1 Threat Analysis

1.1 Authentication

According to the Annual Cyber Threat Report(ACTR) 2023-2024, the most frequently reported threat in Australia were Authentication attacks in the form of "compromised accounts or credentials"[1], accounting for nearly one-third of all cybercrime incidents nationwide. This prevalence underscores the critical importance of understanding and mitigating authentication-related threats in the current cybersecurity landscape.

Authentication breaches encompass a wide array of attack categories, each exploiting different weaknesses in user and system behavior. The most prominent include **phishing**, which leverages psychological manipulation to trick users into divulging credentials, and **brute force attacks**, where adversaries systematically guess passwords using automated tools. **Password spraying** represents a "low and slow" approach, targeting many accounts with common passwords to evade detection. **Credential stuffing** utilizes previously breached username-password pairs, often sourced from large-scale data leaks, to gain unauthorized access through automation. These categories highlight the multifaceted nature of authentication threats, demonstrating why password-based attacks remain a critical focus for security research and organizational defense.

1.2 Threats in the Authentication Landscape

1.2.1 Current Threat Landscape

Authentication threats represent a critical challenge in today's cybersecurity landscape, both in Australia and globally. The Albanese Government's commitment of $15–$20 billion through 2033–34 to strengthen cyber domain capabilities underscores the national urgency to address these issues[1]. In the 2023–24 financial year, the Australian Signals Directorate received over 36,700 calls to its Cyber Security Hotline 12% increase from the previous year, reflecting the growing prevalence of cyber incidents[1]. Notably, compromised accounts or credentials accounted for **32% of all cybercrime**, making it the leading contributor to reported incidents. On a global scale, Microsoft Entra data reveals that of more than **600 million identity attacks per day**, over **99% are password-based**[2]. These statistics highlight the widespread and persistent nature of authentication-related threats, demonstrating why robust authentication mechanisms are essential for organizational and national security.

1.2.2 Typical Adversary Types

Authentication attacks are executed through several distinct methods, each exploiting specific vulnerabilities in user behavior and system design.

- **Phishing** is a psychological manipulation technique where adversaries impersonate trusted entities, often via email or messaging platforms, to deceive users into revealing their credentials. This method remains highly effective due to its reliance on social engineering rather than technical flaws.
- **Brute force attacks** involve systematically generating and attempting password combinations until a valid login is achieved. Attackers leverage automated tools to accelerate this process, targeting accounts with weak or commonly used passwords.
- **Password spraying** refines brute force tactics by distributing login attempts across many accounts using a shortlist of popular passwords, thereby evading detection mechanisms that monitor for rapid, repeated failures. A notable example is the 2024 Midnight Blizzard incident, where attackers employed password spraying against Microsoft's infrastructure, prompting significant defensive actions[3].
- **Credential stuffing** utilizes credentials harvested from previous data breaches, exploiting the widespread practice of password reuse across multiple services. The 2022 Optus breach illustrated the impact of this technique, as compromised credentials were repurposed to target other organizations[4]. These methods collectively demonstrate the evolving sophistication and persistence of authentication threats in the modern cyber landscape.

1.2.3 Impact

This section starts with how phishing and credential stuffing can be used as good starts

The organizational impact of authentication breaches is starkly illustrated by the 2022 Optus incident, which exposed sensitive data of nearly 10 million Australians and triggered widespread concerns over identity theft and fraud [4]. More recently, the Qantas breach in July 2025 affected 5.7 million customers, with varying degrees of personal information compromised [5]. Both cases highlight the persistent threat posed by credential stuffing, where attackers leverage previously leaked credentials to infiltrate systems at scale. The consequences include

substantial financial losses, operational disruption, and enduring reputational harm, emphasizing the critical need for organizations to strengthen authentication controls and proactively address credential-based threats.

1.3 Threat Choice Justification

The selection of authentication attacks as the focal threat for this analysis is driven by their overwhelming prevalence and critical impact on both Australian and global organizations. Recent reports indicate that compromised credentials account for nearly one-third of all cybercrime incidents in Australia, with high-profile breaches such as Optus and Qantas underscoring the real-world consequences of these attacks[1], [4], [5]. The universal reliance on password-based authentication across industries makes this threat highly relevant and widely applicable. From a technical perspective, authentication attacks such as brute force, password spraying, and credential stuffing offer a rich landscape for analysis, enabling clear success and failure metrics and supporting laboratory-based experimentation.

