Report di Vulnerability Assessment

Sistema Target: Metasploitable 2 (Linux)

IP Target: 192.168.100.12

Data: 7 Gennaio 2026

Stato Scansione: Completata con Autenticazione (Credentialed Patch Audit)

---

1. Executive Summary (Sintesi per il Management)

È stata condotta un'analisi approfondita della superficie di attacco del server 192.168.100.12. L'attività ha combinato scansioni automatizzate con privilegi amministrativi e verifiche manuali (Proof of Concept).

Il risultato evidenzia una **compromissione totale** della sicurezza dell'asset. Il sistema presenta configurazioni obsolete, backdoor intenzionali e password di default che lo rendono indifendibile nello stato attuale.

🔍 Key Takeaways (Punti Chiave)

- **Superficie d'Attacco Critica:** Rilevate **30 vulnerabilità CRITICHE** e **98 ad ALTO rischio**. Un attaccante può ottenere il controllo totale del sistema in meno di 60 secondi.
- **Visibilità Totale (Auth Success):** La scansione è stata eseguita con credenziali (Auth: Pass), permettendo di identificare **162 vulnerabilità medie** legate a software non patchato che una scansione esterna non avrebbe visto.
- **Fattore Umano:** Le criticità più gravi derivano da errori di configurazione (password banali) e non solo da bug software.

---

2. Panoramica dei Risultati (Dashboard)

La scansione ha riportato un totale di **535 problematiche** di sicurezza. La distribuzione per gravità conferma l'urgenza dell'intervento.

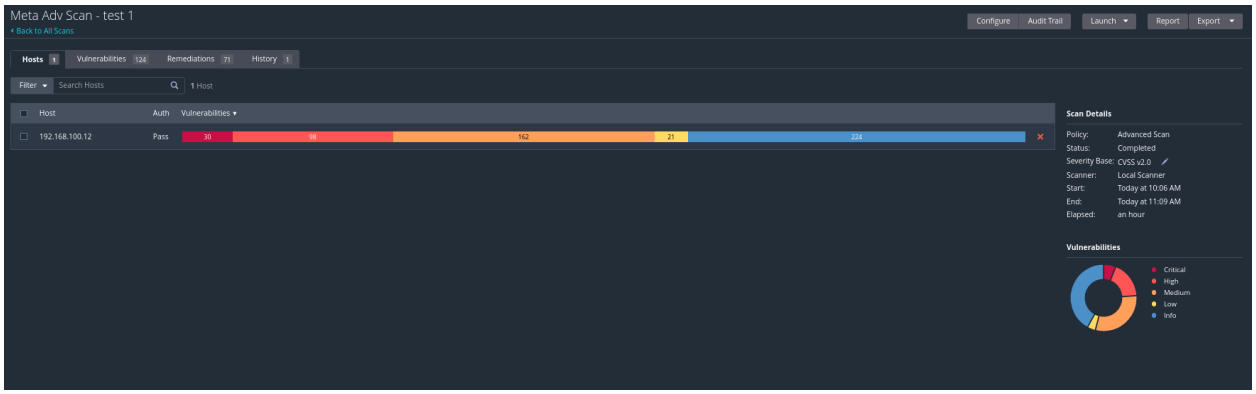

Figura 1: Dashboard riassuntiva. Si noti la barra rossa/arancione predominante e lo stato "Auth: Pass" che conferma il successo della scansione autenticata.

Matrice di Rischio

Livello di Gravità	Conteggio	Descrizione e Azione Richiesta
🔴 **Critico**	**30**	**Patch Immediata (<24h).** Vulnerabilità sfruttabili da remoto che garantiscono accesso Root (es. Backdoor, VNC debole).
🟠 **Alto**	**98**	**Patch Prioritaria (<7gg).** Vulnerabilità che richiedono condizioni specifiche ma hanno impatto elevato (es. Kernel obsoleto).
🟡 **Medio**	**162**	Configurazioni insicure che facilitano movimenti laterali (es. Info Disclosure).
🔵 **Info/Basso**	**245**	Inventario software e porte aperte.

