Report finale M3 Scansione finale Manini Sara

Indice generale

Introduzione

In questo report andremo ad eseguire una nuova scansione sulla vm di Metasploitable 2, utilizzando sempre Nessus ed eseguendola dalla vm di Kali Linux.
Noteremo che le vulnerabilità sono diminuite a fronte delle remediations eseguite ed illustrate in precedenza, ai fini di presentare un report più completo possibile, andrò a presentare in una tabella riassuntiva le vulnerabilità ancora presenti in modo che un eventuale “cliente” possa valutare come muoversi a riguardo.
Per maggiori informazioni riguardo le vulnerabilità consultare il report Scansione inizio Manini Sara.pdf .

Executive summary

Informazioni sulla scansione

Persona che ha eseguito la scansione: Manini Sara
Software utilizzato per la scansione: Nessus 10.8.4 (#28) LINUX
Inizio scansione: Dom 18/05/2025 15:23:19
Fine scansione: Dom 18/05/2025 15:56:55
Durata scansione: 33 min. 36 sec.
Tipo scansione: Basic Network Scan
Porte interessate dalla scansione: 1-65535

Informazioni Host

Netbios name: METASPLOITABLE
IP: 192.168.32.101
MAC address: 08:00:27:E0:12:C1
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Tabella riassuntiva Vulnerabilità

Livello rischio	Numero vulnerabilità
Critical	2
High	6
Medium	27
Low	7
Info	132
Totali	174

Grafico Vulnerabilità

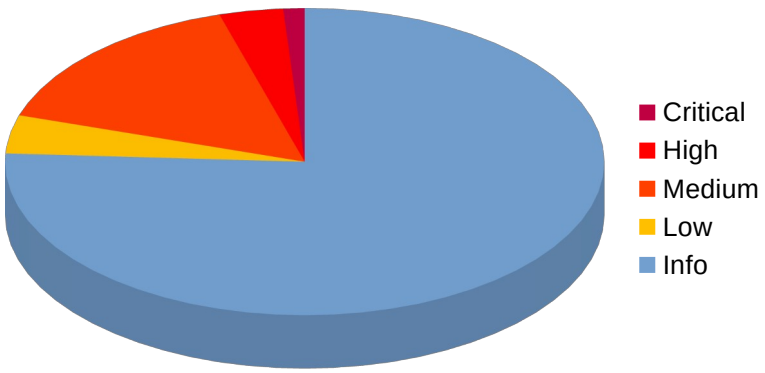

Tabella riassuntiva vulnerabilità residue

Criticità	Titolo vulnerabilità
Critical	32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Critical	125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
High	39469 - CGI Generic Remote File Inclusion
High	136769 - ISC BIND Service Downgrade / Reflected DoS
High	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
High	90509 - Samba Badlock Vulnerability
High	19704 - TWiki 'rev' Parameter Arbitrary Command Execution
High	36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
Medium	11411 - Backup Files Disclosure
Medium	40984 - Browsable Web Directories
Medium	44136 - CGI Generic Cookie Injection Scripting
Medium	49067 - CGI Generic HTML Injections (quick test)
Medium	42872 - CGI Generic Local File Inclusion (2nd pass)
Medium	39466 - CGI Generic XSS (quick test)
Medium	10595 - DNS Server Zone Transfer Information Disclosure (AXFR)
Medium	11213 - HTTP TRACE / TRACK Methods Allowed
Medium	139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
Medium	136808 - ISC BIND Denial of Service
Medium	46803 - PHP expose_php Information Disclosure
Medium	57608 - SMB Signing not required
Medium	52611 - SMTP Service STARTTLS Plaintext Command Injection
Medium	90317 - SSH Weak Algorithms Supported
Medium	31705 - SSL Anonymous Cipher Suites Supported
Medium	51192 - SSL Certificate Cannot Be Trusted
Medium	15901 - SSL Certificate Expiry
Medium	45411 - SSL Certificate with Wrong Hostname
Medium	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medium	57582 - SSL Self-Signed Certificate
Medium	104743 - TLS Version 1.0 Protocol Detection

Medium	57640 - Web Application Information Disclosure
Medium	85582 - Web Application Potentially Vulnerable to Clickjacking
Medium	11229 - Web Server info.php / phpinfo.php Detection
Medium	51425 - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
Medium	36083 - phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
Medium	49142 - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
Low	10114 - ICMP Timestamp Request Remote Date Disclosure
Low	70658 - SSH Server CBC Mode Ciphers Enabled
Low	153953 - SSH Weak Key Exchange Algorithms Enabled
Low	71049 - SSH Weak MAC Algorithms Enabled
Low	42057 - Web Server Allows Password Auto-Completion
Low	26194 - Web Server Transmits Cleartext Credentials
Low	10407 - X Server Detection

Conclusione

Come evidenziato nell'executive summary e nella tabella riassuntiva, molte vulnerabilità non esplicitamente menzionate nella documentazione delle attività di remediation sono state comunque risolte e, di conseguenza, non sono più emerse nella scansione finale.
Questo risultato è attribuibile al fatto che alcuni dei servizi coinvolti nelle azioni correttive erano condivisi tra più vulnerabilità; pertanto, la loro modifica ha portato a una riduzione complessiva del numero di criticità rilevate.