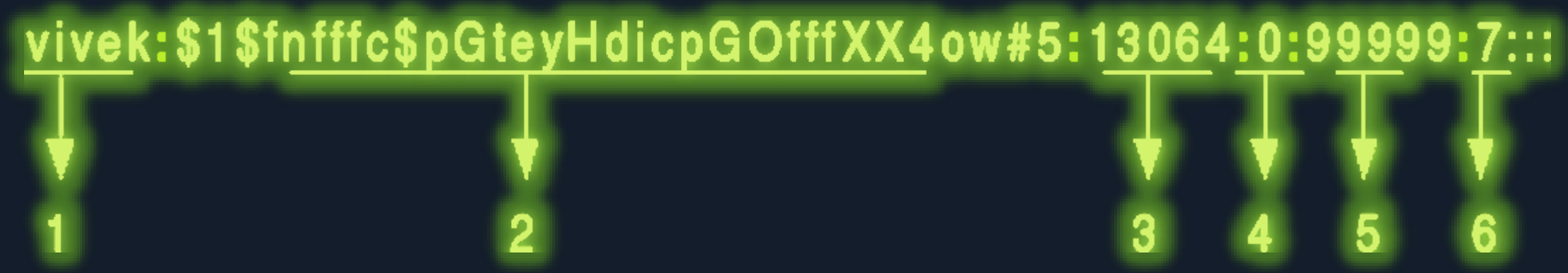
Cracking
Common Hashes

HACK THE BOX FRIDAY

LINUX SHADOW FILE

- /etc/shadow is where Linux stores all of its encrypted passwords
- It requires root access to view
- All fields in a shadow entry are separated by colons



1: Username

2: Password

3: Last Password Change

4: Minimum days between passwords

5: Maximum days the password is valid

6: User is warned this many days before expiration

Not shown

7: Number of days after the password expires before the account is disabled

8: Date of the expiration of the account

SHADOW FILE PASSWORD SELECTION

- The password section of the shadow entry starts with a $, then a number, letter, or both, then another $. This lets you know what kind of hash it is.
  - 1 MD5
  - $2a$ Blowfish
  - $2y$ Blowfish
  - 5 SHA-256
  - 6 SHA-512
  - y yescrypt
- If we look at this shadow entry:
  - root:6tOA0cyybhb/Hr7DN$htr2vffCWiPGnyFOicJiXJVMbk1muPORR.eRGYfBYUnNPUjWABGPFiphjIjJC5xPfFUASIbVKDAHS3vTW1qU.1:18285:0:99999:7:::
- This is the part that we'll want to crack
  - 6tOA0cyybhb/Hr7DN$htr2vffCWiPGnyFOicJiXJVMbk1muPORR.eRGYfBYUnNPUjWABGPFiphjIjJC5xPfFUASIbVKDAHS3vTW1qU.1
- Broken down:
  - SHA-512
    - 6
  - Salt
    - tOA0cyybhb/Hr7DN
  - Hash
    - htr2vffCWiPGnyFOicJiXJVMbk1muPORR.eRGYfBYUnNPUjWABGPFiphjIjJC5xPfFUASIbVKDAHS3vTW1qU.1

Active Directory

LM

LANman, we should ***NEVER*** use LM for anything.

It's super old and can be cracked in literal seconds

- 14 char max and case insensitive
- There are better tools than hashcat to crack these

Example:

- e52cac67419a9a224a3b108f3fa6cb6d

NTLM

Usually dumped from memory using a tool like Mimikatz

- But you don't need Mimikatz to do this!

Example:

- 7100a909c7ff05b266af3c42ec058c33

NetNTLMv2

Typically gathered with on-path (MITM) attack tools like Responder

Format:

- username::domain:challenge:response

Example:

- admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c78303100000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030

HTB Challenge

- Create the hash file

  echo '7106812752615cdfe427e01b98cd4083' > ntlm.hash
- Identify the hash (to get the mode)

  hashid ntlm.hash -m
- Crack the file

  hashcat –a 0 –m 1000 ntlm.hash /usr/share/wordlists/rockyou.txt.gz –r <SOME RULE GOES HERE!>

JohnTheRipper (jtr, john) Tools

JohnTheRipper is another tool for password cracking.

Most people prefer john if they don't have a GPU

It's useful to people who use hashcat as well because it comes with a suite of tools which compliment password cracking capabilities

Some of the most useful tools are:

Unshadow	Combines /etc/passwd and /etc/shadow so john can crack them
SSH2John	Convers SSH private keys into a format that john can crack
ZIP2John	**Extracts password hashes from zip files**
PDF2John	**Extract password hashes from pdf files**
7Z2John	**Extracts password hashes from 7z files**
OFFICE2John	**Extracts password hashes from M$ Office files**

Installing and Using John Tools

- To get the tools, we have to install the whole thing
  - This takes a little bit to compile.
  - Oneliner:
    - sudo git clone https://github.com/magnumripper/JohnTheRipper.git && cd JohnTheRipper/src && sudo ./configure && sudo make
- Using the tools is incredibly easy.
  - Usually, it's just the tool's name + the file from where you wish to extract the hash.
    - Ex:
      - office2john password_protected_document.docx
      - zip2john password_protected_zipfile.zip
      - 7z2john password_protected_7zfile.7z

HTB Challenge

- Extract the password hash from the 7z file
  7z2john hashcat.7z
- Identify the hash (to get the mode)
  hashid 7z.hash -m
- Crack the file
  hashcat –a 0 –m 11600 7z.hash /usr/share/wordlists/rockyou.txt.gz
- Open the zip file with the password
  7z x hashcat.7z