TASK 5: BRUTE FORCE

What is Brute Force Attack?

A Brute Force Attack is a hacking method used to gain unauthorized access to systems, accounts, or encrypted data by systematically trying every possible combination of credentials or keys until the correct one is found. This attack relies on computational power to exhaustively "guess" login credentials, making it time-intensive, especially for complex passwords. Brute force can target login pages, network services, or encrypted files, and is often automated through software tools that can rapidly test combinations. While simple passwords fall quickly, strong passwords with a mix of characters take significantly longer to crack. Techniques like rate limiting, CAPTCHAs, and account lockouts are commonly employed to defend against brute force attacks. Despite its simplicity, brute force remains effective against weak security setups.

What is Wordlist?

A wordlist is a collection of words or phrases commonly used in password-cracking attacks, especially in brute force and dictionary attacks. This list contains potential passwords, which an attacker systematically tests to find valid credentials for an account or encrypted file. Wordlists vary in complexity, from simple lists of common passwords to extensive collections derived from real-world breaches, containing millions of entries. These lists can be tailored for specific languages, themes, or password patterns to increase their effectiveness against targeted systems. Cybersecurity professionals also use wordlists in penetration testing to assess password strength and improve security measures. Tools like John the Ripper or Hydra are commonly used to automate wordlist-based attacks, making them efficient in password-cracking tasks.

How to prepare Wordlist?

A wordlist is a collection of words or phrases commonly used in password-cracking attacks, especially in brute force and dictionary attacks. This list contains potential passwords, which an attacker systematically tests to find valid credentials for an account or encrypted file.

1. Define Target-Specific Keywords:

Research information relevant to the target, like common names, hobbies, birthdates, or related terms, to make the wordlist more effective.

2. Use Wordlist Generation Tools:

Tools like **Crunch** allow you to create custom wordlists based on criteria like character length, number combinations, or patterns.

3. Extract Keywords from Web Content:

Tools such as **CeWL** can scrape keywords from web pages, generating words from publicly available content that may be used as passwords.

4. Incorporate Real-World Passwords:

To enhance your list, download wordlists from real-world data breaches (like RockYou), which contain common passwords and variations used widely.

5. Apply Filters and Remove Duplicates:

Use sorting tools to remove duplicate entries, ensuring that each password attempt is unique and the list is efficient.

6. Format and Organize the List:

Organize the wordlist in a logical order, starting with common or shorter words to test basic passwords before moving to complex entries.

7. Test and Refine:

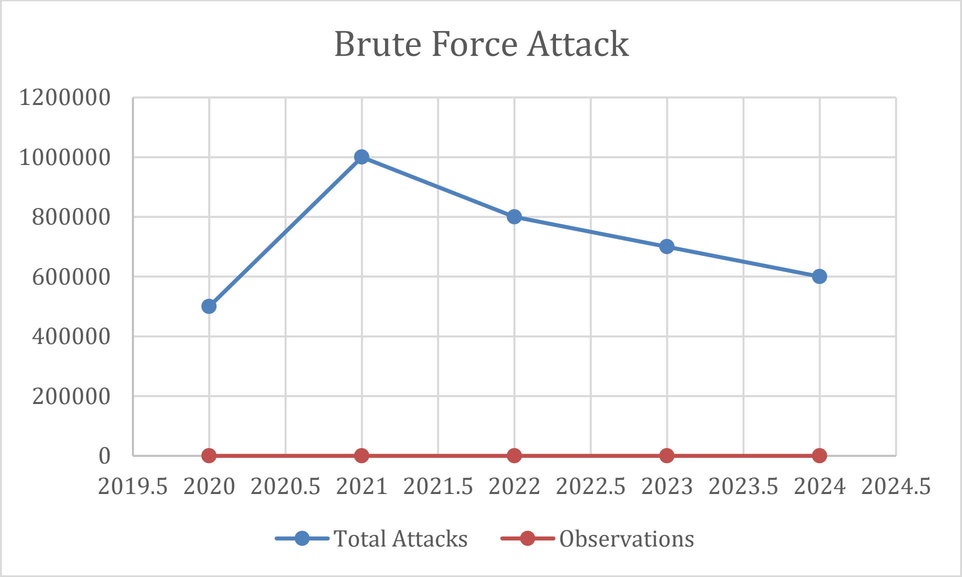
Conduct tests with the wordlist in tools like **John the Ripper** or **Hydra** to see its effectiveness, and adjust entries based on findings or additional context.

8. Maintain and Update Regularly:

Keep the wordlist updated by adding new common passwords or terms based on changing trends in password habits and data leaks.

Total Breaches Caused by Brute Force Attack:

5% of all data breaches are caused by brute force attacks. Of breaches caused by hacking, 80% involve brute force or lost/stolen credentials. Theoretically, brute force attacks have a 100% success rate, though the hacker may have to wait years for their automated systems to correctly guess a complex password. Realistically, brute force attacks are popular and effective for determining weak passwords, particularly for web application, accounting for 80% of all attacks. Here is a graph on Brute Force Attacks from 2020 to 2024, give a threat intelligence on "Total Attacks" and "Observations".



Dunkin' Donuts pays over half a million in penalties

In a famous 2015 incident involving the use of brute force, Dunkin' Donuts digital customer accounts were targeted by hackers who used a leaked list of previously stolen credential information and ran brute force algorithms. They gained access to 19,715 user accounts for the customer loyalty application and stole tens of thousands of dollars of rewards cash.

The result of the brute force attack and breach on customer accounts at Dunkin' Donuts resulted in $650,000 in fines and damages and forced the company to reset all user passwords and upgrade security protocols for the application.

20.6 million accounts compromised at Alibaba

In 2016, a team of hackers used a previously breached database with over 99 million credentials for multiple web applications. Taking advantage of weak passwords and users implementing the same password across other accounts, they used brute force and credential stuffing to successfully access nearly 20% of all the targeted accounts.

While no dollar amount of damages has been indicated, it was confirmed that nearly 20.6 million Alibaba accounts were successfully compromised and accessed maliciously, and all users were asked to change their passwords.

References:

https://www.strongdm.com

https://chatgpt.com

https://www.kaspersky.co.in

https://abnormalsecurity.com