Gaining Access:
More Cracking Methods

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

https://t.me/learningnets

NTLM Authentication

https://t.me/learningnets

How It Works

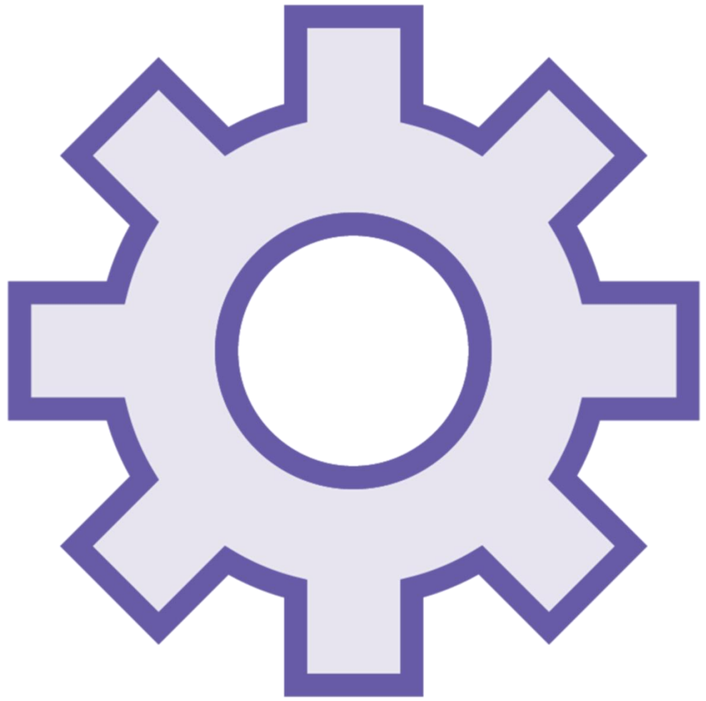
NTLM is used when:

There is no Kerberos trust between two different forests

Authentication is attempted by IP

If one or both systems are not in the same domain

If your firewall is blocking Kerberos ports



https://t.me/learningnets

How It Works

How it's used

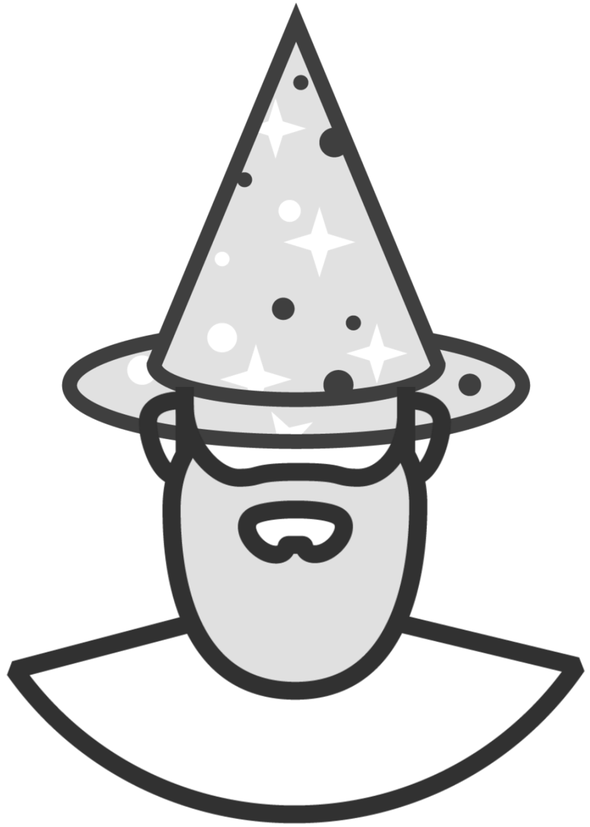
Challenge response algorithm

Passwords are not transmitted

V1 came with NT

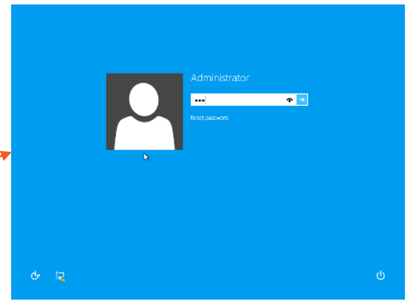
- Just say NO!

