Password ~~Audit~~ Cracking in AD

The Fun Part of Compliance

Mathieu Saulnier

Chercheur Indépendant
20+ année en sécurité

The Top 10 Reasons You Got Hacked in 2022

Firewalls	10	Deploy and manage
Message Integrity	9	Enforce Signing
Default Configurations	8	Manage Configurations
Patching	7	Patch Management
Protocol Abuse	6	Harden Protocols
WebApps	5	OWASP Practices
Employees	4	Security Awareness
Weak Optics	3	EDR & SIEM
AD Certificate Services	2	Configure and Manage
Credentials	1	Longer Passwords

AND HOW TO PREVENT IT IN 2023

BLACK HILLS
Information Security
• 2008 •

WebApps	5	OWASP Practices
Employees	4	Security Awareness
Weak Optics	3	EDR & SIEM
Certificate Services	2	Configure and Manage
Credentials	1	Longer Passwords

TO PREVENT IT IN 2023

Home » Cybersecurity » Security Awareness » 8 Most Common Causes of a Data Breach

8 Most Common Causes of a Data Breach

Search for: What are the two main causes of data breaches?

Dat
high
atta
sam
The
und
about the most common causes of data leak
lines, we discuss eight common **causes of se**

Weak Passwords

What is the number one cause of data brea
to the Harris Poll, 75% of Americans are duly
24% use common passwords such as sequer
numbers. 49% of password users only chang
update them.

Who is the leading cause of security breaches?

Hacking attacks may well be the most common cause of a data breach but it is often a weak or lost password that is the vulnerability that is being exploited by the opportunist hacker.

https://www.sutcliffeinsurance.co.uk › news › 8-most-c...

People also ask

What are the 3 main causes of data breaches?

In the report, ITRC identified threee primary causes of a data breach: data was exposed or stolen because of a cyberattack, such as phishing or stolen credentials; a mistake, such as lost devices or incorrect configuration a system; and a physical attack, such as a skimmer at a gas station pump that steals payment card ... Feb 4, 2022

https://www.darkreading.com › edge-threat-monitor › mo...

What are the two main causes of data breaches?

Six Common Causes of Data Breaches

- Cause 1. Insider Threats Due to Misuse of Privileged Access. ...
- Cause 2. Weak and Stolen Passwords. ...
- Cause 3. Unpatched Applications. ...
- ause 4. Malware. ...
- ause 5. Social Engineering. ...
- ause 6. Physical Attacks.

), 2022

//www.lepide.com › blog › six-common-causes-of...