3. Metodologia e Configurazione

Per massimizzare l'efficacia del test, è stato adottato un approccio **White Box** (scansione autenticata).

- **Targeting:** La scansione è stata limitata alle porte critiche per i servizi aziendali (21-3389).
- **Deep Inspection:** Sono state fornite a Nessus le credenziali SSH msfadmin con privilegi sudo. Questo ha permesso di catalogare ogni pacchetto installato e confrontarlo con i database delle vulnerabilità (CVE).

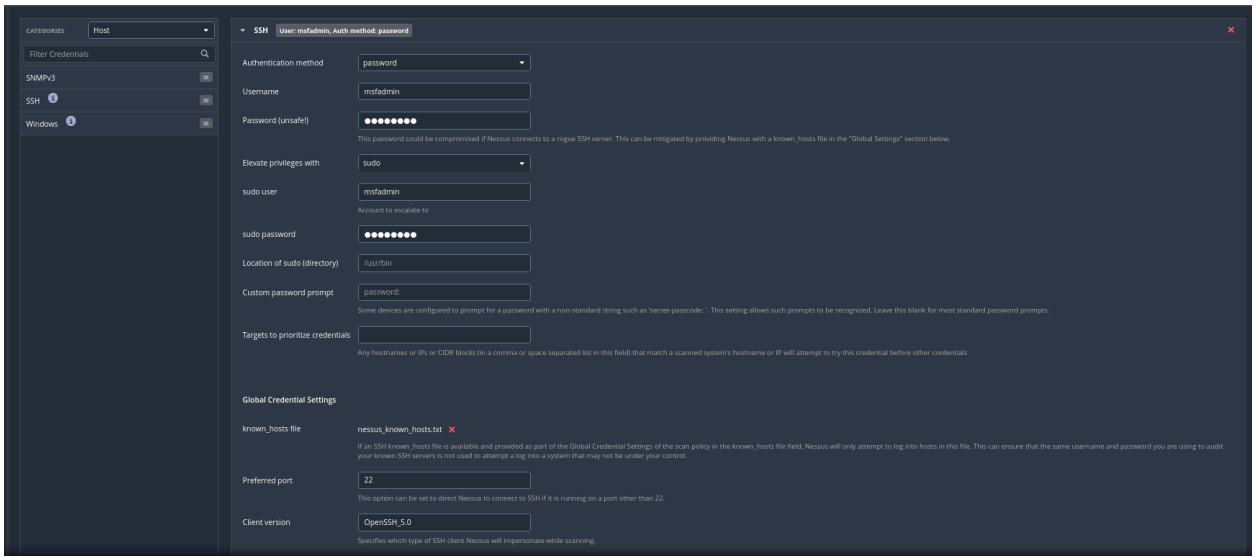

Figura 2: Configurazione delle credenziali SSH con escalation privilegiata.

4. Dettaglio Tecnico e Proof of Concept (PoC)

Di seguito sono analizzate le 3 vulnerabilità più rappresentative del rischio aziendale, verificate manualmente.

Finding #1: Supply Chain Backdoor (vsftpd)

- **Gravità:** 🔴 **CRITICA** (CVSS 10.0)
- **Impatto di Business:** Accesso non autorizzato immediato ai dati aziendali, rischio di installazione Ransomware e furto di proprietà intellettuale.
- **Dettaglio:** Il servizio FTP (porta 21) contiene una backdoor nota. Inserendo uno "smile" :) nel nome utente, il server apre una porta segreta (6200).
- **Verifica (PoC):** L'attaccante ha ottenuto una shell di comando Root senza conoscere la password reale.

