# ADPA - How to get an X-Ray of your AD domains

Marcel Keiffenheim | Solutions Architect Team Lead

PENTERACON 2023

Pentera's Annual Customer Summit

# Agenda

- What are we talking about? Setting the scene
- Why do I crack passwords?
- Why should you?
- How does it work?
- What kind of results do we get?

# What are we talking about?

PENTERA

# Marcel Keiffenheim

Solutions Architect Team Lead
Central Europe, Western Europe, Southern Africa

Relevant work experience:

- Hacking organisations

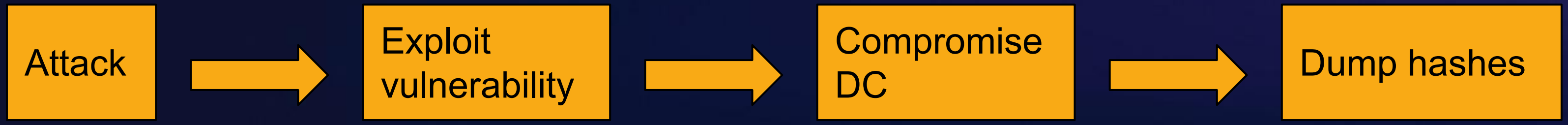
Relevant interests:

- Cracking passwords
- Gathering leaking credentials

Relevant qualifications:

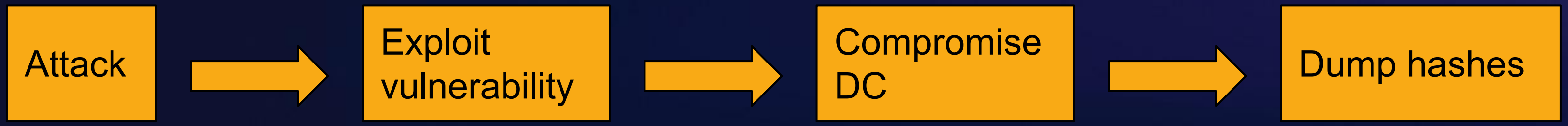
- I love my job

# Worst case scenario - successful pentest

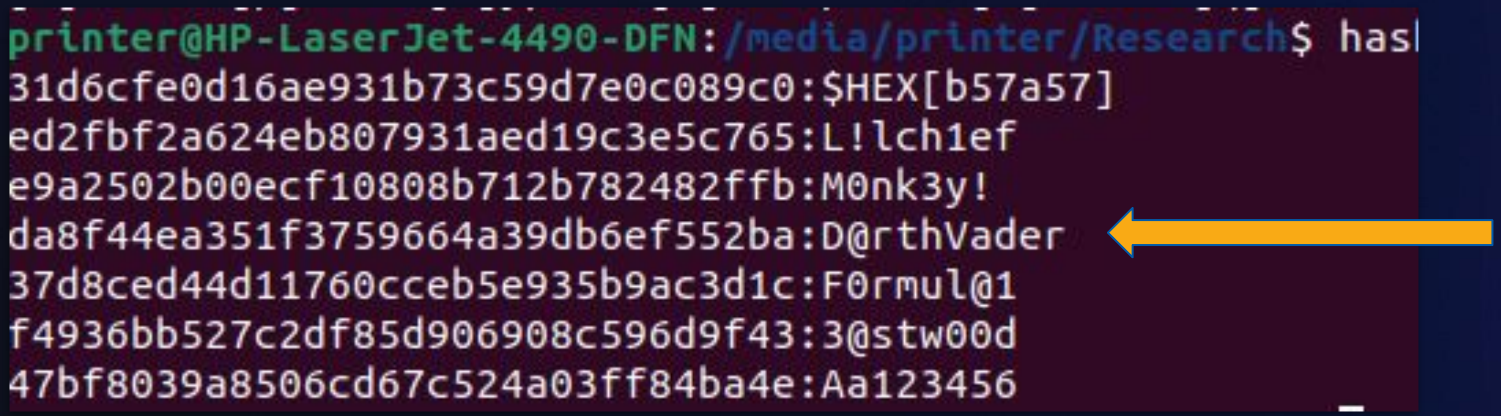


Attack → Exploit vulnerability → Compromise DC → Dump hashes

# Worst case scenario - successful pentest



Attack → Exploit vulnerability → Compromise DC → Dump hashes



```
printer@HP-LaserJet-4490-DFN:/media/printer/Research$ has
31d6cfe0d16ae931b73c59d7e0c089c0:$HEX[b57a57]
ed2fbf2a624eb807931aed19c3e5c765:L!lch1ef
e9a2502b00ecf10808b712b782482ffb:M0nk3y!
da8f44ea351f3759664a39db6ef552ba:D@rthVader
37d8ced44d11760cceb5e935b9ac3d1c:F0rmul@1
f4936bb527c2df85d906908c596d9f43:3@stw00d
47bf8039a8506cd67c524a03ff84ba4e:Aa123456
```