any. Don't
ne. Learning

YOLO Corp

YOLO Corp

PCI Compliant
GDPR Compliant

Cool Sec

Cool Sec

PCI Compliant
GDPR Compliant
NIST Compliant

EvilCats

EvilCats

Se fichent de votre

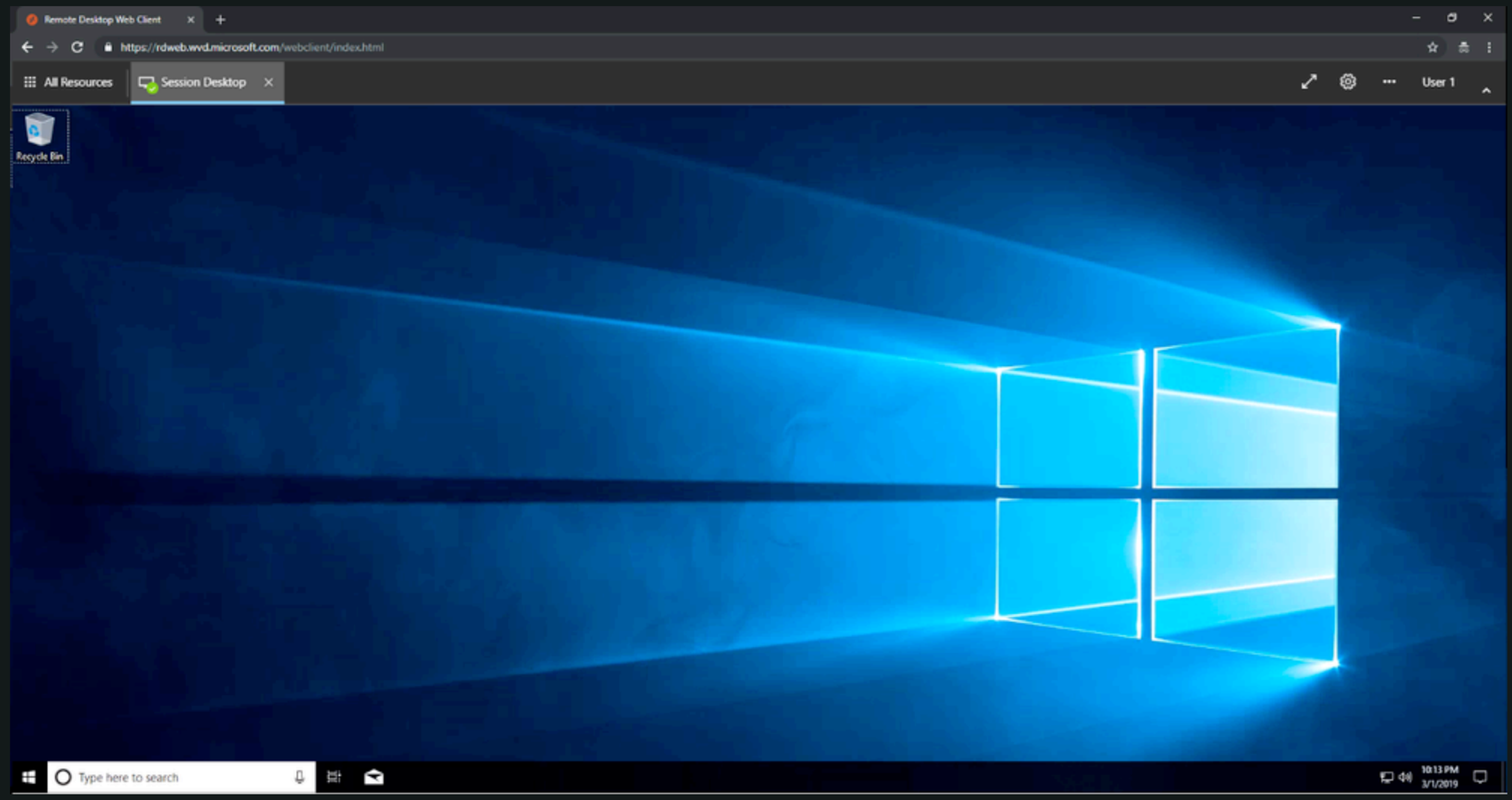
Compliance

Password Spray

Password Spray

Password Spray

YOLO Corp


Remote Desktop Web Client
https://rdweb.wvd.microsoft.com/webclient/index.html
All Resources
Session Desktop
User 1
Recycle Bin
Type here to search
10:13 PM
3/1/2019

Cool Sec


YO_Windows_7 - Console - VMware ESXi
Non sécurisé | esx/ui/#/console/933
FR
OpenOTP Login
Enter your TOKEN password
One-Time Password
Windows 7 Enterprise

Selon Microsoft

MFA can reduce the risk of identity compromise by as much as 99.9% over passwords alone.

Cool Sec

Alerts

Password Spray

First Connection from IP

Multiple Failed MFA

PCI

7 caractères
Changer tous les 90 jours


WAIT
WHAT?
makeameme.org

Combien de temps pour cracker 7 caractères?

7 Minutes

Revenons à PCI

PCI

7 caractères
Changer tous les 90 jours

PCI

Mais...

PCI

En 2022 ils ont changé!

PCI

12 caractères

Changer tous les 90 jours

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years

GDPR

8 caractères
Éviter les mots du dictionnaire
Utiliser Passphrase

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years

NIST 800-63B

15 caractères
N'expire jamais


WOAH WOAH WEE WAH
I LIKE
VERY NICE

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years

Password Cracking

Password Cracking

Rockyou.txt

NTDS.DIT

Password Cracking

hashcat -m 1000 -a 0 myhash.txt rockyou.txt -r rules/dive.rule

50% en moins de 24h

80%+ en semaine

Lequel est meilleur?

Welcome2023!

Passw0rdPassw0rd!

