Penetration Testing Report

Author: ke.i
Client: LZD
Date: June 17, 2025

---

1. Introduction

Test Objective: Security assessment of the resources saratov-bankrotstvo.ru and justhost.ru.
Scope: Port scanning, vulnerability discovery, and service configuration analysis.
Methodology: Use of tools such as Nmap, Nikto, and DNS AXFR transfer tests.

---

2. Tools Used

- Nmap
- Dig
- Nikto
- DirectAdmin
- Masscan
- Whois
- nslookup
- FTP / SSH
- OWASP ZAP
- Gobuster
- Metasploit Framework
- ExploitDB
- Searchsploit

---

3. Summary of Findings

- **Exposed services:** OpenSSH 8.0, Pure-FTPd, LiteSpeed HTTP(S), ISC BIND 9.11.36, Dovecot, Postfix SMTP
- **Critical vulnerabilities** found in SSH, DNS (BIND), and HTTP services
- **AXFR zone transfer** was open, allowing a full DNS dump
- **DirectAdmin login panel** found at port 2222 and `/evo/`

---

4. Nmap Vulnerability Scan Results

🔐 OpenSSH 8.0 (Port 22)

- CVE-2023-38408: RCE via ssh-agent and PKCS#11 (CVSS 9.8)
- CVE-2020-15778: Command injection in `scp`
- CVE-2019-16905: Memory leak in `gsskeyex.c`
- CVE-2021-41617: Privilege escalation with incorrect configuration
- CVE-2023-51385: Weak SSH key handling
- CVE-2023-48795: Downgrade attack in SSH protocol
- CVE-2020-14145: Logic flaw in SSH
- CVE-2016-20012: DoS condition
- CVE-2025-26465 / CVE-2025-32728: Low-severity future vulnerabilities
- CVE-2021-36368: Vulnerability in PAM auth module

🌐 DNS - ISC BIND 9.11.36 (Port 53)

- CVE-2023-50387: DoS via DNSSEC validation
- CVE-2023-4408: Request parsing vulnerability
- CVE-2023-3341: Buffer overflow

- CVE-2023-2828: TSIG misconfiguration
- CVE-2022-38178/38177: Incorrect DNS request handling
- CVE-2021-25220: Issue in `forwarders`
- CVE-2022-2795: Info leak on DNS error

📬 SMTP (Ports 587, 465)

- No vulnerabilities found related to Exim (e.g., CVE-2010-4344 not applicable)

🌍 HTTP (LiteSpeed)

- CVE-2003-1418: Inode leakage via ETag header

📌 Misc (from Vulners)

- CVE-1337DAY-ID-2657: Suspected vulnerability in DirectAdmin or plugin
- CVE-2025-32728: Low severity

---

5. Nikto Web Scan

5.1 Overview

- **Target:** saratov-bankrotstvo.ru
- **Method:** Nikto web vulnerability scanning
- **Date:** June 17, 2025
- **Tool:** Nikto v2.5.0

5.2 Target Info

- **IP:** 185.22.155.27, 2a00:b700::1c
- **Port:** 443 (HTTPS)
- **Web Server:** LiteSpeed

- **SSL:** Let's Encrypt, TLS_AES_256_GCM_SHA384

5.3 Vulnerabilities Found

- **ETag Inode Leakage**
    - *Risk:* Reveals internal file structure
- **Missing X-Frame-Options**
    - *Risk:* Clickjacking vulnerability
    - *Fix:* Add `X-Frame-Options` header
- **Missing Strict-Transport-Security (HSTS)**
    - *Risk:* MITM attack possibility
    - *Fix:* Add HSTS header
- **Missing X-Content-Type-Options**
    - *Risk:* MIME-sniffing vulnerability
    - *Fix:* Add `X-Content-Type-Options: nosniff`
- **BREACH attack vector**
    - *Risk:* Data leakage via compression
    - *Fix:* Disable `deflate` encoding or add mitigations

5.4 Limitations

- **Errors:** 20
- **Main issue:** SSL negotiation failed (host dropped connection)
- **Impact:** Incomplete scan

5.5 Conclusion

- Critical misconfigurations were discovered

- Security headers and HTTPS configuration are missing
- Retesting is recommended after fixes

---

6. AXFR Zone Transfer Test

- **AXFR was open**, allowing full domain zone export
- Revealed internal structure, subdomains, mail servers (MX), and IPv6 records
- **Severity:** High. Could allow attack planning and phishing
- **CVSS v3 Estimate:** 5.3 – 7.5 depending on internal exposure

Example Zone Records:

- `saratov-bankrotstvo.ru` → A: 185.22.155.27
- AAAA: 2a00:b700::1c

---

7. Test Limitations

- **No validation of patching:** No follow-up scans were conducted after initial discovery
- **No active exploitation:** Vulnerabilities were identified, not exploited

Recommendations:

- Validate patching and configuration fixes
- Conduct PoC exploitation in a controlled environment
- Retest for new vulnerabilities in future