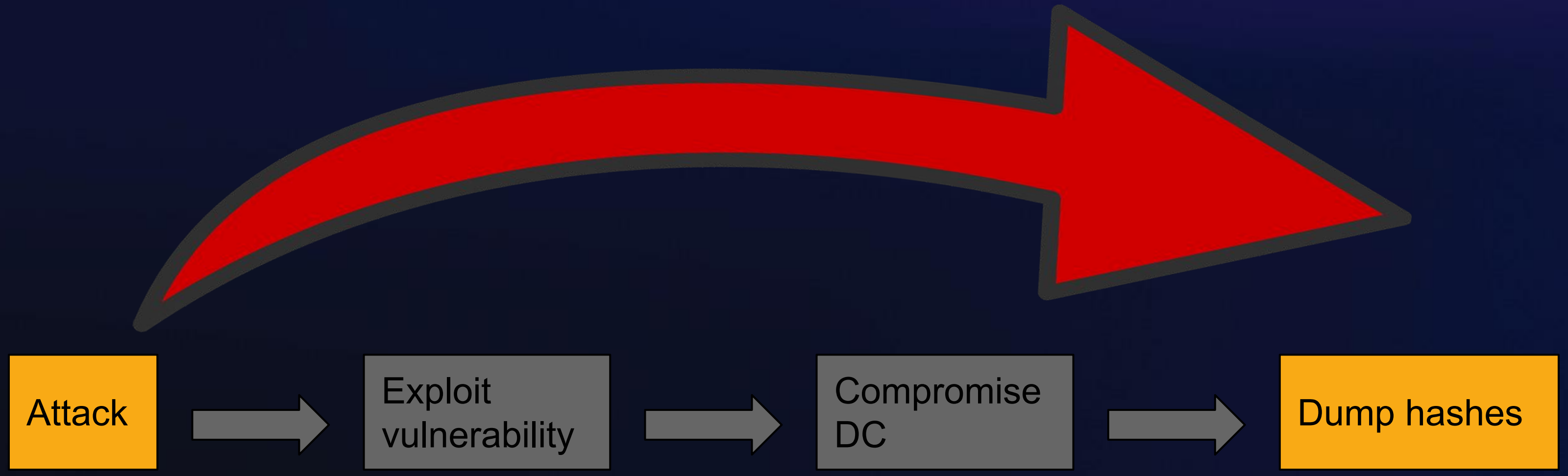
# What’s in it for me?

# Why did I crack the AD passwords?

For effect:

- Access user's data quietly
- Hammer home the message!
- How many users have good passwords?
- Because it's fun

# Targeted Test



Attack

Exploit vulnerability

Compromise DC

Dump hashes

# What’s in it for you?

# Why run the Active Directory Password Strength Assessment?

To get answers:

- What's an effective password?
- Does my organisation use effective passwords?
- What other attack surface would an attacker find?

And because it's fun

# How does it work?

# How does it work?

Microsoft Directory Replication Service Remote Protocol (MS-DRSR)

ntds.dit

| | |
|---|---|
| andre.young | 60BA79B4EBD88149226D5127D6E33DED |
| eric.wright | 1C207040F4283A7116A05D0C7DD1EA4D |
| oshea.jackson | 850C75DE61D82737B2E9CF55D2998D45 |

# How Pentera cracks passwords

| | | |
|---|---|---|
| Level 1: Dictionary attack | CPU | password |
| Level 2: Mask attack | GPU | P4ssw0rd |
| Level 3: Mask attack + | GPU | #P4ssw0rd# |
| Level 4: Mask attack ++ | GPU | 2023#P4ssw0rd# |

