

# Password Audit Cracking in AD

## The Fun Part of Compliance



# Mathieu Saulnier

Independent Researcher  
20+ years in security



# 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



|                      |   |                      |
|----------------------|---|----------------------|
| 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



## 8 Most Common Causes of a Data Breach

Search for: [What are the two main causes of data breaches?](#)

Dat: Who is the leading cause of security breaches?

high  
atta  
sam 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.

The

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

about the most common causes of data leak

lines, we discuss eight common causes of se

### People also ask :

## Weak Passwords

What is the number one cause of data bre

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.

### 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

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. ...
- cause 4. Malware. ...
- cause 5. Social Engineering. ...
- cause 6. Physical Attacks.

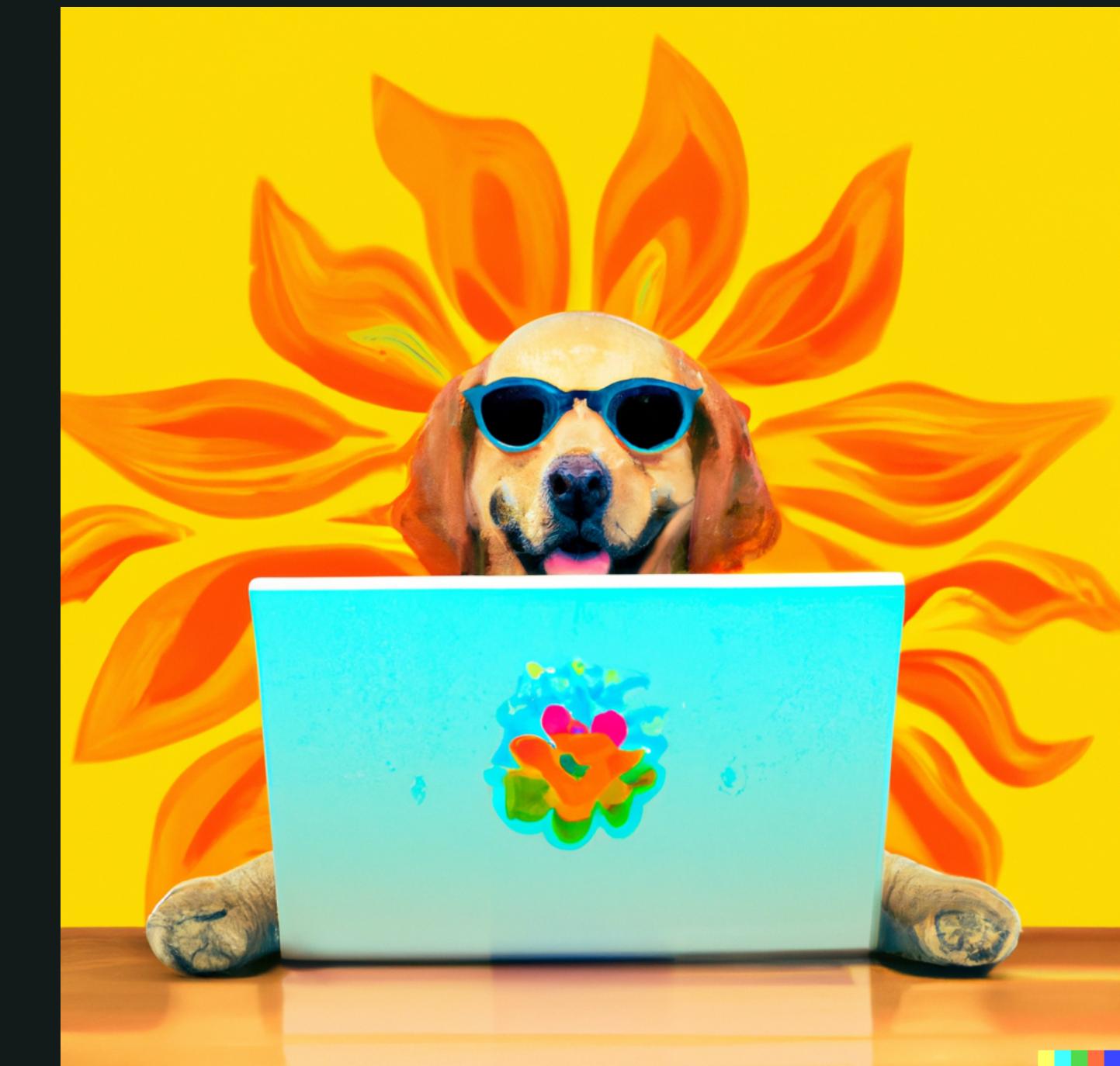
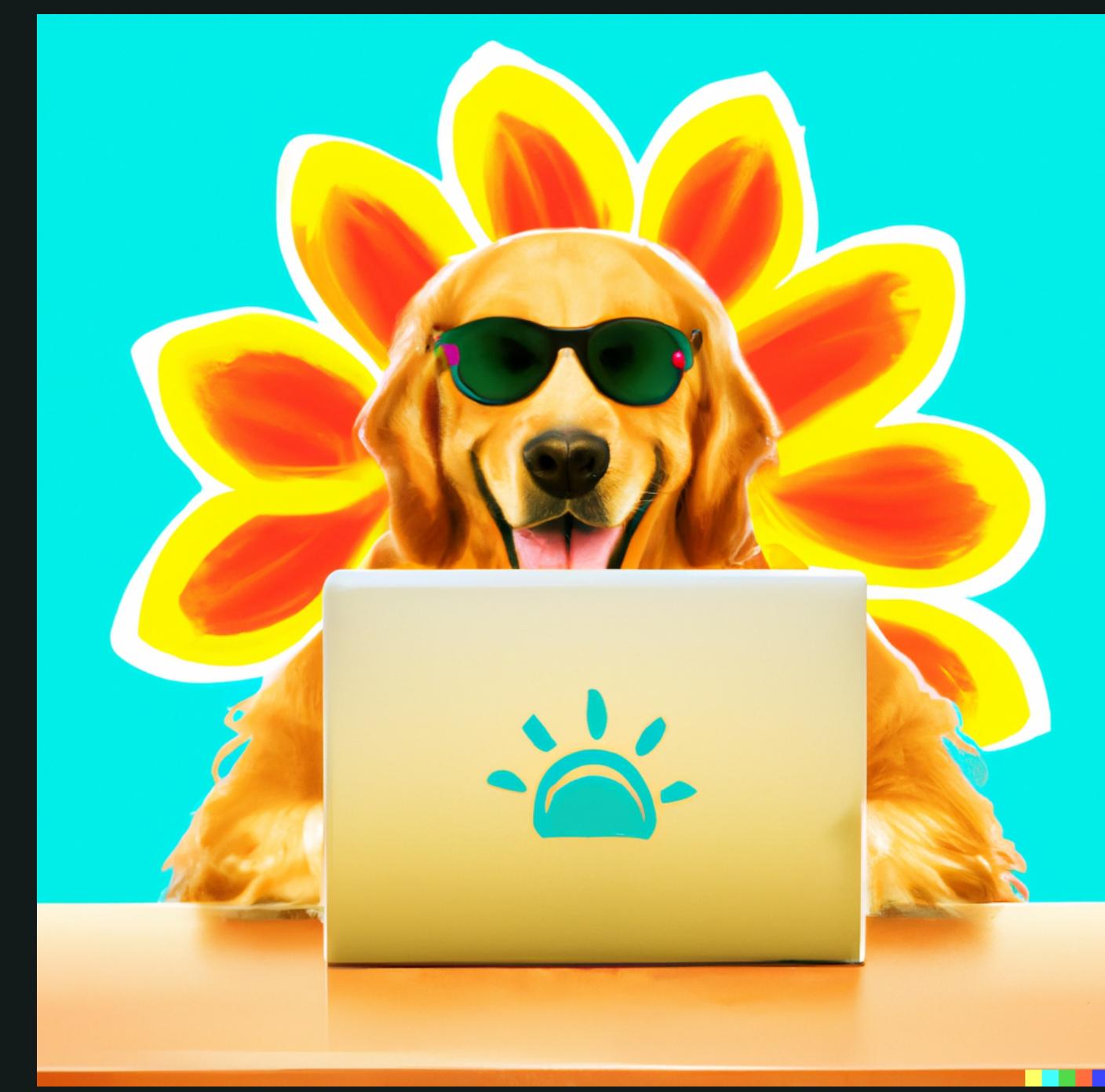
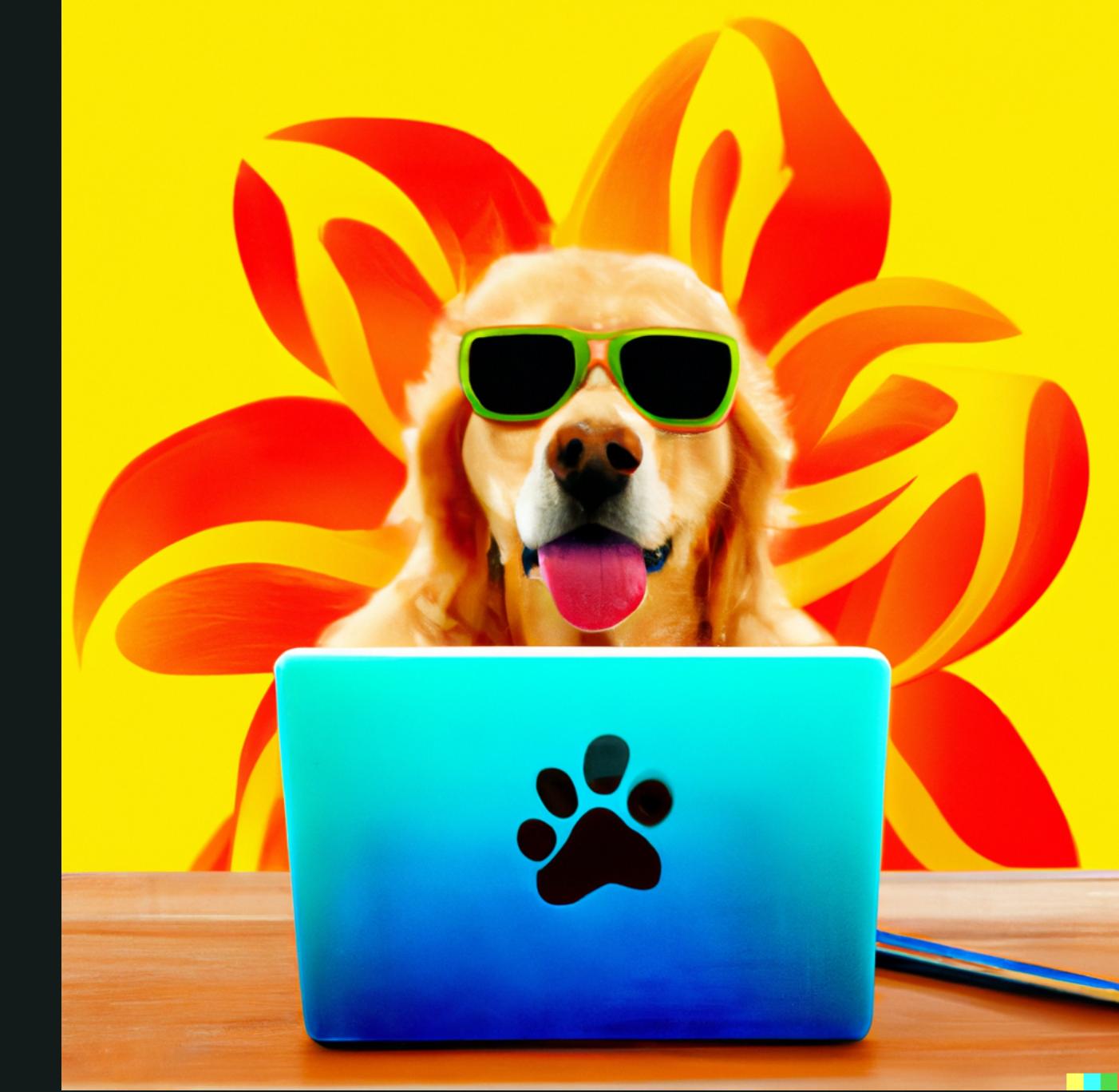
), 2022