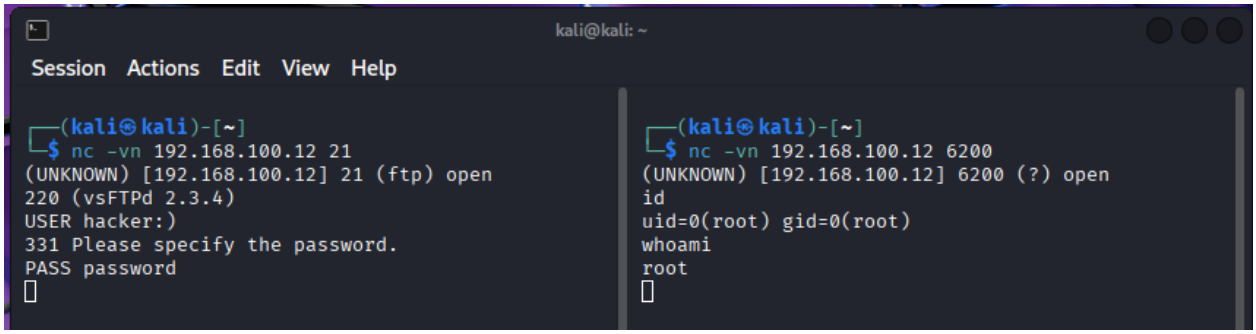

Figura 3: Exploitation manuale della backdoor vsftpd.

Finding #2: Ingreslock Bind Shell

- **Gravità:** 🔴 **CRITICA** (CVSS 10.0)
- **Impatto di Business:** Violazione totale della confidenzialità e integrità del server. Permette a qualsiasi utente nella rete (anche ospiti o dispositivi IoT compromessi) di diventare amministratori.
- **Dettaglio:** La porta 1524 è in ascolto e fornisce accesso Root diretto senza alcuna autenticazione.
- **Verifica (PoC):** Connessione netcat riuscita con privilegi amministrativi istantanei.

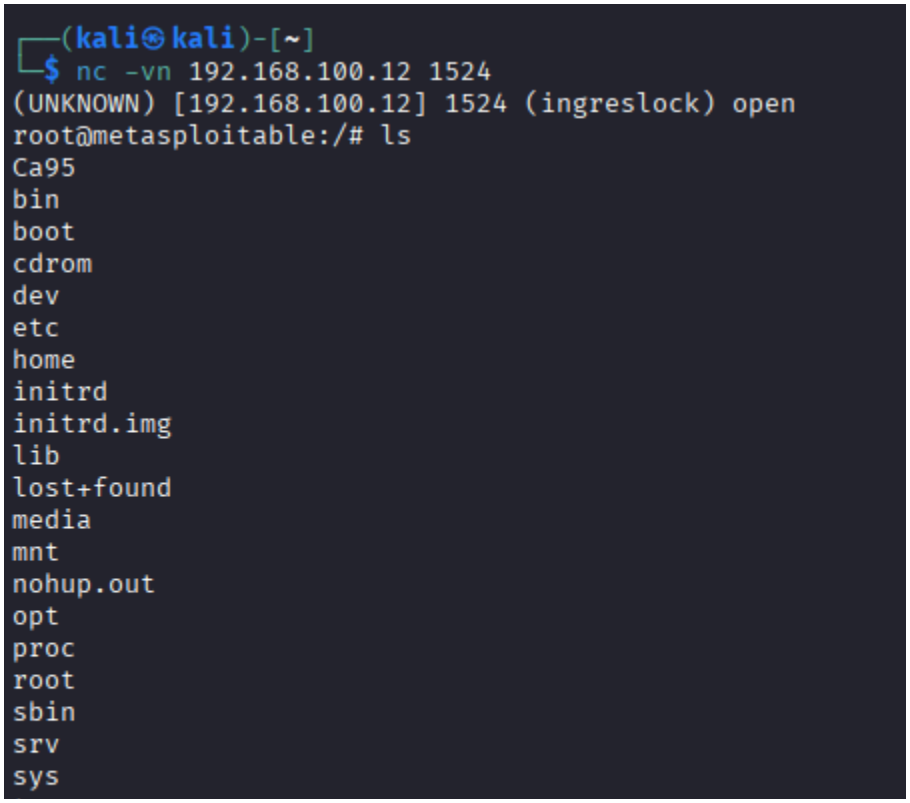

Figura 4: Accesso root senza password tramite la porta 1524.