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years

4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

SAME

SAME

BUT

DIFFERENT

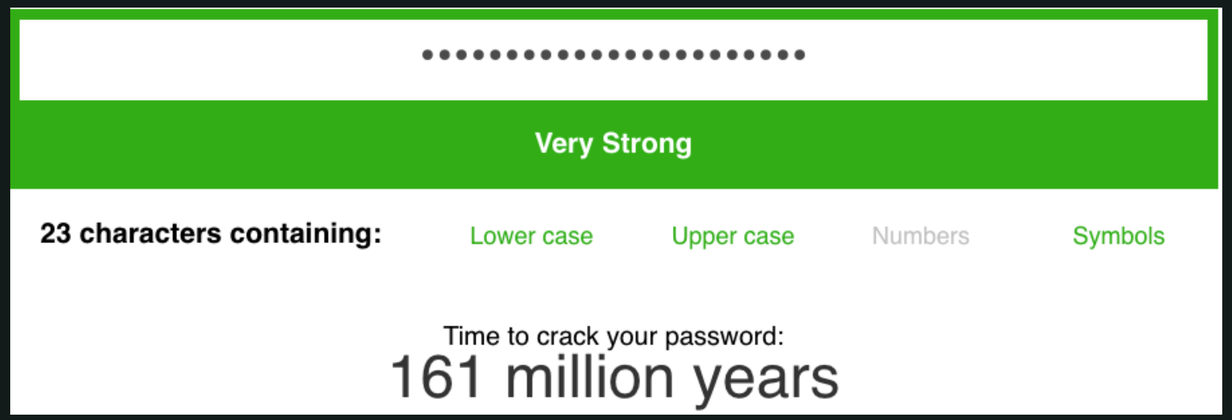
Lequel est meilleur?