<http://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



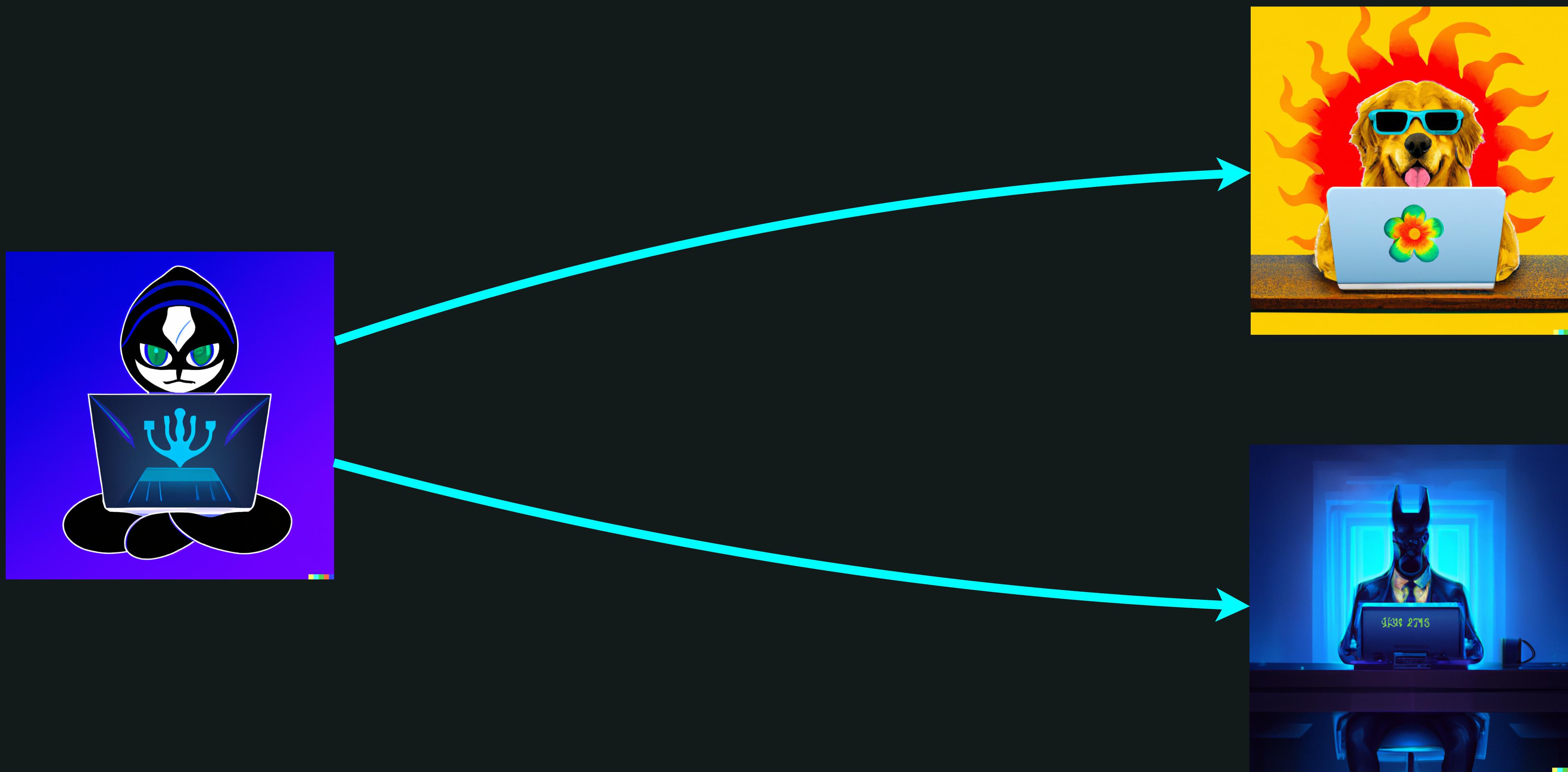
# EvilCats

Does not care about your  
Compliance

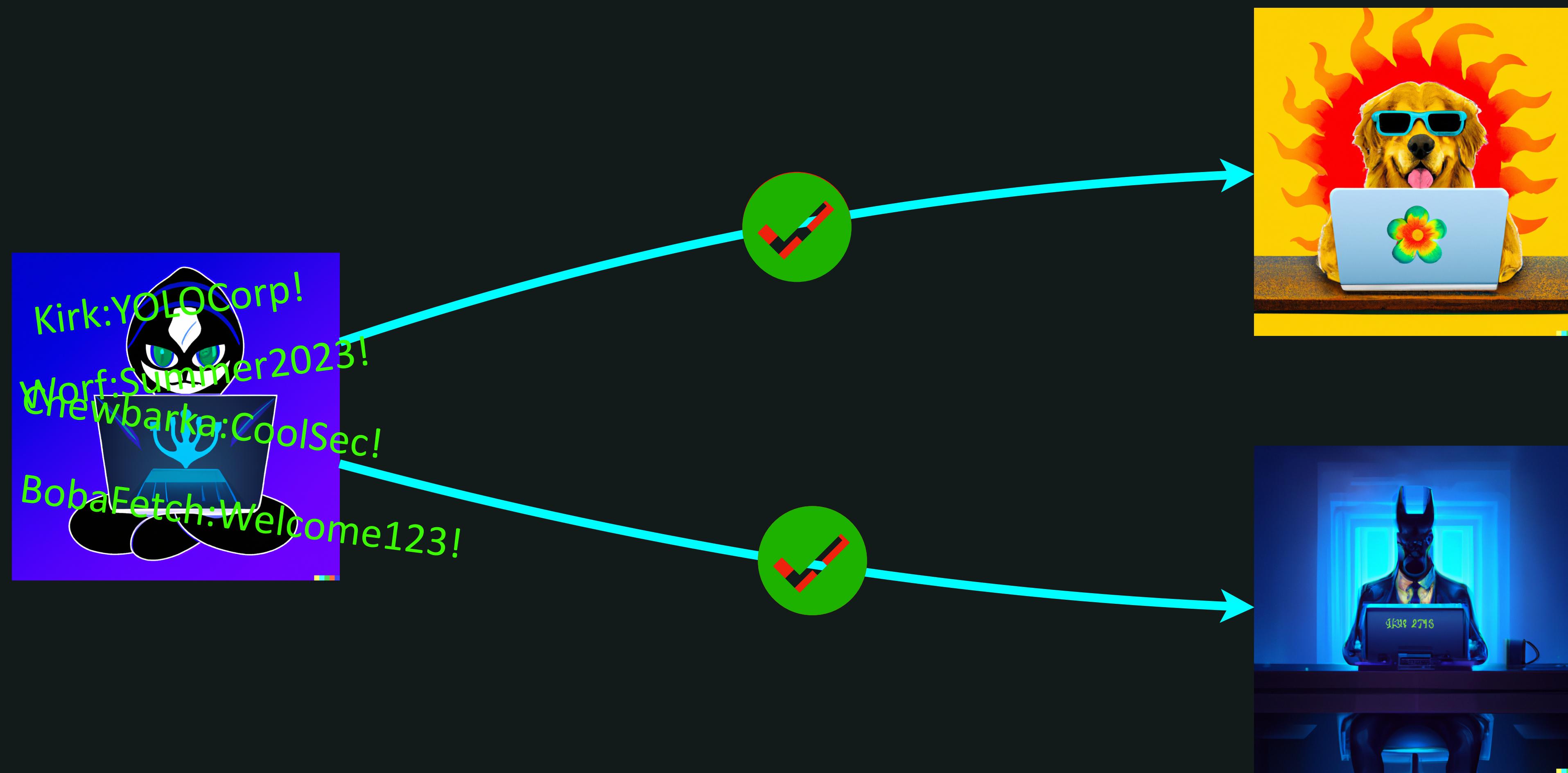
# Password Spray



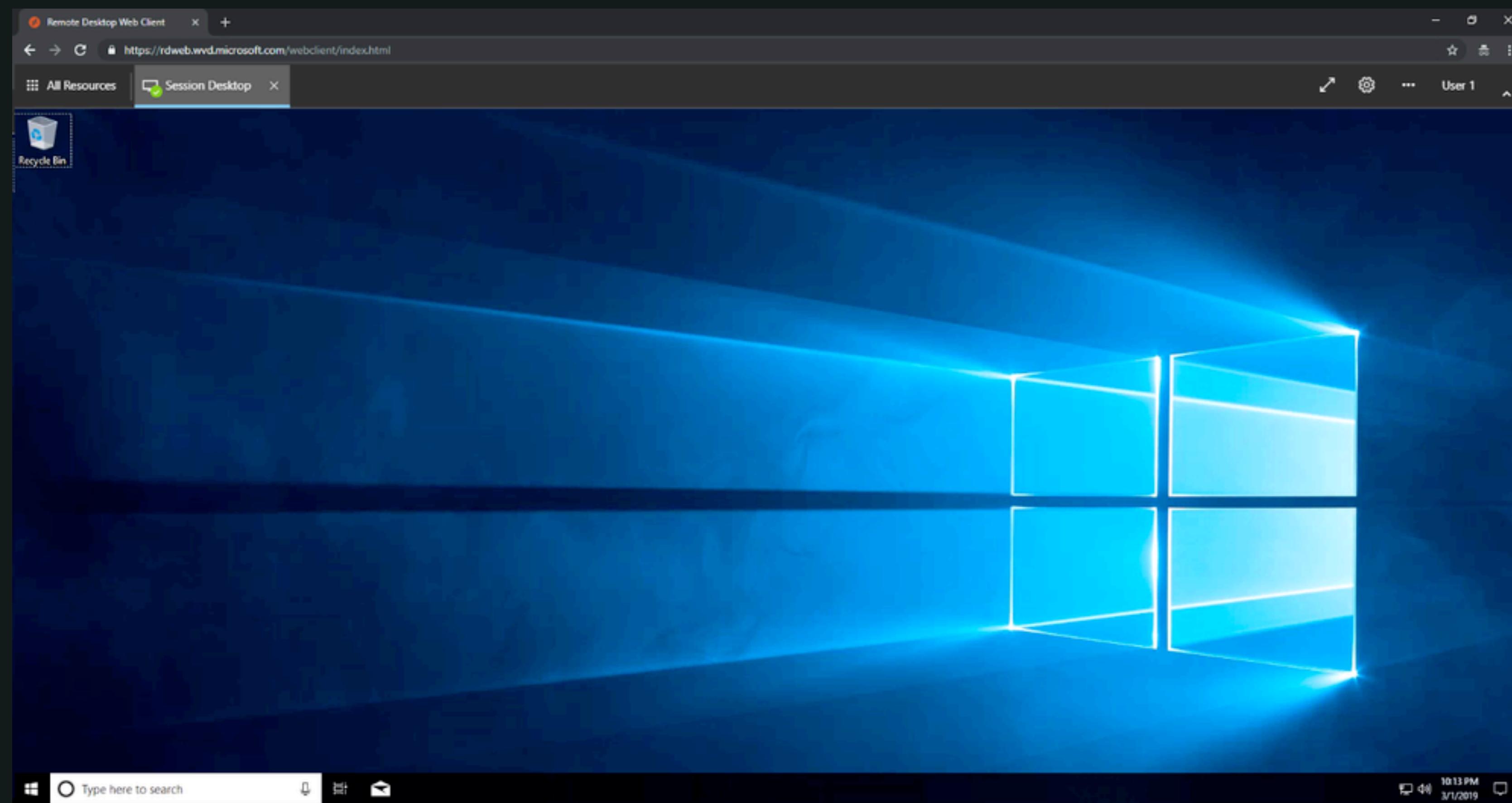
# Password Spray



# Password Spray



# YOLO Corp



# Cool Sec



# According to 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 characters  
Change every 90 days



**WAIT**

**WHAT?**

[makeameme.org](http://makeameme.org)

How long does it take  
to crack 7 characters?

7 Minutes



# Back to PCI

PCI

7 characters  
Change every 90 days

PCI

But...

PCI

In 2022 they changed!

PCI

12 characters  
Change every 90 days

# 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                                   |



› Learn about our methodology at [hivesystems.io/password](https://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                                     |
| 16                   | 5 hrs        | 51 years          | 150 years                   | 31 years                             | 321 years                                     |

# GDPR

8 characters  
Avoid dictionary words  
Use 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                                     |
| 16                   | 5 hrs        | 51 years          | 150 years                   | 31 years                             | 62k years                                     |

NIST 800-63B

15 characters

Never expire

**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                                     |
| 16                   | Estimated    | Estimated         | Estimated                   | Estimated                            | Estimated                                     |

# Password Cracking



# Password Cracking



Rockyou.txt

NTDS.DIT

# Password Cracking



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

50% in less than 24h  
80%+ in a week

# Which is best?

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                                     |
| 16                   | 5 hrs        | 51 years          | 150 years                   | 31 years                             | 321 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

