

# Gaining Access: Cracking Passwords

---

## The Issue with Passwords



### **Dale Meredith**

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

[dalemeredith.com](http://dalemeredith.com) | Twitter: [@dalemeredith](https://twitter.com/dalemeredith) | LinkedIn: [dalemeredith](https://www.linkedin.com/in/dalemeredith)

Love is great, but not as a password

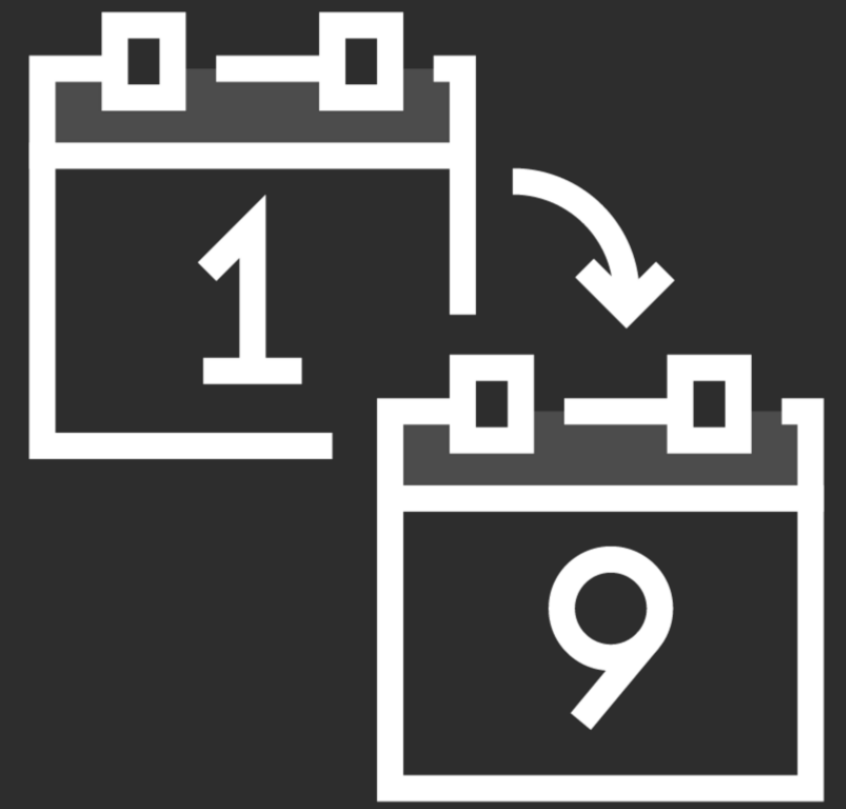
**Matt Mullenweb**

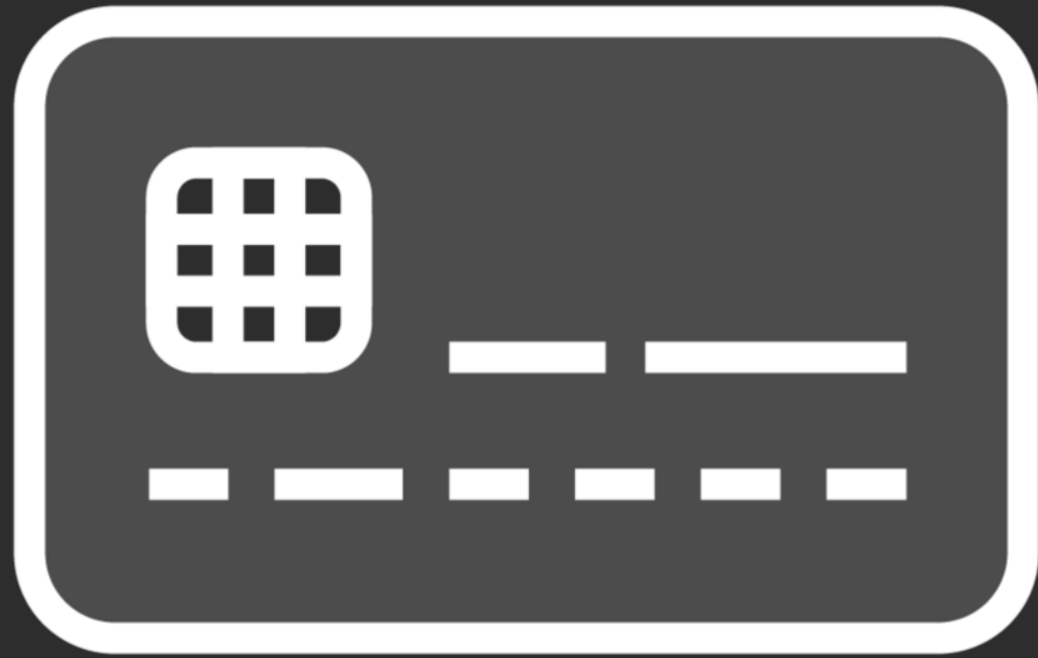
# Issues with Passwords

**Grab locally or while in transit**

**Is there any good reason to crack passwords?**

**Most users pick something they know**





# Complexity

---

# Complexity



**Upper case**



**Lower case**



**Numbers**



**Special characters**

# Be Careful!

Using @,\$,3,0,! Also known as the “Fab-Five”:

Pa\$\$w0rd = You’re not fooling anyone

0penm3up = Yeah, right

L3tm3in = I’m gonna pwn you!

