SECUREB4
We Strengthen Your Security

Secureb4.io

Brute Force Attacks

(Techniques, Types & Prevention)

SECUREB4
We Strengthen Your Security

Brute Force Attacks

These attacks are often used against password-protected accounts. The attacker uses software that generates many consecutive guesses to gain unauthorized access to a user's account.

Brute force attacks can be performed quickly for simple and short passwords, particularly if they are not protected by other security measures like account lockout policies after a certain number of failed attempts or CAPTCHAs designed to prevent automated submissions.

However, as password complexity increases, brute force attacks become less practical due to the exponential increase in the number of possible combinations that the attacker's software must test.

1

Secureb4.io

Simple Brute Force

This is the basic form, where the attacker manually tries various combinations of characters, numbers, and symbols to guess the password. It's time-consuming and inefficient, but surprisingly effective against weak, predictable passwords like "123456" or "password123".

SECUREB4
We Strengthen Your Security

2

Dictionary Attacks

Instead of random guesses, dictionary attacks use pre-made lists of common words, phrases, variations, and leaked passwords. These lists can be extensive and even tailored to the target's background or interests. Dictionary attacks are significantly faster and more efficient than simple brute force, especially against users who reuse passwords across different accounts.

3

Secureb4.io

Hybrid Brute Force

This combines the brute-force approach with dictionary attacks. It starts with a smaller list of common passwords and then expands it with character substitutions, variations, and dictionary entries. This increases the attack's scope while still focusing on likely password choices.

SECUREB4
We Strengthen Your Security

4

Secureb4.io

Reverse Brute Force

Here, the attacker already knows some information about the password, like its length or specific characters used. They then build targeted lists based on this knowledge, significantly reducing the number of possibilities and increasing the attack's speed and success rate.

5

Credential Stuffing

This involves using leaked or stolen username and password pairs from data breaches to try them on other platforms. Attackers leverage the fact that many users reuse credentials across different accounts. Credential stuffing can be automated and highly effective, especially against platforms with weak login security.

SECUREB4
We Strengthen Your Security

6

Rainbow Table Attacks

These attacks use pre-computed hashes of common passwords and then compare them to the hashed password of the target system. While not directly revealing the password, a successful match identifies the corresponding password in the rainbow table. This can be faster than brute-forcing the actual password, but requires significant resources to generate and store the rainbow tables.

7

Password Spraying

Instead of targeting specific accounts, password spraying uses a single common password against a large number of accounts. This aims to exploit weak password policies or password reuse across different platforms. While less targeted, it can effectively identify vulnerable accounts and gain access to multiple systems at once.

SECUREB4
We Strengthen Your Security

8

Brute Force Attacks on RDP Connections

Remote Desktop Protocol (RDP) is a popular tool for remote access to computers. Attackers can use brute force techniques to guess RDP login credentials and gain unauthorized access to the remote system. This can be a gateway to further attacks on the network or data stored on the system.

Tips To Prevent Brute Force Attacks

- **Strong Password Policies:** Enforce complex passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. This exponentially increases the number of possible permutations a brute force attack would need to try.

- **Account Lockout Mechanisms:** Set up account lockouts after a certain number of failed login attempts. This stops continuous password guessing dead in its tracks but should be implemented thoughtfully to prevent denial of service situations through account lockout abuse.

- **Two-Factor Authentication (2FA):** Adding an additional layer of security beyond just a password significantly diminishes the effectiveness of brute force attacks, as the attacker also needs the second factor—usually a temporary code sent to a mobile device or generated by an authenticator app.

- **CAPTCHA:** Implement CAPTCHAs to challenge and block automated login attempts, ensuring that only humans can proceed with login attempts.

- **Use of Security Software:** Deploy security solutions that detect and block repeated failed login attempts, which are indicative of brute force attacks.

- **Monitoring and Alerting:** Monitor systems for unusual login activity and set up alerts for multiple failed login attempts.

- **Network-Level Security:** Utilize network security tools like firewalls and intrusion prevention systems to block traffic from IP addresses that are known sources of attacks.

- **Password Managers:** Encourage the use of password managers to help users maintain unique, complex passwords for different sites and services, reducing the temptation to reuse passwords.

- **Educate Users:** Regularly educate users about the importance of using strong passwords and the risks associated with weak authentication practices.

- **VPN and Encrypted Connections:** Use VPNs and ensure connections are encrypted to prevent attackers from intercepting credentials that could be used in brute force attacks.

- **Banning IP Addresses:** Implement rules to ban IP addresses that show signs of brute force attack behavior over a defined period.

Our Services

SECUREB4
We Strengthen Your Security

Breach and Attack Simulation

Vigilantly assess and enhance your security controls with our 24/7 breach simulations, identifying and rectifying vulnerabilities before they are exploited.

Security Hardening

Boost your network's resilience with our robust gap analysis, fortifying your defenses without disrupting existing settings.

Privacy & Consent Management

Ensure compliance with Personal Data Protection regulations, safeguarding user data rights and privacy.

Passworldess Authentication

Revolutionize your authentication process with our state-of-the-art biometric, cryptography, and multi-user verification solutions.

Open-Source Software Protection

Shield your software stack with our pre-hardened open-source packages, bolstering your defenses against threats.

End-to-End Encryption & Data Protection

Protect sensitive data with our encryption services, ensuring safety across both public and private clouds.

E-Commerce & Merchant Cyber Risk Management

Defend your online business platforms with our comprehensive cyber risk strategies, tailored to e-commerce.

Identity First Security Platform

Secure your enterprise cloud assets from cyber threats with AI-powered automation and sophisticated privilege controls.

Threat Intelligence and Domain Protection

Mitigate financial losses from fraud with our advanced domain protection, identifying and neutralizing impostor websites.

Manage Your GRC Compliance

Our scalable and customizable GRC framework aligns with global compliance standards, ensuring your organization meets ISO, PCI, RBI, and GDPR requirements.

Cloud Email Security

Stay ahead of email threats with our behavioral-based security solutions, combating sophisticated attacks like ransomware and phishing.

Cloud Security Center of Excellence

Strengthen your cloud security posture with our all-encompassing suite featuring CNAPP, WAAP, KSPM, CSPM, CWPP, CIEM, CASB, DSPM, and CNSP.

+971 565612349 | info@secureb4.io

Contact us!

SECUREB4
We Strengthen Your Security

Like

Share

Save

Follow us!