# How Pentera cracks passwords

4 levels of password cracking with unique dictionaries & rulesets

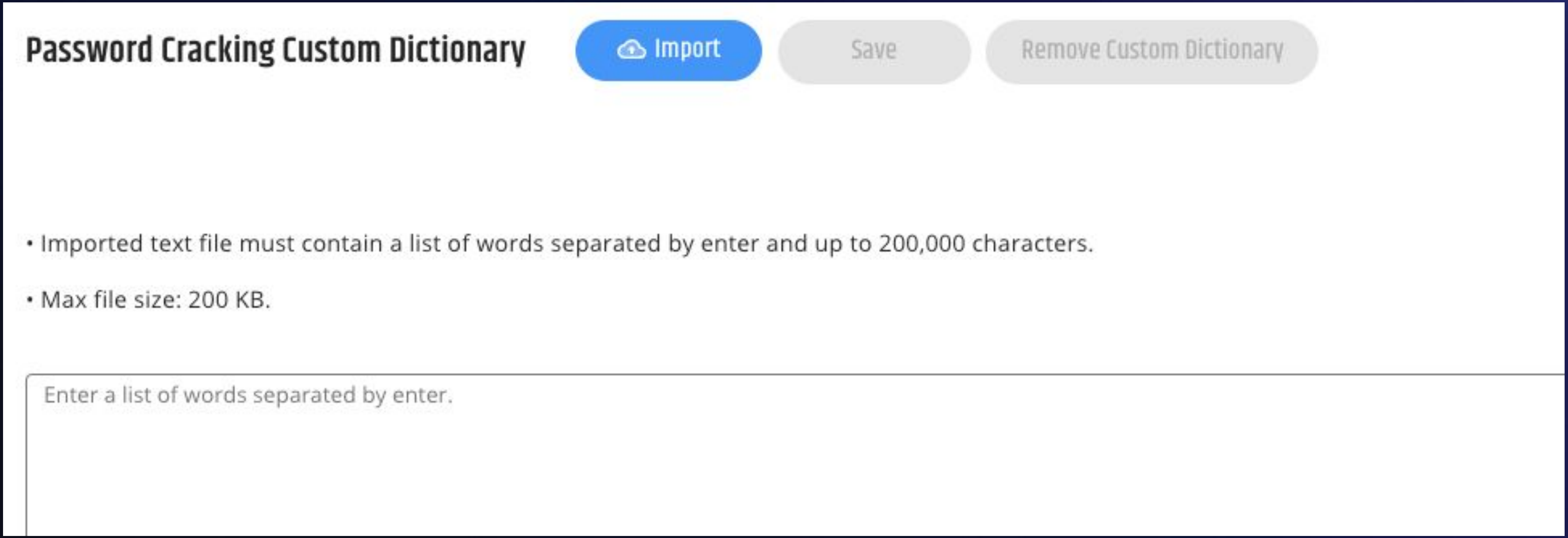
One dictionary has 44,106,118 words

One rule set has 34,158 modifiers for each dictionary word

That's 1,506576779 $\times 10^{12}$ possibilities

PENTERA

# Custom Password Dictionary



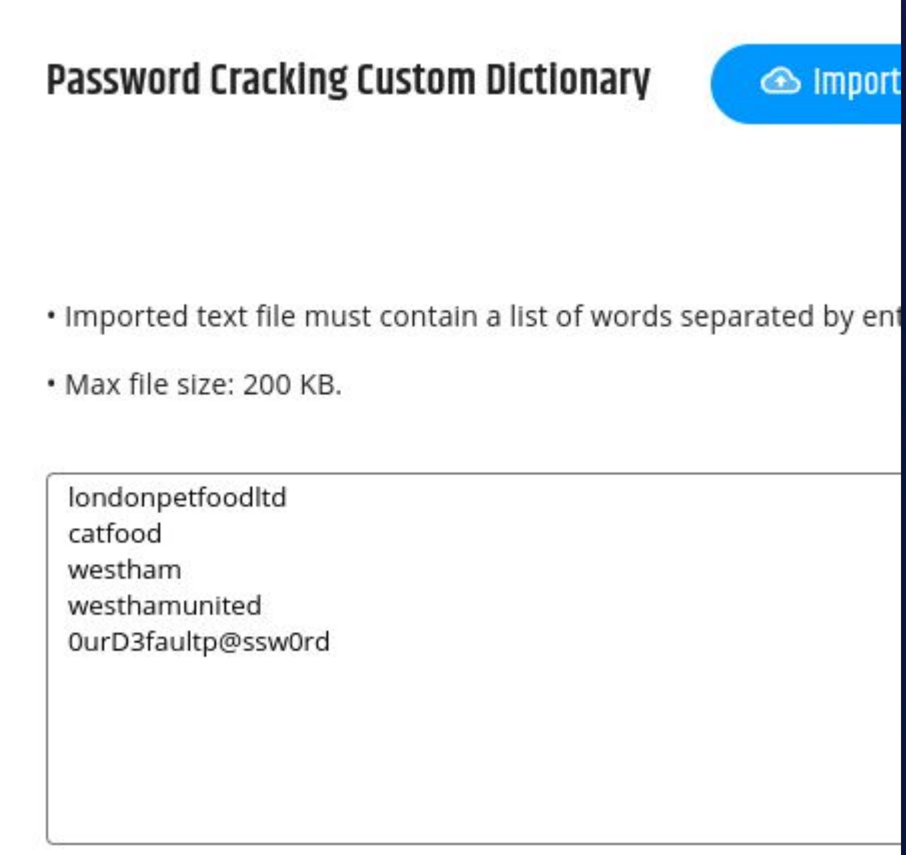
- Imported text file must contain a list of words separated by enter and up to 200,000 characters.
- Max file size: 200 KB.

Enter a list of words separated by enter.

# Custom Password Dictionary

**London Pet food Ltd.**
**Stratford, East London**

```
londonpetfoodltd
catfood
westham
westhamunited
0urD3faultp@ssw0rd
```



Password Cracking Custom Dictionary

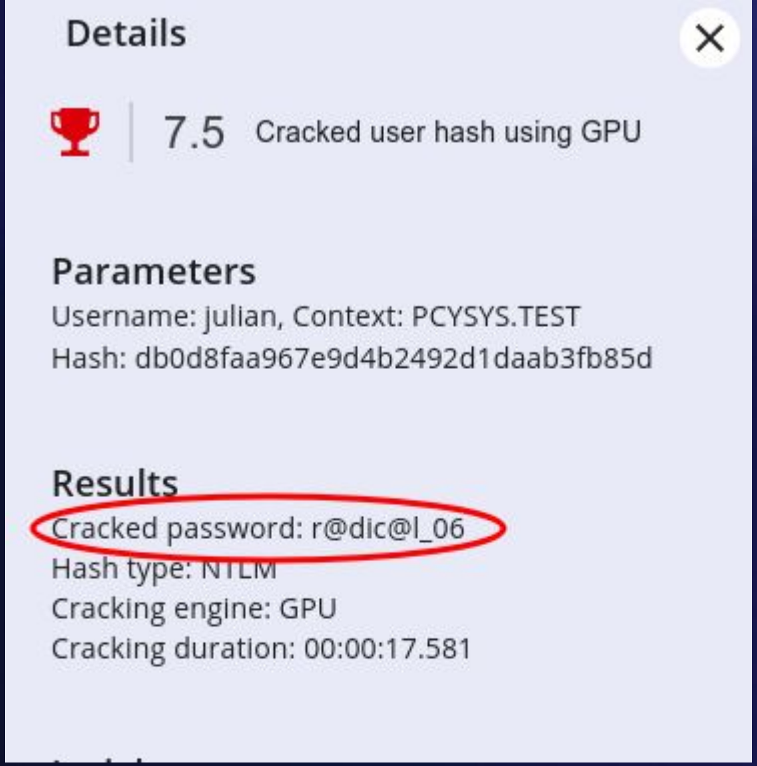
- Imported text file must contain a list of words separated by ent
- Max file size: 200 KB.

```
londonpetfoodltd
catfood
westham
westhamunited
0urD3faultp@ssw0rd
```