B@tm@n = Although “cool”, won’t fool the Joker!

Demo



**Testing password strength**

# Where Are All the Passwords?

---

# Where Are Passwords Stored?



## Windows

- Local machines: SAM Database
  - C:\windows\system32\config\sam
  - Mounted as HKLM/SAM
  - \* C:\windows\repair
- Active Directory: ntds.dit
  - C:\windows\ntds

## Linux

- Local machines:
  - /etc/shadow

# Where Are Passwords Stored?



## Apple

- `/var/db/dslocal/nods/default/users`
- `<user>.plist =>ShadowHashData Property`

# Oh, So I Just Grab Those Files?

**Contains authentication credentials**

**Stored as “Hash values”**

One way algorithm

You can't reverse it

**Cool. I'm secure then**

Guess again... I can steal it



# Demo

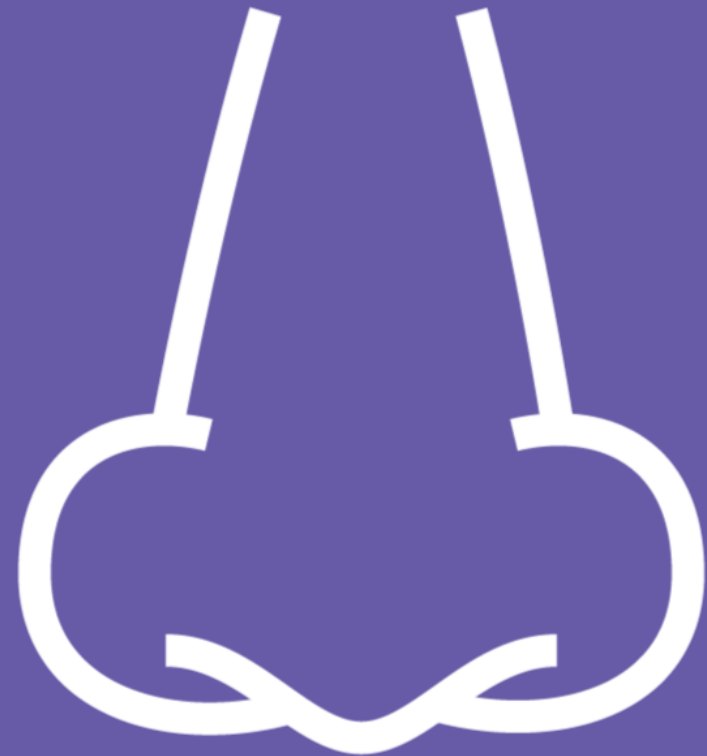


## Looking at the SAM and ntds.dit

# Types of Attacks

---

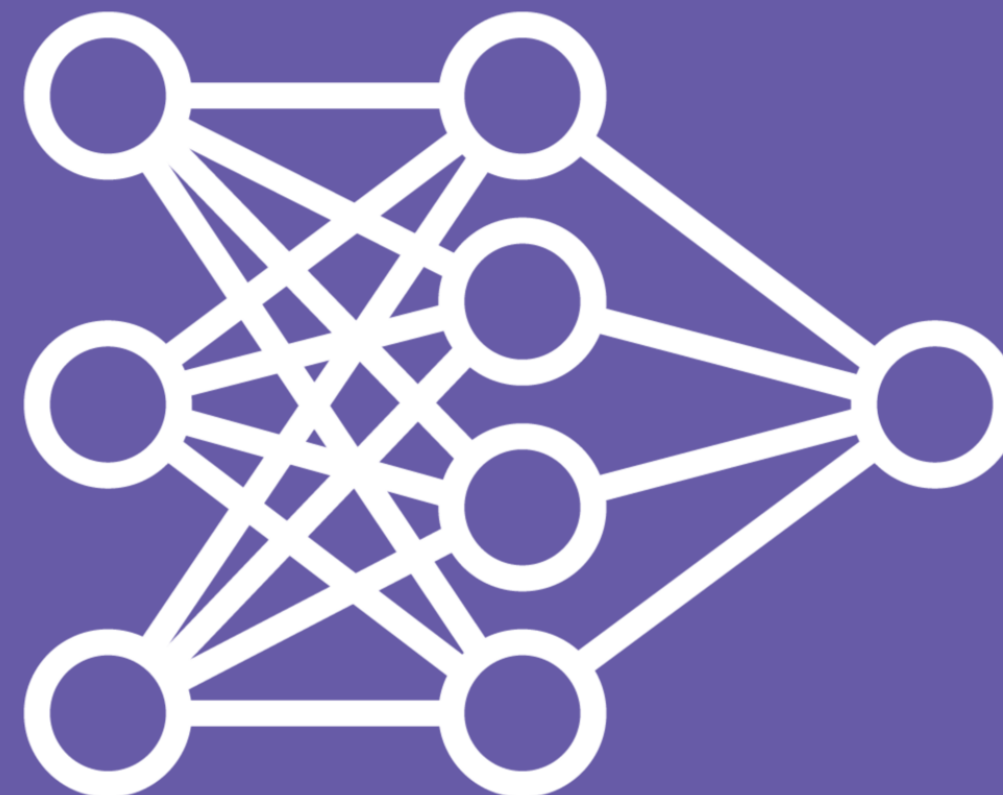
# Passive



# Non-electronic



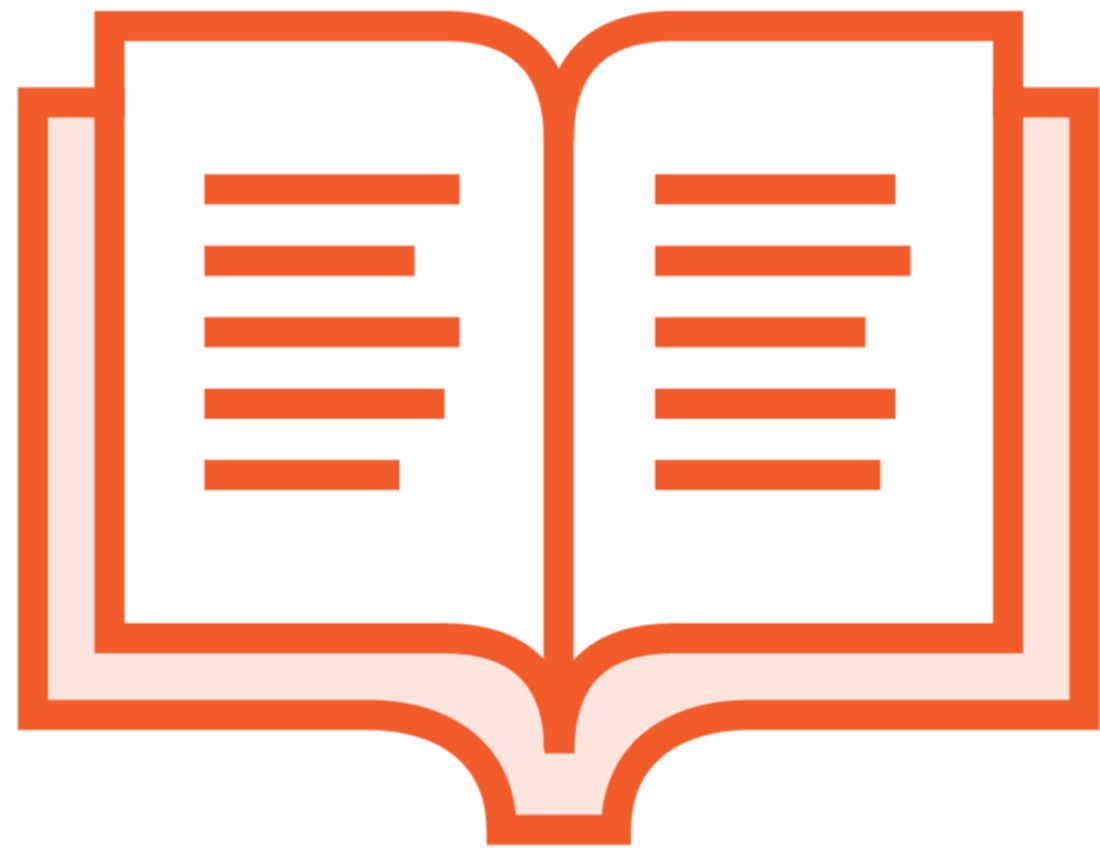
# Offline Attacks



# Active Online Attacks

---

# Dictionary Attacks



**Text file that you can download**

**Languages**

**Subjects**

**Characters**

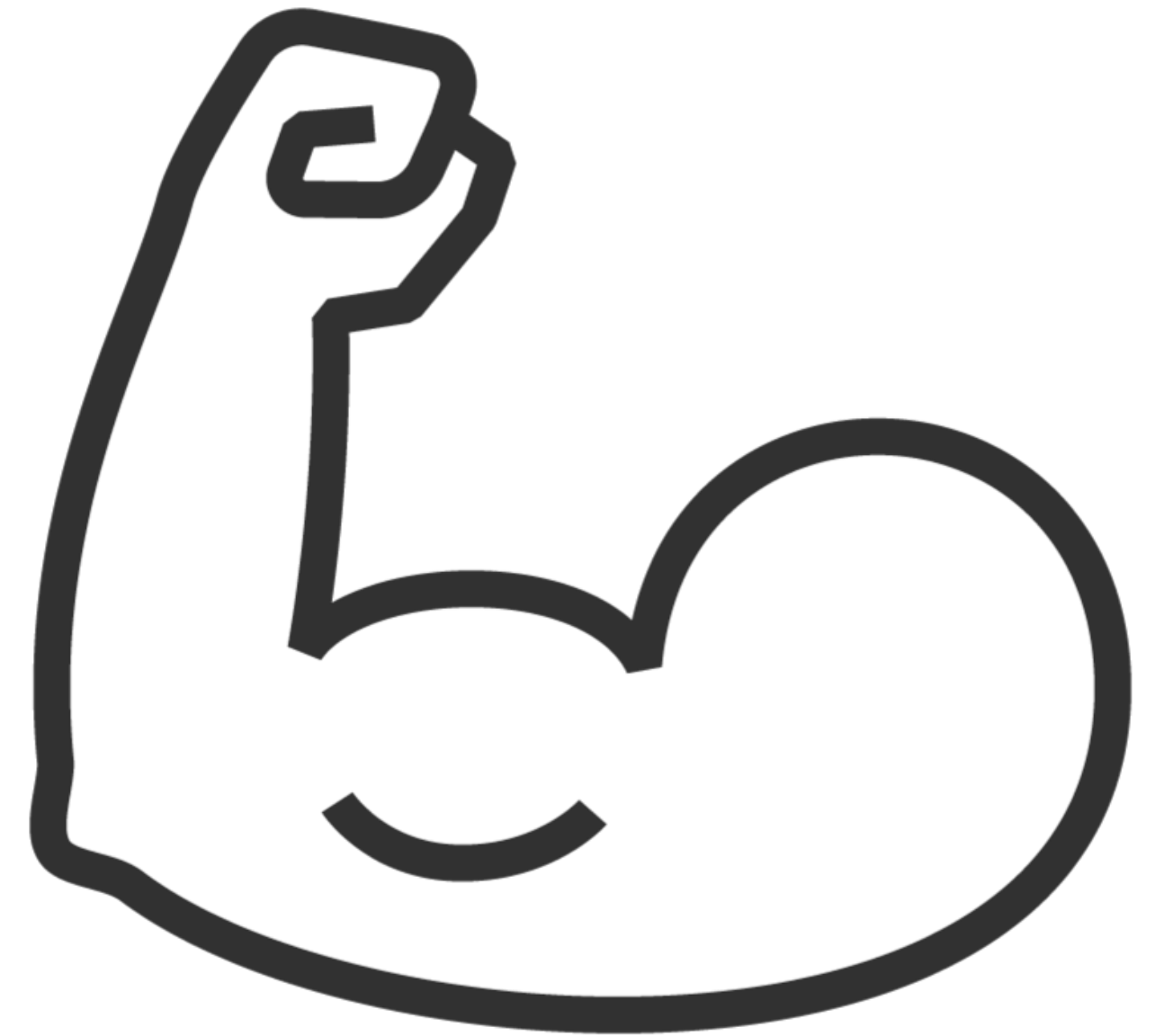
**Famous people, locations, events**

**String manipulation**

Computer = putercom

# Brute-force Attacks

- It does take longer**
- Tries every combination**
- More cycles**
- It's ALWAYS 100% effective**



