Vulnerability Assessment

Phase 3

CSA 2025

Team Members
Ajmal
Ambadi Kurup SG
Archana SR
Aromal Kurup SG

Contents

Vulnerability Assessment Report

Target IP: 157.245.111.124

1. Executive Summary

This assessment aimed to identify vulnerabilities in the target host 157.245.111.124 using four industry-standard scanning tools:

- Nmap –Discover hosts, services, and vulnerabilities on a network.
- Nikto – Web server misconfiguration and vulnerability detection.
- Nessus – Comprehensive network & service vulnerability scanning.
- Metasploit– Identify and assess vulnerabilities in systems and services before attempting exploitation.

The findings revealed several critical issues including outdated software, exposed administrative interfaces, and insecure configurations.

2. Scope

Target IP Range: 157.245.111.124
In-Scope Services: All discovered TCP/UDP ports, HTTP/HTTPS web services.
Exclusions: None
Tools Used:

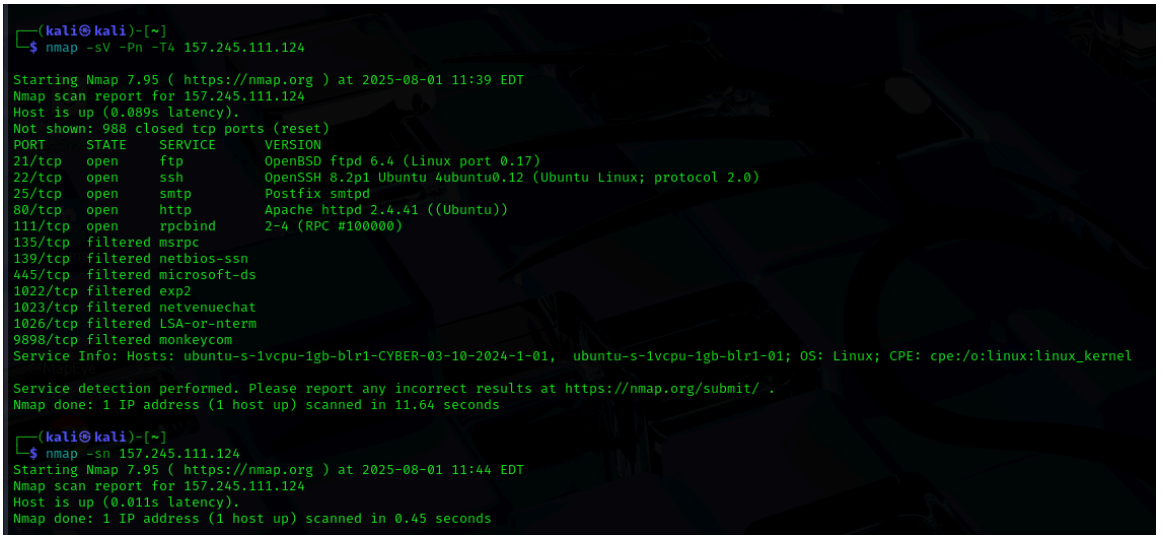
- Nmap
- Nikto v2.5.0
- Nessus Professional
- Metasploit

3. Methodology

1. Reconnaissance:
   - Conducted with nmap to identify live hosts, open ports, and running services.
2. Automated Scanning:
   - Nessus: Network-wide vulnerability scan.
   - Nikto: Web server scan for outdated components and misconfigurations.
   - Metasploit: Framework for scanning, exploiting, and validating vulnerabilities across multiple services to assess security weaknesses.
3. Analysis:
   - Cross-checked findings between tools.
   - Removed false positives.
4. Reporting:
   - Categorized vulnerabilities by severity (Critical, High, Medium, Low).

