Threat Analysis

Authentication Attacks

According to the "Annual Cyber Threat Report 2023-2024", the most frequently reported threat in Australia were Authentication attacks in the form of "compromised accounts or credentials"(Australian Cyber Security Centre, 2024), 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.

Section 2: Authentication Threats Case Study (~300 words)

Purpose: Deep analysis of the threat landscape
Subsections:

2.1 Current Threat Landscape Background (~100 words)

Content: In July 2025, Qantas confirmed that 5.7 million customers were impacted in a cyberattack, demonstrating the ongoing threat to Australian organizations (Chalmers, 2025).

- 2024-2025 statistics on authentication attacks
- Prevalence in recent breach reports
- Evolution of attack sophistication
- Industry sectors most affected

Key Stats to Include: - 99% of identity attacks are password attacks (Microsoft) - 88% of breaches involve stolen credentials (Verizon) - Password reuse statistics

2.2 Typical Adversary Tradecraft (~150 words)

Purpose: Technical analysis of attack methods

Content:

- **Brute Force:** Traditional systematic guessing, tools, detectability
- **Password Spraying:** "Low and slow" methodology, evasion techniques, recent examples
- **Credential Stuffing:** Leveraging breach data, automation, success factors
- **Attack Infrastructure:** Tools, botnets, scaling methods

Technical Details:

- Specific tools used (Hydra, Hashcat, etc.)
- Attack timing and patterns
- Evasion techniques

2.3 Organizational Impact (~50 words)

Content:

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 (Maguire, 2022). More recently, the Qantas breach in July 2025 affected 5.7 million customers, with varying degrees of personal information compromised (Chalmers, 2025). 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.

- Financial costs (cite specific figures)
- Operational disruption
- Detection and containment timelines
- Reputation and compliance implications

Rubric Alignment: Addresses "typical adversary trade craft, the potential impact for an organisation"

Section 3: Threat Choice Justification (~150 words)

Purpose: Argumentative section explaining selection rationale

Structure:

3.1 Prevalence and Relevance (~50 words)

- Current threat statistics
- Real-world case studies from 2024
- Universal applicability across organizations

3.2 Technical Analysis Opportunities (~50 words)

- Multiple attack vectors to examine
- Rich tool ecosystem for analysis
- Clear success/failure metrics
- Laboratory feasibility

3.3 Framework Integration Potential (~50 words)

- Strong MITRE ATT&CK mapping (T1110 family)
- Essential 8 mitigation alignment
- Comprehensive defensive strategies available

Rubric Alignment: Addresses "Justify your threat choice" and demonstrates "consultation of the landscape and relatedness to modern challenges"

Section 4: Research Foundation (~50 words)

Purpose: Bridge to tool selection phase **Content:** - Summary of research methodology - Key sources consulted - Transition statement to tool comparison phase

Rubric Alignment: Shows "consultation of the landscape" through reference quality

---

Structural Notes:

Writing Style Requirements:

- Academic tone with IEEE citations
- Avoid bullet points (use prose paragraphs)
- Bold key statistics for scannability
- Logical flow between sections

Citation Strategy:

- **15-20 sources minimum** (IEEE format)
- **Primary sources preferred:** Verizon DBIR, Microsoft reports, IBM studies
- **Current data:** 2024-2025 reports and statistics
- **Mix of:** Industry reports, academic sources, case studies

Connection Points:

- **Forward Links:** Sets up tool selection criteria
- **Backward Links:** References assignment objectives
- **Framework Prep:** Establishes MITRE/Essential 8 foundation

Assessment Criteria Focus:

This structure targets **Criteria 1: Planning and Justification** specifically: - Case study provided - Justification with examples
- Landscape consultation through reference - Modern challenges and relevance addressed - Foundation for TTPs and metrics

---

Quality Checkpoints:

Before Writing:

☐ All sections have clear purpose
☐ Word count targets realistic
☐ Rubric requirements mapped
☐ Citation sources identified

During Writing:

☐ Each paragraph advances the argument
☐ Statistics properly cited
☐ Technical depth appropriate
☐ Flow between sections logical

After Writing:

☐ Word count within target (~500)
☐ All citations in IEEE format
☐ No bullet points or lists used
☐ Sets up tool selection phase effectively

Authentication Attack Scenario Design - Dot Point Plan

Testing Scenario Overview

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

Environment Setup

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

Target Applications

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

Phase 1: Synthetic Data Generation

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

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

Phase 2: Attack Implementation (Offensive Tool)

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

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

Phase 3: Defensive Implementation

Baseline Testing (No Defenses)

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

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

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

Defense Tool 3: Enhanced Monitoring

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

Success Metrics Definition

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

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

Overall Effectiveness Metrics

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

MITRE ATT&CK Framework Mapping

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

Supporting Techniques

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

Testing Timeline

Week 1: Environment setup and data generation

Week 2: Attack tool development and testing

Week 3: Baseline attack execution (no defenses)

Week 4: Defense implementation and protected testing

Week 5: Analysis, comparison, and documentation

Expected Outcomes

Attack Tool Analysis

- Personalized passwords significantly more effective than generic wordlists

- Lower detection rates with slow, targeted approach
- Pattern effectiveness varies by demographic correlation

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

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

Australian Cyber Security Centre (2024) *Annual cyber threat report 2023-2024*. Australian Signals Directorate. Available at: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024.

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

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