# Rule Based Attacks



**Remember enumeration?!**

**Use your rules against you!**

8 Characters – Require 2 digits

**Combination of Brute-Force, Dictionary and Syllable Attacks**

# Syllable Attack

**Pass**

**Assp**

**Sspa**

**Spas**

**Pssa**

**Ssap**

**Combines Dictionary and Brute-Force**

**Uses every possible arrangement of every entry in the dictionary**

# Hybrid Attack

Using a dictionary

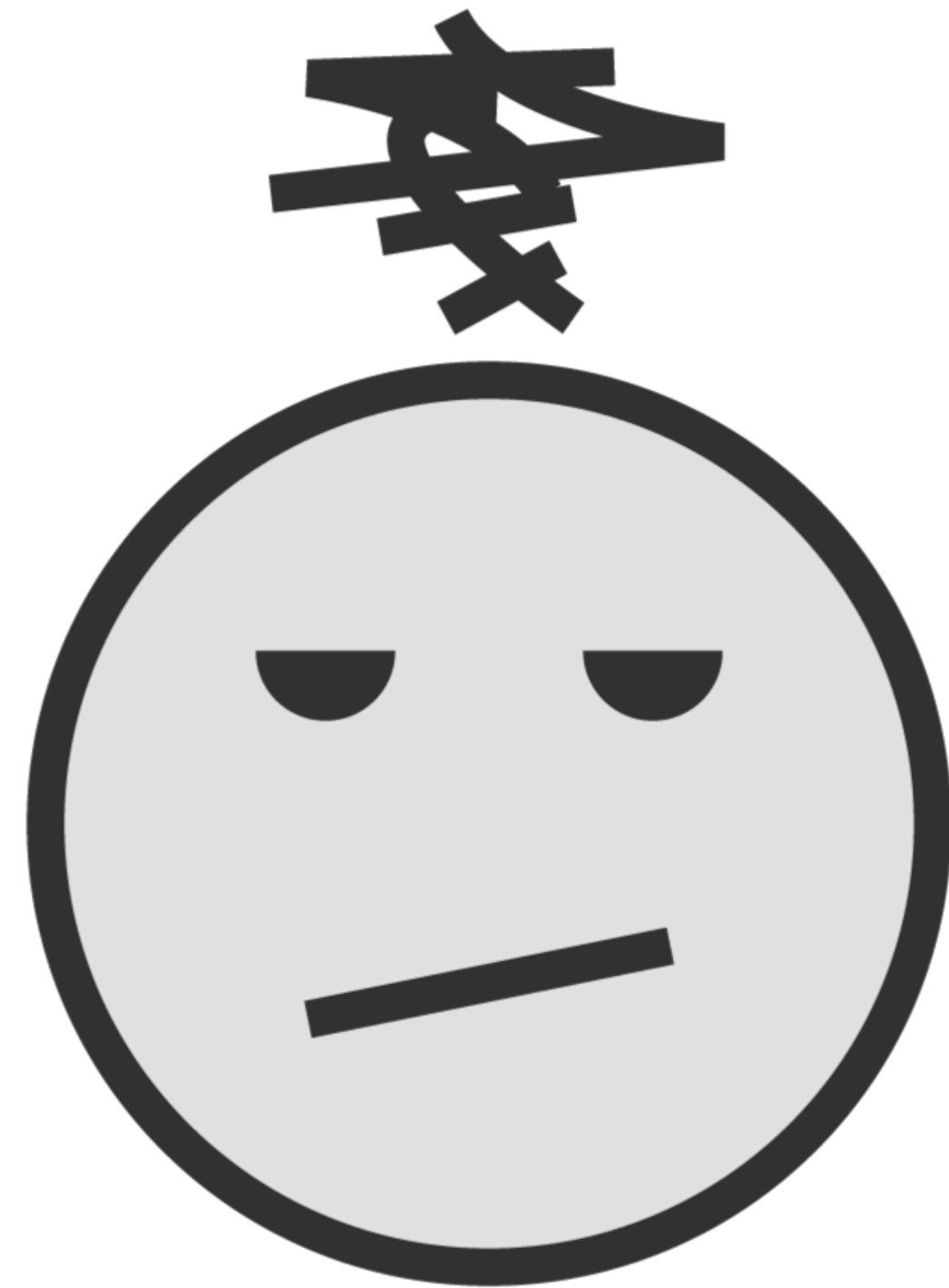
Based on users being complacent

Tries variations by including numbers & special characters

Batman

Batman1

Batman2



# Guessing




## Find a user

- List of possible
- Rank them
- Type away

# Default Passwords

**Main Menu**

- Home
- Dlink Password
- Netgear Password
- Linksys Default Password
- Westell Password
- Netopia Password
- SMC Password
- TP Link Password
- Other Password
- 2Wire Default Password
- Belkin Password
- Motorola Password
- Zoom Password
- ZyXEL Password
- Dell Password
- ZTE Password
- SpeedTouch Password
- SAGEM Password
- Aztech Password
- Canon Default Password
- Siemens Password
- Airlink Default Password
- Polycom Password
- Yealink Password
- Wapopia Blog

Netgear WNR854T password  
User Rating:  / 6  
Poor      Best




Default Netgear Password

WNR854T is a RangeMax NEXT Wireless-N Router from Netgear it has a built-in 4-Port Gigabit Switch

◆ Access IP = 192.168.0.1  
Default User = admin  
Default Password = password

**Comments**

If the password does not work or if you have some updated information then post here