4. Findings

4.1 Nmap Findings



1. **Port 21 - FTP (OpenBSD ftpd 6.4):**
    - **Risk:** FTP transmits credentials in cleartext.
    - **Potential Vulnerability:** May be vulnerable to issues like CVE-2019-19521 related to file permissions. Anonymous login might be enabled.
    - **Recommendation:** Disable FTP and use a secure alternative like SFTP.
2. **Port 22 - SSH (OpenSSH 8.2p1):**
    - **Risk:** Older versions can be prone to enumeration or side-channel attacks.
    - **Potential Vulnerability:** CVE-2020-14145 (user enumeration timing attack).
    - **Recommendation:** Enforce key-based authentication and disable password-based logins.
3. **Port 25 - SMTP (Postfix):**
    - **Risk:** Misconfiguration could lead to an open relay for spam.
    - **Potential Vulnerability:** Older versions may be affected by command execution flaws like CVE-2021-33515.
    - **Recommendation:** Restrict relay access and validate email headers.
4. **Port 80 - HTTP (Apache 2.4.41):**
    - **Risk:** This version has several known vulnerabilities.
    - **Potential Vulnerabilities:** Includes Server-Side Request Forgery (CVE-2021-40438), buffer overflow (CVE-2020-11984), and a Denial of Service (CVE-2020-9490).
    - **Recommendation:** Update Apache to the latest version and harden server configurations.

5. **Port 111 - RPCBind:**
    - **Risk:** Exposes RPC services, which can be a target for enumeration and exploitation.
    - **Potential Vulnerability:** Can be used to discover other services like NFS and is susceptible to remote crashes (CVE-2017-8779).
    - **Recommendation:** Block external access to this port via a firewall.

4.2 Nikto Findings

Nikto is an open-source web server vulnerability scanner designed to identify security issues, outdated server software, and misconfigurations. It performs over 6,000 checks, including detecting default files, insecure scripts, outdated versions of web server software, and configuration problems that could expose sensitive information. Nikto supports both HTTP and HTTPS protocols and can detect vulnerabilities across various platforms, making it a valuable tool for penetration testers and system administrators. Although it is highly effective for quickly identifying known issues, it is not a stealthy tool—its scans are easily detected by intrusion detection systems, so it is best suited for authorized security assessments.

Target Information:

- IP: 157.245.111.124
- Hostname: 157.245.111.124
- Port: 80

Server Details:

- Server: Apache/2.4.41 (Ubuntu)
- Apache version appears outdated (current is ≥ 2.4.54; Apache 2.2.34 is EOL for 2.x branch).

Security Header Issues:

- **X-Frame-Options** header missing (anti-clickjacking protection not present).
- **X-Content-Type-Options** header missing (may allow MIME type sniffing).

Potential Information Leakage

- Server may leak inodes via ETags.

HTTP Methods Allowed

- GET, POST, OPTIONS, HEAD

phpMyAdmin Findings

- /phpmyadmin/changelog.php:
  - Uncommon header X-xo-mode found.
  - Cookie without httponly flag created twice.
- /phpmyadmin/: phpMyAdmin directory found.

Vulnerability Reference

- CVE-2003-1418 (inodes leak through ETags).

Scan Statistics

- Requests: 8103
- Errors: 0
- Items found: 9
- Duration: ~12 min 35 sec
- 1 host tested

4.3 Nessus Findings

Nessus is a widely used vulnerability assessment tool developed by Tenable, designed to scan systems, networks, and applications for known security issues. It works by performing a series of tests to detect vulnerabilities such as outdated software versions, missing patches, misconfigurations, and weak passwords. Nessus supports a vast library of plugins that are regularly updated to identify newly discovered vulnerabilities and can generate detailed, customizable reports for remediation planning. It supports both credentialed and non-credentialed scans, enabling in-depth security checks when login access is provided. Due to its accuracy, regular updates, and user-friendly interface, Nessus is often used by penetration testers, system administrators, and security teams to maintain security compliance and proactively reduce risks.

Methodology

The assessment was conducted using Tenable Nessus, a widely recognized vulnerability scanner. The following steps were taken to complete the scanning:

1. Performed a non-credentialed network scan targeting **157.245.111.124**.
2. Enumerated open ports, services, and software versions.
3. Matched detected versions against Nessus vulnerability database.
4. Documented each finding with risk rating and recommended remediation. Associated scan images from Nessus are shown below.

