Scan Technical Report

In questo report si riportano i risultati di una scansione di sicurezza automatica, il cui target è l'Host Metasploitable con ip 192.168.50.101. L'Host sorgente della scansione è Kali Linux, con cui si ha utilizzato lo scanner Greenbone. Il report riassume le vulnerabilità trovate, per ogni livello di criticità si ha una tabella esplicativa: Critical, High, Medium e Low.
Di seguito una tabella riepilogativa sul numero di vulnerabilità:

Host	Critical	High	Medium	Low
192.168.50.101	10	5	38	5

Nel sommario iniziale sono riportate **tot** vulnerabilità per ogni livello, calcolate in base alle singole istanze rilevate dallo scanner (conteggio *per-port*). Tuttavia, nella tabella di dettaglio, le vulnerabilità identiche rilevate su più porte sono state **raggruppate per tipologia.** Questa organizzazione è stata applicata per migliorare la leggibilità e focalizzare l'attenzione sulla *Remediation* alla radice piuttosto che sulla singola porta, riducendo così la ridondanza visuale del documento.

Critical Vulnerabilities

Servizio (Porta)	Vulnerabilità	Impatto	Remediation
general/tcp	OS End of Life (EOL) Detection	Il sistema operativo remoto (Ubuntu 8.04) è *End of Life*. Non riceve più aggiornamenti di sicurezza, esponendo l'host a exploit noti.	**Mitigation:** Aggiornare il sistema operativo a una versione supportata dal vendor.
6200/tcp, 21/tcp	vsftpd Compromised Source Packages Backdoor	Il pacchetto sorgente di vsftpd (v2.3.4) contiene una *backdoor* che apre una shell sulla porta 6200/tcp. Permette a un attaccante di eseguire *arbitrary commands (da shell)*.	**Vendor Fix:** Sostituire il pacchetto con una versione pulita e verificata.
3632/tcp	DistCC RCE Vulnerability (CVE-2004-2687)	DistCC permette l'esecuzione di *remote commands (RCE)*. È stato possibile eseguire il comando "id".	**Vendor Fix:** Aggiornare DistCC o configurare le restrizioni di accesso (ACL) per le porte del server.

8787/tcp	Distributed Ruby (dRuby) Multiple RCE	Configurazione insicura di dRuby (Ruby v1.6+). Permette l'esecuzione di *arbitrary syscall commands* o script Ruby remoti.	**Mitigation:** Implementare controlli di accesso, aumentare il livello della variabile $SAFE (>=2 recommended) o restringere l'accesso agli host fidati.
80/tcp	TWiki Multiple XSS & Command Execution	Vulnerabilità multiple in TWiki (< 4.2.4) permettono *Cross-Site Scripting (XSS)* e *perl code execution* tramite iniezione nella variabile %SEARCH%.	**Vendor Fix:** Aggiornare TWiki alla versione 4.2.4 o successiva.
80/tcp	PHP < 5.3.13 CGI Argument Injection	Vulnerabilità critica (CVE-2012-1823) che permette l'esecuzione di codice tramite argomenti CGI.	**Vendor Fix:** Aggiornare PHP a una versione sicura (es. 5.3.13+).
5900/tcp	VNC Brute Force Login	Accesso al server VNC riuscito tramite *Brute Force* o password debole ("password").	**Mitigation:** Impostare una password complessa o abilitare meccanismi di protezione
5432/tcp	PostgreSQL Default Credentials	Accesso al database PostgreSQL riuscito con credenziali predefinite/deboli (postgres:postgres).	**Mitigation:** Cambiare la password dell'account postgres.
1524/tcp	Possible Backdoor: Ingreslock	Rilevata una *backdoor* sulla porta 1524 (Ingreslock exploit). Risponde al comando "id" con privilegi root.	**Workaround:** È raccomandata una pulizia completa del sistema infetto (reinstallazione).