`The Empire Barks Back`

Patience.young.Pawdawan

Selon passwordmonster.com

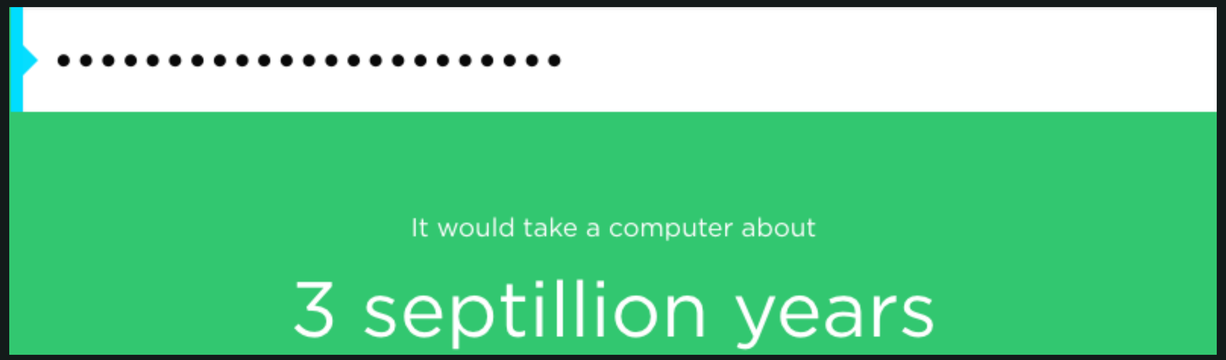
`The Empire Barks Back`



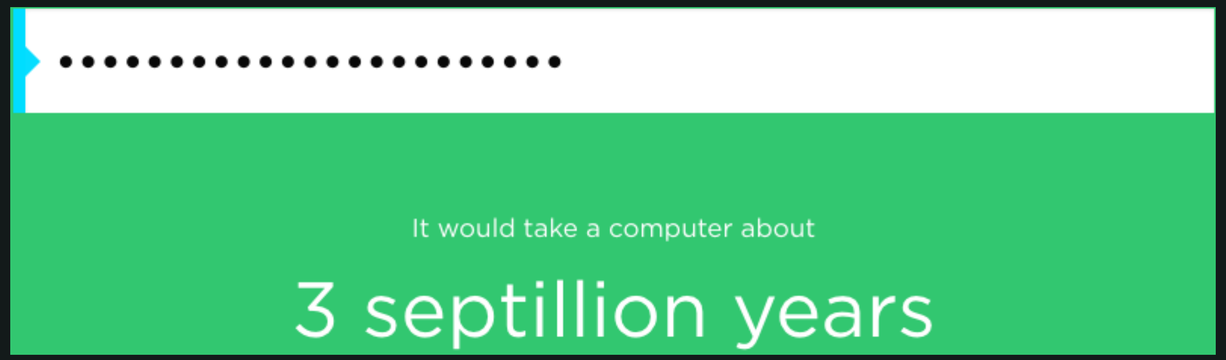
Patience.young.Pawdawan

Selon security.org

`The Empire Barks Back`



Patience.young.Pawdawan



SAME

SAME

BUT

DIFFERENT

BUT STILL THE SAME

Password Cracking

80%

<1%

Ce que Cool Sec a fait

15 caractères

N'expire jamais

Crack mdp hebdomadaire

Cracké = changé

Comment Cool Sec a fait

#1 Créer un compte de service

#2 Assigner les droits "Replicating Directory Changes All"

#3 Appliquer les recom de NIST

#4 Avisez leurs utilisateurs

#5 Changement de GPO

#6 Force Change Password

Comment Cool Sec a fait

```
PS> Install-Module -Name DSInternals
PS> Import-Module DSInternals
PS> $cred = Get-Credential
PS>
```

Comment Cool Sec a fait

```
PS> Get-ADReplAccount -All -Server COOLDC01
        -Credential $cred
    I Where-Object Enabled -eq "True"
    I Format-Custom -View HashcatNT > usershashes.txt
PS> Get-ADReplAccount -All -Server COOLDC01
        -Credential $cred
    I Test-PasswordQuality
        -WeakPasswordHashes weakhashes.txt >
        Pass_Result.txt
```

Compte Admin vs User

Avez-vous 1, 2 ou 3 types de compte?

Comment Cool Sec a fait

```
PS> hashcat -m 1000 -a 0 --username usershashes.txt
    rockyou.txt -r rules/dive.rule
PS> hashcat -m 1000 -a 0 --username usershashes.txt
    rockyou.txt -r rules/d3adhob0.rule
PS> hashcat -m 1000 -a 3 --username usershashes.txt
PS> copy hashcat.potfile weakhashes.txt
```

Comment Cool Sec a fait

```
PS> $file=Get-Content .\userbadpass.txt
    foreach ($user in $file) {
        Get-ADUser -Identity $user -Properties * I Select Name,
    SamAccountName,
    @{Name='LastLogon';Expression={[DateTime]::FromFileTi
    me($_.LastLogon)}}, whenCreated, PasswordLastSet,
    Enabled, UserPrincipalName I export-csv users-bad-
    pass.csv -append
        Set-ADUser -Identity $user -ChangePasswordAtLogon:
    $true
    }
```

Prochaines Étapes

#8 Travis Palmer - Passwd Cracking Beyond 15 Chars, Under $500
youtube.com/watch?v=_bYDbr853Uw