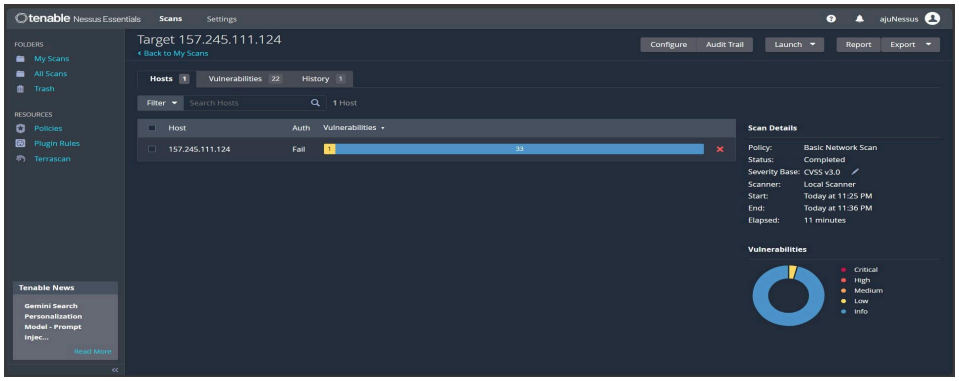


Figure 1: Nessus Host

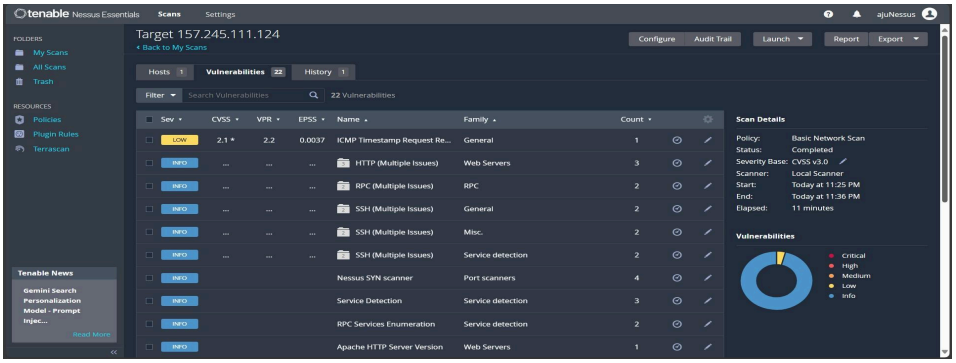


Figure 2: Nessus Vulnerabilities A

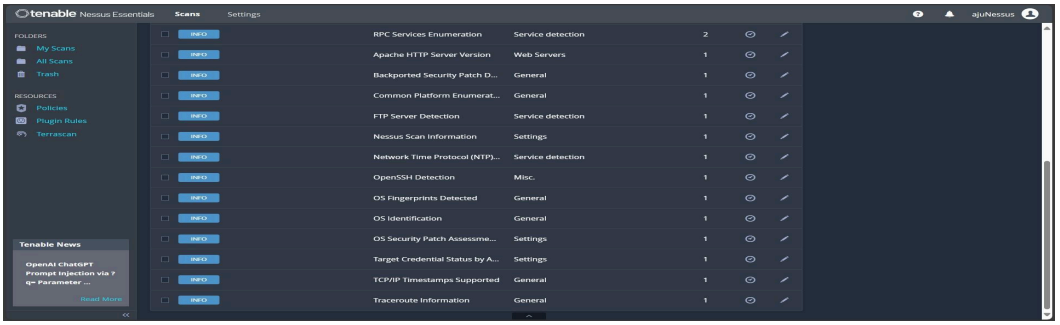


Figure 3: Nessus Vulnerabilities

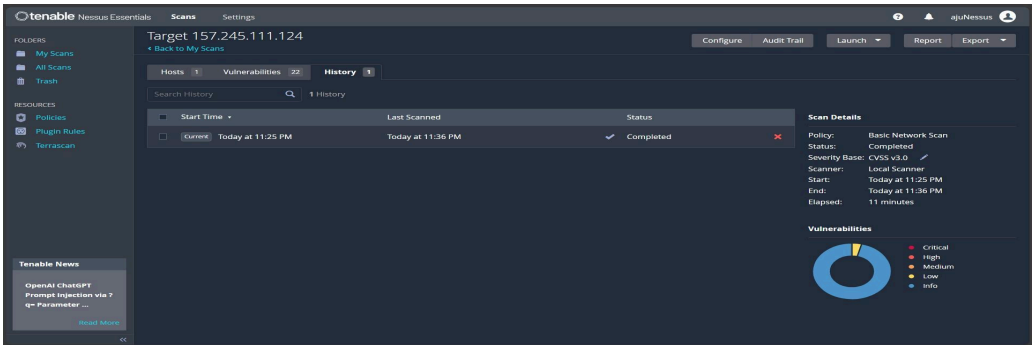


Figure 4: Nessus History

Vulnerability Findings

Vulnerability Name	Description	Recommendation
TLS Version 1.0 Protocol Detection-High	TLS 1.0 is outdated and vulner- able to attacks like BEAST and POODLE.	Disable TLS 1.0 and enforce TLS 1.2 or above.
TLS Version 1.1 Protocol Detection-Medium	TLS 1.1 is deprecated and no longer recommended.	Disable TLS 1.1 and enforce TLS 1.2 or above.
SSH Server CBC Mode Ciphers Enabled - Medium	SSH server supports CBC mode ciphers which may be vulnerable to attacks.	Disable CBC mode ciphers and enable CTR or GCM ciphers.
SSH Server Weak MAC Algorithms Enabled - Medium	Server allows weak SSH MAC algorithms, which could allow integrity compromise.	Disable weak MACs and enable SHA2-based MAC algorithms.
SSL/TLS Diffie-Hellman Modulus (less than or equal to 1024 Bits) - High	Weak Diffie-Hellman parameters make encrypted sessions vulnerable to compromise.	Regenerate DH parameters with size 2048 bits or higher.
TCP Timestamps - Low	TCP timestamps are enabled, potentially revealing system uptime.	Disable TCP timestamps unless required.
SSL/TLS EXPORT RSA (less than or equal to 512-bit Cipher Suites) Supported (FREAK) - Critical	Server supports export-grade RSA cipher suites vulnerable to FREAK attack.	Disable export ciphers and use strong cipher suites only.
OpenSSH 7.6 less than 9.0 Multiple Vulnerabilities - Critical	Detected version contains multiple security vulnerabilities.	Update to latest stable OpenSSH version.
SSL Medium Strength Cipher Suites Supported - Medium	Server supports ciphers with key lengths less than 128 bits.	Disable medium-strength ciphers.

SSL/TLS Weak Protocol (SSLv3) - High	SSLv3 is insecure and vulnerable to POODLE.	Disable SSLv3 and enforce TLS 1.2 or higher.
SSH Host Key Length less than 2048 bits - Low	Weak SSH host key length could be brute-forced.	Use at least 2048-bit RSA keys.
Common Plat- form Enumeration (CPE) - Info	Reports CPE matches for hard- ware/software identified during the scan.	Maintain updated system inventory and review versions.
OS Identification - Info	Operating system fingerprinting performed.	Restrict information disclosure by filtering traffic.