# Which is best?

EG

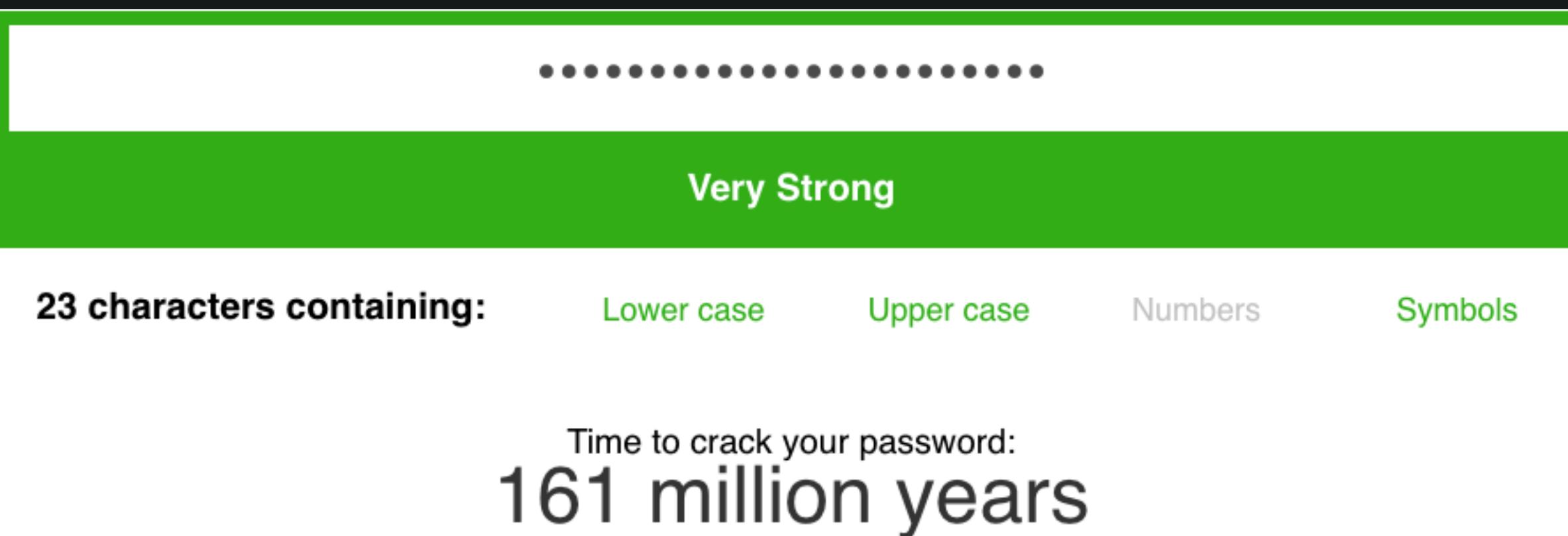


Patience.young.Pawdawan

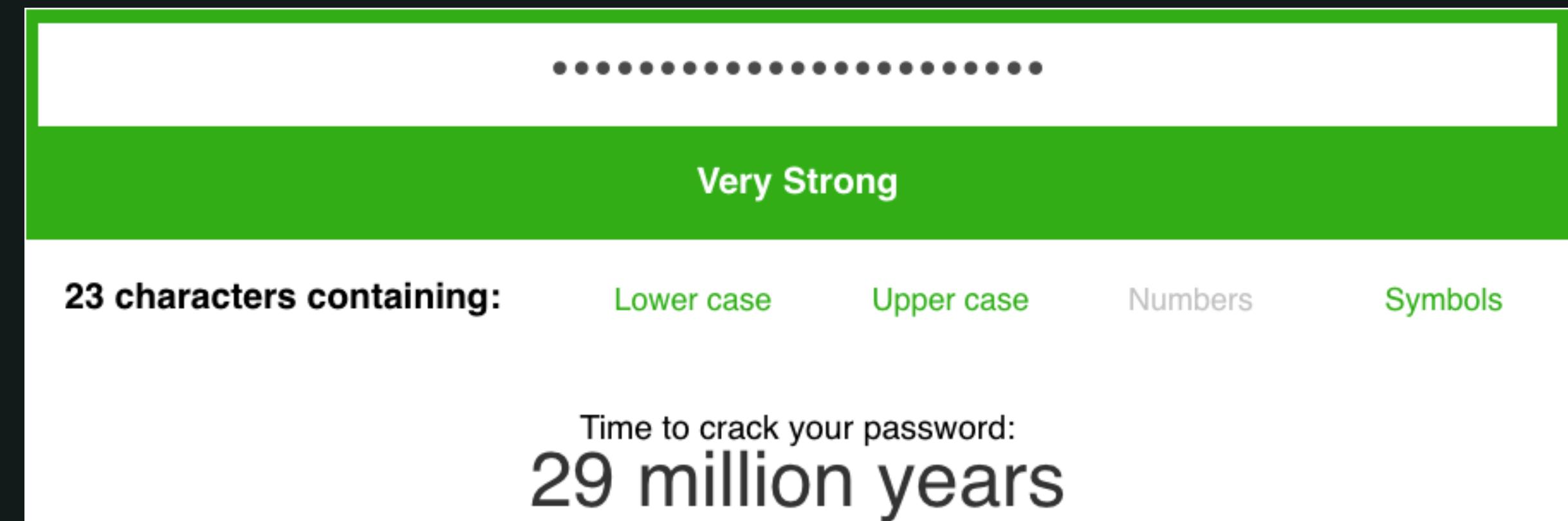


# According to passwordmonster

`The Empire Barks Back`



Patience.young.Pawdawan



# According to security.org

`The Empire Barks Back`

Patience.young.Pawdawan

.....

