Sentra.AI - Security Audit Report

Target: localhost

Date: 2026-02-02 01:26:26

Scan ID: 069e8e12-54cc-4df1-aee3-3994d8a291c4

Executive Summary (AI Analysis)

1. Summary

The target (localhost) is a Windows-based host exposing SMB/RPC services (ports 135/445) and two HTTP services (ports 80 and 8000). The scan on port 8000 reveals a Ruby/Rack-based application (likely Sinatra) running in development mode, as evidenced by the leaked CLI help menu (showing options for `-e env`, `-s server`, etc.) rather than actual Nikto vulnerability output.

2. Risks

* Windows Services (135/445): Exposure of SMB and MSRPC presents high-risk attack vectors (e.g., EternalBlue, NTLM relaying, remote code execution) if unpatched or misconfigured.

* Development Mode Exposure: The application on port 8000 is leaking its internal command-line structure and confirms it is running in "development" environment. This typically implies verbose debugging, stack traces, and potentially dangerous routes are enabled.

* Information Disclosure: The "Nikto" output suggests the application is echoing its own CLI help text in response to HTTP probes, indicating potential command injection vulnerabilities or severe misconfiguration.

* Alternative Port Mention: The help text references default port 4567; ensure the service isn't accidentally bound to additional interfaces.

3. Recommendations

* Harden Windows Services: Disable SMBv1, ensure MS17-010 (EternalBlue) and recent SMB patches are applied, and restrict ports 135/445 via host firewall if remote access is unnecessary.

* Secure Web Application: Immediately switch the port 8000 application to production mode (`-e production`), disable verbose errors, and remove any debug endpoints.

* Re-run Assessment: The Nikto output appears to be the target application's help menu, not a scan result. Re-run Nikto with correct syntax (`nikto -h http://localhost:8000`) to identify web-specific vulnerabilities (XSS, misconfigurations).

* Service Minimization: Close port 8000 if it is a development/debug service accidentally exposed, or place it behind authentication and an SSL/TLS reverse proxy.

Sentra.AI - Security Audit Report

Technical Details (Nmap)

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-02 01:22 +0800
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 96 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Sentra.AI - Security Audit Report

Web Vulnerabilities (Nikto)

```
Usage: main [options]
    -p port                          set the port (default is 4567)
    -o addr                          set the host (default is localhost)
    -e env                           set the environment (default is development)
    -s server                        specify rack server/handler (default is thin)
    -q                               turn on quiet mode (default is off)
    -x                               turn on the mutex lock (default is off)
```