Brute-force Attacks – Project

By Inlighn Tech

Objective

To simulate and analyze brute-force attacks against vulnerable web login forms and SSH services using tools like Burp Suite and Hydra. This project demonstrates how weak authentication systems can be broken and teaches how to prevent such attacks.

Prerequisites

- Basic understanding of HTTP requests and forms
- Familiarity with Linux terminal
- Kali Linux or any Linux distribution with Hydra and Burp Suite
- A vulnerable app like bWAPP or DVWA installed locally or on a VM

Lab 1: Brute-force Using Burp Suite (Cluster Bomb)

Use Burp Suite's Intruder to perform a brute-force attack against a login page using the Cluster Bomb attack type.

🔸 Steps

1. Open bWAPP and navigate to the login page.
2. In Burp Suite, intercept a login request with dummy credentials.
3. Right-click ➜ "Send to Intruder".
4. Choose `Cluster Bomb` attack type.

5. Set payload positions:
    - `login=` → payload 1 (username)
    - `password=` → payload 2 (password)
6. Use small username/password lists for faster testing.
7. Start attack and analyze the status and response length to detect valid credentials.

Expected Outcome

:) You will find a valid username-password pair from the payload list.

Lab 2: Hydra Web Form Bruteforce (bWAPP Login)

Automate brute-forcing a web login form using Hydra.

Steps

1. **Identify form action and field names (e.g., `login.php`, `login`, `password`).**
2. **Use this command:**

```
hydra -l admin -P passwords.txt <target-ip> http-post-form "/bwapp/login.php:login=^USER^&password=^PASS^:Invalid"
```

3. **Replace `Invalid` with the exact error message returned by the form for failed logins.**
4. **Monitor Hydra's output for successful login credentials.**

Expected Outcome

Hydra will discover valid login credentials by checking server responses.

Deliverables

- Report with screenshots of each lab
- Hydra command syntax for different services
- List of successful username-password pairs (only for lab purposes)
- Mitigation checklist