SECURITY AUDIT REPORT

Server: tatlin — Infrastructure Security Assessment

Periodo analizzato: 2026-07-18 (giornata del giorno precedente)

Data emissione: 2026-07-19 17:53

CRITICITA RILEVATE - VERIFICA CONSIGLIATA

1. SINTESI ESECUTIVA

Nel periodo analizzato sono stati rilevati tentativi automatizzati di accesso (SSH e FTP) e attivita di scansione web, tutti gestiti e bloccati dai sistemi di difesa (fail2ban). Non e' stato riscontrato alcun accesso non autorizzato riuscito. Il server e' da considerarsi in stato di sicurezza operativa, con superfici esposte da valutare (vedi sezioni 4-5).

2. ACCESSI E AUTENTICAZIONE (SSH)

Tentativi SSH falliti	102
Login SSH riusciti	5
Utenti con login riuscito	monnis

Analisi: gli account SSH sul sistema sono 5 (root, debian, bione, sermi, monnis), tutti legittimi e riferibili a persone fisiche note. Un numero elevato di tentativi falliti indicherebbe brute-force; in questo periodo il valore e' contenuto/assente, segno che SSH non e' sotto attacco diretto riuscito. SSH e' esposto sulla porta non standard 22672 (IPv4 e IPv6) e filtrato dal firewall TinyCP.

3. SISTEMA DI DIFESA - FAIL2BAN

IP bannati nel periodo	4
Jail attive	apache-auth, apache-noscript, apache-badbots, apache-overflows, apache-botsearch

IP bannati (top): 20.206.105.145 (1x); 20.226.26.5 (1x)

Le jail che hanno effettuato ban: apache-noscript (2)

Analisi: fail2ban e' operativo e aggiorna dinamicamente la blacklist. I ban riguardano tipicamente scansioni automatiche di URL vulnerabili (wp-admin, script PHP) e tentativi su servizi mail/FTP. La presenza di ban e' attesa su un server pubblico ed e' indice che il sistema di difesa funziona.

4. SERVIZIO FTP (vsftpd)

Connessioni FTP	20
Login FTP falliti	1

Client FTP osservati (esempio): 100.31.87.143, 20.163.15.172, 20.65.138.97, 208.181.90.27, 213.136.83.63, 217.146.80.104, 34.14.66.43, 34.78.173.223 ...

Analisi: il servizio FTP e' esposto su porta 21 e 2121 (0.0.0.0) ed e' oggetto di connessioni da IP vari, incluse tentate autenticazioni anonime fallite. Non risultano accessi riusciti non autorizzati, ma la superficie e' esposta. Raccomandazione: se il servizio FTP non e' piu' necessario, disabilitarlo per ridurre la superficie d'attacco; in alternativa limitare l'accesso per IP o usare SFTP.

5. PORTE DI RETE ESPOSTE

```
:59326  ->  TinyCP (pannello admin)
:8005  ->  sc_trans (streaming radio CentovaCast)
:8200  ->  minidlnad (media server DLNA)
:2121  ->  vsftpd (FTP alternativo)
:22672  ->  sshd (SSH)
:21  ->  vsftpd (FTP standard)
```

Analisi: le porte 8005 (radio) e 8200 (DLNA) mostrano un elevato numero di connessioni stabili; quelle su :8005 corrispondono ad ascoltatori legittimi dello streaming radio (non a un attacco). SSH su 22672 e FTP su 21/2121 sono le superfici piu' a rischio e dovrebbero essere ulteriormente limitate (es. allowlist per IP, o disabilitazione FTP se non usato).

6. RISORSE E INTEGRITA DEL SISTEMA

Spazio disco (/)	28% (479G/1.8T)

Uptime sistema	~520 giorni (kernel 4.19, da aggiornare)
Utenti con shell	5

Analisi: il disco e' ampiamente sotto soglia (28%). Il sistema e' attivo da oltre 500 giorni senza reboot: stabile ma con kernel non aggiornato rispetto alle patch di sicurezza recenti. Con il linger di Hermes ora attivo, un reboot programmato per aggiornamento kernel e' fattibile. Gli utenti con shell sono tutti noti e legittimi.

7. NOTE METODOLOGICHE

- Report generato automaticamente da Hermes Agent in modalita read-only (nessuna modifica al sistema).
- Fonti: /var/log/auth.log, /var/log/fail2ban.log, /var/log/vsftpd.log, stato porte (ss), stato dischi (df).
- I tentativi di accesso automatici (bot) sono normali su server pubblici e gestiti da fail2ban.
- Per azioni correttive (es. disabilitazione FTP, hardening SSH) contattare l'amministratore di sistema.