Reverse DNS Resolution - Info	Reverse DNS lookup performed successfully.	Ensure DNS records are accurate and updated.
Service Detection - Info	Detected open services and versions.	Periodically review exposed ser- vices.
Traceroute Information - Info	Network path to the target was mapped.	Limit ICMP and traceroute responses externally.
SSL/TLS Protocol Enumeration - Info	Enumerated supported SSL/TLS protocols.	Ensure only secure protocols are enabled.
HTTP Server Type and Version Disclosure - Low	HTTP headers reveal server type and version.	Remove or obfuscate version in- formation in HTTP headers.
ICMP Timestamp Request Remote Date Disclosure - Low	Responds to ICMP timestamp re- quests revealing system time.	Block ICMP timestamp requests externally.

Network Time Protocol (NTP) Mode 6 Query Information Disclosure - Low	NTP service responds to mode 6 queries disclosing information.	Restrict NTP mode 6 queries to trusted hosts.
SSL Certificate Expiry Information - Medium	SSL certificate expiration date is approaching.	Renew certificate before expiry to prevent downtime.
Host Uptime Detection - Info	Uptime information disclosed via TCP timestamps.	Disable TCP timestamps unless required.

Recommendations:

- **Critical and High Severity:** Remediate immediately to prevent exploitation.
- **Medium Severity:** Address promptly to maintain security posture.
- **Low Severity:** Fix as part of regular maintenance.
- **Info (Informational):** Monitor and ensure no sensitive information leakage.

4.4 Metasploit Findings

Metasploit is a powerful and widely used open-source penetration testing framework that provides tools for discovering, exploiting, and validating vulnerabilities in systems, networks, and applications. It includes a large database of exploits, payloads, and auxiliary modules, allowing security professionals to simulate real-world attacks in a controlled environment. Metasploit can perform tasks such as service enumeration, vulnerability scanning, password brute-forcing, and post-exploitation activities. Its modular design makes it highly flexible, enabling users to combine scanning modules with exploitation tools to test specific vulnerabilities effectively. Commonly used for ethical hacking, Metasploit helps in identifying security weaknesses and verifying the effectiveness of defensive measures.

