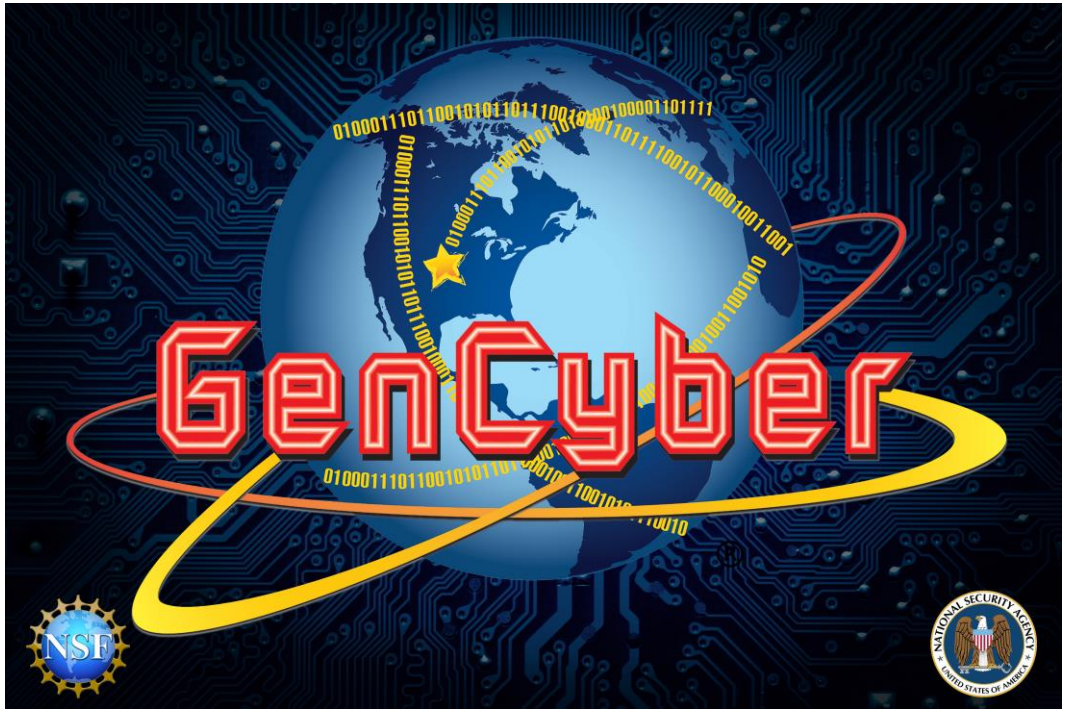


Password Auditing Lab

Wednesday Afternoon

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Authentication and Authorization

- Authenticate – verify ID (you are who you say you are)
  - Something you know (password)*
  - Something you have (SMS phone, RSA key)
  - Something you are (biometrics like fingerprint)
- Authorize – grant access to resources based on authentication
  - R-BAC – based on your role

Password Auditing Lab Objectives

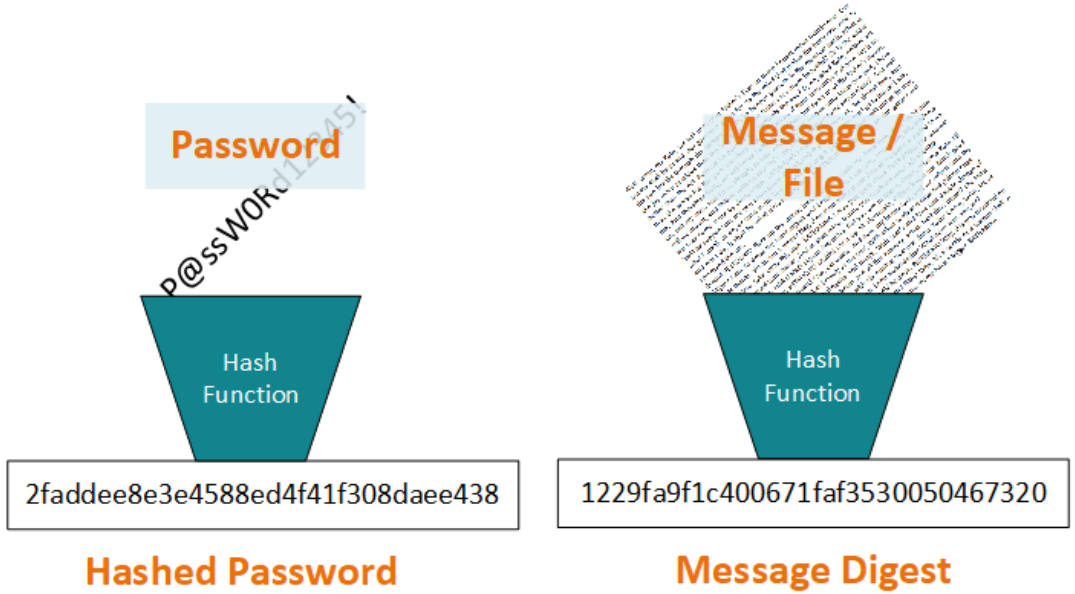
- Understand what makes weak and strong passwords
- Demonstrate creating hashes from plain text passwords
- Demonstrate how to use password cracking tools
- Understand the difference between dictionary and brute force password cracking

