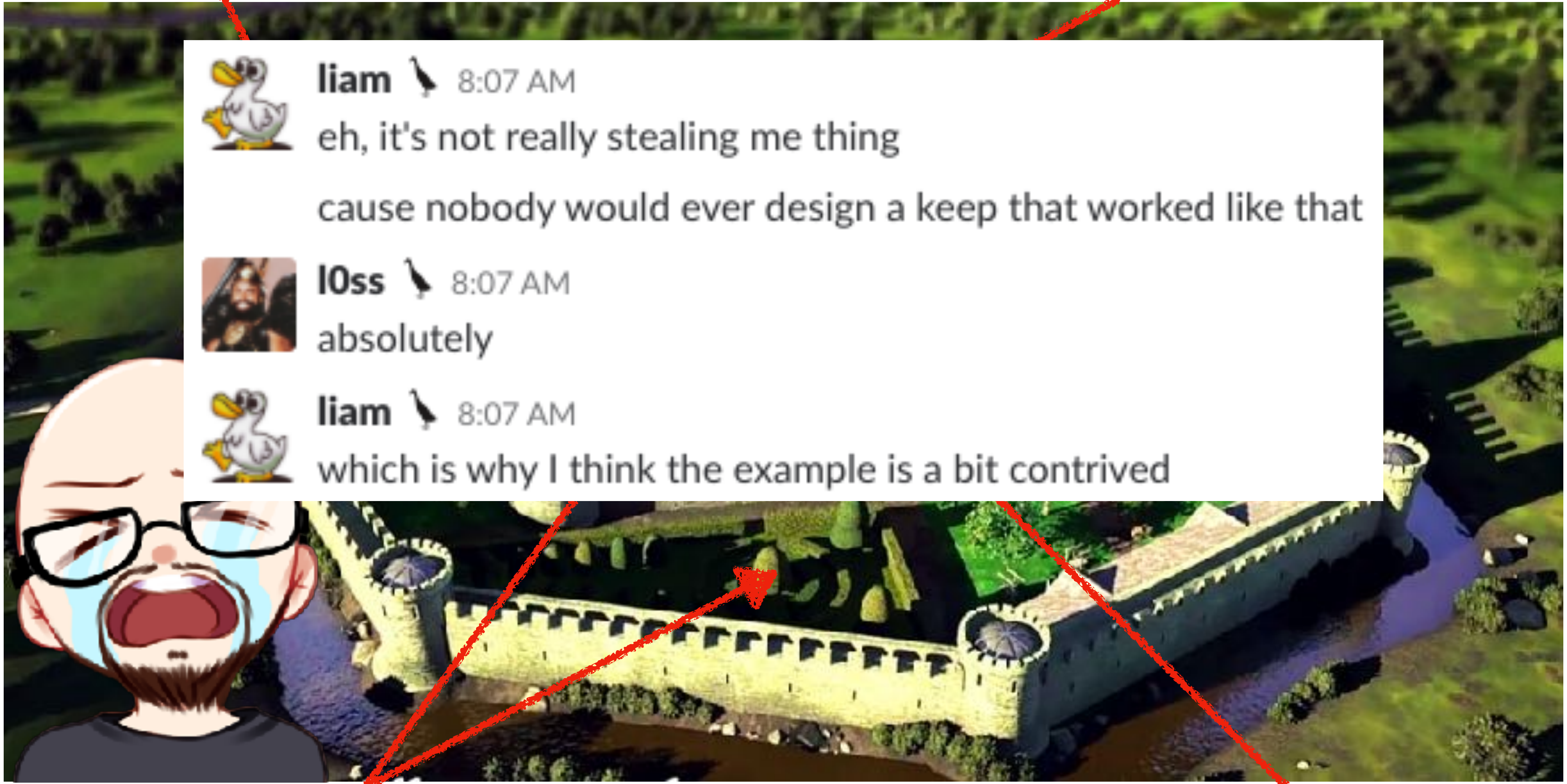
MFA on MFA-ing EVERYTHING

- Yes, it's hard, and they won't want to let you do it.
- If you can manage it in the right places, MFA is a colossal pain in my arse.

Put your MFA or password vault servers in the right place.

Your outer network perimeter

A jump host type thing with MFA



liam 8:07 AM

eh, it's not really stealing me thing

cause nobody would ever design a keep that worked like that

l0ss 8:07 AM

absolutely

liam 8:07 AM

which is why I think the example is a bit contrived

The RADIUS appliance thing that backs the MFA on the jump host, and the password vault that contains admin creds for said appliance.

Your highly sensitive SCADA network

“But I can't implement X, because half our users need Y, and X would break that.”

