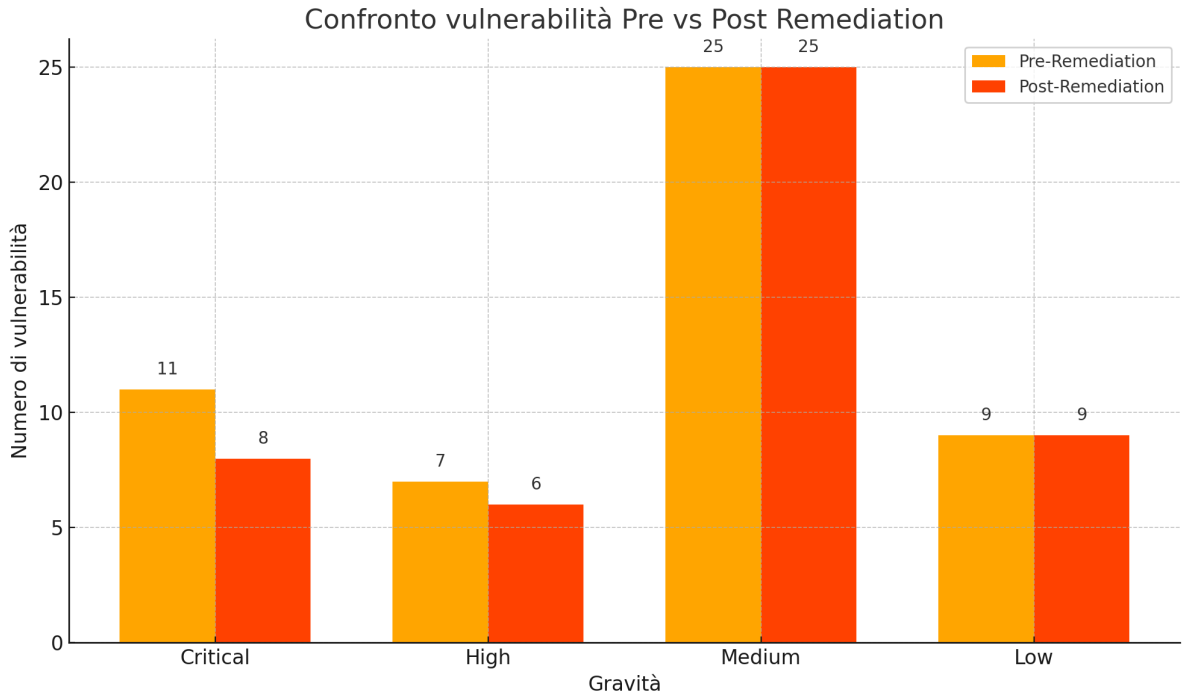
REPORT TECNICO - PRE REMEDIATION



Host Analizzato: 192.168.50.101
Sistema operativo: Linux Kernel 2.6 su Ubuntu 8.04 (hardy)
Data scansione: 16 maggio 2025 – ore 00:10

Gravità	Numero Vulnerabilità
CRITICAL	11
HIGH	7
MEDIUM	25
LOW	9

Vulnerabilità CRITICAL rilevate:

1. **Apache Tomcat SEoL (<= 5.5.x)**
   Versione non più supportata e priva di aggiornamenti di sicurezza, vulnerabile a molteplici exploit.

2. **Canonical Ubuntu Linux SEoL (8.04.x)**
   Sistema operativo obsoleto non più mantenuto, privo di patch critiche, vulnerabile

per natura.

3. **Debian OpenSSH/OpenSSL RNG Weakness (SSH)**
   Bug noto che rende prevedibili le chiavi SSH generate, consentendo attacchi Man-in-the-Middle.

4. **Debian OpenSSH/OpenSSL RNG Weakness (SSL - SMTP)**
   Come sopra, ma rilevato sul certificato SSL del servizio SMTP.

