Brute Force Attack Project using Hydra

This project demonstrates a brute-force attack on a vulnerable web application running on IP **192.168.29.186** using Hydra. The goal is to understand how brute-force attacks work, practice offensive techniques in a controlled lab, and learn mitigation strategies.

Objectives

1 Understand brute-force attacks in web applications.
2 Use Hydra to perform brute-force login attempts.
3 Perform brute-force on different services (HTTP, SSH).
4 Learn how to detect and prevent brute-force attacks.

Tools Used

Kali Linux Hydra Burp Suite (for capturing requests) OWASP bWAPP / DVWA vulnerable applications

Methodology

1. Setup a vulnerable target machine at IP 192.168.29.186 (bWAPP or DVWA).
2. Capture the login request using Burp Suite to identify form parameters.
3. Prepare a wordlist for usernames and passwords.
4. Run Hydra with appropriate parameters against the target.
5. Analyze results and document successful login attempts.
6. Repeat the test on different services (HTTP-POST, SSH).

Hydra Commands Used

HTTP POST Form Bruteforce:

```
hydra -l admin -P passwords.txt 192.168.29.186 http-post-form
"/bWAPP/login.php:login=^USER^&password;=^PASS^:Invalid login"
```

Cluster Bomb Attack (Multiple Users and Passwords):

```
hydra -L users.txt -P passwords.txt 192.168.29.186 http-post-form
"/bWAPP/login.php:login=^USER^&password;=^PASS^:Invalid login"
```

SSH Bruteforce:

```
hydra -l root -P passwords.txt ssh://192.168.29.186
```

Findings

- Successful brute-force attack revealed valid credentials.
- Weak or default passwords were identified.
- Login attempts can be easily automated with Hydra.

Mitigations

- Implement account lockout after multiple failed attempts.
- Use CAPTCHA on login forms.
- Enforce strong password policies.
- Enable multi-factor authentication (MFA).
- Monitor logs for brute-force attempts.

Conclusion

This project demonstrated the use of Hydra for brute-force attacks against web applications and SSH services. While brute-force remains a common attack vector, it can be mitigated effectively with proper security controls. This project helps understand both the attack methodology and defensive measures, which are crucial for a cybersecurity career.