# What kind of results do we get?

# The Results

- Shows unique cracked passwords



Details

7.5 Cracked user hash using GPU

**Parameters**

Username: julian, Context: PCYSYS.TEST
Hash: db0d8faa967e9d4b2492d1daab3fb85d

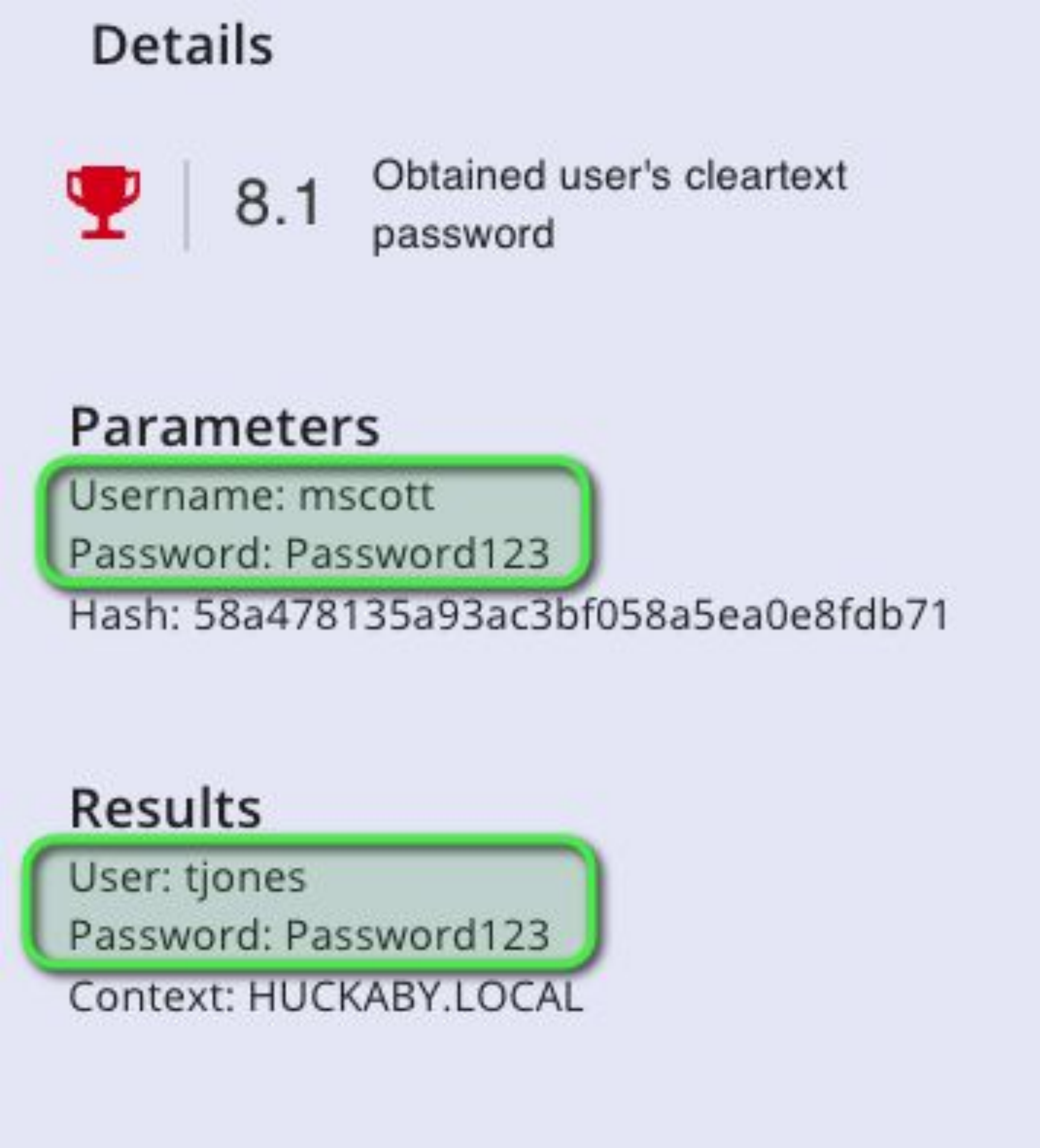
**Results**

Cracked password: r@dic@l_06
Hash type: NTLM
Cracking engine: GPU
Cracking duration: 00:00:17.581