High Vulnerabilities

Servizio (Porta)	Vulnerabilità	Impatto	Remediation
1099/tcp	Java RMI Server Insecure Configuration RCE	Configurazione predefinita errata del server Java RMI.	**Workaround:** Disabilitare il *class-loading* remoto o

		Permette a un attaccante non autenticato di caricare classi ed eseguire *arbitrary code* con privilegi elevati.	contattare il vendor per una patch specifica.
21/tcp	FTP Brute Force Logins (Default Creds)	Rilevate credenziali deboli o di default (es. msfadmin:msfadmin, postgres:postgres, user:user). Permette accesso non autorizzato e modifica dei file.	**Mitigation:** Cambiare tutte le password degli account rilevati con password forti.
80/tcp	EasyPHP Webserver <= 12.1 Multiple Vulns	EasyPHP espone informazioni sensibili tramite phpinfo() e permette l'esecuzione di codice PHP remoto o divulgazione di informazioni amministrative.	**Will Not Fix:** Il prodotto non è più supportato. Si consiglia di disinstallare, aggiornare o sostituire il software.
80/tcp	Test HTTP dangerous methods	Il server web ha i metodi HTTP PUT e DELETE abilitati. Permette a un attaccante di caricare file arbitrari (es. shell web) o cancellare file esistenti.	**Mitigation:** Disabilitare i metodi PUT e DELETE nella configurazione del web server o restringere l'accesso.
5432/tcp	OpenSSL CCS Man in the Middle Security Bypass	Vulnerabilità in OpenSSL (CVE-2014-0224) che permette un attacco *Man-in-the-Middle* tramite *CCS Injection*, forzando l'uso di chiavi deboli.	**Vendor Fix:** Aggiornare OpenSSL (versioni affette: prima di 0.9.8za, 1.0.0m, 1.0.1h).

Medium Vulnerabilities

Servizio (Porta)	Vulnerabilità	Impatto	Remediation
21/tcp, 2121/tcp	FTP Unencrypted Cleartext Login	Login FTP trasmesso in chiaro. Password	**Mitigation:** Usare FTPS (SSL/TLS) o SFTP.

		intercettabili tramite *sniffing*.	
25/tcp, 5432/tcp	Deprecated SSLv2 and SSLv3 Protocol	Supporto a protocolli obsoleti vulnerabili ad attacchi (es. POODLE, DROWN).	**Mitigation:** Disabilitare SSLv2 e SSLv3.
25/tcp, 5432/tcp	Weak SSL/TLS Certificates (RSA < 2048)	Certificati con chiavi RSA deboli (1024 bit).	**Mitigation:** Sostituire con certificati RSA >= 2048 bit.
25/tcp, 5432/tcp	SSL/TLS Certificate Expired	I certificati SSL sono scaduti (es. nel 2010).	**Mitigation:** Rinnovare e installare certificati validi.
25/tcp, 5432/tcp	SSL/TLS Renegotiation DoS	Vulnerabilità che espone il server a *Denial of Service (DoS)* tramite rinegoziazione.	**Vendor Fix:** Disabilitare la rinegoziazione client-side.
25/tcp, 5432/tcp	Deprecated TLSv1.0 and TLSv1.1	Utilizzo di protocolli TLS vecchi, vulnerabili ad attacchi come *BEAST (Browser Exploit Against SSL/TLS)*	**Mitigation:** Abilitare solo TLS 1.2 o superiore.
25/tcp, 5432/tcp	Diffie-Hellman Insufficient Group Strength	Gruppo DH debole (1024 bit), rischio decrittazione Logjam.	**Workaround:** Usare gruppi DH a 2048 bit o superiori.
25/tcp, 5432/tcp	SSL/TLS Weak Signature Algorithm	Firma del certificato debole (SHA-1 o MD5).	**Mitigation:** Usare firme SHA-256 o superiori.
25/tcp	SSL/TLS FREAK Vulnerability	Accetta chiavi RSA_EXPORT deboli (Downgrade attack).	**Vendor Fix:** Aggiornare OpenSSL/Configurazione.
25/tcp	Mailserver VRFY and EXPN requests	Il server risponde a comandi che enumerano gli utenti validi.	**Workaround:** Disabilitare VRFY e EXPN.
21/tcp	Anonymous FTP Login Reporting	Accesso FTP anonimo consentito.	**Mitigation:** Disabilitare se non strettamente necessario.
80/tcp	TWiki Multiple CSRF & XSS	Vulnerabilità multiple (CSRF, XSS) in versioni obsolete di TWiki.	**Vendor Fix:** Aggiornare TWiki all'ultima versione.