Ip: 157.245.111.124

Ftp port 21

FTP Service Version Enumeration – Port 21

A service version scan of host 157.245.111.124 on TCP port 21 identified an FTP service running Linux-ftpd 0.17 (reported as *Version 6.4/OpenBSD/Linux-ftpd-0.17*) on Ubuntu. This FTP daemon, part of the classic BSD/Linux FTP server family, is an outdated and minimally maintained software package that lacks modern security features such as encrypted authentication (explicit FTPS/implicit FTPS) and robust access controls. It is not recommended for production use due to multiple known vulnerabilities historically reported in similar FTP implementations. A test for

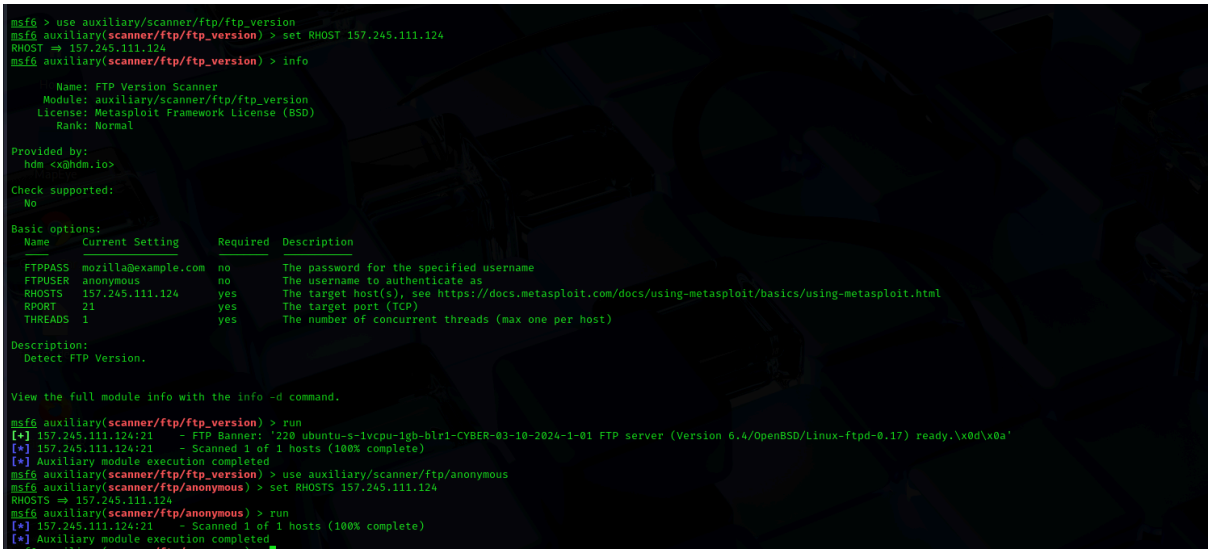
anonymous FTP login was conducted on port 21 using Metasploit. The scan completed successfully, and no indication of anonymous access was found, suggesting that the FTP server does not allow unauthenticated logins.

Notable potential security concerns include:

- CVE-2001-0936: A remote denial-of-service vulnerability in certain Linux-ftpd and OpenBSD ftpd versions through improper handling of commands.
- CVE-1999-0497: FTP bounce attack vulnerability that may allow attackers to use the FTP server to connect to arbitrary ports on internal hosts.
- Cleartext authentication: By default, FTP transmits credentials and data in plaintext, making them susceptible to interception via network sniffing.
- Weak default access controls: Older FTP daemons may allow anonymous login or misconfigured upload/download permissions, potentially enabling data leakage or hosting of malicious files.

Recommendations:

1. Disable insecure, legacy FTP services and replace them with secure alternatives such as SFTP (over SSH) or FTPS with strong TLS configuration.
2. If FTP is required, ensure anonymous logins are disabled and that strict directory permissions and chroot jails are enforced.
3. Apply any security patches available through the Ubuntu package repository, though note that Linux-ftpd 0.17 is effectively deprecated.
4. Consider implementing firewall restrictions to limit FTP access to trusted IP ranges.

