VANTAGE POINT

AI Odyssey Labs

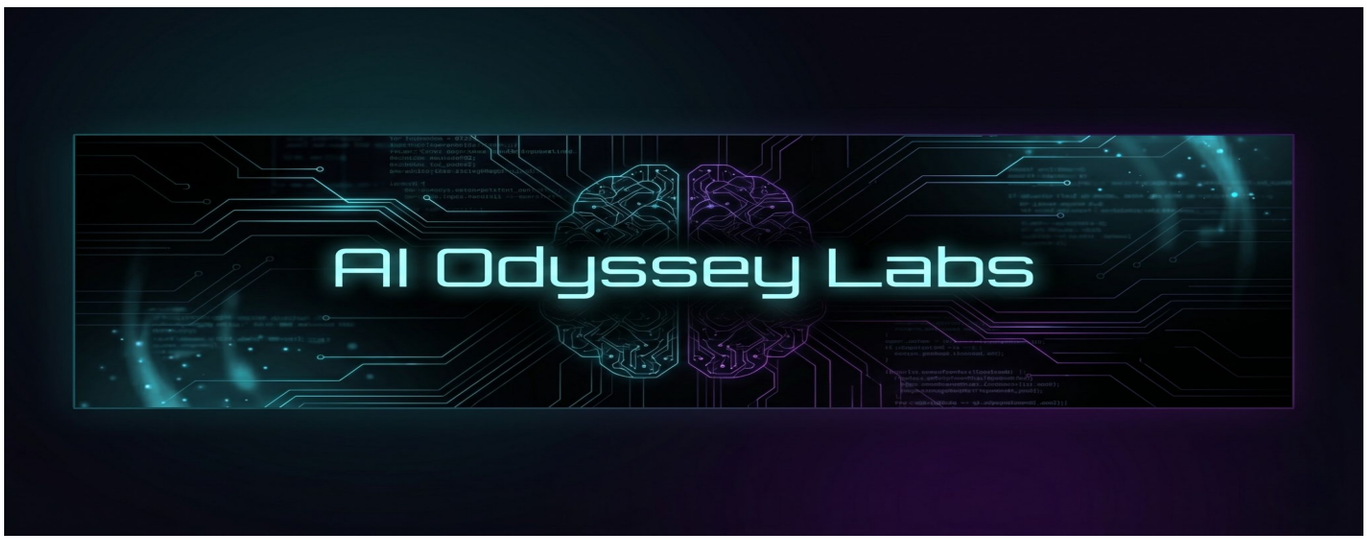
Hacking Lab Guide

Candidate Handbook

1. Introduction

Welcome to **AI Odyssey Labs**.
Experience what it takes to weaponize AI against real applications and attack AI-powered systems themselves. This is a specialized, hands-on environment built around carefully curated challenges that reflect the evolving intersection of AI and security.

These aren't simplified CTF puzzles. You will utilize intelligent AI agents, craft sophisticated attacks, and critically validate findings against live targets in isolated, real-world-like environments. AI Odyssey Labs is your starting line. It is designed to test your practical skills at using AI in offensive security and give you a definitive taste of this rapidly emerging domain. Once you successfully navigate these challenges, your next adventure awaits.

