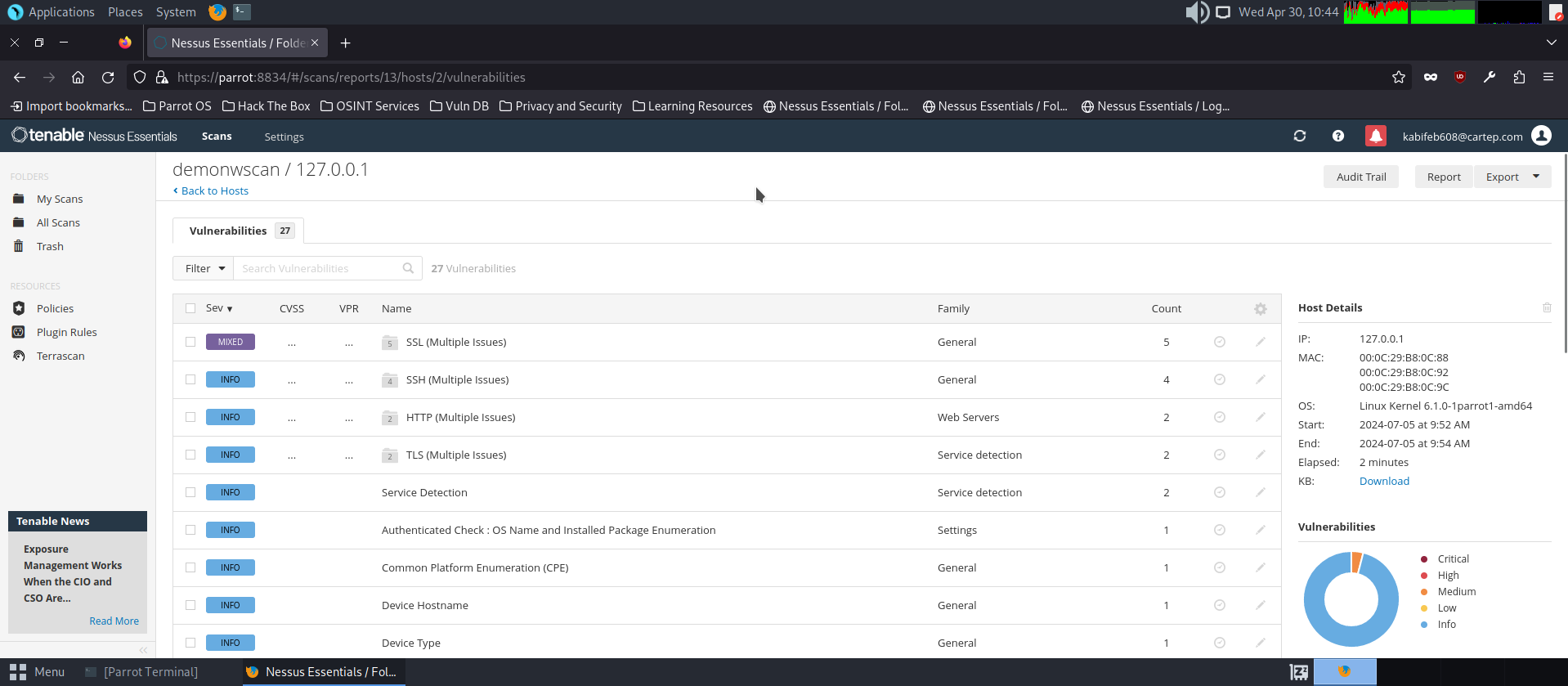
**Vulnerability Scanning with Nessus:**

● Perform a vulnerability scan on the target network/system to identify potential security vulnerabilities.

● Document the vulnerabilities, their severity, and any recommendations provided by Nessus.

Chosen Metasploit for the vulnerability scan (IP-127.0.0.1)



**Analysis Report:**

1. SSL (Multiple Issues) — *Medium*

SSL misconfigurations may allow downgrade attacks, weak cipher use, or insecure protocols.

2. SSH (Multiple Issues) — *Info*

May include weak algorithms or missing configuration best practices.

3. HTTP (Multiple Issues) — *Info*

May include server misconfigurations or version disclosure.

4. TLS (Multiple Issues) — *Info*

Use of insecure protocol versions or weak cipher suites.

**Recommended Actions**

1. **Harden SSL/TLS Configuration**
2. **Secure SSH Configuration**
   * Disable weak ciphers and key exchange algorithms (e.g., diffie-hellman-group1-sha1)
   * Enforce key-based authentication
3. **Strengthen HTTP Server Settings**
   * Enforce HTTPS using a valid SSL/TLS certificate
   * Regularly update the HTTP server software
4. **Limit Information Disclosure**
   * Block unnecessary ports/services with a firewall
5. **Patch & Update**
   * Apply all available system and software patches
   * Keep services like OpenSSH, Apache/Nginx, and OpenSSL updated
6. **Follow Best Practices for Hardening**
   * Implement CIS Benchmarks for your Linux distro
   * Regularly audit your system for open ports and running services
   * Set up intrusion detection or honeypot monitoring for unusual behavior.
7. Rescan after Fixes made.