Project Title

"Ethical Analysis of FTP Server Exposure in Pretoria: A Shodan-Driven Security Audit"

Project Overview

As part of my ongoing exploration of cybersecurity threats in public-facing infrastructure, I conducted a **controlled, educational assessment** of FTP servers (port 21) in Pretoria, South Africa, using Shodan. This project aimed to identify misconfigurations, outdated software, and insecure practices while adhering to strict ethical guidelines. No malicious actions were performed—only passive data collection and analysis.

Key Objectives

1. **Identify Exposed FTP Servers**:
    - Locate publicly accessible FTP services (`port:21`) within Pretoria.
2. **Assess Security Posture**:
    - Detect anonymous logins, outdated software, and unpatched vulnerabilities.
3. **Educate on Mitigations**:
    - Propose hardening strategies aligned with industry best practices.

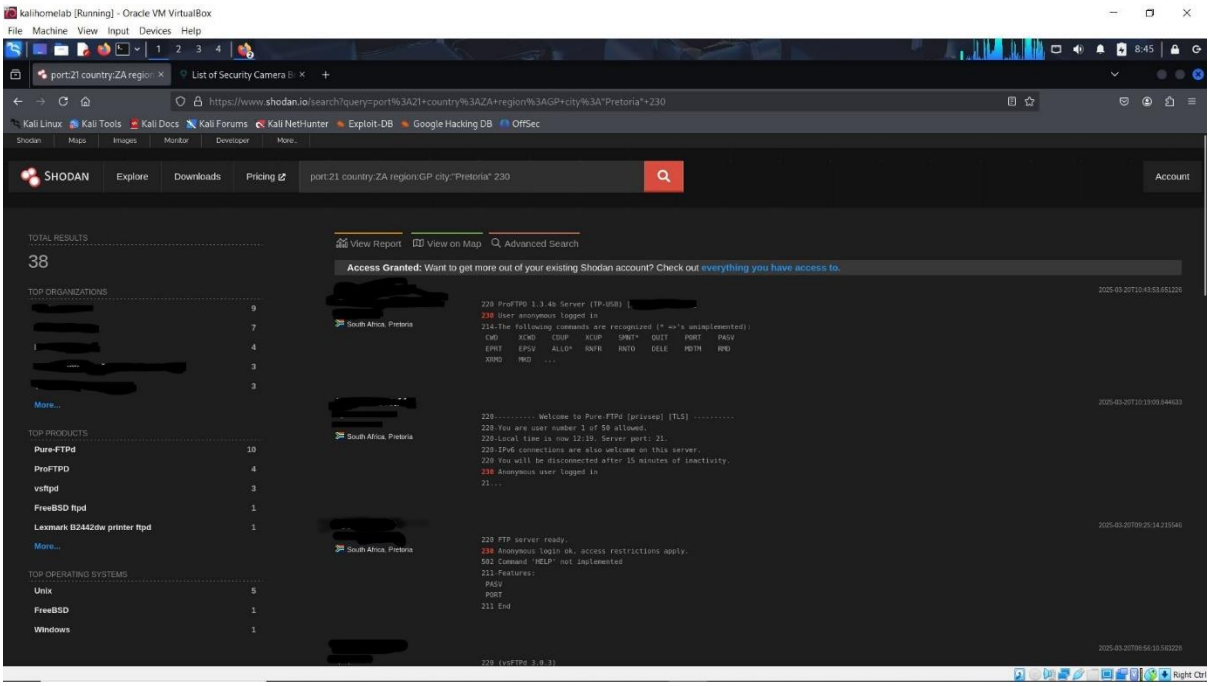
Technical Implementation

Tools: Shodan, NVD/CVE Database, Wireshark (for protocol analysis)
Methodology:

1. **Targeted Search**:

```
port:21 country:ZA region:GP city:"Pretoria" 230
```

    - `country:ZA`: South Africa
    - `230`: FTP response code indicating successful logins (including anonymous access).
2. **Analysis**:



- Identified **38 FTP servers** across organizations not mentioned for security purposes.
- Flagged **10 servers allowing anonymous logins** (e.g., `230 Anonymous user logged in`).
- Discovered outdated software:
  - `ProFTPD 1.3.4b` (CVE-2020-9273, CVE-2020-9274)
  - `vsFTPd 3.0.3` (CVE-2021-27612)

Key Findings

1. High-Risk Configurations

- **Anonymous Access**: 10 servers allowed unauthenticated access, risking data breaches.
- **Outdated Software**: 5 instances of end-of-life FTP daemons (e.g., ProFTPD 1.3.4b).
- **Unencrypted Transfers**: Majority lacked TLS/SSL, exposing credentials/data to sniffing.

2. Organizational Exposure

Organization	Exposed Servers	Critical Risks
[redacted].	10	2 servers with anonymous logins
[redacted]	8	4 outdated ProFTPD instances
	1	vsFTPd 3.0.3 (CVE-2021-27612)

Deliverables

1. **Anonymized Technical Report**:
    - *"23% of analysed FTP servers in Pretoria permitted anonymous access, violating basic security principles."*
    - *"Identified 5 instances of ProFTPD 1.3.4b, a version linked to critical CVEs."*
2. **Mitigation Strategies**:
    - Enforce TLS encryption for FTP traffic.
    - Disable anonymous logins and upgrade end-of-life software.
    - Implement network segmentation for FTP services.
3. **Educational Summary**:
    - Created a guide: *"Securing FTP Servers: A Checklist for System Administrators."*

Ethical Considerations

- **No Intrusive Scanning**: Only passive Shodan data collection.
- **Anonymization**: All IPs, organizations, and identifiers redacted in public reports.
- **Responsible Disclosure**: Private vulnerability notifications sent to affected organizations.