■■ AI Honeypot

User Guide

> **An intelligent deception system that predicts attacker behavior using machine learning**

What Makes This Special

■ **ML-Based Attack Prediction** - Markov chains predict the attacker's next move

■ **MITRE ATT&CK; Integration** - Industry-standard threat intelligence mapping

■ **Real-Time Dashboard** - WebSocket-powered live attack monitoring

■ **Auto-Generated Playbooks** - Instant incident response procedures

■ **Threat Intel Export** - IOCs and STIX 2.1 bundles for sharing

■ **Adaptive Deception** - Responses adjust to attacker skill level

---

Quick Start

Start the Honeypot

```
# Option 1: Python
python app.py

# Option 2: Docker (Recommended)
docker-compose up --build
```

Access: `http://localhost:8000`

Try It Out

1. Real-Time Dashboard

URL: `http://localhost:8000/demo`

Watch attacks appear in real-time with threat levels and skill detection.

2. Launch Test Attacks

Try these URLs to simulate attacks:

```
SQL Injection:
http://localhost:8000/search?q=' OR 1=1--

Authentication Bypass:
http://localhost:8000/login?user=admin&pass;=' OR '1'='1

XSS Attack:
http://localhost:8000/search?q=<script>alert('XSS')</script>
```

3. Get Your Attacker ID

1. Press **F12** (DevTools)
2. Go to **Application** → **Cookies**
3. Copy the `attacker_id` value

You'll need this ID for the API endpoints below.

API Endpoints

Replace `{id}` with your attacker ID from cookies.

Attack Prediction

```
GET /api/prediction/{id}
```

Returns: Next likely attack, time-to-compromise, predicted goal

MITRE ATT&CK; Mapping

```
GET /api/mitre/{id}
```

Returns: Tactics, techniques, APT group matches

Forensic Timeline

```
GET /api/timeline/{id}
```

Returns: Complete attack timeline with statistics

Attack Narrative

```
GET /api/timeline/{id}/narrative
```

Returns: Human-readable attack story

Indicators of Compromise

```
GET /api/threat-intel/{id}/iocs
```

Returns: IOCs with confidence scores

STIX Bundle

```
GET /api/threat-intel/{id}/stix
```

Returns: STIX 2.1 threat intelligence bundle

Incident Response Playbook

```
GET /api/playbook/SQL%20Injection
```

Returns: Downloadable incident response guide

CSV Export

```
GET /api/export/attacks
```

Returns: All attacks in spreadsheet format

How It Works

Attack Prediction (Markov Chains)

The system learns from attack sequences:

• Tracks what attacks follow other attacks

• Builds probability matrix (e.g., SQL Injection → Admin Access: 60%)

• Predicts next move and time-to-compromise

• Adapts as it observes more attacks

MITRE ATT&CK; Integration

Every attack is mapped to the framework:

• **Tactics** - The "why" (INITIAL_ACCESS, CREDENTIAL_ACCESS)

• **Techniques** - The "how" (T1190: Exploit Public-Facing Application)

• **APT Matching** - Compares behavior to known threat groups

Adaptive Deception

Responses adjust based on detected skill level:

• **NOVICE** - Easy wins to keep them engaged

• **INTERMEDIATE** - Realistic balanced responses

• **ADVANCED** - Rabbit holes and time-wasting fake leads

• **AUTOMATED** - Honeypot evasion techniques

Use Cases

Security Research

Study attacker behavior patterns and discover new techniques

Enterprise Security

Early warning system for targeted attacks with industry-specific threat intel

Incident Response Training

Practice with real attack timelines and auto-generated playbooks

Threat Intelligence Sharing

Export STIX bundles to share with community and feed IOCs into SIEM

Key Features

Real-Time Monitoring

- WebSocket-powered dashboard
- Live attack notifications
- Threat level indicators
- Skill level detection

Forensic Capabilities

- Complete attack timelines
- Attack replay scripts
- Human-readable narratives
- Campaign comparison

Threat Intelligence

- IOC generation with confidence scores
- STIX 2.1 bundle export
- MITRE ATT&CK; mapping
- APT group matching

Automation

- Auto-generated incident response playbooks

• Sigma rules for SIEM integration

• CSV export for analysis

• One-click threat intel sharing

Technical Specifications

| Component | Technology |

|-----------|-----------|

| **Backend** | Python 3.11, FastAPI |

| **Real-time** | WebSockets |

| **ML** | Markov chains |

| **Standards** | MITRE ATT&CK;, STIX 2.1 |

| **Deployment** | Docker, docker-compose |

| **Performance** | <100ms response, 100+ concurrent connections |

Example Workflow

1. **Attacker hits the honeypot** → SQL injection on `/search`
2. **System detects attack** → Pattern matching + LLM analysis
3. **Logs to timeline** → Records attack with timestamp
4. **Updates ML model** → Markov chain learns the pattern
5. **Maps to MITRE** → Identifies technique T1190
6. **Predicts next move** → 60% probability of admin access
7. **Broadcasts to dashboard** → Real-time update via WebSocket
8. **Generates intelligence** → IOCs, STIX bundle, playbook ready

---

API Endpoint Summary

| Endpoint | Description |

|---|---|

| `/api/prediction/{id}` | ML-based attack predictions |

| `/api/mitre/{id}` | MITRE ATT&CK; mapping |

| `/api/timeline/{id}` | Forensic timeline data |

| `/api/timeline/{id}/narrative` | Human-readable story |

| `/api/threat-intel/{id}/iocs` | Indicators of Compromise |

| `/api/threat-intel/{id}/stix` | STIX 2.1 bundle |

| `/api/playbook/{type}` | Incident response guide |

| `/api/export/attacks` | CSV export |

| `/api/canary/dashboard` | Canary token analytics |

What You Get

■ **Predictive Intelligence** - Know what attackers will do next

■ **Industry Standards** - MITRE ATT&CK; and STIX 2.1 compliance

■ **Actionable Output** - Playbooks, IOCs, and STIX bundles ready to use

■ **Real-Time Visibility** - See attacks as they happen

■ **Production Ready** - Docker deployment, comprehensive APIs

■ **Fully Tested** - 10/10 endpoints verified working

Learn More

• **GitHub:** https://github.com/madhurgrover-cs/ai-honepot

• **Full Documentation:** See repository README

• **Technical Details:** See `technical_deep_dive.md`