PENTERA

# The Results

- Shows unique cracked passwords
- Shows re-used passwords



Details

🏆 8.1 Obtained user's cleartext password

Parameters

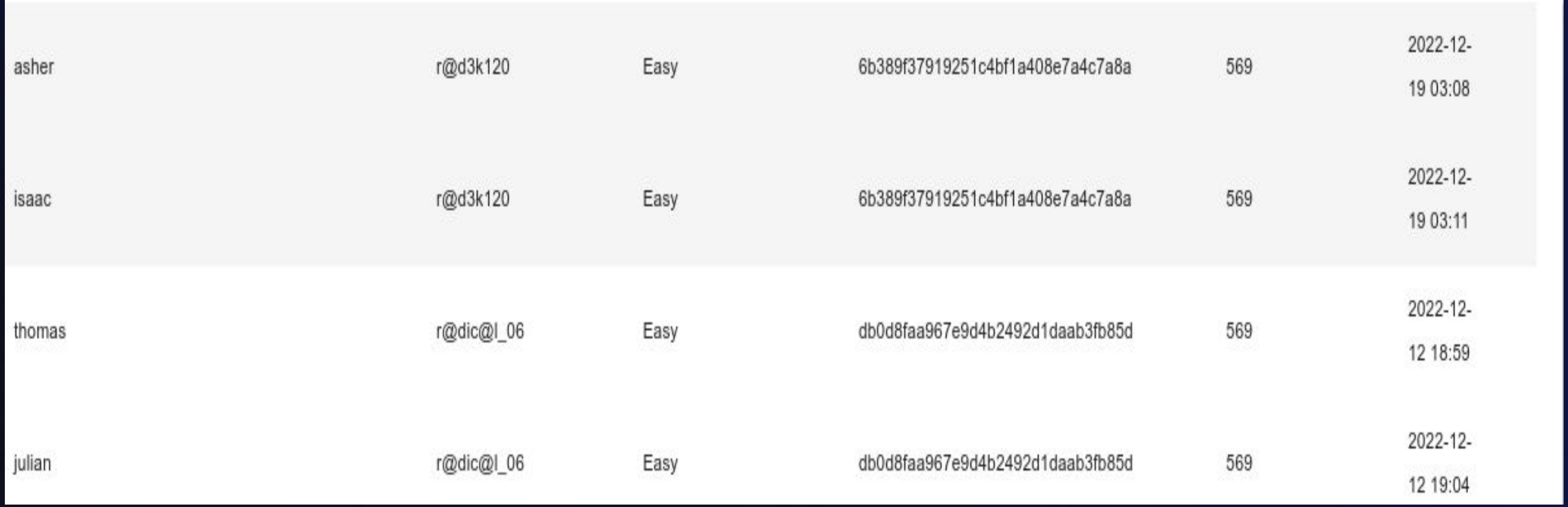
Username: mscott
Password: Password123
Hash: 58a478135a93ac3bf058a5ea0e8fdb71

Results

User: tjones
Password: Password123
Context: HUCKABY.LOCAL

# The Results

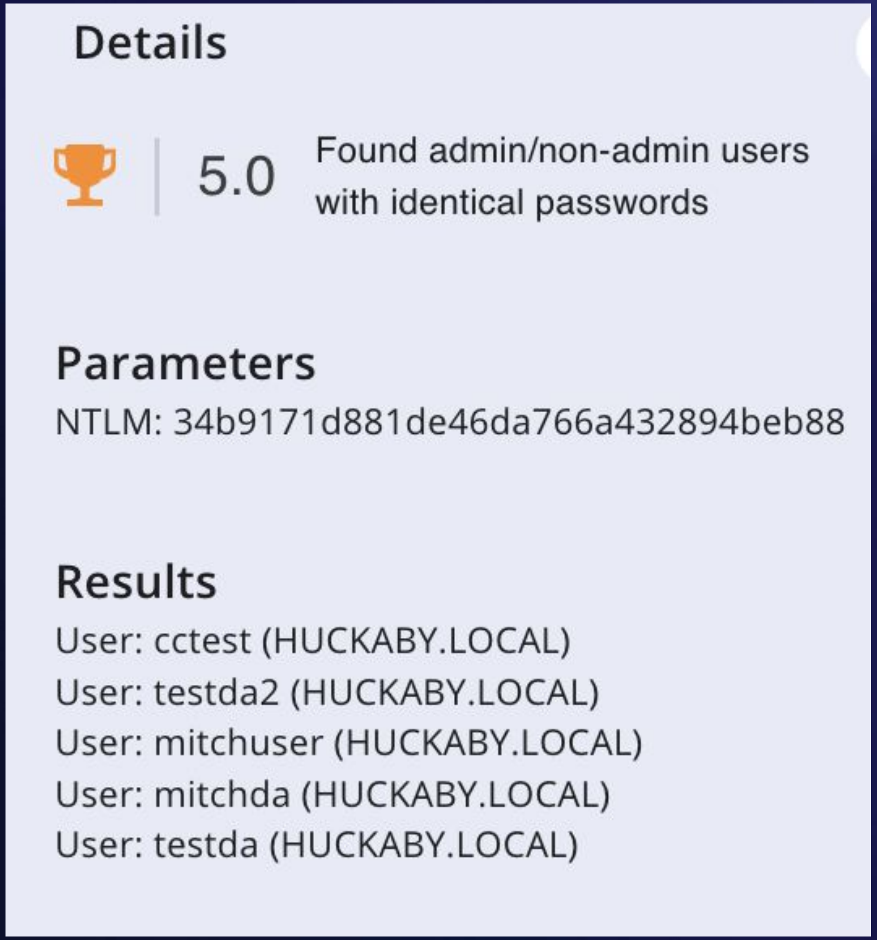
- Shows unique cracked passwords
- Shows re-used passwords