 Wendelboe, Fred 0  

abc

Wednesday 09 June 2010, 21:49

PO

<https://www.fortypoundhead.com>

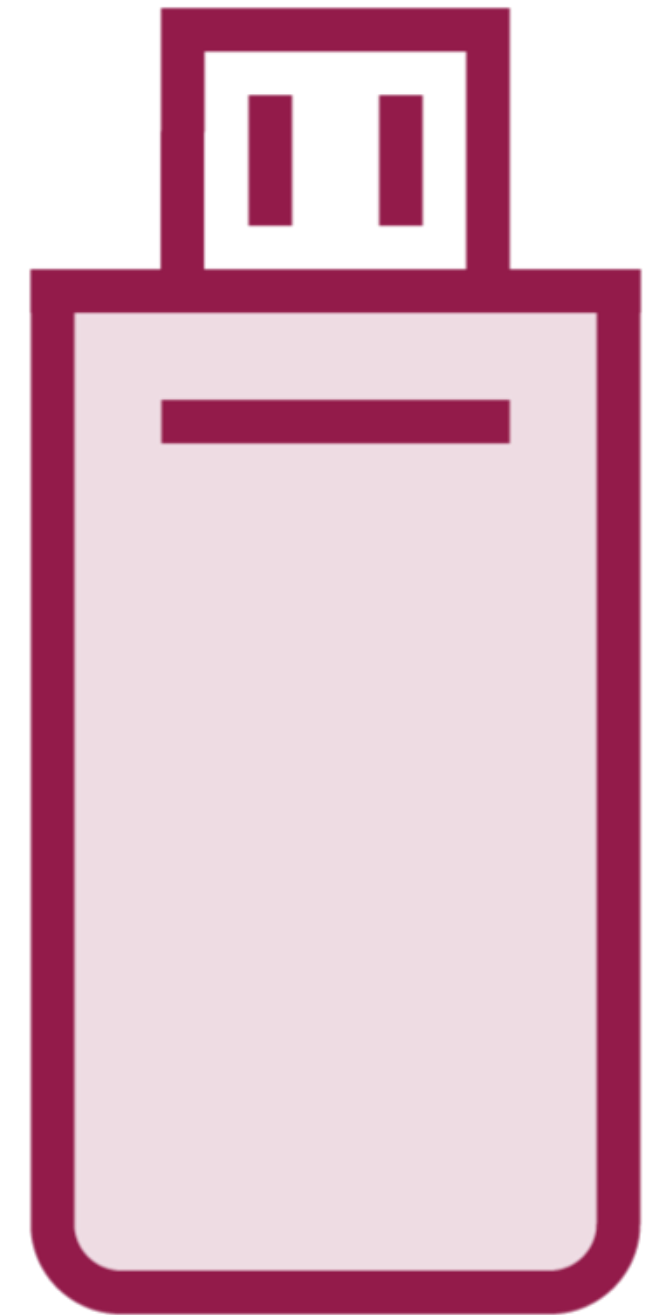
