Red Team Reconnaissance Report

1. Executive Summary

This report outlines the reconnaissance phase of a red team penetration testing engagement for a fictional organization, SecureNexus Inc. The goal is to identify exposed infrastructure, gather information using passive and active reconnaissance techniques, and recommend mitigation steps to reduce attack surfaces.

2. Company Profile (Fictional)

Company: SecureNexus Inc.
Industry: Cybersecurity Solutions
Website: www.securenexus.io
Employees: ~250
Cloud Platforms: AWS, Azure, GitHub
Public Services: Web App, VPN, Email, DevOps CI/CD
IP Range: 45.82.12.0/24 (Simulated)
ASN: AS394758 – SecureNexus Private Network (Fictional)

3. Reconnaissance Methodology

3.1 Passive Reconnaissance

Passive reconnaissance was conducted using publicly available information and open-source tools. No direct interaction with SecureNexus Inc.'s infrastructure was performed.

Tools and Techniques:

- WHOIS lookup
- Subdomain Enumeration (Subfinder, crt.sh)
- GitHub Dorking for credential leaks
- Shodan search for exposed services
- Google Dorking
- Hunter.io for employee email identification

3.2 Active Reconnaissance

Simulated active reconnaissance techniques were used to probe the discovered assets for open ports, services, and technologies. This included scanning for vulnerabilities and fingerprinting servers.

Tools and Techniques:

- Nmap for port scanning and service detection

- DIG for DNS record extraction
- DNSenum for DNS zone enumeration
- Traceroute and Ping for network mapping
- curl for web server banner grabbing
- OS fingerprinting with Nmap and TTL analysis

4. Collected Reconnaissance Data (To Be Continued)

The next sections will simulate the recon outputs for SecureNexus Inc., including WHOIS data, subdomain findings, port scans, and service banners.