V2 came with NT SP4



https://t.me/learningnets

The Process



Admin:500:5837
39372495373948
573739282749

Domain Controller

Bb e8 pdq rsvp8
abc

Bb e8 pdq rsvp8
abc

Admin:500:5837
39372495373948
573739282749

https://t.me/learningnets

Kerberos Authentication

https://t.me/learningnets

The 3-headed Dog (Fluffy)

Better, stronger, faster

Ticket based

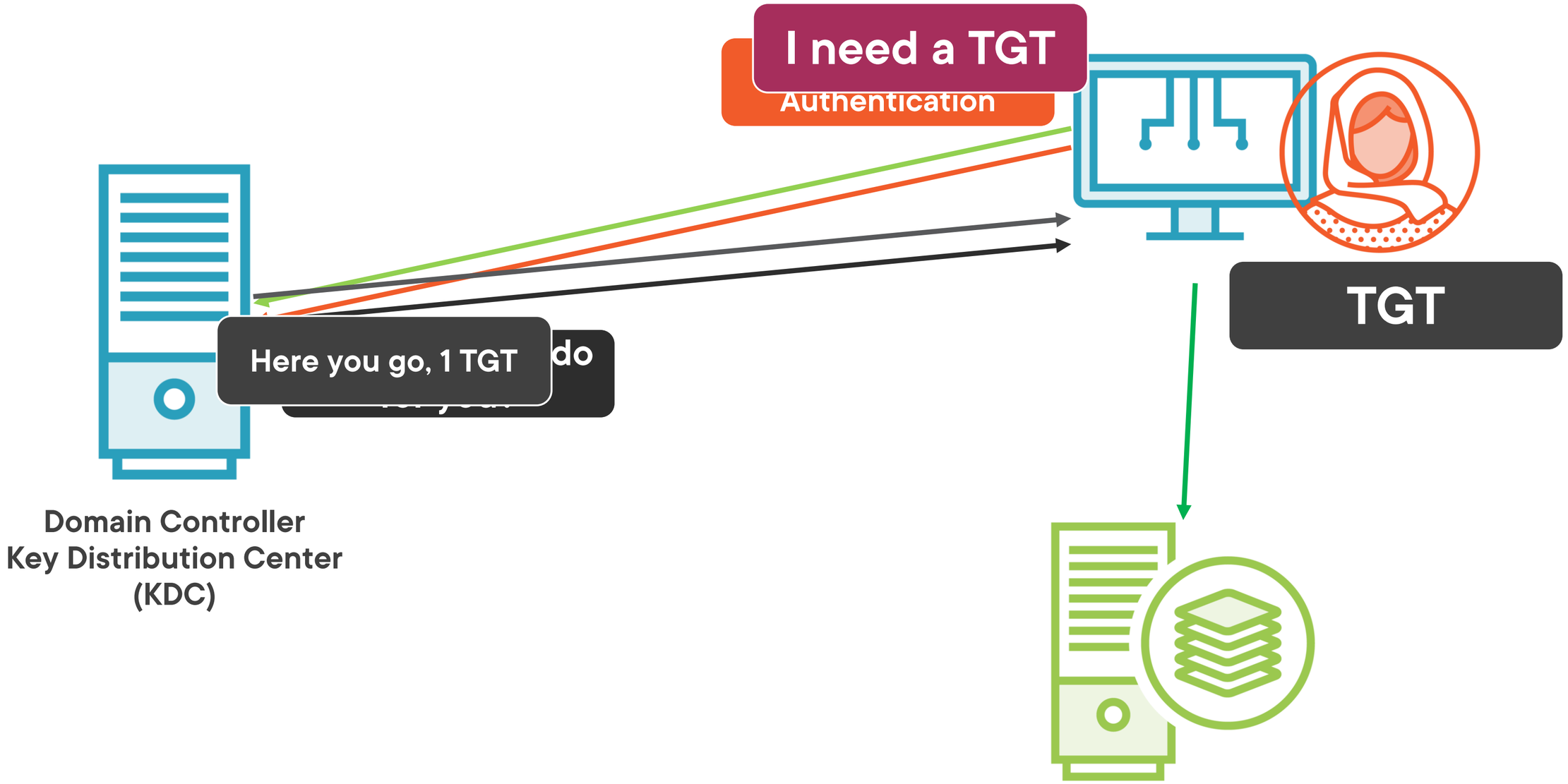
Fast

Avoids transmitting passwords

Time based (Remember the PDC?)