| | | | | | |
|---|---|---|---|---|---|
| asher | r@d3k120 | Easy | 6b389f37919251c4bf1a408e7a4c7a8a | 569 | 2022-12-19 03:08 |
| isaac | r@d3k120 | Easy | 6b389f37919251c4bf1a408e7a4c7a8a | 569 | 2022-12-19 03:11 |
| thomas | r@dic@l_06 | Easy | db0d8faa967e9d4b2492d1daab3fb85d | 569 | 2022-12-12 18:59 |
| julian | r@dic@l_06 | Easy | db0d8faa967e9d4b2492d1daab3fb85d | 569 | 2022-12-12 19:04 |

# The Results

- Shows unique cracked passwords
- Shows re-used passwords
- Shows re-use amongst admins & non-admins



## Details

5.0 Found admin/non-admin users with identical passwords

## Parameters

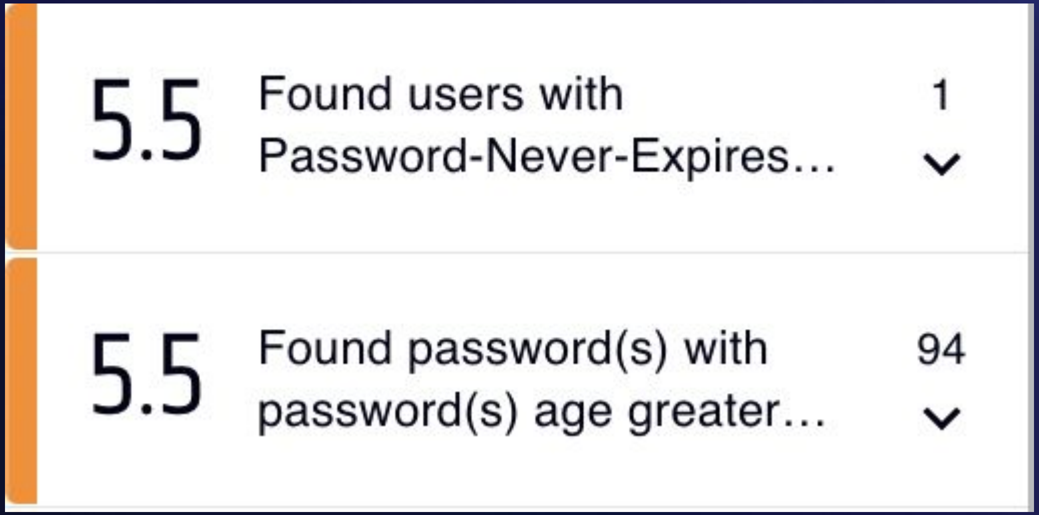
NTLM: 34b9171d881de46da766a432894beb88

## Results

User: cctest (HUCKABY.LOCAL)
User: testda2 (HUCKABY.LOCAL)
User: mitchuser (HUCKABY.LOCAL)
User: mitchda (HUCKABY.LOCAL)
User: testda (HUCKABY.LOCAL)

# The Results

- Accounts with outdated passwords
- Accounts with password never expires
- Accounts with passwords not complex enough



5.5 Found users with Password-Never-Expires… 1

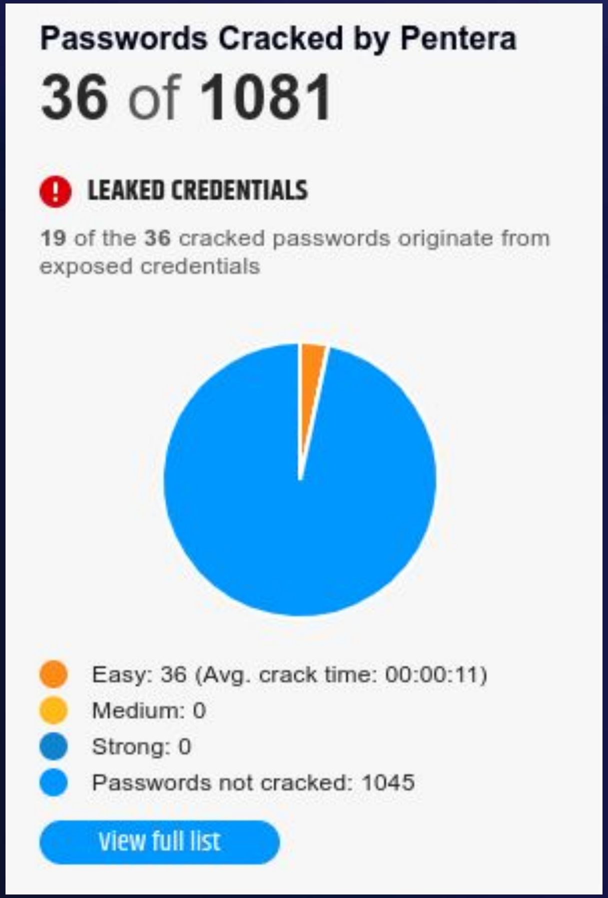
5.5 Found password(s) with password(s) age greater… 94

