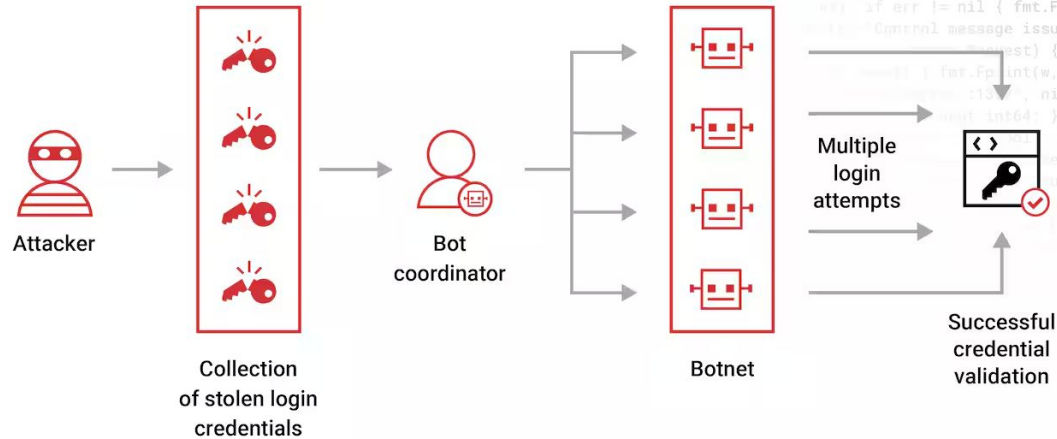


Credential Stuffing as a Method of Unauthorized Network Access (Unit 4)

Presented by: Lina, Akilah, Sai, Timothy, Jose, and Veronika

Credential Stuffing



Example of how credential stuffing works



Example of how credential stuffing works





Risk Analysis - Lina

- **Credential Stuffing:** A cyberattack where attackers use stolen usernames and passwords from data breaches
- **Why it's effective:** It exploits common practice of password reuse across sites
- How does it work?
 - **Obtain Credentials** such as usernames and passwords from data breaches or the dark web
 - **Automated Attacks** to attempt logins on multiple websites in seconds
- **Widespread Impact:** One breach can compromise accounts in many platforms
- **Difficult to Detect:** Difficult to distinguish credential stuffing from usual login attempts
- **Data Compromise:** Grants unauthorized access to sensitive user or organizational data
- **Real-World Impact:** Credential stuffing accounted for 16.5% of account takeover attacks in 2022 (Verizon Data Breach Report)

Sources: <https://www.verizon.com/business/resources/reports/dbir/>

<https://owasp.org/www-project-automated-threats-to-web-applications/assets/oats/credential-stuffing>

Mitigations Strategies

1. Multi-Factor Authentication (MFA) 
2. Rate Limiting & Account Lockouts 
3. CAPTCHA 
4. Monitor for Unusual Login Behavior 
5. Password Enforcement 

1. Multi-Factor Authentication (MFA) - Akilah

What is MFA ?

- A method that requires the user to provide more information than only a password

What does it do?

- MFA strengthens authentication, blocks unauthorized access, and reduces risks from phishing, credential theft, and data breaches

Sources: <https://www.microsoft.com/security/>

<https://duo.com/pricing>

<https://staysafeonline.org/mfa/>

- **Risk Reduction:** Reduces account compromise by 99.9% when implemented correctly (Microsoft)
- **Time Investment:** Setting up MFA takes 2–3 hours for most systems, while individual users only spend 2–5 minutes setting up their authentication
- **Money Investment:** Business solutions cost \$3–\$6 per user per month using providers like Duo Security, with free options available for personal accounts