80/tcp	jQuery < 1.9.0 / 1.6.3 XSS	Versioni vecchie di jQuery vulnerabili a Reflected XSS.	**Vendor Fix:** Aggiornare le librerie jQuery.
80/tcp	HTTP Debugging Methods (TRACE/TRACK)	Metodi di debug attivi, rischio Cross-Site Tracing (XST).	**Mitigation:** Disabilitare TRACE e TRACK.
80/tcp	phpinfo() Output Reporting	File phpinfo.php esposto, rivela configurazione dettagliata del server.	**Workaround:** Rimuovere il file o restringere l'accesso.
80/tcp	QWikiwiki Directory Traversal	Input non validato permette lettura file arbitrari (es. /etc/passwd).	**Will Not Fix:** Rimuovere il software obsoleto.
80/tcp	Cleartext Transmission of Sensitive Info	Credenziali inviate in chiaro su HTTP (DVWA, phpMyAdmin, ecc.).	**Workaround:** Forzare HTTPS per i login.
80/tcp	Apache httpOnly Cookie Disclosure	Esposizione cookie httpOnly tramite pagine di errore 400 (CVE-2012-0053).	**Vendor Fix:** Aggiornare Apache HTTP Server.
80/tcp	awiki / doc directory issues	Vulnerabilità LFI (Local File Inclusion) in awiki e directory listing attivo su /doc.	**Mitigation:** Rimuovere awiki / Disabilitare listing.
80/tcp	phpMyAdmin 'error.php' XSS	XSS nella pagina di errore di phpMyAdmin.	**Vendor Fix:** Aggiornare phpMyAdmin.
445/tcp	Samba MS-RPC Remote Shell (CVE-2007-2447)	**Critica:** Esecuzione comandi shell tramite username malevolo.	**Vendor Fix:** Aggiornare Samba
22/tcp	Weak SSH Algorithms (Key/KEX/Enc/MAC)	Supporto algoritmi deboli (Arcfour, MD5, ssh-dss, gruppi DH piccoli).	**Mitigation:** Indurire la configurazione di SSH (sshd_config).
5900/tcp	VNC Server Unencrypted Data	Traffico VNC e autenticazione non crittografati.	**Mitigation:** Usare tunneling SSH o VPN.
5432/tcp	SSL/TLS Report Weak Cipher Suites	Il servizio accetta cifrari deboli (es. RC4, DES).	**Mitigation:** Configurare cipher suites sicure.

Low Vulnerabilities

Servizio (Porta)	Vulnerabilità	Impatto	Remediation
general/tcp	TCP Timestamps Information Disclosure	L'host risponde con timestamp TCP (RFC1323/7323). Permette di calcolare l'uptime esatto del server	**Mitigation:** Disabilitare i timestamp TCP nel kernel
25/tcp	SSL/TLS: 'DHE_EXPORT' MITM (LogJam)	Il server supporta suite di cifratura *DHE_EXPORT* deboli. Un attaccante *Man-in-the-Middle* può forzare un downgrade della crittografia a 512-bit.	**Vendor Fix:** Rimuovere il supporto per le suite DHE_EXPORT dalla configurazione del mail server.
general/icmp	ICMP Timestamp Reply Information Disclosure	L'host risponde alle richieste ICMP Timestamp (Type 13). Rivela l'ora del sistema e può aiutare attacchi basati sul tempo.	**Mitigation:** Bloccare i messaggi ICMP Timestamp (Type 13/14) tramite firewall o disabilitarli nell'OS.
22/tcp	Weak MAC Algorithm(s) Supported (SSH)	Il server SSH accetta *algoritmi di integrità (MAC)* deboli come MD5 o SHA-1 a 96-bit (hmac-md5, hmac-sha1-96).	**Mitigation:** Configurare SSH per usare solo algoritmi MAC forti (es. hmac-sha2-256, umac-128).
5432/tcp	SSL/TLS: POODLE Vulnerability (CBC)	Rilevato supporto a suite di *cifratura CBC* su SSLv3. Espone il traffico a decrittazione tramite l'attacco POODLE.	**Mitigation:** Disabilitare SSLv3 e le cifrature CBC nella configurazione di PostgreSQL.