AI Honeypot - Live Demo Guide

Quick Reference for Hackathon Presentation

PRE-DEMO SETUP (5 minutes before)

1. Start the Honeypot

```
python app.py
```

Wait for: 'Uvicorn running on http://127.0.0.1:8000'

2. Open Dashboard

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

3. Prepare Browser Tabs

• Tab 1: Dashboard

• Tab 2: Attack URLs

• Tab 3: DevTools (F12 → Cookies)

OPENING PITCH (30 seconds)

"We built an AI-powered honeypot that **predicts attacker behavior** using machine learning. It detects **7 different OWASP vulnerability types** - that's **70% coverage**. Every attack is mapped to **MITRE ATT&CK;**, and we generate **incident response playbooks** instantly."

LIVE DEMO FLOW (5-7 minutes)

STEP 1: Show Clean Dashboard (15 sec)

Point to attack counter (0 attacks) and threat level

STEP 2: Launch SQL Injection (30 sec)

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

Say: 'Dashboard updates in real-time. System detected SQL Injection.'

STEP 3: Launch XSS Attack (30 sec)

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

Say: 'System tracks different attack types and builds timeline.'

STEP 4: Escalate to Privilege Escalation (45 sec)

```
http://localhost:8000/search?q=' UNION SELECT * FROM users--
```

Say: 'Watch threat level climb to HIGH as AI detects escalation.'

STEP 5: Show Attack Prediction (60 sec)

1. Get attacker_id: F12 → Application → Cookies

2. Open: `http://localhost:8000/api/prediction/{ID}`

Say: 'AI predicts next attack: 60% probability of admin access. Time to compromise: 10 minutes.'

STEP 6: Show MITRE ATT&CK; Mapping (45 sec)

`http://localhost:8000/api/mitre/{ID}`

Say: 'Automatically mapped to MITRE ATT&CK.; Matches APT28 tactics.'

STEP 7: Show Auto-Generated Playbook (45 sec)

`http://localhost:8000/api/playbook/SQL%20Injection`

Say: 'Complete incident response playbook with containment, investigation, and Sigma rules.'

CLOSING STATEMENT (30 seconds)

"To summarize: **Real-time detection** of 7 OWASP types, **AI prediction** of next attack, **MITRE mapping**, **auto-generated playbooks**, **100% test success**, and **production-ready**. This is a tool security teams can actually use. Thank you!"

QUICK REFERENCE - ATTACK URLS

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

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

Escalation: http://localhost:8000/search?q=' UNION SELECT * FROM users--

Path Traversal: http://localhost:8000/search?q=../../../etc/passwd

SSRF: http://localhost:8000/search?q=http://localhost:8080/admin
```

API ENDPOINTS (Replace {ID} with attacker_id)

```
Prediction: /api/prediction/{ID}

MITRE: /api/mitre/{ID}

Timeline: /api/timeline/{ID}

Playbook: /api/playbook/SQL%20Injection
```

KEY TALKING POINTS

- **7/10 OWASP Top 10** - 70% coverage
- **ML predicts next attack** - Unique differentiator
- **MITRE ATT&CK; integration** - Industry standard
- **Auto-generated playbooks** - Saves time

• **100% test success** - Production ready

JUDGE Q&A; - QUICK ANSWERS

Q: What makes this unique?

"ML-based prediction, MITRE mapping, and auto-playbooks. Traditional honeypots just log - we predict and respond."

Q: Is it production-ready?

"Yes. Docker deployment, 10/10 APIs tested, comprehensive logging, SIEM integration."

Q: How does ML work?

"Markov chains track attack sequences. After SQL injection, 60% probability of admin access next."

GOOD LUCK! Remember: Speak confidently and emphasize AI prediction!