Password Cracking

Hamza Haroon

Overview

- Passwords
  - Hashing
- Breaking Passwords
  - Dictionary
  - Hybrid
  - Brute-Force
  - Rainbow Tables
- Countermeasures

Passwords

- A secret code for verifying the identity of a person logging into a system
- They are not stored as plaintext on a system
  - This would be a very bad thing!!!
- Passwords are stored as *hashes* based on the type of system
  - Windows: LM Hash, NTLM
  - Unix/Linux: DES, MD5

Hashing

- Process of processing data through a mathematical formula, and producing a new set of data (called the *hash*).
  - Process is one-way (you cannot get the original data from the hash.
  - There should be few collisions (two sets of data producing the same hash). Ideally there should be no collisions.
- Examples:
  - MD5, SHA-1, LM Hash

Windows Passwords

- Set or change password → Windows generates a LM hash and a NT hash.
- Two hashing functions used to encrypt passwords
  - LAN Manager hash (LM hash)
  - NT hash (NT hash)
- Hashes are stored in the Security Accounts Manager database
  - Commonly known as “ SAM” or “the SAM file”
- SAM is locked by system kernel when system is running.
  - File location: C:\WINNT\SYSTEM32\CONFIG

Linux Passwords

- MD5 passwords
  - Take the entire password string, send it through the MD5 algorithm, and store that as the password in the /etc/shadow file
- When the user logs in, the password entered is sent through the MD5 algorithm, and if the strings are the same, then the user is authenticated

Passwords

Shadow

- Utilized in UNIX systems
- Store hashed passwords in /etc/shadow file which is only readable by system administrator (root)
- Add expiration dates for passwords
- Early Shadow implementations on Linux called the login program which had a buffer overflow!

Password Breaking

- Dictionary attack
  - List of dictionary words that are tried one after another
  - Very quick
  - If the password is not an exact match to a word on the list, then it will fail
- Hybrid attack
  - Uses a dictionary list but can detect slight variations to words, or combinations of words.
  - Example: if the word *hello* is in the database, but the password is *Hello*, a dictionary attack will not break the password, but a Hybrid attack will
  - Generally finds many more words than a Dictionary attack
  - Not as quick as Dictionary attack

Password Breaking

- Bruteforce attack
  - Will try every character combination until it finds the password
  - EXTREMELY SLOW
  - Will always find the password
- These techniques can either be used against a system or a file containing the passwords

Rainbow Tables

- Uses a reduce function to attempt to map a hash to a password
- Uses chains to determine the exact password
- Pros
  - Can break any password in a matter of minutes
- Cons
  - Must have specific Rainbow Table for a particular hashing function
  - Can be defeated using Salts

Security Levels

- Filing System
  - Clear text
- Dedicated Authentication Server
  - Clear text
- Encrypted
  - Password + Encryption = bf4ee8HjaQkbw
- Hashed
  - Password + Hash function = aad3b435b51404eeaad3b435b51404ee
- Salted Hash
  - (Username + Salt + Password) + Hash function = e3ed2cb1f5e0162199be16b12419c012

Offline Password Cracking

- Collect password hashes
- Crack passwords
- Eavesdropping (Sniffing)
- Password file
  - Windows – SAM,NTDS.dit file (pwdump[2-6] and fgdump)
  - Linux – shadow file (unshadow)
- Memory Dump (debug tools: WinDgb, gdb), System calls (APImonitor, strace)
- SQL database, configuration file
- Source code

Online Password Cracking

- Use online hash crackers like hashes.com to compare your password hashes with known passwords.
- Use a tool like JohnTheRipper, Hydra, Hashcat, RainbowCrack or such tools to use some wordlists to crack the password.
- A commonly used wordlist is rockyou.txt
- It all depends on the type of encryption you are working with so cracking is variable for every situation
- Python is well known for cracking using custom scripting techniques

Countermeasures

- Eavesdropping: Encrypt the channel, e.g. using SSL or SSH
- Offline dictionary attacks: Limit access to password hashes, strong passwords, password lifetime, use salt
- Online dictionary attacks: Delayed answers, strong passwords, account lockouts

Questions