Sentra.AI - Security Audit Report

Target: 127.0.0.1

Date: 2026-02-02 00:44:56

Scan ID: fc6bc7fe-a403-4500-b104-d40f9d2c3c48

Executive Summary (AI Analysis)

1. Summary

- Windows Services: Microsoft RPC (port 135) and SMB/CIFS (port 445) indicate a Windows host with core networking protocols active.

- Web Server: HTTP service on port 8000 (commonly used for development servers like Django, PHP built-in server, or HTTP File Server).

- Scope: Scan limited to localhost (127.0.0.1); services may or may not be exposed externally depending on binding configuration (0.0.0.0 vs 127.0.0.1).

2. Risks

- SMB (445/tcp): High-value attack vector. Historically targeted by exploits like EternalBlue (MS17-010), SMBGhost, and used for lateral movement/ransomware propagation. Risk depends on Windows version and patch level (not detected in scan).

- RPC (135/tcp): Potential for DCOM/MSRPC abuse (e.g., PetitPotam, forced authentication attacks) and lateral movement if credentials are compromised.

- HTTP:8000: Unknown service/version. Development servers often run with debug mode enabled, weak authentication, or directory traversal vulnerabilities. Missing Nikto scan leaves web-tier risks unassessed.

- Information Disclosure: SMB may expose shares, user lists, or OS version to authenticated/unauthenticated users.

3. Recommendations

- Immediate: Verify what is bound to port 8000 (`netstat -an | findstr 8000`). If it's a dev server, ensure it binds to 127.0.0.1 only, not 0.0.0.0.

- SMB Hardening:

- Disable SMBv1 (legacy protocol) via Windows Features or PowerShell: `Set-SmbServerConfiguration -EnableSMB1Protocol $false`

- Apply latest Windows security updates (critical for MS17-010 and subsequent SMB patches)

- Enable SMB signing and disable guest access

- RPC Restrictions: Block port 135 from external networks via Windows Firewall; restrict to necessary

administrative hosts only.

- Web Assessment: Install Nikto or use `curl -I http://localhost:8000` and `whatweb` (if available) to identify the service on port 8000. Disable debug modes and implement authentication if exposed.

- General: Run `nmap -sV -p 135,445,8000 localhost` to obtain version details for precise CVE mapping, and verify external exposure with `nmap -p 135,445,8000 <external_IP>`.

Technical Details (Nmap)

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-02 00:44 +0800
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000069s latency).
Not shown: 97 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Sentra.AI - Security Audit Report

Web Vulnerabilities (Nikto)

```
Nikto not installed (and Docker not found). Skipping web scan.
```