5. **Debian OpenSSH/OpenSSL RNG Weakness (SSL - PostgreSQL)**
   Come sopra, ma sul servizio PostgreSQL, rendendo possibile intercettazione o compromissione.

6. **SSL v2/v3 Protocol Detection (SMTP)**
   Uso di protocolli SSL 2.0/3.0 deboli, vulnerabili a downgrade e attacchi POODLE.

7. **SSL v2/v3 Protocol Detection (PostgreSQL)**
   Come sopra, rilevato sulla porta PostgreSQL.

8. **UnrealIRCd Backdoor Detection**
   Versione compromessa di UnrealIRCd contenente una backdoor che permette RCE (Remote Command Execution).

9. **VNC Server Weak Password (‘password’)**
   Accesso remoto consentito con password debolissima (‘password’), facilmente sfruttabile da chiunque.

10. **Bind Shell Backdoor Detection**
    Una shell remota è in ascolto senza autenticazione sulla porta 1524, indice di compromissione attiva.

11. **SSLv2/SSLv3 Weak Protocols (multipli servizi)**
    Cifrature deboli attivate su più servizi, rendendo vulnerabili le comunicazioni cifrate.

POST-REMEDIATION

Host Analizzato: 192.168.50.101
Data scansione: 16 maggio 2025 – ore 01:28

Gravità	Numero Vulnerabilità
CRITICAL	8
HIGH	6

MEDIUM	25
LOW	9

Vulnerabilità CRITICAL ancora presenti:

1. **Apache Tomcat SEoL (<= 5.5.x)**
   Versione obsoleta non più supportata, esposta a molteplici CVE critici senza possibilità di patch.

2. **Canonical Ubuntu Linux SEoL (8.04.x)**
   Sistema operativo privo di supporto e aggiornamenti da oltre 10 anni, altamente vulnerabile.

3. **Debian OpenSSH/OpenSSL RNG Weakness (SSH)**
   Bug che causa la generazione di chiavi deboli, consentendo intercettazioni o spoofing su SSH.

4. **Debian OpenSSH/OpenSSL RNG Weakness (SSL - SMTP)**
   Stessa debolezza applicata al certificato SSL usato nel servizio SMTP.

5. **Debian OpenSSH/OpenSSL RNG Weakness (SSL - PostgreSQL)**
   Chiavi deboli presenti anche nei certificati SSL per il servizio PostgreSQL.

6. **SSL v2/v3 Protocol Detection (SMTP)**
   Uso di protocolli SSL insicuri e obsoleti che permettono attacchi di downgrade della connessione.

7. **SSL v2/v3 Protocol Detection (PostgreSQL)**
   Configurazione debole sulla porta del database, esponendo a rischio critico le connessioni cifrate.

8. **UnrealIRCd Backdoor Detection**
   Presenza di un software IRC compromesso con una backdoor attiva, permette esecuzione remota come root.

Vulnerabilità CRITICAL eliminate dopo la remediation:

- **Apache Tomcat AJP Ghostcat (CVE-2020-1938)**
  Vulnerabilità che permetteva l'inclusione arbitraria di file o l'esecuzione di codice tramite il connettore AJP.

- **Bind Shell Backdoor Detection**
  Rilevamento e rimozione di una shell attiva in ascolto sulla porta 1524.

- **VNC Weak Password**
  Disabilitato o messo in sicurezza l'accesso VNC precedentemente protetto da una password predefinita banale.

Conclusione tecnica

Il test post-remediation dimostra un miglioramento, con la **rimozione di 4 vulnerabilità**. Tuttavia, **8 vulnerabilità critiche permangono**, la maggior parte legate a:

- uso di software obsoleto non aggiornabile (Tomcat 5.5, Ubuntu 8.04)

- debolezze strutturali nei protocolli di cifratura

- servizi storicamente vulnerabili non ancora sostituiti

Il mantenimento di **25 vulnerabilità MEDIUM** e **9 LOW** suggerisce la presenza di configurazioni deboli e servizi da mappare e aggiornare nel medio termine.