Password Auditing*

- Review and learn about password files in Linux
- Using the John the Ripper
  - Free password auditing (cracking) tool
  - Find trivial passwords in a short amount of time
  - Accessible on multiple platforms
    - Can be run from within Metasploit or on its own
  - Takes the entry from salted password hash from `/etc/shadow`:
    - `jsmith:$6$JRF8OgFTYSP1zDeO$2PuYhV7jFxrdY8x.4P73BspAXQZiv2S8Dr.hrFIGNXTWrIt6gdTiwnTr9cTgFurP4NPWT8isXwizoGRqt/iJ./:18659:0:99999:7:::`
    - Reduces it to the password: 12345

- **Hint: be careful where you use the word "hack"*

Background: What is a Hash?



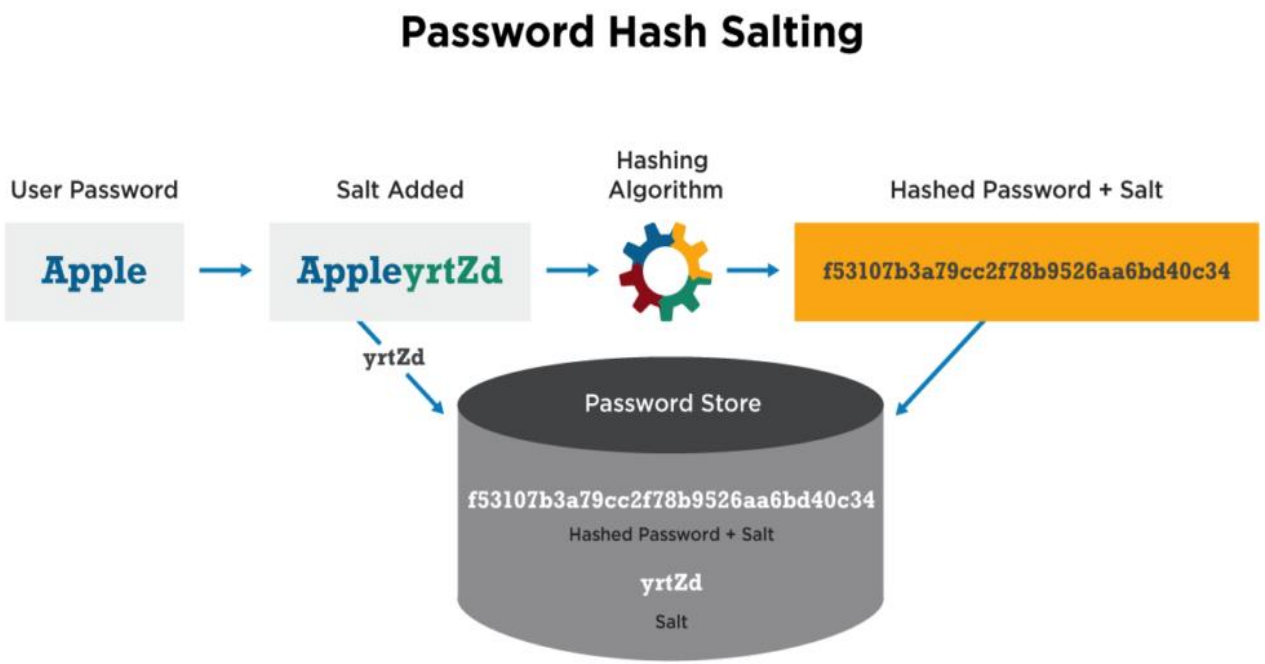
Same cryptographic hash function can be used.

