Executive Summary: Security Assessment Report (Host 192.168.50.101)

Data: 19 Dicembre 2025 **Target:** 192.168.50.101 (Metasploitable) **Stato Complessivo: CRITICAL**

1. Overview & Business Risk

L'analisi automatizzata ha rilevato che l'host in esame è completamente compromesso e non idoneo a un ambiente di produzione. Il sistema espone **59 vulnerabilità totali**, di cui **10 Critiche** e **5 Alte**.

Il rischio di business è massimo: un attaccante può ottenere il controllo totale del server (Root Access) in pochi secondi senza possedere alcuna credenziale, portando a esfiltrazione dati, interruzione del servizio e potenziale movimento laterale verso altri sistemi della rete aziendale.

2. Key Findings (Punti Critici)

- **Operating System End of Life (EOL):** Il server esegue **Ubuntu 8.04**, un sistema operativo obsoleto (EOL dal 2013) che non riceve aggiornamenti di sicurezza da oltre un decennio.
- **Unauthorized Root Access (Backdoors & RCE):**
    - È presente una **Backdoor** sul servizio vsftpd (porta 6200) e Ingreslock (porta 1524) che garantisce accesso root immediato.
    - Vulnerabilità di **Remote Code Execution (RCE)** sono presenti su servizi DistCC, Java RMI e Distributed Ruby, permettendo l'esecuzione di comandi arbitrari da remoto.
- **Weak Credentials:** Servizi critici come VNC, PostgreSQL e FTP utilizzano password di default o deboli (es. "password", "postgres", "msfadmin"), rendendo banali gli attacchi **Brute Force**.
- **Broken Encryption:** L'infrastruttura crittografica è insicura. Sono abilitati protocolli deprecati (**SSLv2/SSLv3/TLSv1.0**) e certificati scaduti nel 2010, esponendo il traffico ad attacchi **Man-in-the-Middle (MitM)**.

3. Impact Analysis

La combinazione di un OS obsoleto e servizi non configurati correttamente crea una superficie di attacco enorme. Non si tratta di "se" il sistema verrà compromesso, ma di "quando". Attualmente, il sistema viola qualsiasi standard di compliance (GDPR, ISO 27001, PCI-DSS).

4. Recommendations & Action Plan (CTA)

Si raccomanda l'azione immediata secondo le seguenti priorità:

1. **Immediate Isolation (Urgent):** Disconnettere immediatamente l'host dalla rete per prevenire infezioni o attacchi attivi.
2. **Decommissioning:** Non è possibile applicare patch a un sistema così obsoleto. Il server deve essere dismesso.
3. **Re-platforming:** Migrare i servizi essenziali su una nuova infrastruttura con un OS supportato (es. ultima versione LTS) e hardening applicato fin dal "day one".
4. **Network Segmentation:** Assicurarsi che nessuna porta di management (SSH, VNC, Database) sia esposta direttamente su internet o segmenti di rete non fidati.

Conclusione

Basandosi sull'evidenza cumulativa presentata in questo report di scansione, la postura di sicurezza dell'host **192.168.50.101** è classificata come **Critica**. La presenza simultanea di **Backdoors** , vulnerabilità di **Remote Code Execution (RCE)** e sistemi operativi **End-of-Life (EOL)** crea un livello di rischio inaccettabile.

Le strategie di **remediation** tradizionali, come l'applicazione di patch, non sono percorribili a causa dell'obsolescenza della piattaforma sottostante. Di conseguenza, l'unica linea d'azione efficace è l'immediato **decommissioning** (dismissione) dell'asset e un completo **re-platforming** dei suoi servizi su un'infrastruttura supportata, per garantire la compliance e l'integrità dei dati.