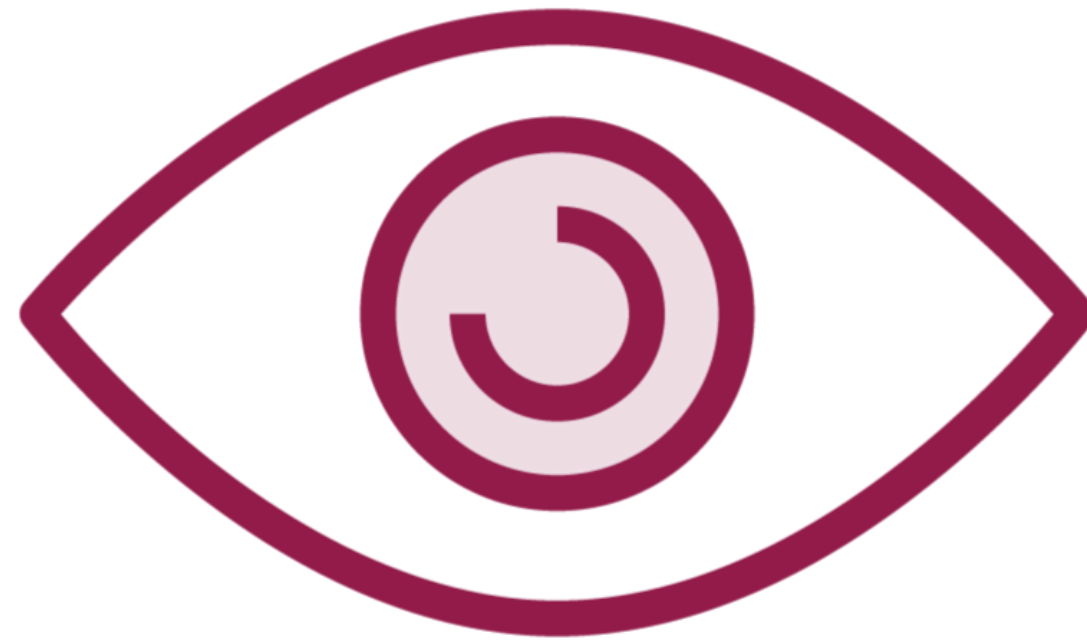
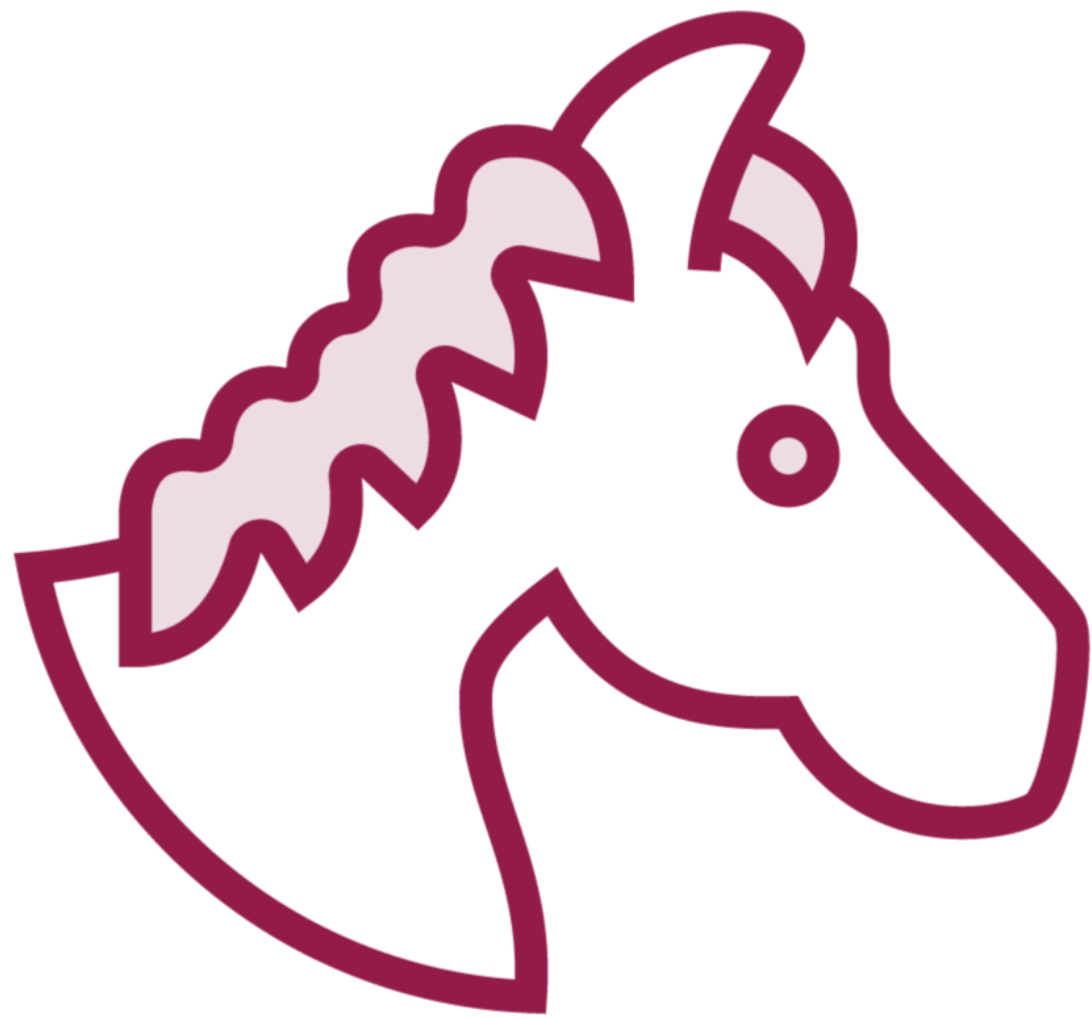
<https://cirt.net>