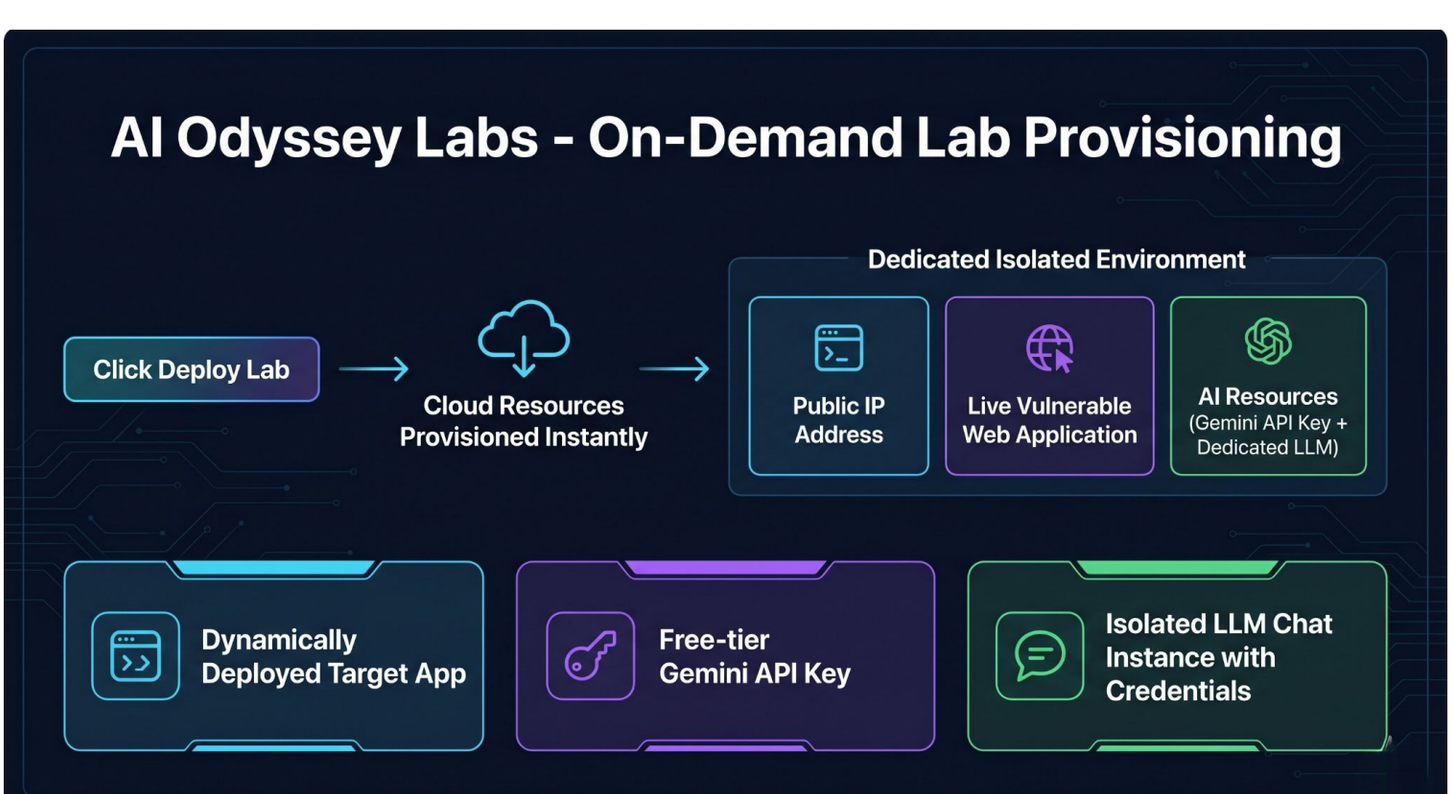


IMPORTANT: Before You Begin

Before solving a challenge, ensure you click the Deploy Lab button on the challenge description page. This will automatically provision and launch the target application for you to work on.

2. About The Lab Infrastructure

AI Odyssey Labs is a dynamic, hands-on adversarial AI security environment designed to push the boundaries of offensive AI capabilities. Participants receive dedicated, isolated lab instances that are automatically provisioned on demand. Each challenge blends real-world scenarios where you will use AI to attack applications, attack AI systems directly, and validate AI-generated security findings — offering a unique journey into the future of AI-powered red teaming.



> As part of the deployment process, the lab environment provisions the following core components:

Containerized Target Application:
A standalone, vulnerable service running within a Docker container, precisely configured to replicate the exact conditions of real-world targets.

Dedicated Host Infrastructure:
A dedicated Linux or Windows machine hosting the target, providing a realistic, production-grade environment essential for deep enumeration.

