SiT SINGAPORE INSTITUTE OF TECHNOLOGY

M3I0N37🍉

Faculty: Information and Communication Technology (Information Security)

Students: Wong Xin Ying, Goh Dong Jing, Lang Jun Feng, Antonia Angela Hatem Attieh, Wong Jia Liang

A HONEYNET INFRASTRUCTURE

Objectives

Cybersecurity is a dynamic field where threats evolve constantly. The M3I0N37 project employs a honeynet to understand hacker's strategies and enhance defense mechanisms.

- Deploy a comprehensive **HONEYNET** infrastructure
- Capture and monitor attacker Tactics, Techniques, and Tools. (TTPs)
- Capture malicious file upload attempts.
- Capture attempts to retrieve and/or modify deceptive high-value data.
- Enhance understanding of **attacker's intent**.
- Analyze attacker's behaviors and motivations.

Features

HoneyPot Deployment

- **Conpot:** **Simulates** Industrial Control System to trap hackers.
- **Cowrie:** **Captures** and analyzes **SSH** and **Telnet** attacks.
- **DDoSPot**: Mitigates **DDoS** attacks by luring attackers.

File Transfer Protocol (FTP) File Upload

- **Secure file** upload via Docker containers.

Deceptive Directories

- Fake "**admin**" directory: **Tracks** attacker's actions with hidden attributes.
- Fake "**FTP**" directory: **Captures** unauthorized access attempts and monitors database/file changes.

FAKED FAKED FAKED

Live Attack Map

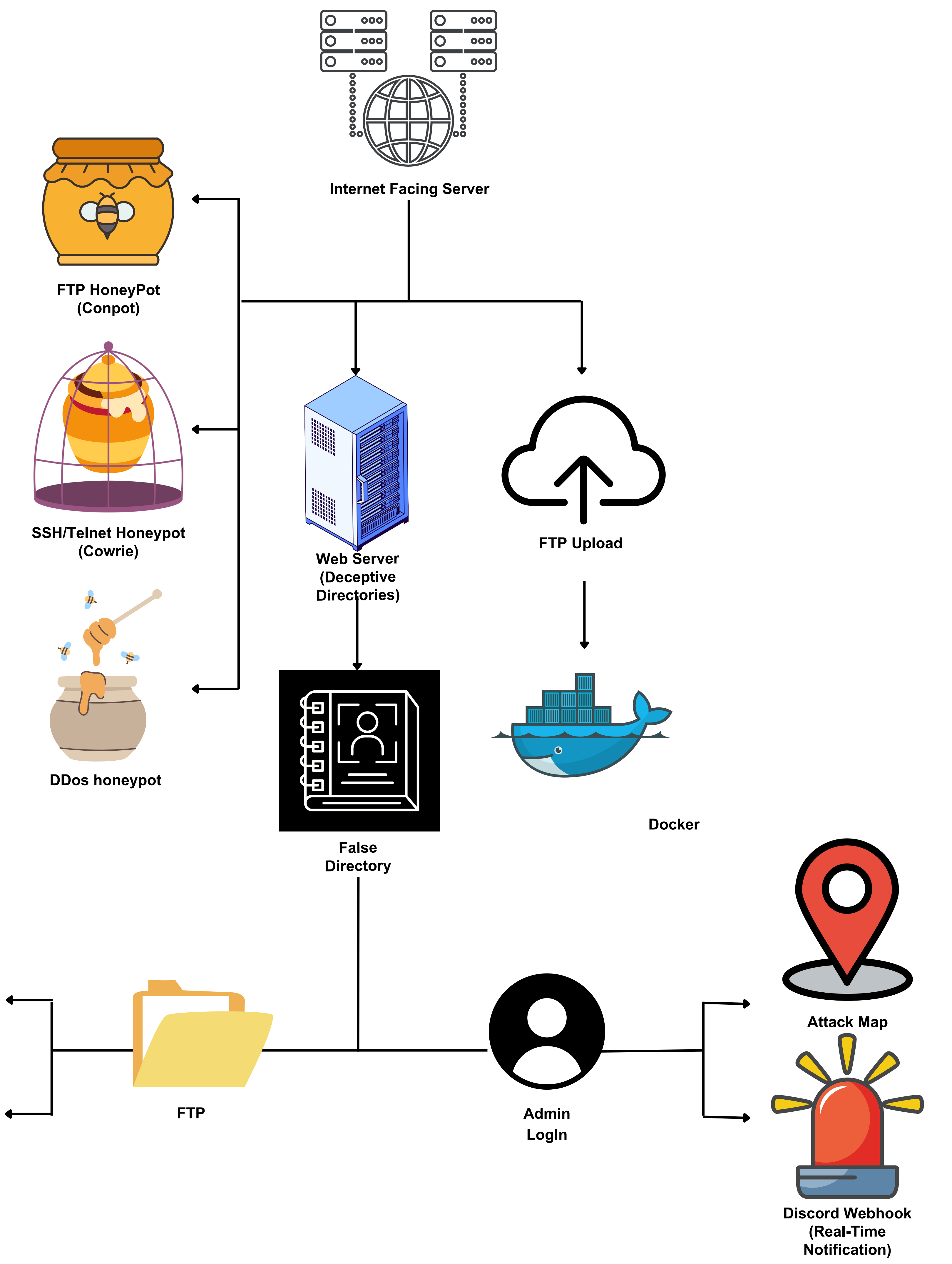
- Display **real-time** attacks based on logging database, showcasing the effectiveness of the HONEYNET.

Scan to watch our video demonstration

Technologies Used

KALI LINUX

HoneyPot Architecture



Flow (Attacker's POV)

This project flow illustrates how an attacker might engage with the M3I0N37 honeynet, highlighting the deception techniques, monitoring capabilities, and response mechanisms employed to defend against malicious activies.

Initial Reconnaissance

- **Scanning** the internet for potential targets, stumbling upon the website melonet.ddns.net.
- Perform **Reconnaissance** on target website, **Identifying** potential vulnerabilities and entry points.
- Tools like **Gobuster**, the attacks **Scans** for hidden directories and files.

Upload Attempt

- There is a **hidden** file upload directory.
- Upon **enumeration**, attackers would be aware of the existence of fileupload.php, upload.php, and an uploads folder.
- Fileupload.php, attackers would realize that they can **upload** files of any extension type to our server.

Identifying & Accessing Suspicious Directories

- Unaware of being monitored, the attacker interacts with the page, triggering tracking beacons and logging events.