PROJECT: NEXUS V1 SUBMISSION

CHAMELEON DEFENSE SYSTEM

Moving Target Defense & Active Deception

FOCUS DOMAIN: Innovation & Emerging Tech

Created by Shashwat Shekhar

THE PROBLEM: STATIC TARGETS

In modern cloud architecture, security relies on thicker walls, but the **door never moves.**

- **Infinite Attack Window:** Once a hacker discovers an endpoint like `/admin/login`, they have unlimited time to exploit it.
- **Automated Scanning:** Bots can map an entire API surface in minutes and store the vulnerabilities for later use.
- **Reactive Defense:** Firewalls only block known threats. They cannot stop legitimate-looking requests to exposed endpoints.

STATIC = VULNERABLE

THE SOLUTION: MOVING TARGET DEFENSE

DYNAMIC MUTATION

We use **Python AST** to rewrite the server code every 30 seconds, randomizing API routes (e.g., /login_x9k2). The attack surface effectively vanishes.

ZERO-DOWNTIME SWITCHING

Utilizes an **Active/Passive Node architecture**. While one server mutates (restarts), the other handles traffic, ensuring 100% availability.

ACTIVE DECEPTION

We don't just block attacks. If a hacker uses a stale URL, the Proxy returns a **Honeypot Payload** (Fake DB), wasting their time and resources.

CLOUD ISOLATION

Fully containerized using **Docker** to bypass host-level interference and ensure deployment consistency on platforms like Render.

TECHNOLOGY STACK

PYTHON 3.9 | FASTAPI | UVICORN (STATRELOAD) | DOCKER | STREAMLIT | HTTPX ASYNC

CORE INNOVATION: AST MUTATION ENGINE

Unlike simple URL redirects, we modify the **Abstract Syntax Tree** of the running application code to physically change the Python function decorators on the disk.

DEMO HIGHLIGHTS

- The Mutation Event: Every 30 seconds the backend rewrites itself. You will see live console logs confirming the AST rewrite and node switch.

- The Bait (Phase 1): The Hacker Bot initially succeeds (200 OK), capturing the "current" secret route.

- The Trap (Phase 3): 26 seconds later, the bot replays the old endpoint. Because the system has mutated, it falls into the Honeypot.

- Visual Telemetry: The dashboard shows real-time node rotation, replay attempts, and defense posture.

- Log Evidence: Mutation cycles, proxy rewrites, and honeypot triggers are all visible via runtime logs.

ACTIVE DEFENSE

IMPACT & FUTURE ROADMAP

POTENTIAL IMPACT

Economic Asymmetry: We drastically increase the cost of an attack. A hacker must be right every 30 seconds; we only need them to fail once.

Devaluation of Intelligence: Automated scanning data becomes worthless within seconds of being gathered.

FUTURE ROADMAP

> **Kubernetes Integration:** Scaling from 2 nodes to a dynamic swarm of mutating pods.

> **AI-Driven Mutation:** Adjusting the mutation interval dynamically based on threat levels (e.g., speed up during an attack).

> **Production Ban-Lists:** Automatically propagating IP bans from the Honeypot to the Cloud Firewall.

```
user@nexus-v1:~/defense-system$ ./execute_slide.sh
```

TARGET APPLICATIONS

BANKING & FINANCIAL APIS

Protecting high-value transactional routes and sensitive gateways from automated exploitation.

GOVERNMENT INFRASTRUCTURE

Securing critical citizen services and internal databases against persistent state-level threats.

HEALTHCARE SYSTEMS

Ensuring HIPAA compliance by masking patient data portals from unauthorized scanning.

SAAS COMPANIES

Securing multi-tenant architectures and API keys for enterprise-grade service delivery.

PUBLIC INTERNET ROUTES

Any system exposing endpoints to the internet. If the door is visible, it can be attacked. We make the door invisible.