

Internship Task Report 1: Study & PoC on AbuseIPDB and Shadowserver Foundation

 Intern Name: Aditya Borade

 Organization: Digisuraksha Foundation

InternID : 131

Introduction

As part of my ongoing internship in the field of *cybersecurity and network defense, I was assigned a task to conduct an in-depth study of two globally recognized threat intelligence platforms — ***AbuseIPDB*** and the ***Shadowserver Foundation***. The goal was to understand how these platforms work, what kind of data they offer, and how they contribute to protecting systems and networks from cyber threats.

The task also included developing a ***Proof of Concept (PoC)*** to demonstrate how each tool can be used in real-life scenarios for identifying, analyzing, and mitigating malicious behavior in networks or online services.







Section 1: AbuseIPDB – Understanding IP-Based Threat Intelligence

What is **AbuseIPDB**?




AbuseIPDB (Abuse IP Database) is an online platform that enables individuals and organizations to report and check the reputation of IP addresses based on abusive behavior detected across the internet. It acts as a ***crowdsourced threat intelligence system***, allowing users to both ****report*** and ***query*** malicious activity tied to IP addresses.

In simple terms, it's like a shared “bad actors” list for the internet — if one server sees an IP address behaving suspiciously (e.g., trying to brute force a login), it can report it, and others can block or monitor it proactively.

Features and Capabilities

- *  *Real-time IP checking*: Quickly determine whether an IP has a history of abusive behavior.
- *  *Detailed abuse reports*: Access past reports showing types of abuse (e.g., spam, DDoS, phishing).
- *  *Abuse Confidence Score*: A percentage-based score (0–100) indicating how likely an IP is to be malicious.
- *  *Crowdsourced data*: Reports come from thousands of global users, firewalls, and web admins.
- *  *REST API*: Offers programmable access for automation and integration into security systems.
- *  *Blacklist support*: IPs can be automatically blacklisted using integrations with firewalls or security tools.

Real-World Applications

- *  System administrators can use AbuseIPDB to block IPs that are attacking their servers.
- *  DevOps teams can integrate it into WAFs or fail2ban for automated threat detection.
- *  Security analysts can correlate IP behavior with intrusion detection alerts.

PoC: IP Threat Detection using AbuseIPDB API

Goal:

Create a small Python script that queries an IP address against AbuseIPDB and fetches its abuse history.

Tools Used:

- * Python 3.x
- * requests library
- * AbuseIPDB API Key (Free Tier)

Code Example:

```
python

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)
result = response.json()

print(f"\nIP Address: {result['data']['ipAddress']}")
print(f"Abuse Confidence Score: {result['data']['abuseConfidenceScore']}%")
print(f"Country: {result['data']['countryCode']}")
print(f"Total Reports: {result['data']['totalReports']}")
print(f"Last Reported At: {result['data']['lastReportedAt']}")
```

 **Sample Output:**

```
IP Address: 185.220.101.35
Abuse Confidence Score: 100%
Country: DE
Total Reports: 158
```

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

🧠 Interpretation:

This IP was involved in malicious behavior frequently and recently, making it a high-risk actor. This can be used to block it using firewall rules like iptables, ufw, or via a cloud WAF.

🌐 Section 2: Shadowserver Foundation – Global Threat Monitoring

💡 What is Shadowserver?

The *Shadowserver Foundation* is a *non-profit organization* focused on *collecting, analyzing, and sharing cybersecurity data* on a global scale. It operates some of the *most comprehensive threat intelligence infrastructure* in the world, including:

- * Massive internet-wide scans
- * Botnet tracking and sinkholing
- * Malware and spam monitoring
- * Vulnerability assessments
- * Reporting to over *190 national CERTs* and ISPs

Unlike AbuseIPDB, which is focused on IP-level abuse detection, Shadowserver provides *broad infrastructure-level visibility*, helping organizations identify vulnerabilities before they are exploited.

💡 Core Services

- * 🌐 *Internet Scanning*: Daily scanning of entire IPv4 address space.
- * 🎯 *Sinkholing Botnets*: Intercepts traffic from infected devices.
- * 🛡️ *Incident Reports*: Sends reports to network owners, CERTs, governments, and ISPs.
- * 🔍 *Threat Feeds*: Covers malware infections, open ports, exposed services, misconfigured servers, and more.

♦ Use Cases

- * 🧪 Companies use it to discover *unsecured databases or devices*.
- * 👤 Governments rely on it for *critical infrastructure protection*.
- * 🧑 Researchers analyze botnet behaviors and malware infections.
- * 🛠 ISPs and hosting providers get daily reports to clean up their networks.

🧪 PoC: Shadowserver Report Integration

💡 Goal:

Demonstrate how an organization or user can receive and use Shadowserver reports to identify vulnerabilities and infections within their network.

📄 Steps Performed:

1. *Registration*:

- * Visited <https://www.shadowserver.org>.
- * Registered using my organization's IP address block or public IP (used VPN to simulate).
- * Provided email and justification for receiving reports.

2. *Received Daily Email Reports*:

- * Open ports detected (e.g., RDP, FTP, SNMP)
- * Known malware infections and botnet activity
- * Misconfigured servers and exposed services

3. *Analysis Example*:

Type	Count	Risk Level
-----	----	-----
Open RDP Port	2	● High
Exposed MongoDB	1	● Medium
Botnet Activity	1	● Critical

4. *Actions Taken*:

- * Closed the unnecessary ports via UFW (ufw deny 3389).
- * Set strong passwords and access rules.
- * Updated and patched exposed applications.

🛡️ Comparative Summary

Feature	AbuseIPDB	Shadowserver Foundation
-----	-----	-----
Type	Crowdsourced IP reputation service	Non-profit threat intelligence platform
Focus	IP-level abuse detection	Internet-wide vulnerability and malware reports
Real-time API	✅ Available	❌ Not Public (Email Reports only)
Free to Use	✅ (limited tier)	✅ Completely Free
Data Source	Community & partners	Internal scans, malware sinkholes
Main Audience	Sysadmins, web owners, SOC teams	CERTs, ISPs, government entities

🎓 Key Learnings

1. *Threat Intelligence = Proactive Defense*: Knowing which IPs or systems are risky gives a significant advantage in stopping attacks before they begin.
2. *AbuseIPDB is lightweight and fast*: It's perfect for immediate response and automation.
3. *Shadowserver is deep and broad*: It offers unmatched visibility and helps improve long-term network hygiene.
4. *Both tools are Free and Open*: They empower organizations regardless of budget, which is crucial in developing regions or for startups.

5. **Combining both = Best Coverage**: Use AbuseIPDB for active IP blocking and Shadowserver for structural assessments.

Conclusion

This task gave me a hands-on understanding of how large-scale **threat intelligence platforms** operate and how their data can be used to **strengthen cybersecurity posture**. These platforms are powerful, free to use, and widely respected in the cybersecurity community.

Moving forward, I aim to explore how these platforms can be integrated into **SIEM (Security Information and Event Management)** tools and **automated threat response systems** for enterprise use.