# Task 1: Threat Identification

#### Threat: Brute Force Attacks

#### Characteristics:

* Brute Force Attacks: These involve attempting to gain unauthorized access to accounts by systematically trying all possible combinations of passwords until the correct one is found.

#### References:

* <https://www.cloudflare.com/en-gb/learning/bots/what-is-credential-stuffing/>
* <https://www.fortinet.com/resources/cyberglossary/brute-force-attack>

# Task 2: Basic Case Study

#### Background of the Threat

Brute force attacks are one of the simplest forms of cyber attacks, relying on computational power to guess passwords. Attackers use automated tools to try different combinations of characters until the correct password is found.

#### Typical Adversary Trade Craft

Attackers often use lists of common passwords or dictionaries of words to speed up the guessing process. They might also use information about the target to make educated guesses.

#### Potential Impact for an Organization

If successful, brute force attacks can lead to unauthorized access to sensitive information, data breaches, and potentially severe financial and reputational damage.

#### Resources:

* <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories>
* <https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A94>

# Task 3: Map Out Your Testing Scenario

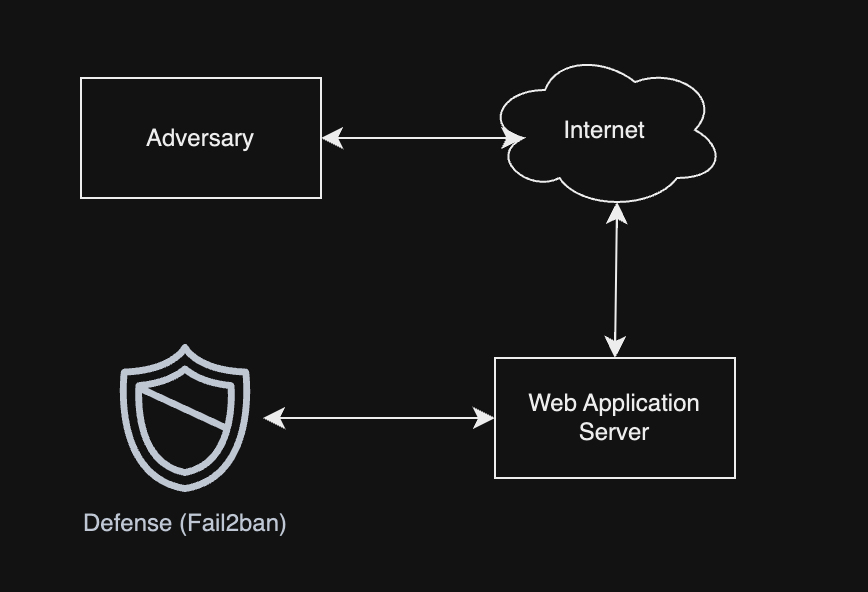
#### Scenario

We will simulate a brute force attack on a web application’s login page and implement measures to detect and block these attempts.

#### Steps:

1. Adversary connects to the web application.
2. Adversary uses a tool (e.g., Hydra) to perform a brute force attack on the login page.
3. The application logs the login attempts.
4. Implement a defense mechanism (e.g., Fail2ban) to detect and block IP addresses with too many failed login attempts.
5. Re-run the attack to verify the defense mechanism is effective.

#### Topology Diagram



1. Adversary initiates brute force attack on Web Application Server through Internet.

2. Web Application Server logs each login attempt.

3. Fail2ban monitors logs and detects suspicious activity.

4. Fail2ban blocks IP address of the adversary.

5. Web Application Server blocks further requests from the adversary's IP address.

# Task 4: Tool/Activity Research

#### Offensive Tools

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tool / Activity | Ease of Install | Documentation | Community Activity | Features |
| Hydra | Easy (sudo apt install hydra) | Extensive (https://www.kali.org/tools/hydra/) | High (https://salsa.debian.org/pkg-  security-team/hydra) | Fast brute force tool |
| Medusa | Easy (sudo apt install medusa) | Moderate  (https://www.kali.org/tools/medusa/) | Moderate  (https://salsa.debian.org/pkg-security-team/medusa) | Parallel login brute forcer |
| John the Ripper | Moderate (sudo apt install john) | Extensive  (https://www.kali.org/tools/john/) | High  (https://gitlab.com/kalilinux/packages/john) | Password cracker |

#### Defensive Tools

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tool / Activity | Ease of Install | Documentation | Community Activity | Features |
| Fail2ban | Easy | Moderate (https://github.com/fail2ban/fail2ban) | High | Prevents brute force attacks |
| Snort | Easy (cloning git repository) | Moderate (https://www.snort.org/) | High | Network intrusion detection |
| Iptables | Moderate (sudo apt get iptables) | Extensive (https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/) | High | Firewall rule management |

#### References:

* <https://github.com/enaqx/awesome-pentest>
* <https://github.com/sbilly/awesome-security>

# Task 5: MITRE ATT&CK TTPs

#### Techniques

* T1110: Brute Force
* T1078: Valid Accounts

#### Tactics

* Initial Access
* Persistence

#### Reference:

* <https://attack.mitre.org/>

#### Summary

We have chosen Brute Force Attacks as our focus for this case study. We have identified its characteristics, researched relevant information, created a testing scenario, identified tools for both offensive and defensive roles, and mapped relevant MITRE ATT&CK techniques and tactics.