–You, Probably

Credit where credit is due:

- sharrow
    - BSidesCBR 2018 "That's Not How This Works"
- metlstorm
    - BsidesWLG 2017 "Metlstorm's Empiricism Emporium: Unpleasant Truths Our Speciality"
- pipes
    - BSidesWLG 2017 "Confessions of a Red Teamer"

Special Thanks

Jess Dodson
@girlgerms

Tweets
76.3K

Fo
1

Tweets

Pinned T

Jess Do

To new fol

Hi, I'm a *WIND

. Datacenter. Rants on

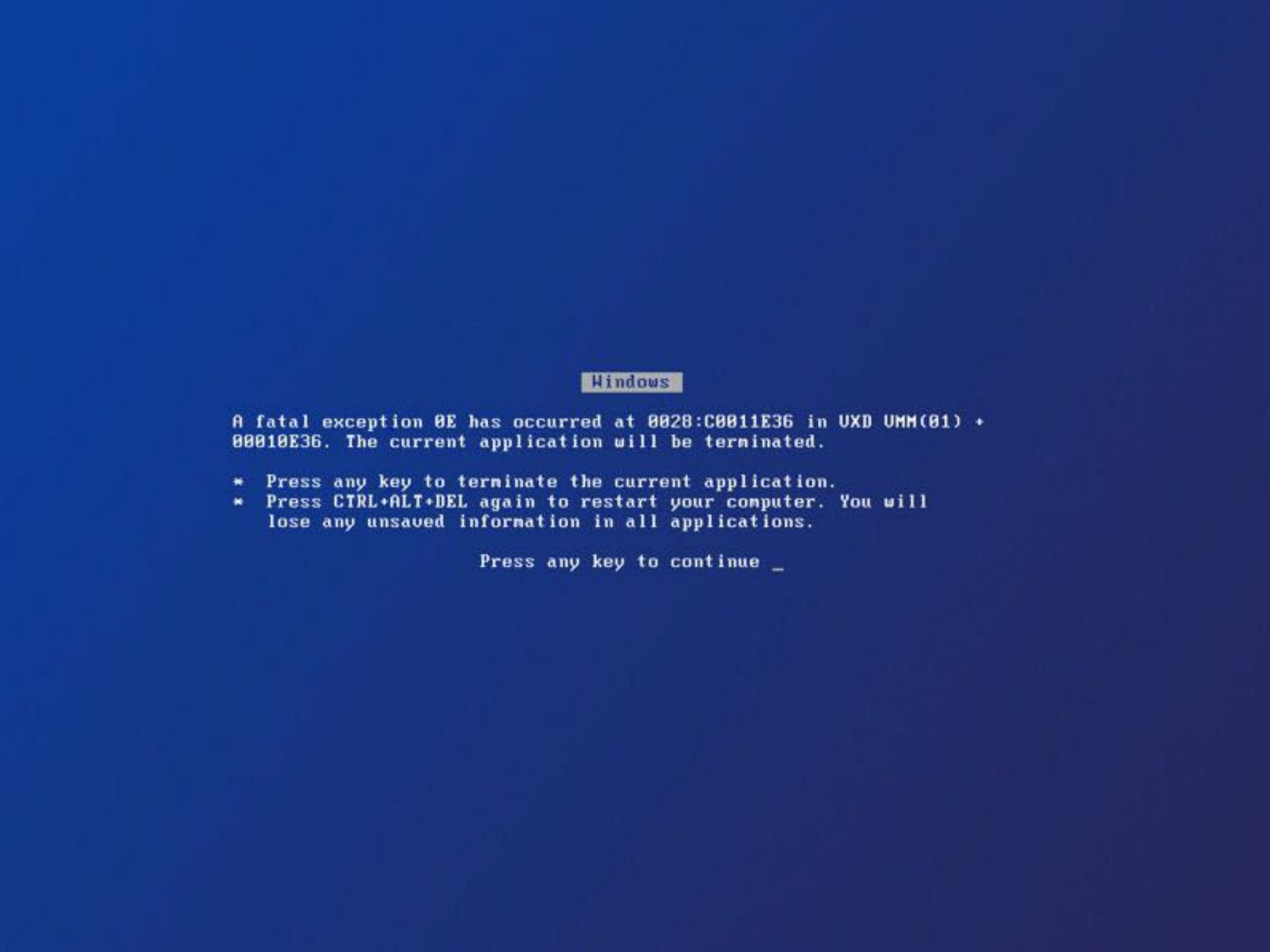
AD security, separat

firewalls, locker-down of

group policies.

Revolutionary Pingu sez: Join your union.

www.australianunions.org.au
www.union.org.nz



```
                              Windows

A fatal exception 0E has occurred at 0028:C0011E36 in VXD VMM(01) +
00010E36. The current application will be terminated.

*  Press any key to terminate the current application.
*  Press CTRL+ALT+DEL again to restart your computer. You will
   lose any unsaved information in all applications.

                      Press any key to continue _
```