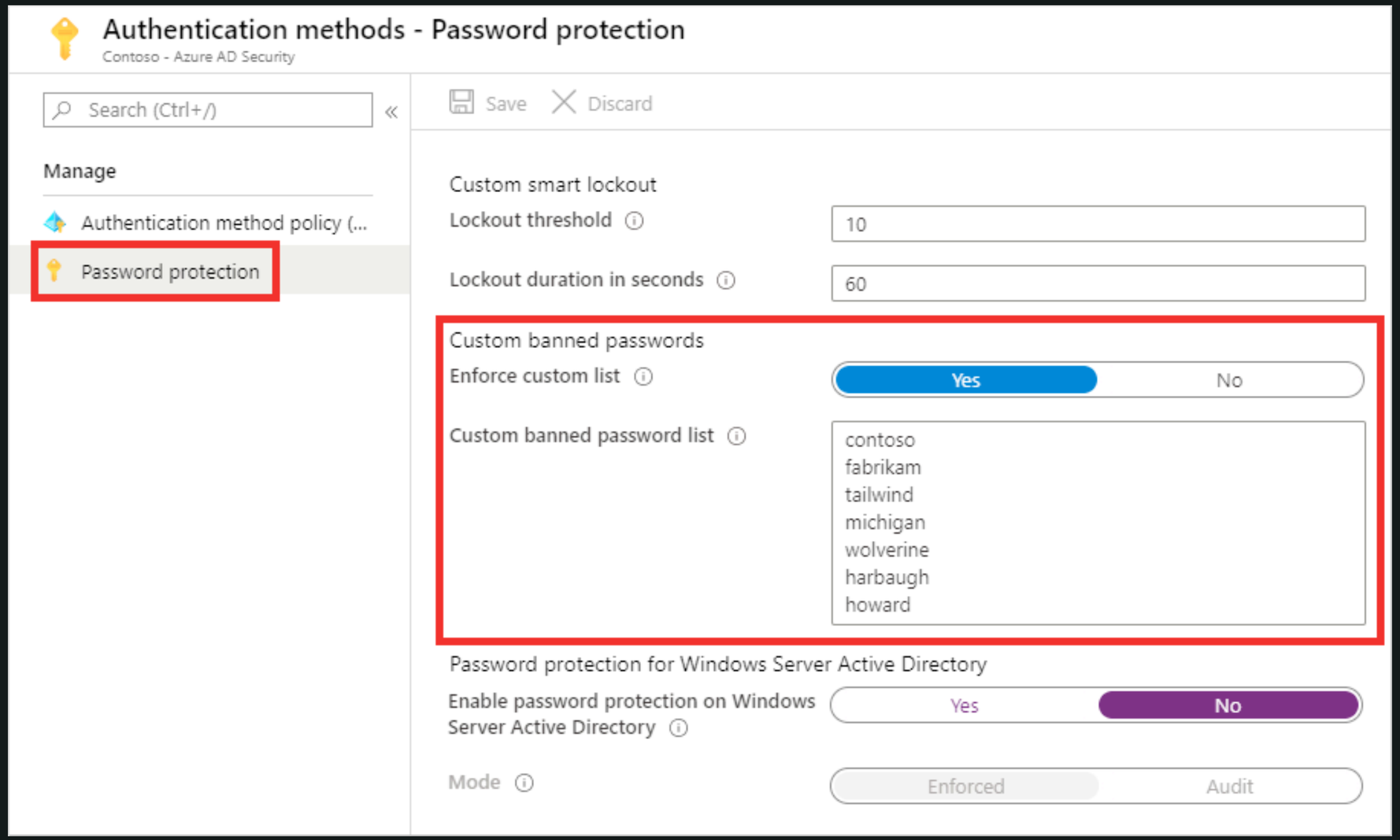
#9 More info on dsinternals.com

youtube.com/watch?v=soSRV8KFr2c

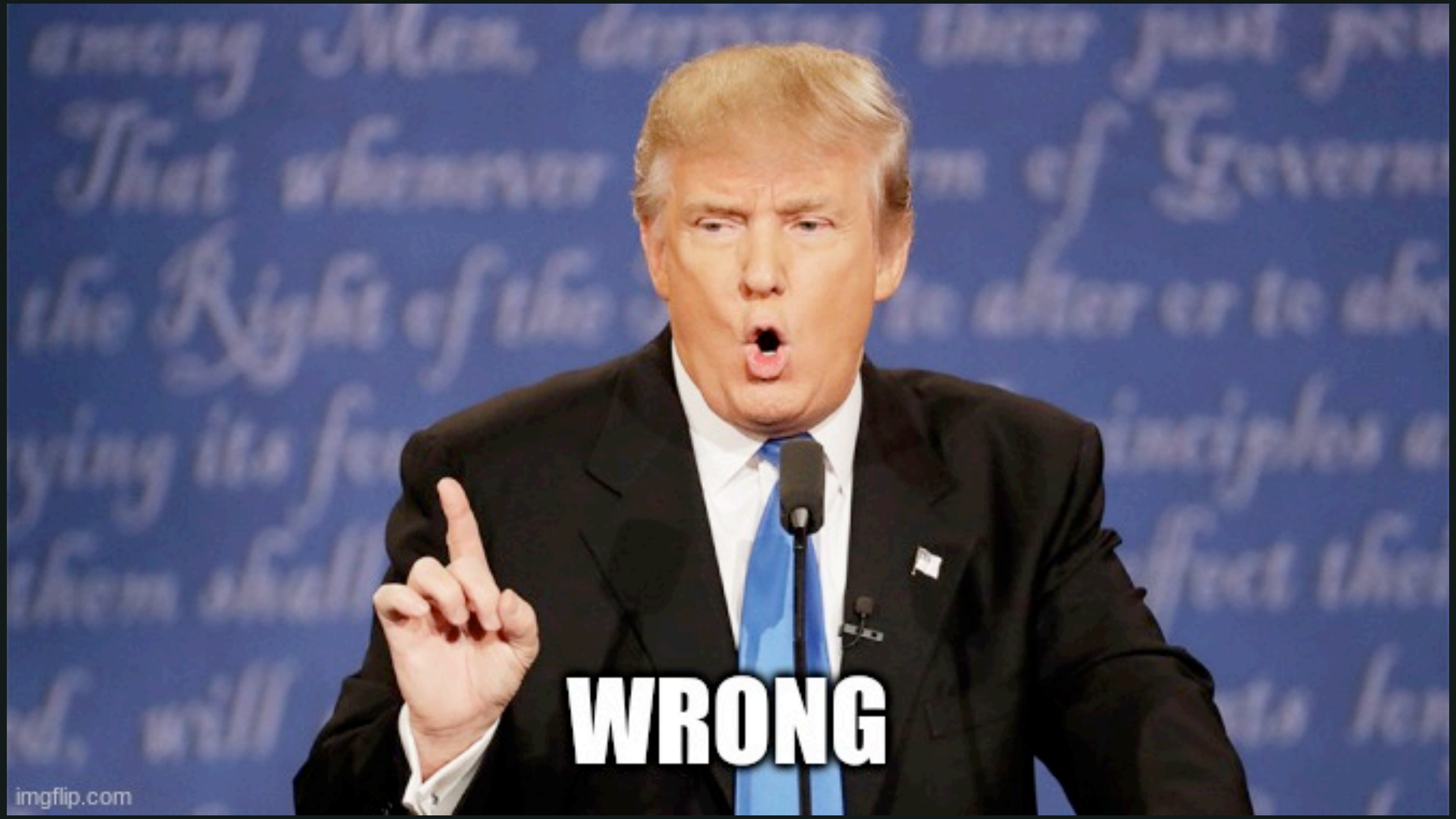
Mais si on a

AzureAD Mat?