# Leaked Credentials!

**Real leaks** from dark web, deep web, clear web

- Usernames
- Email addresses
- Cleartext passwords
- Password hashes

**Used & updated automatically**



Passwords Cracked by Pentera

36 of 1081

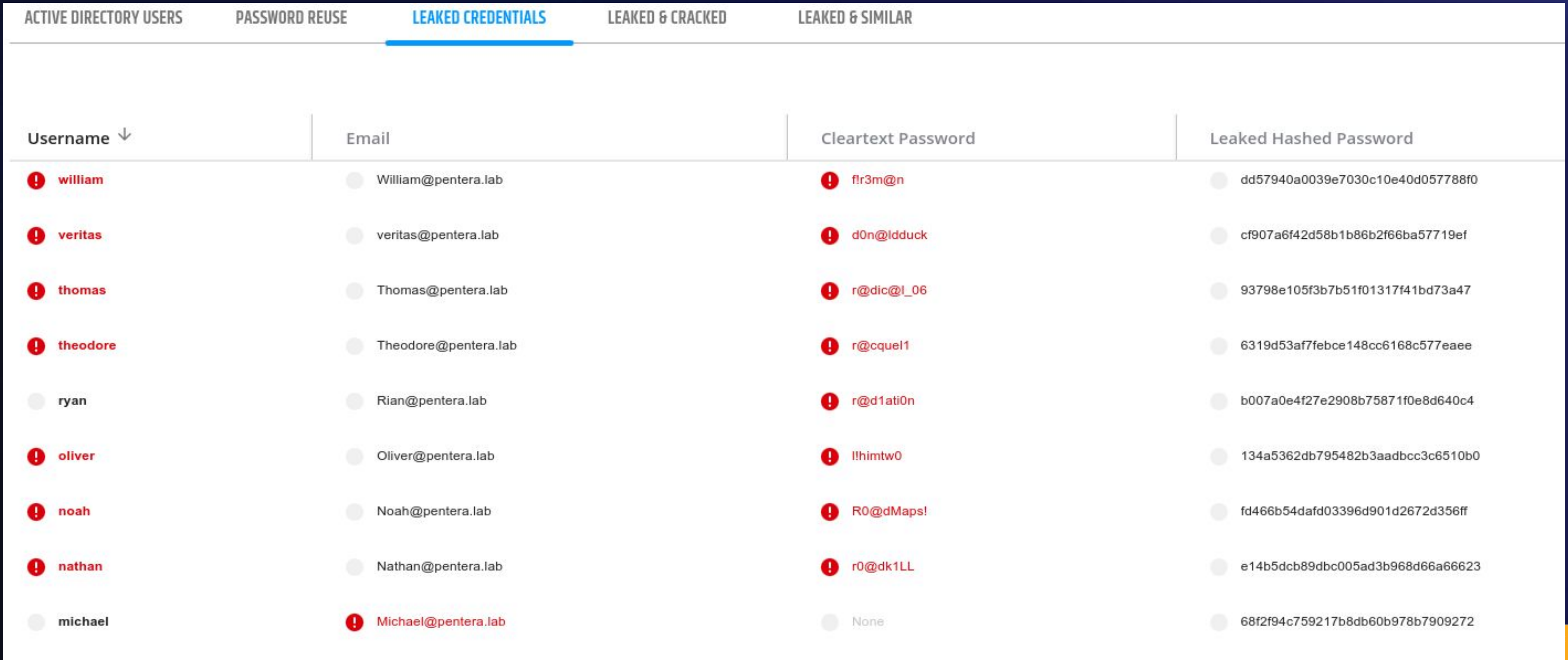
LEAKED CREDENTIALS

19 of the 36 cracked passwords originate from exposed credentials

● Easy: 36 (Avg. crack time: 00:00:11)
● Medium: 0
● Strong: 0
● Passwords not cracked: 1045