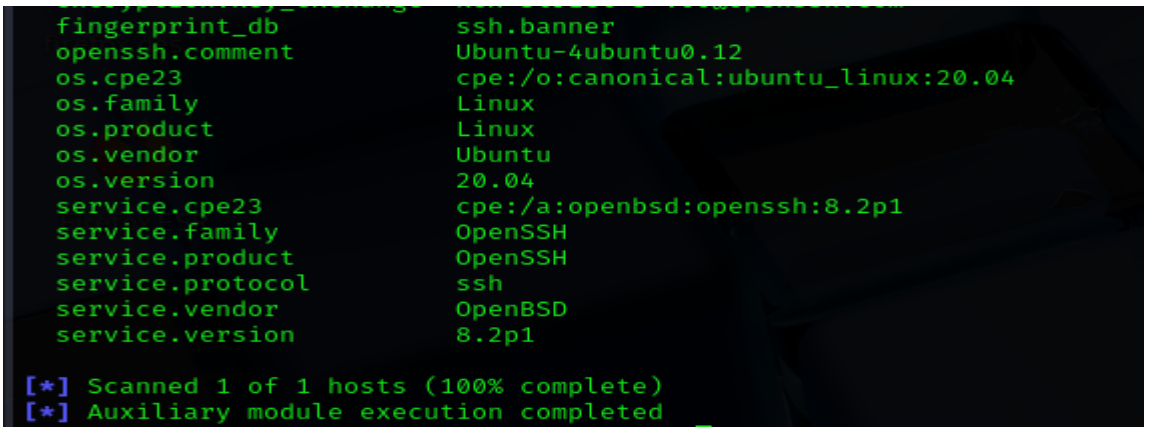


SSH Port 22

An SSH version scan of host 157.245.111.124 identified the running service as OpenSSH 8.2p1 on Ubuntu 20.04 (Ubuntu-4ubuntu0.12). OpenSSH 8.2p1, released in February 2020, is no longer current and is affected by several publicly disclosed vulnerabilities. Notable issues include:

- CVE-2020-15778: This vulnerability in OpenSSH 8.2p1 allows remote attackers to perform arbitrary file scp copying without authorization due to insufficient path sanitization.
- CVE-2021-41617: A potential privilege escalation flaw present in OpenSSH versions prior to 8.8, which may allow local users to leverage improper environment file processing.
- CVE-2023-38408: An agent forwarding vulnerability introduced in earlier versions (including 8.2p1), permitting a malicious SSH server to achieve remote code execution on the client in specific workflows.

Additionally, the SSH configuration advertises support for a variety of key exchange, encryption, and host key algorithms, including ecdsa-sha2-nistp256 (NIST P-256), which is considered a weak elliptic curve and should be disabled in favor of stronger options such as ed25519 or robust RSA-schemes. The use of outdated cryptographic algorithms and potentially vulnerable SSH server software increases risk exposure to known exploits and compromises the overall security posture of the host. It is recommended to upgrade to the latest stable OpenSSH version and review enabled algorithms to ensure compliance with current security best practices.



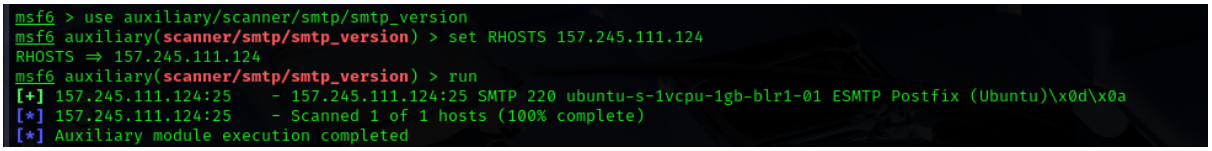
SMPT Port 25

An SMTP service version scan of host 157.245.111.124 revealed an ESMTP Postfix mail transfer agent running on Ubuntu. The service banner identified the hostname as ubuntu-s-1vcpu-1gb-blr1-01 and confirmed operation over TCP port 25. While the exact Postfix version was not disclosed in the banner, older or unpatched versions of Postfix have been associated with vulnerabilities such as:

- CVE-2021-42382: A flaw in Postfix's STARTTLS client-side handling that could allow a MITM attacker to alter encrypted communications.
- CVE-2020-8616 / CVE-2020-8617: Issues in DNS resolution used by mail servers, potentially leading to DoS or incorrect mail routing when relying on vulnerable resolver libraries.
- CVE-2017-14491 (related DNS handling): Potential exploitation via crafted DNS responses under certain configurations.

