🛡 Internship Task Report : Exploration & Proof of Concept on AbuseIPDB and Shadowserver Foundation

Intern Name: Anoop Shivadas
Organization: Digisuraksha Foundation
Intern ID: 129

📌 Introduction

As part of my cybersecurity internship, I was given the responsibility to study and practically test two widely recognized threat intelligence platforms: **AbuseIPDB** and the **Shadowserver Foundation**.

The objective of this task was twofold:

1. To understand how these platforms collect, analyze, and share threat intelligence.
2. To create a **Proof of Concept (PoC)** showing how they can be leveraged in real-world environments for preventing and mitigating cyber threats.

This exercise enhanced my knowledge of IP reputation services and global threat monitoring while also providing insights into their use in enterprise security.

🔎 Section 1: AbuseIPDB – IP Reputation & Abuse Tracking

What is AbuseIPDB?

AbuseIPDB is a community-driven project that tracks malicious activity tied to IP addresses. It acts as a reputation database, enabling users to **report** suspicious IPs and **check** whether an IP has been involved in abusive activities such as spam, phishing, DDoS, or brute force attacks.

Essentially, it is a **shared intelligence system** that helps administrators and security teams block malicious actors before they cause damage.

Key Features

- **Instant IP Reputation Check** – Verify if an IP has been flagged for abusive behavior.
- **Abuse Confidence Score** – A numerical score indicating how likely an IP is to be malicious.
- **Historical Reports** – View records of malicious activity reported by global users.
- **REST API** – Provides easy automation for integrating with firewalls or monitoring systems.

- **Crowdsourced Intelligence** – Powered by reports from system admins, firewalls, and security researchers worldwide.

Practical Applications

- 🖥️ **System Admins** – Block attackers attempting brute force or scanning.
- ⚙️ **DevOps Teams** – Integrate with tools like Fail2Ban or WAFs for automated blocking.
- 🔐 **Security Analysts** – Correlate IP data with SIEM alerts for deeper investigation.

PoC: IP Threat Lookup with AbuseIPDB

Goal: Build a Python script that queries AbuseIPDB for the reputation of a given IP.

Tools Used:

- Python 3.x
- requests library
- AbuseIPDB Free API Key

Code Snippet:

```
import requests

API_KEY = "your_api_key_here"

ip_address = input("Enter IP to check: ")

url = f"https://api.abuseipdb.com/api/v2/check?ipAddress={ip_address}&maxAgeInDays=90"

headers = {
    "Accept": "application/json",
    "Key": API_KEY
}

response = requests.get(url, headers=headers)

data = response.json()

print(f"\nIP Address: {data['data']['ipAddress']}")

print(f"Abuse Confidence Score: {data['data']['abuseConfidenceScore']}%")

print(f"Country: {data['data']['countryCode']}")

print(f"Total Reports: {data['data']['totalReports']}")
```

print(f"Last Reported At: {data['data']['lastReportedAt']}")

Sample Output (for a malicious IP):

yaml

Copy code

IP Address: 185.220.101.35

Abuse Confidence Score: 100%

Country: DE

Total Reports: 158

Last Reported At: 2025-07-22T08:45:31Z

Interpretation:

The IP shows repeated malicious activity and should be blocked using firewall rules or security gateways.

🌐 Section 2: Shadowserver Foundation – Global Threat Intelligence

What is Shadowserver?

The Shadowserver Foundation is a non-profit organization dedicated to large-scale cybersecurity monitoring. It collects data from internet-wide scans, sinkholes, and malware tracking to provide actionable reports to organizations, governments, and CERTs worldwide.

Unlike AbuseIPDB, which is focused on IP reputation, Shadowserver offers broad visibility across internet infrastructure, helping detect misconfigurations and large-scale vulnerabilities.

Core Capabilities

🌍 Daily Internet Scans – Covers the entire IPv4 space.

🛡 Botnet Sinkholing – Tracks infected machines and malicious traffic.

📊 Incident Reports – Shared with ISPs, CERTs, and enterprises.

🔍 Vulnerability Insights – Helps organizations identify weak points before attackers exploit them.

Common Use Cases

- Enterprises detect exposed databases and open ports.
- Governments monitor critical infrastructure threats.
- Researchers analyze malware and botnet behaviors.
- ISPs receive daily feeds to help secure their customers' networks.
- PoC: Receiving and Analyzing Shadowserver Reports

Steps Followed:

- Registration
- Signed up at shadowserver.org with a public IP block.
- Submitted justification for receiving reports.
- Reports Received
- Exposed services (e.g., RDP, FTP).
- Malware infections.
- Botnet activities.

Example Analysis Table:

Finding	Count	Severity
Open RDP Port	2	High
Exposed MongoDB	1	Medium
Botnet Activity	1	Critical

Actions Taken:

- Blocked RDP port (3389) using firewall rules.
- Enforced stronger authentication.
- Patched exposed services and updated software.

⚖ Comparative Overview

Feature	AbuseIPDB	Shadowserver Foundation
Focus	IP reputation & abuse tracking	Internet-wide vulnerability monitoring
Data Source	Community-driven reports	Independent scans & malware sinkholing
Real-time Access	API (Free & Paid tiers)	Email reports only

Best For	Sysadmins, SOC teams, developers	CERTs, ISPs, governments, large enterprises
Cost	Free (limited tier)	Free for all

📘 Key Takeaways

1. Threat intelligence enables proactive defense rather than reactive measures.
2. AbuseIPDB is lightweight, API-driven, and great for quick incident response.
3. Shadowserver provides broader visibility and is well-suited for long-term infrastructure monitoring.
4. Both tools are free to use, making them accessible to organizations with limited budgets.
5. Using both in combination ensures comprehensive protection – AbuseIPDB for real-time IP blocking, and Shadowserver for global security awareness.

✅ Conclusion

This task gave me practical exposure to how threat intelligence services function and how their data can be integrated into security workflows.

Both AbuseIPDB and Shadowserver empower defenders by providing timely and valuable insights into malicious activities. In the future, I plan to integrate these tools into SIEM solutions and experiment with automated response mechanisms to further strengthen security operations.