EntraID

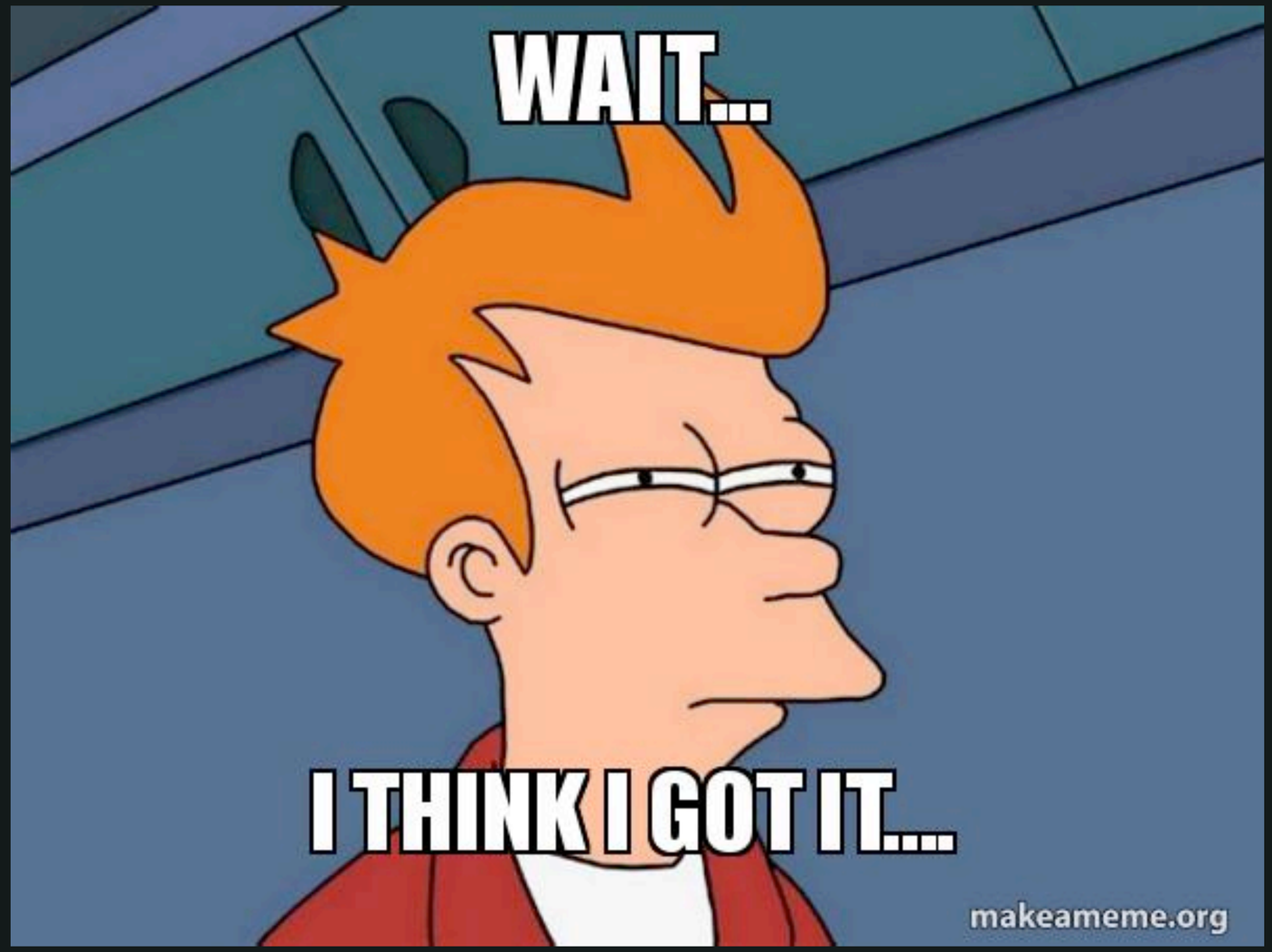

Authentication methods - Password protection
Contoso - Azure AD Security
Search (Ctrl+/)
Manage
Authentication method policy (...
Password protection
Save
Discard
Custom smart lockout
Lockout threshold
10
Lockout duration in seconds
60
Custom banned passwords
Enforce custom list
Yes
No
Custom banned password list
contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard
Password protection for Windows Server Active Directory
Enable password protection on Windows Server Active Directory
Yes
No
Mode
Enforced
Audit

Mais, Mat, on ne peut pas extraire les hash?!?


WRONG
imgflip.com

EntraID

AADInternals à la rescousse!



DSInternals

vs

AADInternals


WARNING

Ce que vous avez besoin

Les hashs dans AADDS

Info d’identité d’une App

Certificat d’encryption

Au CLI


```
PS> Install-Module -Name AADInternals
PS> Import-Module AADInternals
PS> Get-AADIntUserNTHash -ClientPassword
    "vlb8Q~W8iVXwfdt2FjIH4FE0hRc-p9G_kyN_KbtZ"
    -ClientId "23857e6f-7be4-4bb8-84b7-22e92c359c8d"
    -PfxFileName ".\encryption_cert.pfx"
PS>
```

Plus d’information

aadinternals.com

Troopers2023

Video

Slides

C’est vraiment cool Mat, mais comment je crée un bon mdp?

On le tape jamais

64 caractères
Storer dans un Pass Manager

On doit le tapper

Habiller le mot de passe

##$$I have a bad feeling about this$$##

It would take a computer about
17 septendecillion years

Conseil additionnel

Utiliser sa langue maternelle

#$La peur mène à la colère#$

It would take a computer about
9 hundred tredecillion years

Combien y a-t-il

Ç, É, Š, ß, ¡

Remerciements

DSInternals: @MGrafnetter

AADInternals: @DrAzureAD

Hashcat

@obviousmalware #WEDOFF

"Do you want to mitigate against auditors or attackers?"

Someone Clever on Twitter


Firewall
_Decoding...
Access_Denied
@SoubiMtl
linkedin.com/in/
mathieusaulnier