It would take a computer about

3 septillion years

.....

It would take a computer about

3 septillion years

SAME

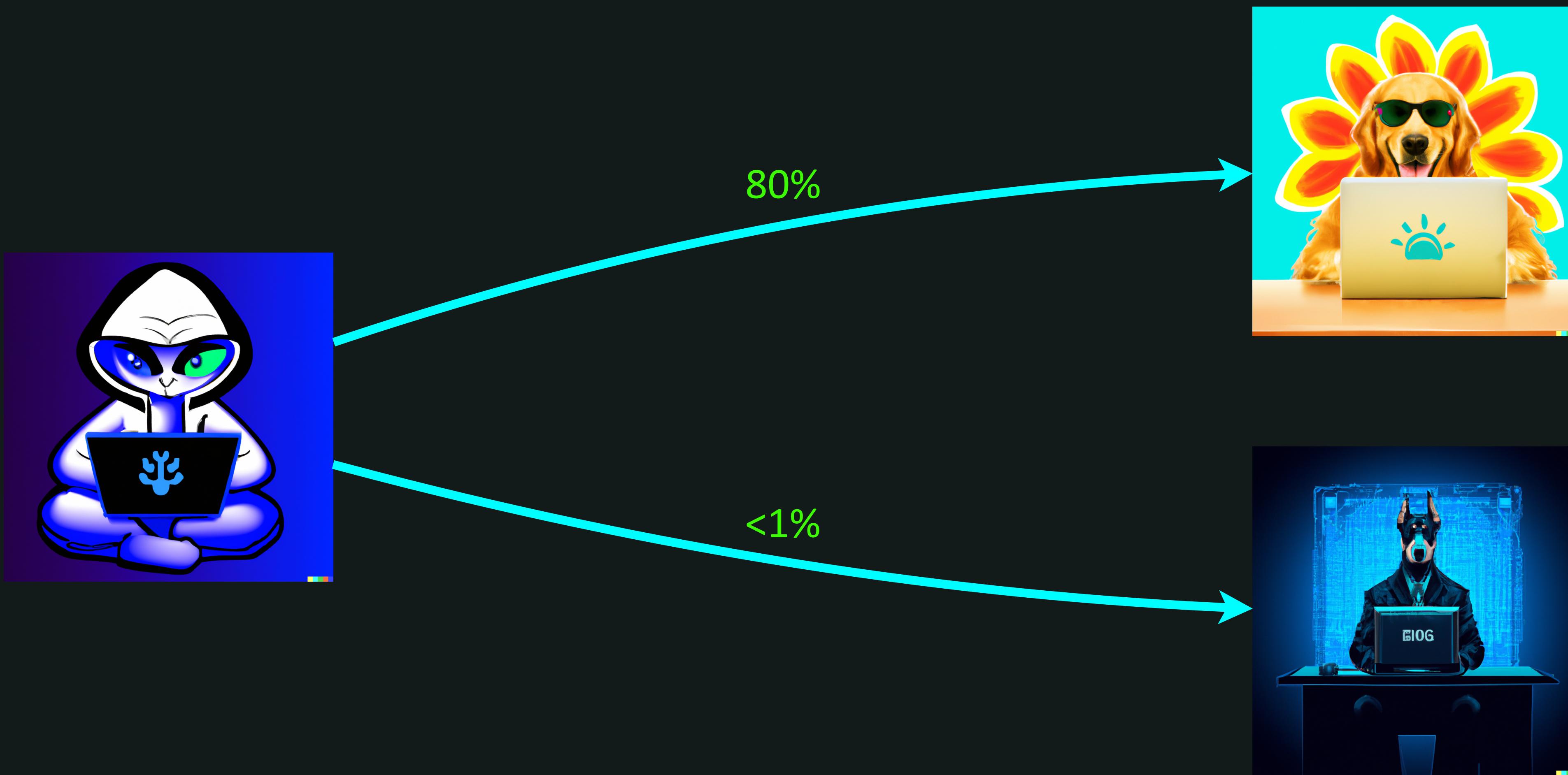
SAME

BUT

DIFFERENT

BUT STILL THE SAME

# Password Cracking



# What did Cool Sec Implement

15 characters

Never Expire

Crack passwords weekly

Cracked = changed

# How Cool Sec did it



- #1 Create a service account
- #2 Assigned rights "Replicating Directory Changes All"
- #3 Apply NIST recommendations
- #4 Inform their users
- #5 Changed GPO
- #6 Force Change Password

# How Cool Sec did it



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

# How Cool Sec did it



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

# Admin vs User accounts

Do you have 1, 2 or 3  
account types?

# How Cool Sec did it



```
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
```

# How Cool Sec did it



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

What about  
AzureAD Mat?

# EntralID

 Authentication methods - Password protection  
Contoso - Azure AD Security

Search (Ctrl+/) <> Save Discard

Manage

 Authentication method policy (...)

