Password Attack Simulations: Dictionary vs. Known Password Attacks

Educational Cybersecurity Demonstration

Tamim Hasan Saad (2005095)
Habiba Rafique (2005096)

Department of Computer Science & Engineering
Bangladesh University of Engineering & Technology

CSE 406 - Computer Security
January 2025

Outline

1. Introduction
2. Dictionary Attack
3. Known Password Attack
4. Attack Comparison

Project Overview

Educational Purpose:

- Defensive security research
- Understanding attack methodologies
- Developing countermeasures
- Academic cybersecurity training

Attack Types Implemented:

1. Dictionary Attack
   - High-volume brute force
   - Common password lists
   - Easily detectable
2. Known Password Attack
   - OSINT-based targeting
   - Personal information exploitation
   - Stealthy approach

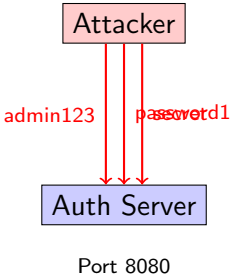
Dictionary Attack: Overview

Attack Methodology:

- Systematic testing of common passwords
- Uses wordlist with 5,530+ passwords
- High-speed automated attempts
- TCP/IP packet-level analysis
- HTTP POST request simulation

Target Configuration:

- Server runs on port 8080
- Admin account with configurable password
- Real-time logging and monitoring



Dictionary Attack: Server Initialization

Description: Dictionary attack victim server starting up on port 8080 with available user accounts and dynamic password configuration capability.

Dictionary Attack: Attacker Initialization

Description: Dictionary attacker initializing with packet-level analysis, loading wordlist containing 5,530+ common passwords for systematic testing.

Dictionary Attack: Execution Process

Description: Attack execution showing TCP/IP packet construction, HTTP request simulation, and systematic password testing with response time analysis.

Dictionary Attack: Success Demonstration

Description: Successful password discovery ("secret") after 12 attempts, demonstrating the effectiveness against weak passwords in common dictionaries.

Dictionary Attack: Results Analysis

Description: Comprehensive attack analysis showing detailed attempt logs, response times, success patterns, and victim server monitoring data.

Dictionary Attack: Technical Implementation

Packet-Level Features:

- IP header construction & logging
- TCP header analysis
- HTTP payload inspection
- Response time measurement
- User-Agent rotation for stealth

Attack Characteristics:

- Speed: 100+ attempts per minute
- Detection: High (volume-based)
- Success rate: High vs. weak passwords
- Wordlist: Common passwords

Sample Attack Log:

```
Dictionary Attack Server (Port 8080)
[*] Server will bind to 0.0.0.0:8080
[*] Dictionary Attack Victim Server Configuration
============================================================
Enter target username (default: admin): admin
Enter password for admin: secret
[*] User configured: admin:secret
[*] Password hash: 2bb80d537b1da3e3...
[+] Authentication server started on 0.0.0.0:8080
[*] Waiting for connections...
[*] Press Ctrl+C to stop the server

[2025-07-30 02:54:48] 127.0.0.1 - admin:password - FAILED
[2025-07-30 02:54:48] 127.0.0.1 - admin:123456 - FAILED
[2025-07-30 02:54:48] 127.0.0.1 - admin:admin - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:letmein - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:welcome - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:password123 - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:admin123 - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:qwerty - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:abc123 - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:12345678 - FAILED
[2025-07-30 02:54:49] 127.0.0.1 - admin:password1 - FAILED
[2025-07-30 02:54:50] 127.0.0.1 - admin:secret - SUCCESS
```

Dictionary Attack: Technical Implementation

FAILED Attack Log:

```
============================================================
[*] ATTEMPT #11: admin:password1
============================================================
[*] Establishing TCP connection to 127.0.0.1:8080
[*] Simulated packet construction:
[!] Packet header construction error: index out of range
[*] Skipping packet simulation due to header error
    HTTP Request: POST /login (user: admin, pass: password1)

[*] Sending actual HTTP request via TCP socket...
[*] Response received: 272 bytes

[-] Failed attempt 11: admin:password1 (Response time: 0.002s)
[*] Progress: 0.2% (12/5530)
```

SUCCESSFUL Attack Log:

```
[*] ATTEMPT #12: admin:secret
============================================================
[*] Establishing TCP connection to 127.0.0.1:8080
[*] Simulated packet construction:
[SIMULATED SEND] Packet Details:
[SEND] IP Header:
    Version: 4, IHL: 5, TOS: 0
    Total Length: 471, ID: 57632
    Flags: 0, Fragment Offset: 0
    TTL: 64, Protocol: 6, Checksum: 0x56f3
    Source IP: 192.168.1.100, Destination IP: 127.0.0.1
[SEND] TCP Header:
    Source Port: 18627, Destination Port: 8080
    Sequence: 43617, Acknowledgment: 52815
    Data Offset: 5, Flags: PSH|ACK (0x18)
    Window: 8192, Checksum: 0x5747, Urgent Pointer: 0
    Payload Length: 431
    HTTP Request: POST /login (user: admin, pass: secret)

[*] Sending actual HTTP request via TCP socket...
[SIMULATED RECV] Response packet details:
[RECV] IP Header:
    Version: 4, IHL: 5, TOS: 0
    Total Length: 343, ID: 9097
    Flags: 0, Fragment Offset: 0
    TTL: 64, Protocol: 6, Checksum: 0x150b
    Source IP: 127.0.0.1, Destination IP: 192.168.1.100
[RECV] TCP Header:
    Source Port: 8080, Destination Port: 40225
    Sequence: 52815, Acknowledgment: 44048
    Data Offset: 5, Flags: PSH|ACK (0x18)
    Window: 8192, Checksum: 0xc54c, Urgent Pointer: 0
    Payload Length: 303

[+] SUCCESS! Found password: secret (Response time: 0.003s)
```

Dictionary Attack: Technical Implementation

Attack Summary

Dictionary Attacker

```
============================================================
              DICTIONARY ATTACK SUMMARY
============================================================
Target: 127.0.0.1:8080
Username: admin
Attack duration: 1.23 seconds
Total attempts: 12
Average response time: 0.002 seconds
Attempts per second: 9.74

[+] ATTACK SUCCESSFUL!
[+] Valid credentials found: admin:secret
[+] Password cracked on attempt #12
[+] Time to success: 1.23 seconds
```

Dictionary Attack: Technical Implementation

Detection Indicators:

- High volume of failed attempts
- Sequential password patterns
- Fast request timing
- Single source IP

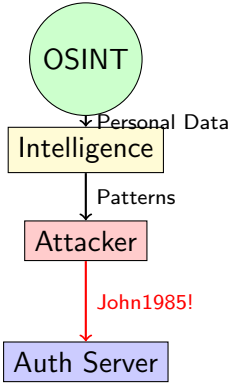
Known Password Attack: Overview

OSINT-Based Methodology:

- Intelligence gathering on target
- Personal information exploitation
- Pattern-based password generation
- Human-like behavior simulation
- Low-volume targeted attempts

Target Profile (John Smith):

- Born: 1985, Pet: Buddy
- Hometown: Boston, Team: Patriots
- Company: TechCorp
- Generates 239 password candidates



Known Password Attack: Server with User Profiles

Description: Known password attack victim server on port 8081 displaying detailed user profiles with personal information patterns for OSINT simulation.

Known Password Attack: OSINT Intelligence Gathering

Description: OSINT-based attacker gathering intelligence on John Smith, collecting personal information including birth year, pet name, hometown, and other identifying data.

Known Password Attack: Pattern Generation

Description: Password candidate generation using personal information patterns, creating 239 targeted password variations based on collected intelligence.

Known Password Attack: Successful Breach

Description: Successful password discovery "John1985!" on attempt 2, demonstrating high effectiveness of personal information-based attacks.

OSINT Intelligence Sources

Real-World OSINT Sources:

- Social media profiles (Facebook, Twitter)
- Professional networks (LinkedIn)
- Public records & databases
- News articles & press releases
- Company directories
- Data breaches & leaks

Collected Intelligence:

- Full name: John Smith
- Birth year: 1985
- Pet name: Buddy
- Hometown: Boston
- Favorite team: Patriots
- Company: TechCorp
- Job title: Developer

Pattern Examples: FirstName + BirthYear + Special → `John1985!`

Known Password Attack: Technical Analysis

Attack Patterns:

1. FirstName + BirthYear + Special
2. PetName + CurrentYear
3. Hometown + BirthYear + Special
4. FavoriteTeam + BirthYear
5. Company + BirthYear
6. Personal variations (239 total)

Stealth Features:

- Human-like delays (0.5–2.0s)
- Limited attempts (avoid lockout)
- Randomized User-Agents
- Pattern analysis tracking

Sample Attack Log:

```
Enter John Smith's password: smith123456
[*] Password configured for john.smith: smith123456
[*] Detected pattern: LastName + CommonNumbers
[*] Password hash: 3f8a7499fe960728...
[+] Known Password Attack Server started on 0.0.0.0:8081
[*] Waiting for connections...
[*] Press Ctrl+C to stop the server

[2025-07-30 03:08:05] 127.0.0.1 - john.smith:john1985 - FAILED [Contains: FirstN
ame, BirthYear]
[2025-07-30 03:08:06] 127.0.0.1 - john.smith:TECHCORP85 - FAILED
[2025-07-30 03:08:08] 127.0.0.1 - john.smith:John6789 - FAILED [Contains: FirstN
ame]
[2025-07-30 03:08:09] 127.0.0.1 - john.smith:1John85 - FAILED [Contains: FirstNa
me]
[2025-07-30 03:08:10] 127.0.0.1 - john.smith:345John - FAILED [Contains: FirstNa
me]
[2025-07-30 03:08:12] 127.0.0.1 - john.smith:johnpassword - FAILED [Contains: Fi
rstName]
[2025-07-30 03:08:13] 127.0.0.1 - john.smith:234john - FAILED [Contains: FirstNa
me]
[2025-07-30 03:08:14] 127.0.0.1 - john.smith:JOHN1985 - FAILED [Contains: FirstN
ame, BirthYear]
```

Known Password Attack: Technical Implementation

FAILED Attack Log:

```
[*] Sending actual OSINT-based HTTP request via TCP socket...
[SIMULATED RECV] Response packet details:
[RECV] IP Header:
    Version: 4, IHL: 5, TOS: 0
    Total Length: 459, ID: 51679
    Flags: 0, Fragment Offset: 0
    TTL: 64, Protocol: 6, Checksum: 0x6e3f
    Source IP: 127.0.0.1, Destination IP: 192.168.1.101
[RECV] TCP Header:
    Source Port: 8081, Destination Port: 52313
    Sequence: 14260, Acknowledgment: 76332
    Data Offset: 5, Flags: PSH|ACK (0x18)
    Window: 8192, Checksum: 0x239d, Urgent Pointer: 0
    Payload Length: 419

[-] Failed attempt 29: 0123John (Pattern: FirstName + CommonNumbers)
[*] Waiting 0.6s before next attempt...
```

SUCCESSFUL Attack Log:

```
======================================================================
[*] OSINT-BASED ATTEMPT #139: john.smith:john1985
======================================================================
[*] Password pattern: BirthYear
[*] Establishing TCP connection to 127.0.0.1:8081
[*] Simulated packet construction:
[SIMULATED SEND] Packet Details:
[SEND] IP Header:
    Version: 4, IHL: 5, TOS: 0
    Total Length: 553, ID: 33856
    Flags: 0, Fragment Offset: 0
    TTL: 64, Protocol: 6, Checksum: 0xb380
    Source IP: 192.168.1.101, Destination IP: 127.0.0.1
[SEND] TCP Header:
    Source Port: 18989, Destination Port: 8081
    Sequence: 52122, Acknowledgment: 31686
    Data Offset: 5, Flags: PSH|ACK (0x18)
    Window: 8192, Checksum: 0x65b8, Urgent Pointer: 0
    Payload Length: 513
    HTTP Request: POST /login (user: john.smith, pass: john1985)
    OSINT Pattern: BirthYear

[*] Sending actual OSINT-based HTTP request via TCP socket...
[SIMULATED RECV] Response packet details:
[RECV] IP Header:
    Version: 4, IHL: 5, TOS: 0
    Total Length: 511, ID: 28002
    Flags: 0, Fragment Offset: 0
```

Known Password Attack: Technical Implementation

Attack Summary

Known Password Attacker

```
==================================================================
              KNOWN PASSWORD ATTACK SUMMARY
==================================================================
Target: 127.0.0.1:8081
Username: john.smith
Intelligence gathering: Successful
Attack duration: 293.39 seconds
Total attempts: 239
Password candidates generated: 239
Average response time: 0.002 seconds
Attempts per minute: 48.9

[-] ATTACK FAILED
[-] No valid password found in generated candidates
```

Known Password Attack: Technical Analysis

Detection Challenges:

- Low attempt volume
- Human-like timing
- Highly targeted approach
- Appears as normal user behavior

Dictionary vs. Known Password Attack Comparison

Characteristic	Dictionary Attack	Known Password Attack
Speed	Fast (100+ attempts/min)	Slow (human-like timing)
Volume	High (5,530+ passwords)	Low (targeted attempts)
Detection	Easy (high volume)	Difficult (stealthy)
Success Rate	High vs. weak passwords	High vs. personal passwords
Intelligence	Generic wordlists	OSINT-based targeting
Preparation	Minimal	Extensive OSINT gathering
Stealth Level	Low	High
Countermeasures	Rate limiting effective	Requires behavioral analysis