Ready-to-Use AI Resources:
Pre-configured free-tier Gemini API key and dedicated LLM instances with access credentials.

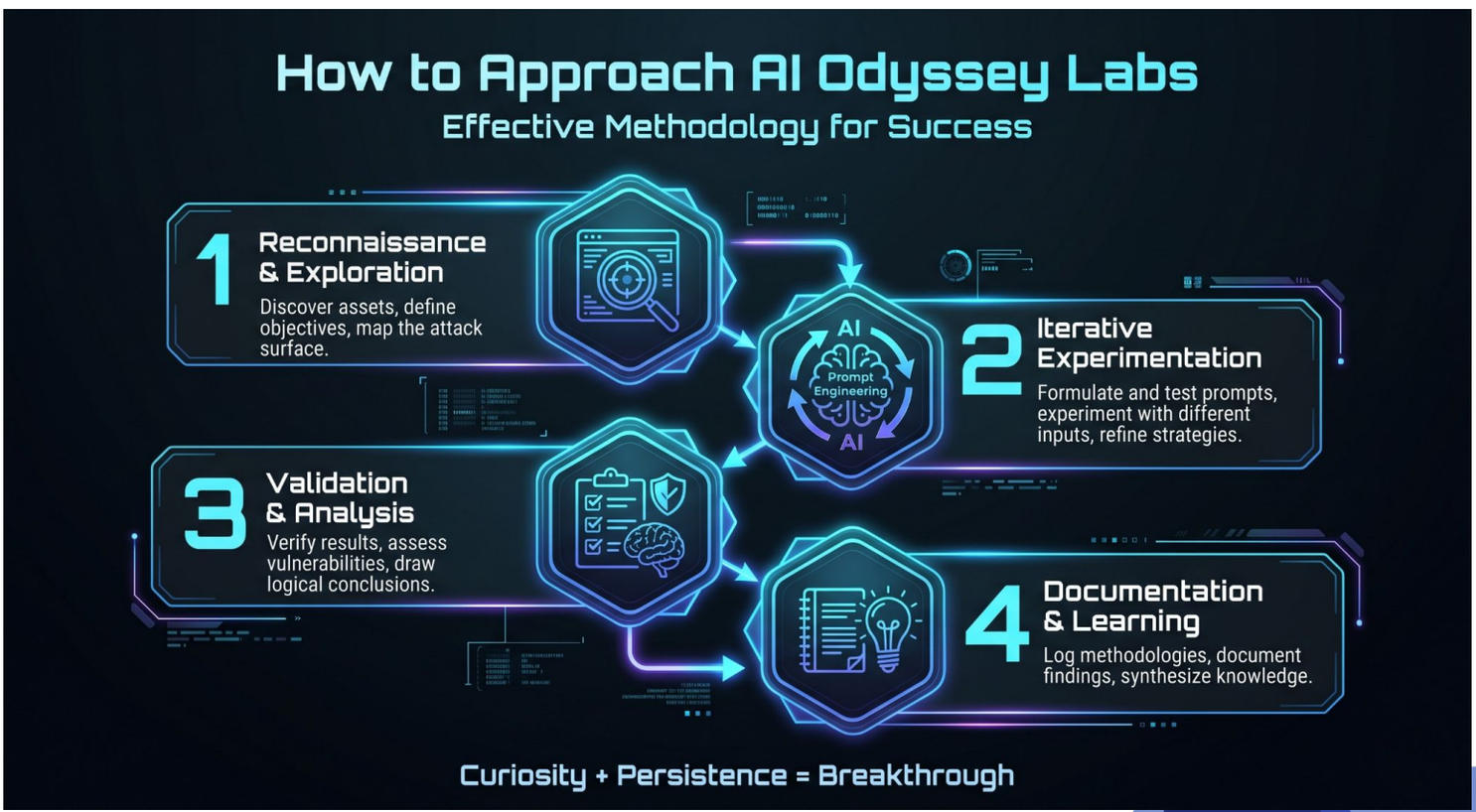
Once the environment is successfully provisioned, the system will provide a "**Dedicated Target IP Address**" and other required resources for the challenge. Using containerized, dedicated machines for each challenge, we provide a realistic and interference-free environment to safely test exploits, payloads, etc., just like in real-world penetration testing.

3. How To Approach The Lab

Approach each lab with curiosity and persistence. Start by thoroughly exploring the deployed environment and understanding its behavior. Use the provided AI resources creatively while maintaining a structured methodology. Remember that success in these challenges often comes from iterative experimentation, thoughtful prompt engineering, and the ability to validate machine-generated outputs with human judgment. Treat every roadblock as part of the learning journey rather than a dead end.

General Methodology

- **Reconnaissance & Exploration**: Spend initial time understanding the target application, its features, and expected behavior before launching any attacks.
- **Iterative Experimentation**: Use trial-and-error with AI agents and prompts, carefully observing responses and refining your approach with each attempt.
- **Validation & Analysis**: Always cross-verify results — whether AI-generated findings or successful injections — using manual testing and logical reasoning.
- **Documentation & Learning**: Record your methodology, successful techniques, and lessons learned for maximum skill development during the event.



4. Event Features & Rules

1

Varied Challenges:

Tackle an ever-updating roster of high-impact vulnerabilities.

2

Comprehensive Content Library:

If you hit a roadblock, the platform provides a detailed content library with walkthroughs and solutions for every lab.

3

Leaderboard Tracking:

Earn points for each successful exploit and track your standing against other cybersecurity enthusiasts in the Vantage Point community.

4

Time Limits & Resets:

If you miss the time limit, you have a maximum of **3 reset requests**. Use the comment box or chat bubble to request a reset with a valid reason.

5. Skills & Tools Required

Core Competencies

Prompt Engineering & AI Interaction:

Ability to craft effective prompts and guide AI agents toward desired outcomes.

Web Application Security Fundamentals:

Good understanding of common web vulnerabilities, APIs, and basic reconnaissance techniques.

Analytical & Critical Thinking:

Sharp judgment to evaluate AI outputs, identify false positives, and connect observations to meaningful conclusions.

Recommended Toolset

- Open-Source Autonomous Pentest Agents like CAI, PentAGI, Redamon, etc.
- Coding Agents like Claude code, gemini-cli, Opencode, codex, etc.
- Netcat, NGROK, or VPS (for catching reverse shells)
- Custom AI Frameworks (if any)
- Public or custom payloads for prompt injection

6. Evaluation Criteria

> Once you submit your proof of concept, the team manually evaluates your submission.

80%

Technical Execution:

Successfully and fully solving the challenge, demonstrating a thorough understanding and execution of the core objectives.

20%

Reporting & Creativity:

Submitting detailed reports with screenshots to showcase the approach taken, as well as demonstrating creativity and out-of-the-box thinking.