Finding #3: Credenziali Deboli (VNC)

- **Gravità: 🔴 CRITICA** (CVSS 10.0)
- **Impatto di Business: Esposizione Visiva.** Un attaccante può spiare le operazioni degli amministratori, rubare altre credenziali digitate a schermo e manipolare file tramite interfaccia grafica.
- **Dettaglio:** Il servizio Desktop Remoto (VNC, porta 5900) utilizza la password "password". Rilevato tramite modulo Hydra.
- **Verifica (PoC):** Accesso GUI riuscito.

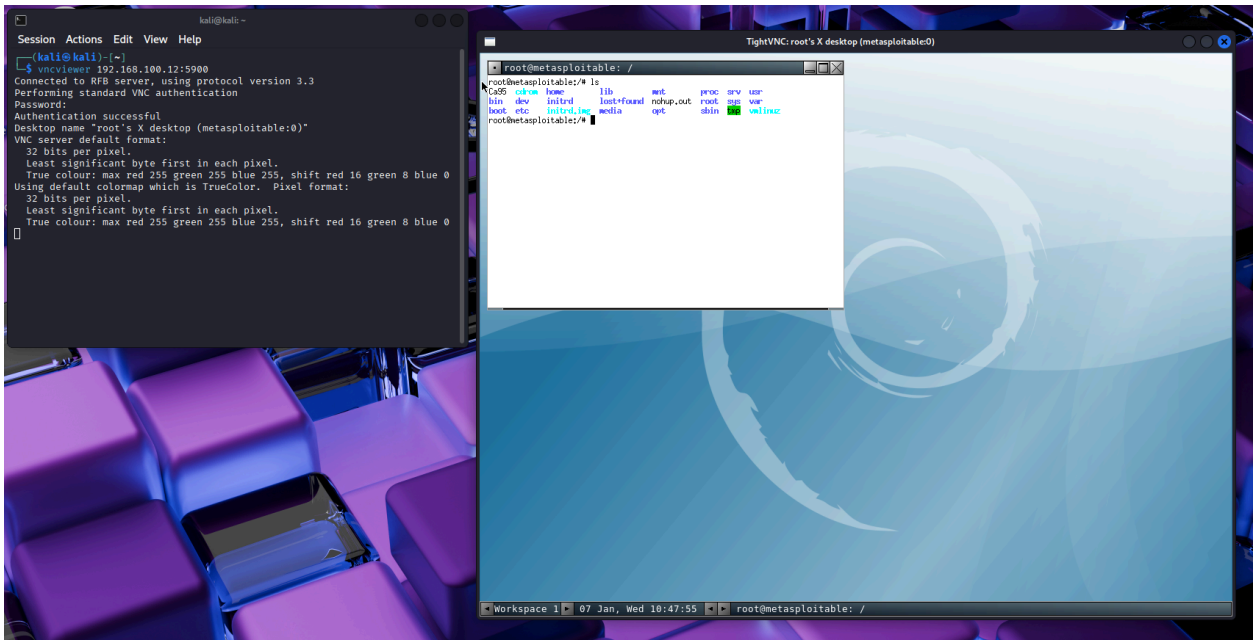

Figura 5: Controllo desktop remoto acquisito.

---

5. Piano di Remediation (Roadmap)

Vista la criticità (30 vulnerabilità gravi), si raccomanda il seguente piano d'azione gerarchico.

Priorità	Azione	Tempistica
1. Contenimento	Isolare immediatamente il server in una VLAN senza accesso a Internet. Chiudere le porte 1524 (Ingreslock) e 21 (FTP) via Firewall.	**Immediato**
2. Hardening	Modificare la password VNC e configurare il servizio per ascoltare solo su localhost (127.0.0.1). Implementare l'accesso tramite **Tunnel SSH** per l'amministrazione remota.	**24 Ore**
3. Strategico	Pianificare la dismissione del sistema operativo Ubuntu 8.04 (End-of-Life) e la migrazione dei servizi su un'infrastruttura supportata e patchabile.	**30 Giorni**