https://t.me/learningnets

Fluffy in Use

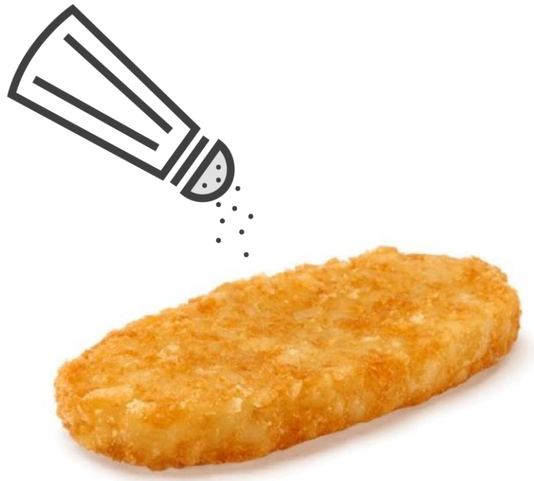


https://t.me/learningnets

Salting

https://t.me/learningnets

My Hash Needs Salt



Append or prepending random strings

Done before hashing

Prevents duplicate hashes

Unique to each password

```
hash(“BatmanRules”) =2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
hash(“BatmanRules”) =2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

hash(“BatmanRules” + “Qiduemx313) =9e209040c863f84a31e719795b2577523954739fe5ed3b58a75cff2127075ed1
hash(“BatmanRules” + “38dkeWqod2)=d1d3ec2e6f20fd420d50e2642992841d8338a314b8ea157c9e18477aaef226ab
```

https://t.me/learningnets

Hash + Username

https://t.me/learningnets

[1,2,3]

https://t.me/learningnets

https://t.me/learningnets

Rainbow Tables and Other Options

https://t.me/learningnets

Somewhere Over the Rainbow...

Precomputed hash tables

Huge files

SSD & cloud computing

https://t.me/learningnets

Lookup Tables

Does any hash equal:
5f4dcc3b5aa765d61d8327deb882cf99:
FOUND: password5

What about:
6cbe615c106f422d23669b610b564800: not in database

Can I get a:
630bf032efe4507f2c57b280995925a9:
FOUND: letMEin12

Here's another one:
386f43fab5d096a7a66d67c8f213e5ec:
FOUND: mcd0nalds

Last one, I swear:
d5ec75d5fe70d428685510fae36492d9:
FOUND:p@ssw0rd!

https://t.me/learningnets

Reverse Lookup Tables

Searching for hash (apple) in users' hash list...
: Matches [alice3, 0bob0, charles8]

Searching for hash(blueberry) in users' hash list...
: Matches [usr10101, timmy, john91]

Searching for hash (letmein) in users' hash list...
: Matches [wilson10, dragonslayerX, joe1984]

Searching for hash (s3cr3t) in users' hash list...
: Matches [bruce19, knuth1337, john87]

Searching for hash (z@29hjja) in users' hash list...
: No users used this password

https://t.me/learningnets

You Gotta Love Technology

GPUs LOVE cracking passwords

Setup: 5 systems/25 AMD GPU/10Gbp

- 348 Billion NTLM passwords per second!
  - 14 character: hacked in 6 mins
- 180 Billion MD5 password per second!
  - 63 Billion per second is using SHA1

https://t.me/learningnets

Demo

Creating a Rainbow Table

https://t.me/learningnets

Password Recovery Tools

https://t.me/learningnets

Top Tools to Know

John the Ripper

hashcat

THC-Hydra

Medusa

https://t.me/learningnets

Countermeasures

- **Use GPO to turn off LLMNR and NetBIOS over TCP/IP**
- **Vindicate / got-responded**
- **Passwords**

https://t.me/learningnets

Demo

Cain & Abel

https://t.me/learningnets

Demo

L0phtCrack

https://t.me/learningnets

Demo

John the Ripper

https://t.me/learningnets

Learning Check

https://t.me/learningnets

Learning Check

- Authentication by IP
- Kerberos
- Salting
- Isolated system
- Rainbow tables

https://t.me/learningnets

Learning Check

- Reverse lookup table
- GPO settings
- NTLM Authenication
- Passwords
- John-the-Ripper

https://t.me/learningnets

Next Up:

Phase 2: Gaining Access - Escalating Privileges

https://t.me/learningnets