Multi-Factor Authentication

Step 1



Username & Password

Step 2



Proof

Step 3



Access
Granted

Username & Password

Proof

Access
Granted

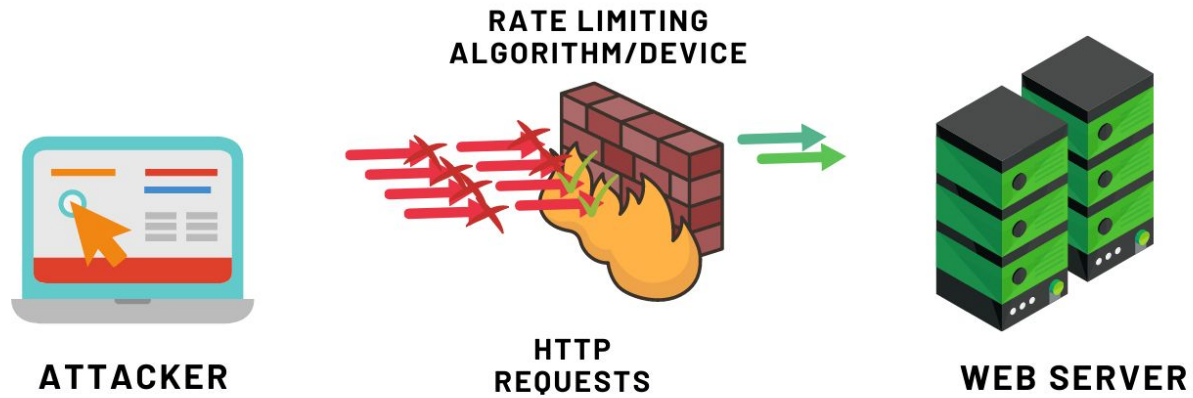
2. Rate Limiting & Account Lockouts - Sai

- **How it works:** Limits the number of failed login attempts with a set time. Exceeding the limit triggers a lockdown, blocking further access
- **Purpose:** Restricts login attempts to prevent credential stuffing attacks
- **Key Benefits:** Prevents automated attacks and Ensures immediate response
- **Risk Reduction:** Implementing rate limiting can significantly reduce the success of credential stuffing attacks by limiting the number of login attempts per user.
- **Time Investment:** Setting up rate limiting typically takes a few hours, depending on system complexity. Ongoing maintenance is menial, often less than an hour per month.
- **Money Investment:** Utilizing a third-party service for rate limiting can cost between \$10-\$50 per month for small applications.

Sources: <https://www.cloudflare.com/application-services/products/rate-limiting/>

<https://www.geeksforgeeks.org/rate-limiting-algorithms-system-design/>





3. CAPTCHA - Timothy

- Prevents Automated Login Attempts
 - By using puzzles, it adds another layer of protection against automated scripts
- Stops Bulk Account Enumeration
 - Forces human interaction, which slows down / stops automated attempts
- Limits Attack Efficiency
 - Increases time and effort required for bots to test credential pairs, making credential stuffing, less efficient.
- A captcha is a challenge-response test for websites/applications to determine whether the user is a human or a bot.
- It is designed to be easily solved by humans but difficult for automated programs.
- Used to prevent spam, abuse, and automated attacks

Sources: [What is a CAPTCHA? CAPTCHA Types and Examples | Radware](#)





i'm not a robot



CAPTCHA
Privacy - Terms

Eps10 vector

Type the two words:



CAPTCHA
Privacy - Terms

4. Monitor for Unusual Login Behavior - Jose

Track and record login sources.

- This will help spot login attempts from new/suspicious devices and IP addresses.
- Check for instances where a user is logged in from two different regions simultaneously

Send one-time code to user

- Stops automated attacks that use stolen credentials to attempt logins on various sites.
- To ensure that the real user is attempting to log in.

- **Risk reduction:** This measure reduces the risk by helping identify and flag login attempts from unknown or suspicious devices
- **Time investment:** Initial implementation may require 2-4 weeks of development and integration
- **Monetary Investment:** Costs may include software development resources ranging from \$0 to \$50,000

Source: <https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events>



5. Password Enforcement - Veronika

A set of security policies to make sure passwords meet specific complexity, and length to enhance security.

- Protects sensitive data by preventing unauthorized access.
- Mitigates risks associated with weak or easily guessed passwords.
- Enforces industry standards and regulatory compliance.

- **Length:** Minimum 12-16 characters reduces credential stuffing success by 80%. No cost.
- **Complexity:** Mix of uppercase, lowercase, numbers, and symbols. Complex passwords are 60% less likely to be compromised. No cost.
- **History:** Prevents reuse of old passwords. Reduces risks of credential stuffing. Software configuration, typically free or included in existing systems.
- **Expiration:** Change every 60-90 days. Decreases exposure window for compromised credentials.
- **Time Investment:** Configuring password policies and enforcement takes minimal time, often included in initial system setup.

Sources: <https://www.cisa.gov/>

<https://www.microsoft.com/security/blog/>



Common Password Security Threats

Recognize these password security threats that can pose a danger to your privacy and data.



Dictionary attacks



Credential stuffing attacks



Password spraying



Keylogging



Phishing scams

Strong password

Password



Rohitkumar

Rohit123

Rohit@123

R0"h"1"t"@123

secure %



10%

15%

20%

99.99%

Thank you for your attention!