While phishing remains a significant aspect of authentication security due to its effectiveness and prevalence, it is not easily testable in a controlled lab environment and will not be the focus of practical testing in this assignment. Nevertheless, its role in the broader authentication threat landscape will be acknowledged. Furthermore, the threat aligns strongly with established frameworks like MITRE ATT&CK (T1110 family) and Essential 8 mitigations, providing a robust foundation for evaluating defensive strategies and mapping adversary techniques.

This combination of prevalence, technical depth, and framework integration makes authentication attacks an ideal subject for comprehensive security analysis. It will also be interesting to see how easy it is to break into hypothetical systems and gain a practical understanding of how secure my own personal passwords really are.

2 Authentication Attack Scenario Design - Dot Point Plan

2.1 Testing Scenario Overview

Objective: Evaluate effectiveness of password spraying attacks using personalized password generation against various defensive measures

2.2 Environment Setup

2.2.1 Virtual Lab Infrastructure

- **Target System:** Ubuntu server with SSH and web application login
- **Attack Platform:** Kali Linux VM with custom tools
- **Network:** Host-only networking (isolated environment)
- **Monitoring:** Centralized logging server for detection analysis

2.2.2 Target Applications

- **Primary:** Custom web application with login form
- **Secondary:** SSH service with username/password authentication
- **Database:** MySQL backend storing user credentials (hashed)

2.3 Phase 1: Synthetic Data Generation

2.3.1 User Profile Database Creation

- Generate **500 realistic user profiles** using Python Faker library
- **Data points per user:**
  - Full name (first, last)
  - Email address
  - Birth year/date
  - Pet names (1-2 per user)
  - Hobbies/interests
  - Favorite foods
  - Location/city
  - Company/job title
  - Previously gained password

2.3.2 Password Generation Algorithm

- **Pattern-based password creation** using personal data
- **Common password patterns to implement:**
  - `{FirstName}{BirthYear}!` (e.g., Sarah1990!)
  - `{Pet}{Number}@` (e.g., Fluffy123@)
  - `{Hobby}{Year}` (e.g., Photography2024)
  - `{Location}{BirthYear}!` (e.g., Sydney1985!)
  - `{Company}@{Year}` (e.g., Microsoft@2024)
  - `{PreviousPassword}` (If available, used once, attributes can also be dissected and rearranged, (e.g., Candy*2000 could be dissected into `[Candy,$,2000]`))
- **Ensure compliance with password policy:** minimum 8 chars, uppercase, lowercase, number, special character

2.4 Phase 2: Attack Implementation (Offensive Tool)

2.4.1 Custom Password Spraying Tool

- **Language:** Python with requests/paramiko libraries
- **Features:**
  - Multi-protocol support (HTTP/SSH)
  - Configurable timing delays (avoid detection)
  - User-agent rotation and IP spoofing simulation
  - Success/failure logging with timestamps
  - Pattern effectiveness tracking

2.4.2 Attack Methodology

- **Stage 1:** Username enumeration (if required)
- **Stage 2:** Single password against all users (classic spraying)
- **Stage 3:** Personalized passwords against specific users
- **Timing:** 1 attempt per user per 30 minutes (avoid lockouts)
- **Duration:** 48-hour attack simulation

2.5 Phase 3: Defensive Implementation

2.5.1 Baseline Testing (No Defenses)

- Document attack success rate without protection
- Establish baseline metrics for comparison

2.5.2 Defense Tool 1: fail2ban

- **Configuration:**
  - SSH protection: 3 failures = 10 minute ban
  - HTTP protection: 5 failures = 15 minute ban
  - Custom rules for web application
- **Monitoring:** Ban events, IP addresses, timing

2.5.3 Defense Tool 2: Account Lockout Policies

- **Application-level:** 5 failed attempts = 30 minute lockout
- **System-level:** PAM modules for SSH protection
- **Progressive delays:** Increasing wait times per failed attempt