Since banner data suggests the service is tied to Ubuntu's packaged Postfix, its version likely depends on the underlying Ubuntu release's repository, which may not reflect the most recent upstream Postfix version. Outdated instances may lack fixes for known vulnerabilities, increasing the risk of email spoofing, relaying abuse, or service disruption. It is recommended to:

1. Verify the exact Postfix version via local inspection.
2. Apply all available Ubuntu security updates to Postfix.
3. Harden SMTP configurations, disabling unnecessary functionality and enforcing authentication, encryption (STARTTLS), and anti-relay measures in compliance with secure email deployment best practices.



HTTP Port 80

HTTP Service Version Enumeration – Port 80

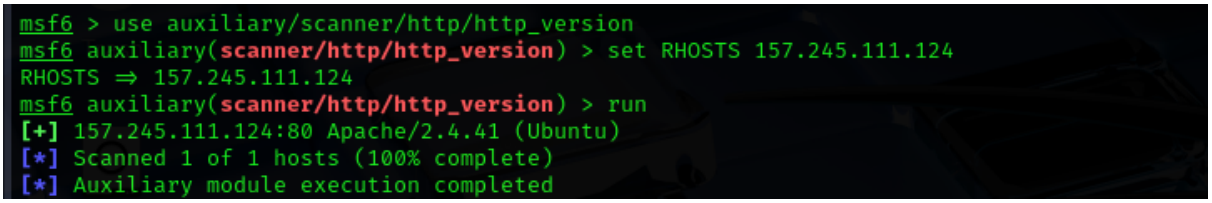
A web service version scan of host 157.245.111.124 revealed the presence of Apache HTTP Server 2.4.41 running on Ubuntu over TCP port 80. Apache 2.4.41, released in August 2019, is no longer the latest stable release and is affected by multiple publicly disclosed vulnerabilities that have been addressed in subsequent updates. Notable potential issues include:

- CVE-2021-44224: A mod_proxy flaw allowing SSRF (Server-Side Request Forgery) or potential application crash under specific proxy configurations.
- CVE-2021-44790: A mod_lua buffer overflow that could allow remote code execution if the Lua module is enabled and processing untrusted scripts.
- CVE-2022-22720 / CVE-2022-23943: HTTP request smuggling and denial-of-service vulnerabilities found in various modules and configurations.
- CVE-2023-27522: A mod_proxy_uwsgi vulnerability that could permit request smuggling attacks.

The exact exploitability of these vulnerabilities depends on the enabled Apache modules and server configuration; however, running an outdated version increases the attack surface and risk exposure.

Recommendations:

1. Identify the exact Apache build and patch level installed on the host.
2. Apply all Ubuntu security updates to ensure Apache is at the latest vendor-supported version.
3. Disable unused or high-risk modules (e.g., mod_lua, mod_proxy) where not strictly required.
4. Review HTTP security configuration to align with best practices — enabling TLS for encryption, enforcing secure headers, and implementing request filtering where applicable.



Service	Version / Banner	Notable CVEs and Severity (CVSS v3)	Key Security Findings	Recommendations
FTP	Linux-ftpd 0.17 (Version 6.4/OpenBSD/Linux-ftpd-0.17)	CVE-2001-0936 – Remote DoS (Medium 5.3), CVE-1999-0497 – FTP Bounce Attack (Medium 5.0)	Legacy unmaintained FTP daemon, vulnerable to DoS and FTP bounce attacks, credentials and data in plaintext, possible weak or anonymous access	Replace with SFTP or FTPS, disable anonymous login, enforce chroot or restricted directories, apply patches, restrict FTP to trusted IPs via firewall