 **Password protection**

Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

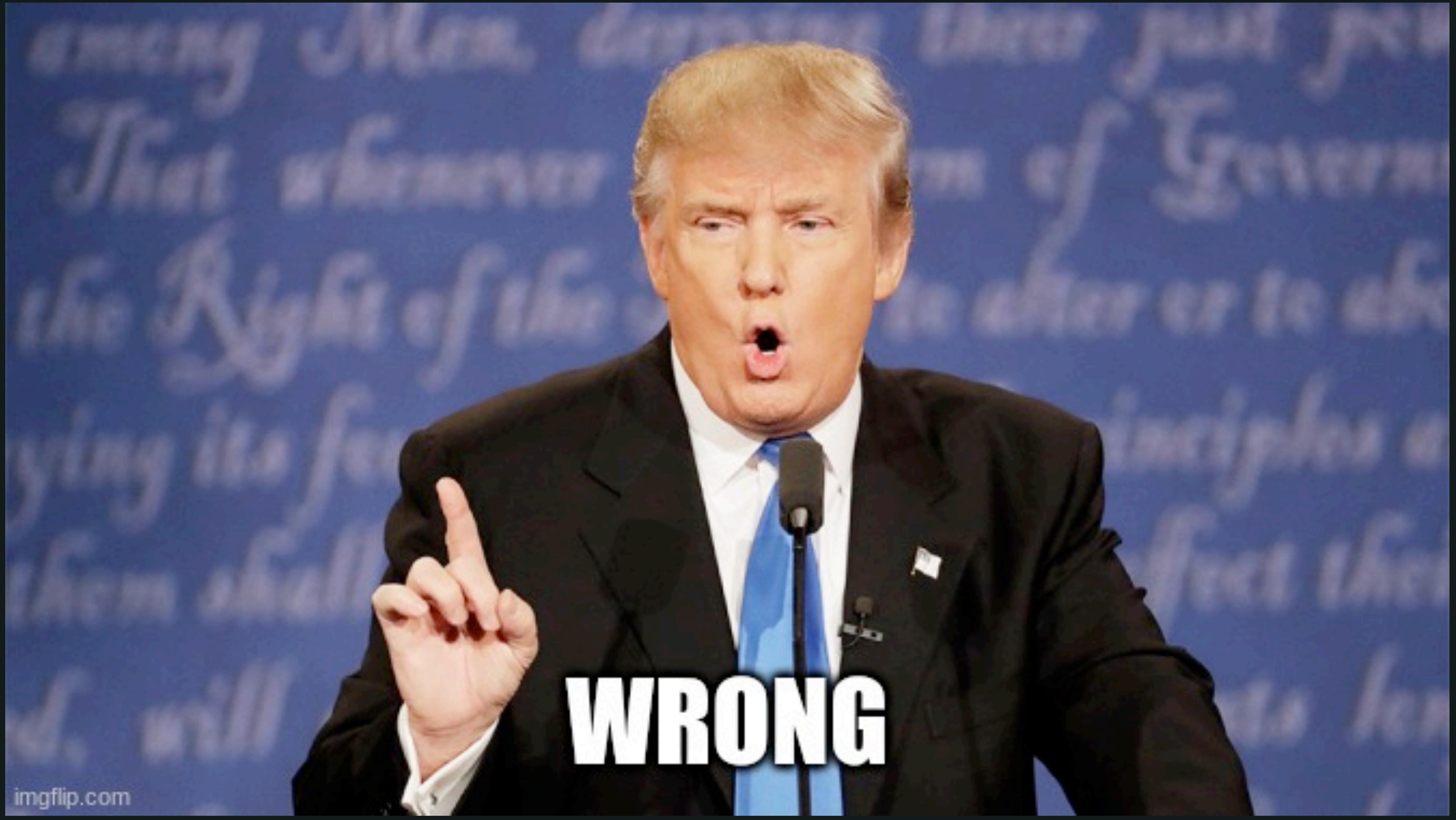
contoso  
fabrikam  
tailwind  
michigan  
wolverine  
harbaugh  
howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

But we can't get  
the hashes from  
AzureAD, right?



EntralD

AADInternals got you  
covered



DSInternals  
VS  
AADInternals



**WARNING**

# What You Need

Hashes in AADDS

Creds for an App

Encryption Cert



# From PowerShell



```
PS> Install-Module -Name AADInternals  
PS> Import-Module AADInternals  
PS> Get-AADIntUserNTHash -ClientPassword  
    "vlb8Q~W8iVXwfdt2FjlH4FE0hRc-p9G_kyN_KbtZ"  
    -ClientId "23857e6f-7be4-4bb8-84b7-22e92c359c8d"  
    -PfxFileName ".\encryption_cert.pfx"  
PS>
```

That's pretty cool  
but how do I  
create a strong  
password Mat?



You never type it

64 characters

Stored in a Pass Manager

Need to type it

Dress the password

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

It would take a computer about  
17 septendecillion years



# Additional tips

Use your mother tongue

#\$La peur mène à la colère\$#

It would take a computer about  
9 hundred tredecillion years

How many of

č, É, š, β, i

# Acknowledgments

DSInternals: @MGrafnetter

AADInternals: @DrAzureAD

Hashcat

@obviousmalware #WEDOFF

Travis Palmer: Passwd Cracking  
Beyond 15 Chars, Under \$500

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

*Someone Clever on Twitter*



@SoubiMtl

[linkedin.com/in/  
mathieusaunier](https://www.linkedin.com/in/mathieusaunier)