<https://www.defaultpasswords.us>

<https://datarecovery.com/rd/default-passwords/>

<https://t.me/learningnets>

# Software/Hardware Based



# The Hash and Attacks

---

# Hash in the Wild

LM Hash/NTLM stores passwords up to 14 characters

All letters are converted to UPPER case

Padded with blank characters to fill out all 14 characters

Then split into 7 character strings

Each 7 character string is then encrypted and combined back

**Password=**

• BatmanRules

**Converted to Upper**

• BATMANRULES

**Padded**

• BATMANRULES---

**Split**

• BATMANR ULES---

# Hash in the Wild

Each 7 character string is then encrypted and combined back

**Encrypted**

- BATMANR= 86D8D0AEB8D112F8
- ULES--- = F9954FC9DF57E012

**Combined**

- 86D8D0AEB8D112F8F9954FC9DF57E012

# Add NTLM and Stored As:

**Bwayne:1005:86D8D0AEB8D112F8F9954FC9DF57E012:ED7B273FDE21FFE559AC8D1B9D3729B  
C:::**

**Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E17D93985B  
F:::**

**Guest:501:NOPASSWORD\*\*\*\*\*:NOPASSWORD\*\*\*\*\*:::**

## NOTE:

Any hash that ends with: AAD3B435B51404EE means something to you:

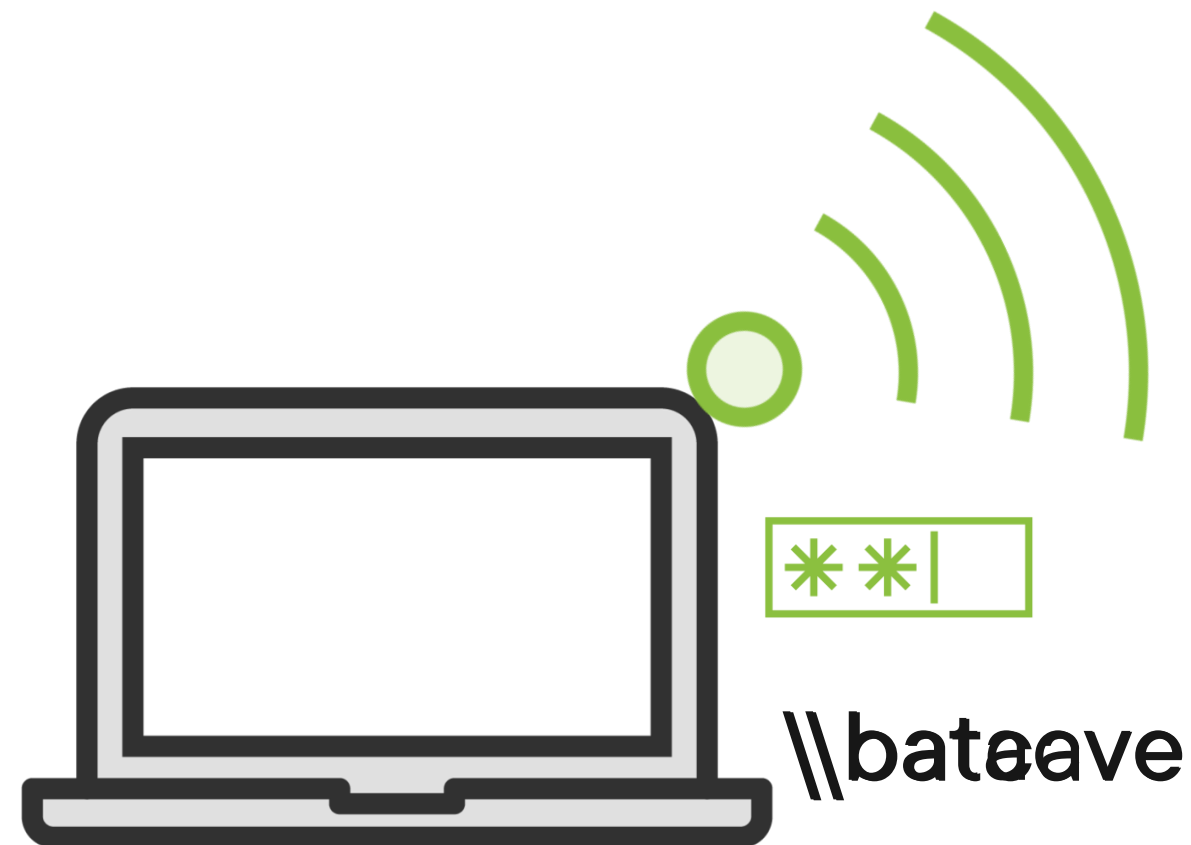
5D567324BA3CCEF8 AAD3B435B51404EE = The last seven characters are blank

Any password over 14 characters: the LM Hash value is “dummied” with AAD3B435B51404EE  
AAD3B435B51404EE

# Hash Injection



# LLMNR/NBT-NS Poisoning



Why yes, I am `\\batacve`



# Demo



## Responder

# Learning Check

---

# Learning Check



**Ntds.dit**



**/etc/shadow**



**SAM**



**<user>.plist**



**AAD3B435B51404EE**



# Learning Check



**Non-electronic**



**Dictionary**



**Brute Force**



**C:\windows\system32\config\**



**Offline attack**



Up Next:

Gaining Access: More Cracking Methods

---