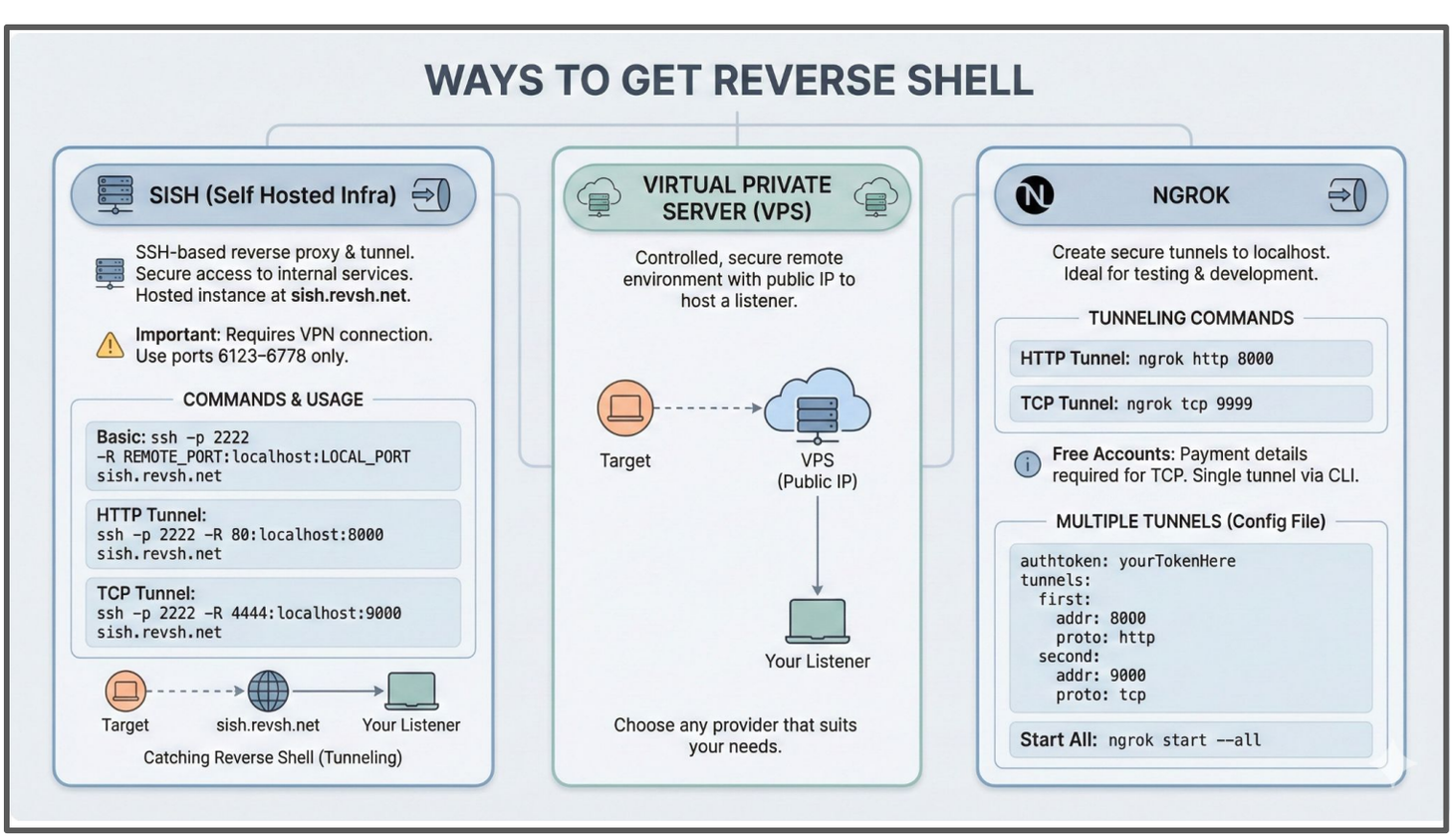
7. Catching Reverse Shells

- After you exploit a target, challenges may require you to obtain a reverse shell to gain interactive control. Normally, this requires a public IP address.
  However, since you are working from a local machine (likely behind NAT), we provide solutions to handle port forwarding and tunnel the connection back to you.

- **Option A:** Use our own self-hosted infra: **sish.revsh.net**

  Option B: Your own VPS

  Option C: Ngrok (Secure tunneling platform)



8. Do’s and Don’ts

9. Badges & Recognition

- **Earning Badges:** As you successfully complete and submit challenges with valid submissions, you will automatically earn exclusive badges and verified skills. These will be showcased directly on your Vantage Point profile to highlight your practical expertise.

Good luck, Analyst.

The AI Lab awaits.

VANTAGE POINT

Vantagepoint

The Future Of Cybersecurity Start Here

Other Certifications & Labs:

- Multi-Cloud Security Expert
- Certified Web Appsec Expert
- Certified Mobile Appsec Expert
- Mobile Hacking Launchpad
- CVE Cipher: Decoding Threats
- Web Hacking Launchpad

training@enciphers.com

vantagepoint.enciphers.com