PENTERA

# Leaked Credentials!

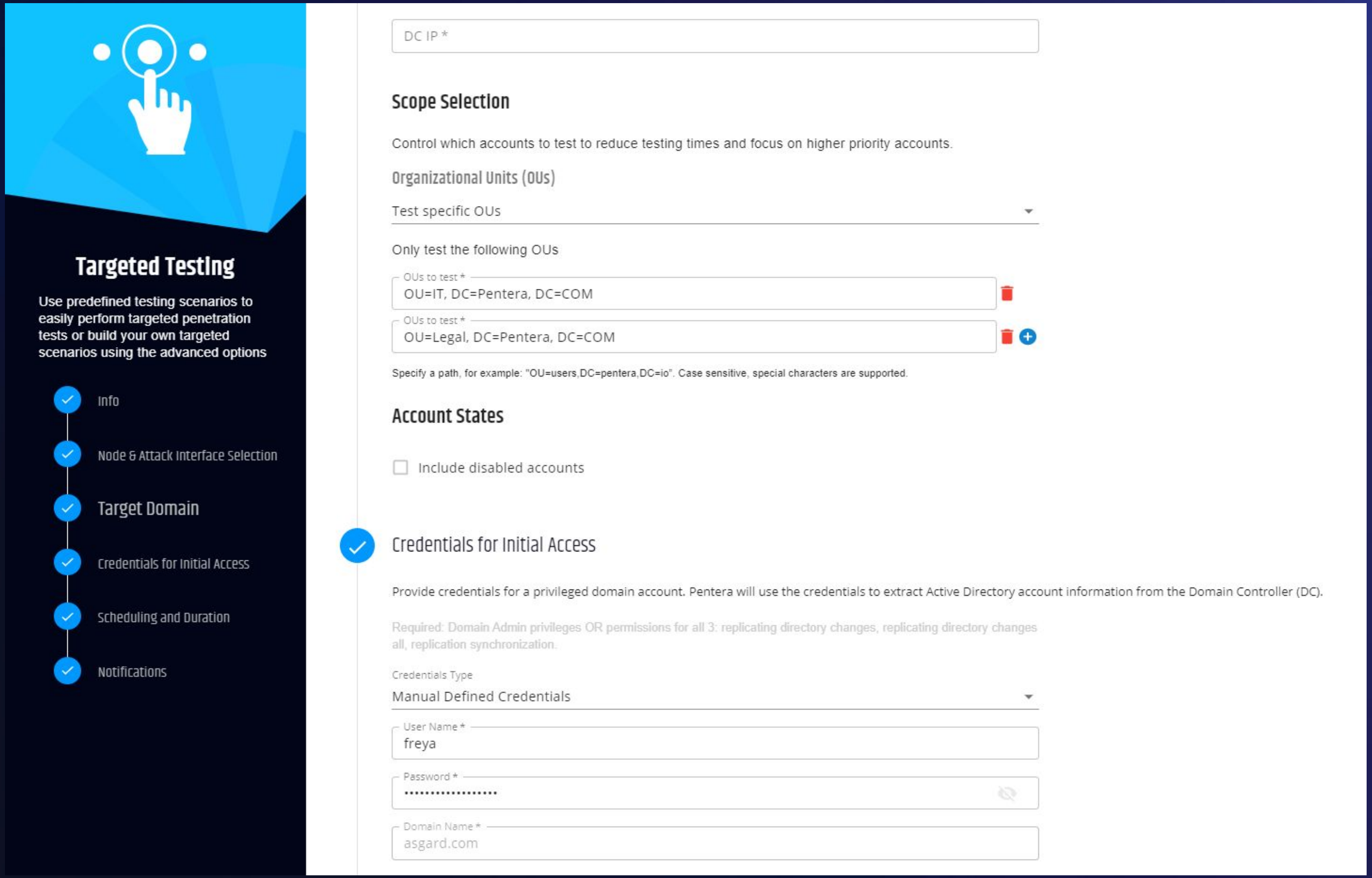


| Username ↓ | Email | Cleartext Password | Leaked Hashed Password |
|---|---|---|---|
| ❗ william | ○ William@pentera.lab | ❗ f!r3m@n | ○ dd57940a0039e7030c10e40d057788f0 |
| ❗ veritas | ○ veritas@pentera.lab | ❗ d0n@ldduck | ○ cf907a6f42d58b1b86b2f66ba57719ef |
| ❗ thomas | ○ Thomas@pentera.lab | ❗ r@dic@l_06 | ○ 93798e105f3b7b51f01317f41bd73a47 |
| ❗ theodore | ○ Theodore@pentera.lab | ❗ r@cquel1 | ○ 6319d53af7febce148cc6168c577eaee |
| ○ ryan | ○ Rian@pentera.lab | ❗ r@d1ati0n | ○ b007a0e4f27e2908b75871f0e8d640c4 |
| ❗ oliver | ○ Oliver@pentera.lab | ❗ l!himtw0 | ○ 134a5362db795482b3aadbcc3c6510b0 |
| ❗ noah | ○ Noah@pentera.lab | ❗ R0@dMaps! | ○ fd466b54dafd03396d901d2672d356ff |
| ❗ nathan | ○ Nathan@pentera.lab | ❗ r0@dk1LL | ○ e14b5dcb89dbc005ad3b968d66a66623 |
| ○ michael | ❗ Michael@pentera.lab | ○ None | ○ 68f2f94c759217b8db60b978b7909272 |

# Scope selection

- Entire domain
- Entire domain & exclude specific OUs
- Specific OUs

Include/exclude disabled accounts



## Targeted Testing

Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options

- ✓ Info
- ✓ Node & Attack Interface Selection
- ✓ Target Domain
- ✓ Credentials for Initial Access
- ✓ Scheduling and Duration
- ✓ Notifications

DC IP *

### Scope Selection

Control which accounts to test to reduce testing times and focus on higher priority accounts.

Organizational Units (OUs)

Test specific OUs

Only test the following OUs

OUs to test *: OU=IT, DC=Pentera, DC=COM

OUs to test *: OU=Legal, DC=Pentera, DC=COM

Specify a path, for example: "OU=users,DC=pentera,DC=io". Case sensitive, special characters are supported.

### Account States

□ Include disabled accounts

### ✓ Credentials for Initial Access

Provide credentials for a privileged domain account. Pentera will use the credentials to extract Active Directory account information from the Domain Controller (DC).

Required: Domain Admin privileges OR permissions for all 3: replicating directory changes, replicating directory changes all, replication synchronization.

Credentials Type: Manual Defined Credentials

User Name *: freya

Password *: ••••••••••••••••••

Domain Name *: asgard.com

# Summary

- Cracking passwords is important (and fun)
- Extensive insights on password policy strength
- Leaked Credentials are a real threat

PENTERACON 2023

# Start cracking your passwords!

**Highest %: Exclusive Swag + $500 Amazon voucher**

**By 24th June 2023:**

**marcel@pentera.io**

# Thank you!