2.5.4 Defense Tool 3: Enhanced Monitoring

- **Log analysis:** Automated pattern detection
- **Alerting:** Real-time notifications for spray patterns
- **SIEM simulation:** Correlation rules for attack identification

2.6 Success Metrics Definition

2.6.1 Attack Success Metrics (Offensive)

- **Primary:** Successful authentication rate (logins/total attempts)
- **Secondary:** Time to first successful login
- **Pattern effectiveness:** Which personal data patterns yield highest success
- **Evasion rate:** Attacks completed without triggering defenses

2.6.2 Defense Success Metrics (Defensive)

- **Primary:** Attack detection rate (alerts/actual attacks)
- **Secondary:** Time to detection (minutes from attack start)
- **False positive rate:** Legitimate users blocked
- **Containment effectiveness:** Attacks stopped vs completed

2.6.3 Overall Effectiveness Metrics

- **Business impact:** Percentage of accounts compromised
- **Operational impact:** Legitimate user disruption
- **Detection accuracy:** True positives vs false positives

2.7 MITRE ATT&CK Framework Mapping

2.7.1 Primary Techniques

- **T1110.003 - Brute Force: Password Spraying**
  - Main attack vector implementation
- **T1589.001 - Gather Victim Identity Information: Credentials**
  - Personal data collection and analysis
- **T1078.004 - Valid Accounts: Cloud Accounts**
  - Successful authentication usage

2.7.2 Supporting Techniques

- **T1201 - Password Policy Discovery**
  - Understanding target password requirements
- **T1087 - Account Discovery**
  - Username enumeration activities
- **T1133 - External Remote Services**
  - SSH/web service targeting

2.8 Testing Timeline

2.8.1 Week 1: Environment setup and data generation

2.8.2 Week 2: Attack tool development and testing

2.8.3 Week 3: Baseline attack execution (no defenses)

2.8.4 Week 4: Defense implementation and protected testing

2.8.5 Week 5: Analysis, comparison, and documentation

2.9 Expected Outcomes

2.9.1 Attack Tool Analysis

- Personalized passwords significantly more effective than generic wordlists
- Lower detection rates with slow, targeted approach
- Pattern effectiveness varies by demographic correlation

2.9.2 Defense Tool Analysis

- fail2ban effective against rapid attacks, less effective against slow spraying
- Account lockouts protect individual accounts but may cause DoS
- Combined defenses provide layered protection with acceptable false positive rates

2.9.3 Scenario Winner Determination

- **Attacker wins:** >10% successful authentication rate
- **Defender wins:** <2% successful authentication rate + >90% detection rate
- **Balanced outcome:** 2-10% success rate with high detection

```
import flask
```

---

extbfTool Name	**Purpose**	**Platform**
Nmap	Network scanning	Linux/Windows/Mac
Wireshark	Packet analysis	Linux/Windows/Mac
Metasploit	Exploitation framework	Linux/Windows
Snort	Intrusion detection	Linux/Windows
Fail2Ban	Brute-force protection	Linux

Table 1: Sample Security Tools Used in Environment Setup

References

[1] Australian Cyber Security Centre, "Annual cyber threat report 2023-2024," Australian Signals Directorate, 2024. Available: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

[2] Microsoft Corporation, "Microsoft digital defense report 2024," Microsoft Corporation, Technical Report, 2024. Available: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

[3] Microsoft Security Response Center, "Microsoft actions following attack by nation state actor midnight blizzard." 2024. Available: https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

[4] D. Maguire, "What's happening with the optus data breach? What we know about the alleged hacker's ransom, data release and apology," *ABC News*, 2022, Available: https://www.abc.net.au/news/2022-09-27/optus-data-breach-cyber-attack-hacker-ransom-sorry/101476316

[5] S. Chalmers, "Qantas confirms 5.7 million customers were impacted in cyber attack," *ABC News*, 2025, Available: https://www.abc.net.au/news/2025-07-09/qantas-confirms-number-of-customers-impacted-in-cyber-attack/105510654