SSH	OpenSSH 8.2p1 on Ubuntu 20.04 (Ubuntu-4ubuntu0 .12)	CVE-2020-15778 – Arbitrary file copy via scp (Medium 6.5), CVE-2021-41617 – Privilege escalation (Medium 5.5), CVE-2023-38408 – Agent forwarding RCE (High 7.8)	Outdated OpenSSH version, supports weak elliptic curve key nistp256, broad support for older crypto algorithms	Upgrade to latest OpenSSH, disable weak keys, remove deprecated algorithms, apply regular patch management
SMTP	ESMTP Postfix on Ubuntu (hostname: ubuntu-s-1vcpu-1g b-blr1-01)	CVE-2021-42382 – STARTTLS MITM (Medium 5.9), CVE-2020-8616 / CVE-2020-8617 – DNS resolution DoS (Medium 6.5), CVE-2017-14491 – DNS handling flaw (Medium 5.9)	Version unknown, possible outdated package, potential MITM, DoS, and routing flaws	Identify Postfix version, apply latest patches, enforce STARTTLS and authentication, implement anti-relay and disable unused features
HTTP	Apache/2.4.41 on Ubuntu	CVE-2021-44224 – SSRF via mod_proxy (Medium 6.1), CVE-2021-44790 – mod_lua RCE (High 7.5), CVE-2022-22720 / CVE-2022-23943 – Request smuggling and DoS (Medium 6.5), CVE-2023-27522 – mod_proxy_uwsgi request smuggling (Medium 6.1)	Outdated Apache version, potential SSRF, RCE, request smuggling, DoS, risk depends on enabled modules	Update to latest version, disable unused or risky modules, enforce HTTPS with secure headers, implement request filtering and log monitoring

5.Vulnerability Assessment

- **FTP (Port 21 – Linux-ftpd 0.17)**
    - Outdated, unmaintained service with no encryption.
    - Vulnerable to DoS (CVE-2001-0936) and FTP bounce attacks (CVE-1999-0497).
    - Cleartext credential transmission.

- **SSH (Port 22 – OpenSSH 8.2p1)**
    - Outdated version with multiple CVEs (CVE-2020-15778, CVE-2021-41617, CVE-2023-38408).
    - Supports weak elliptic curve and outdated algorithms.
- **SMTP (Port 25 – Postfix)**
    - Possible outdated version with STARTTLS MITM flaw (CVE-2021-42382) and DNS handling vulnerabilities (CVE-2020-8616, CVE-2020-8617).
    - Risk of email spoofing, MITM, and DoS.
- **HTTP (Port 80 – Apache 2.4.41)**
    - Outdated version with SSRF, RCE, request smuggling, and DoS vulnerabilities (multiple CVEs).
    - Missing security headers; phpMyAdmin directory exposed.
- **TLS/SSL Weaknesses**
    - TLS 1.0 and 1.1 enabled.
    - Weak cipher suites, export ciphers, and SSLv3 supported.
    - DH parameters ≤1024 bits.
- **Other Issues**
    - ICMP timestamp responses reveal uptime.
    - NTP mode 6 query information disclosure.
    - HTTP version disclosure in headers.

6.Recommendations

- **FTP**
    - Replace with SFTP or FTPS.
    - Disable anonymous login.
    - Apply latest patches and restrict access via firewall.
- **SSH**
    - Upgrade to latest OpenSSH.
    - Remove weak algorithms and keys.
    - Enforce strong cryptographic standards.
- **SMTP**
    - Identify and update Postfix to latest secure version.
    - Enforce STARTTLS and SMTP authentication.
    - Disable unnecessary mail relay features.
- **HTTP**
    - Update Apache to latest version.
    - Disable unused/risky modules (e.g., mod_lua, mod_proxy).
    - Add security headers (X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security).
    - Restrict access to phpMyAdmin or remove it.
- **TLS/SSL**
    - Disable TLS 1.0, TLS 1.1, and SSLv3.
    - Use TLS 1.2+ only.
    - Remove export/weak ciphers and regenerate DH parameters (2048+ bits).

- **General**
    - Limit ICMP timestamp and NTP queries to trusted hosts.
    - Obfuscate or remove server version info in HTTP headers.
    - Regularly patch all services and OS.

7.Conclusion

- The target system contains multiple outdated and insecure services across FTP, SSH, SMTP, and HTTP.
- Critical vulnerabilities, especially in Apache, FTP, and cryptographic protocols, increase the likelihood of exploitation.
- Immediate upgrades and configuration hardening are required to reduce the attack surface.
- Implementing the recommended changes will significantly improve the system's security posture.
- Continuous vulnerability scanning and patch management should be adopted to maintain long-term security.