- A hash function maps digital data of arbitrary size to digital data of **fixed size**. The hash is sometimes called a **message digest.**

- A cryptographic hash function is a hash function that is considered practically impossible to reverse (one-way-ness) or find collisions (i.e. two messages with the same hash value)

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Password Hashing with Salt

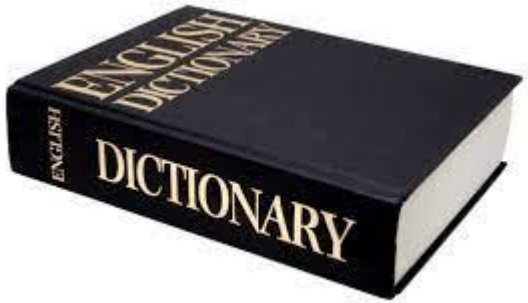


- Passwords aren't stored in plaintext or plain hash, they are salted
- Prevents Rainbow Table Attacks
  - Attack a hashed password in reverse with a table of pre-computed hashes with corresponding passwords
- Adds a layer of security (Defense in Depth)

Image from https://cyberhoot.com/cybrary/password-salting/

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Dictionaries in John



- Not like the dictionary you think of
  - A list of words to try against the password hashes

Image source: https://images2.minutemediacdn.com/image/upload/c_fill,g_auto,h_1248,w_2220/f_auto,q_auto,w_1100/v1555926333/shape/mentalfloss/166091799.jpg

Custom Dictionaries in John

```
root@kali:~/MyCookbook# john --stdout --wordlist=cewl_WackoPicko.txt
WackoPicko
Users
person
unauthorized
Login
Guestbook
Admin
access
password
Upload
agree
Member
posted
personal
responsible
account
illegal
applications
Membership
profile
words: 20  time: 0:00:00:00 DONE (Sun Jun 21 16:25:22 2015)  w/s: 333  current: profile
```

List 1:
cat
dog
panda
racoon
deer

List 2:
cat
dog
panda
racoon
deer
panther
puma
bear
chicken
corgy
welshcorgy
bordercollie
jump
run
audit
goat
horse
palamino
chestnut
…

Image source: https://static.packt-cdn.com/products/9781784392918/graphics/B04027_Ch02_23.jpg

Custom Dictionary

- If know target (person) attacking, what are some good sources for knowledge and possible passwords?

- Even the Linux built in “dictionary”

Defensive Uses of Password Cracking

- Phishing Investigation

To: david@lawfirm.com

Subject: Case Details Attached

Hi David,

I would also like to share with you some additional information regarding this case. It has a password since it is sensitive information.

The password is 284958934.

Regards,

Stacey Adams
29384 Wall Street
Suite 395
New York, NY 1001

LAW FIRM

Defensive Uses of Password Cracking

- Incident Response

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 17 2020 03:07:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # sekurlsa::minidump .\lsass.dmp
Switch to MINIDUMP : '.\lsass.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : '.\lsass.dmp' file for minidump...

Authentication Id : 0 ; 372033 (00000000:0005ad41)
Session           : Interactive from 1
User Name         : Administrator
Domain            : FROG
Logon Server      : AD
Logon Time        : 2021-04-22 11:15:47 PM
SID               : S-1-5-21-2669088251-2370404724-563291528-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : FROG
         * NTLM     : e19ccf75ee54e06b06a5907af13cef42
         * SHA1     : 9131834cf4378828626b1beccaa5dea2c46f9b63
         [00010000] CredentialKeys
         * NTLM     : e19ccf75ee54e06b06a5907af13cef42
         * SHA1     : 9131834cf4378828626b1beccaa5dea2c46f9b63
```

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Defensive Uses of Password Cracking

- Password strength auditing

```
Account stats for: domain.local
  Disabled users ____________________________________________________  418 of  5164 (8%)
  Expired users _____________________________________________________   67 of  5164 (1%)
  Active users unused in 1 year _____________________________________  787 of  4679 (17%)
  Active users unused in 90 days ____________________________________ 1240 of  4679 (27%)
  Active users which do not require a password ______________________  156 of  4679 (3%)
  Active users with non-expiring passwords __________________________ 3907 of  4679 (84%)
  Active users with password unchanged in 1 year ____________________ 1006 of  4679 (22%)
  Active users with password unchanged in 90 days ___________________ 1400 of  4679 (30%)
  Active users with Administrator rights ____________________________   63 of  4679 (1%)
  Active users with Domain Admin rights _____________________________   54 of  4679 (1%)
  Active users with Enterprise Admin rights _________________________    0 of  4679 (0%)

  Disabled computer accounts ________________________________________   86 of  1414 (6%)

Password stats for: domain.local
  Active users using LM hashing _____________________________________   40 of  4679 (1%)
  Active users with duplicate passwords _____________________________ 2312 of  4679 (49%)
  Active users with password stored using reversible encryption ______ 4666 of  4679 (100%)
```

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS