Report finale M3 Scansione iniziale Manini Sara

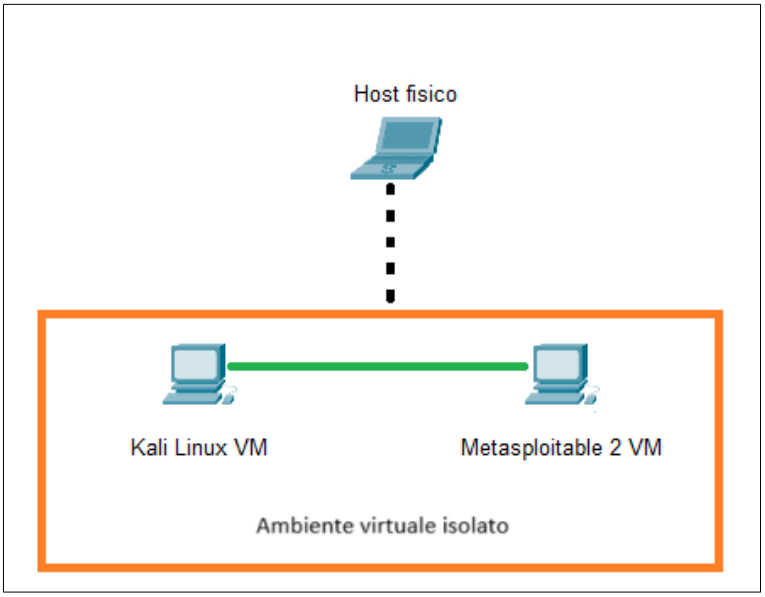
Indice generale

Introduzione

La scansione è stata eseguita con il software di vulnerability assessment Nessus, presente sulla macchina virtuale Kali Linux, con target la macchina virtuale Metasploitable 2.
Le due macchine si trovavano sulla stessa rete al momento della scansione, senza accesso ad internet e senza gateway a fare da tramite per la comunicazione.
Di seguito la struttura del laboratorio con i rispettivi IP.

IP di Kali Linux: 192.168.32.100
IP di Metasploitable 2: 192.168.32.101

Struttura del laboratorio:



Lo scopo di questo vulnerabilty assessment è stato scoprire quali vulnerabilità si trovano sulla macchina interessata dallo scan per poi eseguire delle remediantions mirate e rafforzare così la sicurezza e l'integrità della macchina contro eventuali attacchi informatici.

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: Ven 16/05/2025 23:17:28
Fine scansione: Ven 16/05/2025 23:55:55
Durata scansione: 38 min. 27 sec.
Tipo scansione: Basic Network Scan
Porte interessate dalla scansione: 1-65535

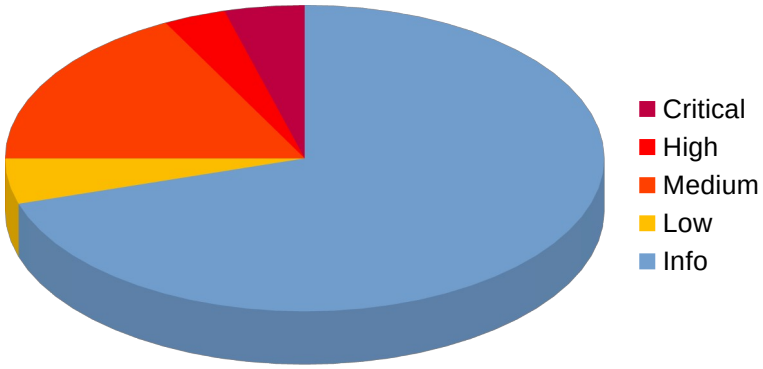
Informazioni Host

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	9
High	7
Medium	36
Low	10
Info	146
Totali	208

Grafico Vulnerabilità



Analisi dettagliata delle vulnerabilità

Di seguito un'analisi tecnica delle vulnerabilità riscontrate, verranno divise per categorie secondo l'ordine di gravità assegnato loro da Nessus al completamento della scansione.
Le remediations suggerite da Nessus verranno incluse per completezza del report ma è doveroso notare che per la fase di remediation non verranno applicate alla lettera in quanto sono state intraprese azioni alternative per aderire al meglio alla consegna dell'esercizio.

Critical

134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)	
Porta: 8009	CVSS: 9.8
Sinossi: Trovato un connettore AJP vulnerabile in ascolto sull'host remoto	
Impatto: Un attaccante remoto non autenticato può sfruttare la vulnerabilità per leggere file delle web application su un server vulnerabile. Se il server consente il caricamento di file, l'attaccante potrebbe caricare codice JSP malevolo e ottenere l'esecuzione remota di codice (RCE).	
Remediation suggerita: Aggiornare la configurazione AJP in modo che richieda l'autorizzazione oppure aggiornare il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successive.	

51988 - Bind Shell Backdoor Detection	
Porta: 1524	CVSS: 9.8
Sinossi: L'host remoto potrebbe essere stato compromesso.	
Impatto: Un attacante potrebbe sfruttare la shell per connettersi alla porta remota ed eseguire direttamente comandi.	
Remediation suggerita: Verificare se l'host remoto è stato compromesso e reinstallare il sistema operativo se necessario.	

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
Porta: 22	CVSS: 10.0
Sinossi: Le chiavi host per l'SSH remoto sono deboli.	
Impatto: Un attaccante potrebbe facilmente ottenere la parte privata della chiave remota ed usarla per decifrare la sessione remota o avviare un attacco man in the middle.	
Remediation suggerita: Considerare come potenzialmente indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.	

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
Porta: 25, 5432	CVSS: 10.0
Sinossi: Il certificato remoto SSL utilizza una chiave debole.	
Impatto: Un attaccante potrebbe facilmente ottenere la parte privata della chiave remota ed usarla per decifrare la sessione remota o avviare un attacco man in the middle.	
Remediation suggerita: Considerare come potenzialmente indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.	

20007 - SSL Version 2 and 3 Protocol Detection	
Porta: 25, 5432	CVSS: 9.8
Sinossi: Il servizio remoto cripta il traffico usando un protocollo con vulnerabilità note.	
Impatto: Un attaccante può sfruttare queste vulnerabilità per eseguire attacchi man in the middle o decifrare le comunicazioni, forzando un downgrade del protocollo SSL/TLS a versioni meno sicure a causa di implementazioni deboli nei browser.	
Remediation suggerita: Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0. Usare TLS 1.2 (con le approvate suite di cifratura) o versioni più recenti.	

61708 - VNC Server 'password' Password	
Porta: 5900	CVSS: 10.0
Sinossi: Server VNC ha una password debole.	
Impatto: Un attaccante remoto privo di autenticazione potrebbe usare questo metodo per prendere il controllo del sistema.	
Remediation suggerita: Cambiare la password con una più forte ed eseguire un password reset periodico.	

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)	
Porta: 80	CVSS: 9.8
Sinossi: Il server web remoto hosta un'applicazione PHP affetta da vulnerabilità SQLi.	
Impatto: Un attaccante remoto senza autenticazione può sfruttare questa vulnerabilità per immettere o manipolare queries SQL nel database di back-end.	
Remediation suggerita: Aggiornare a phpMyAdmin 4.8.6 o versioni successive. In alternativa, applicare le patch suggerite dal vendor.	

High

39469 - CGI Generic Remote File Inclusion	
Porta: 80	CVSS: 7.5
Sinossi: Codice arbitrario potrebbe essere eseguito sul server remoto.	
Impatto: Un attaccante potrebbe essere in grado di caricare un file da server remoto ed eseguire comandi arbitrari sull'host target.	
Remediation suggerita: Limitare l'accesso all'applicazione vulnerabile. Contattare il vendor per patch o aggiornamenti.	

136769 - ISC BIND Service Downgrade / Reflected DoS	
Porta: 53	CVSS: 8.6
Sinossi: Il name server remoto è affetto da vulnerabilità di Service downgrade/Reflected DoS.	
Impatto: Un attaccante remoto non autenticato può sfruttare questa vulnerabilità per causare il downgrade del servizio del server ricorsivo oppure usare il server afflitto come riflettore in un reflection attack.	
Remediation suggerita: Aggiornare alla versione di ISC BIND citata nelle raccomandazioni del vendor.	

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	
Porta: 25, 5432	CVSS: 7.5
Sinossi: Il server remoto supporta l'utilizzo di cifrari SSL di sicurezza media.	
Impatto: Un attaccante sulla stessa rete può circonvenire la criptazione a media sicurezza con facilità.	
Remediation suggerita: Riconfigurare l'applicazione afflitta se possibile per evitare l'uso di cifrari a media sicurezza.	

90509 - Samba Badlock Vulnerability	
Porta: 445	CVSS: 7.5
Sinossi: Un server SMB in esecuzione sull'host remoto è affetto dalla vulnerabilità Badlock.	
Impatto: Un attaccante man-in-the-middle può forzare il downgrade dell'autenticazione tra client e server SAM, eseguendo chiamate Samba arbitrarie come la visualizzazione o modifica di dati sensibili in Active Directory o la disattivazione di servizi critici.	
Remediation suggerita: Aggiornare Samba alla versione 4.2.11/4.3.8/4.4.2 o successive.	

19704 - TWiki 'rev' Parameter Arbitrary Command Execution	
Porta: 80	CVSS: 8.8
Sinossi: Il server remoto hosta un’applicazione CGI affetta da una vulnerabilità di esecuzione comandi arbitrari.	
Impatto: La versione di TWiki sul server remoto presenta una vulnerabilità nel parametro 'rev' che consente a un attaccante di eseguire comandi shell arbitrari con i privilegi dell'utente del web server.	
Remediation suggerita: Applicare gli hotfix appropriati consigliati dal vendor.	

36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)	
Porta: 80	CVSS: 7.5
Sinossi: Il server remoto contiene un’applicazione PHP affetta da una vulnerabilità di esecuzione codice.	
Impatto: Un attaccante remoto potrebbe sfruttare le vulnerabilità per eseguire codice PHP arbitrario.	
Remediation suggerita: Aggiornare alla versione 3.1.3.2 di phpMyAdmin. In alternativa applicare le patch citate nella project’s advisory.	

Medium

11411 - Backup Files Disclosure	
Porta: 80	CVSS: 5.0
Sinossi: È possibile recuperare i backup dei file dal server remoto.	
Impatto: Rischio di divulgazione di dati sensibili.	
Remediation suggerita: Assicurarsi che i file non contengano informazioni sensibili, successivamente cancellare o proteggere i file a cui il pubblico non dovrebbe avere accesso.	

40984 - Browsable Web Directories	
Porta: 80	CVSS: 5.3
Sinossi: Alcune directories nel web server remoto sono consultabili.	
Impatto: Rischio di divulgazione di dati sensibili.	
Remediation suggerita: Assicuratevi che le directory esplorabili non trasmettano informazioni riservate né diano accesso a risorse sensibili. Inoltre, applicate restrizioni di accesso o disabilitate l'indicizzazione delle directory per quelle che lo fanno.	

44136 - CGI Generic Cookie Injection Scripting	
Porta: 80	CVSS: 4.3
Sinossi: Il web server remoto è vulnerabile agli attacchi di cookie injection.	
Impatto: Sfruttando questa vulnerabilità, un attaccante potrebbe essere in grado di immettere cookie arbitrari. A seconda della struttura dell'applicazione web, potrebbe essere possibile lanciare un attacco di "session fixation" utilizzando questo meccanismo.	
Remediation suggerita: Limitare l’accesso all’applicazione vulnerabile, Contattare il vendor per una patch o aggiornamento.	

49067 - CGI Generic HTML Injections (quick test)	
Porta: 80	CVSS: 4.3
Sinossi: Il web server remoto potrebbe essere vulnerabile ad injections HTML.	
Impatto: Un attaccante potrebbe eseguire codice HTML malevolo nel browser di un user, all'interno del contesto di sicurezza del sito interessato.	
Remediation suggerita: Limitare l’accesso all’applicazione vulnerabile oppure contattare il vendor per un aggiornamento.	

42872 - CGI Generic Local File Inclusion (2nd pass)	
Porta: 80	CVSS: 6.8
Sinossi: Codice non autorizzato potrebbe essere eseguito su questo server.	
Impatto: Un attaccante potrebbe includere un file locale distribuire i suoi contenuti, oppure eseguire codice malevolo sull'host remoto.	
Remediation suggerita: Limitare l'accesso all'applicazione vulnerabile. Considerare il vendor per una patch o un upgrade.	

42872 - CGI Generic Local File Inclusion (2nd pass)	
Porta: 80	CVSS: 6.8
Sinossi: Codice non autorizzato potrebbe essere eseguito su questo server.	
Impatto: Un attaccante potrebbe includere un file locale distribuire i suoi contenuti, oppure eseguire codice malevolo sull'host remoto.	
Remediation suggerita: Limitare l'accesso all'applicazione vulnerabile. Contattare il vendor per una patch o un upgrade.	

39466 - CGI Generic XSS (quick test)	
Porta: 80	CVSS: 4.3
Sinossi: Il web server remoto è vulnerabile ad attacchi di cross-site scripting.	
Impatto: Un attaccante potrebbe eseguire codice HTML e script non autorizzati nel browser di un utente, nel contesto di sicurezza del sito interessato.	
Remediation suggerita: Limitare l'accesso all'applicazione vulnerabile. Contattare il vendor per una patch o un upgrade inerente alle vulnerabilità legate al cross-site scripting.	

10595 - DNS Server Zone Transfer Information Disclosure (AXFR)	
Porta: 53	CVSS: 4.4
Sinossi: Il name server remoto consente l'esecuzione di trasferimenti di zona DNS.	
Impatto: Un attaccante potrebbe sfruttare questa vulnerabilità per ottenere informazioni sulla topologia della rete ed individuare nuovi bersagli.	
Remediation suggerita: Limitare il trasferimento DNS solamente ai server che necessitano delle informazioni.	

11213 - HTTP TRACE / TRACK Methods Allowed	
Porta: 80	CVSS: 5.3
Sinossi: Le funzioni di debug sono abilitate sul server web remoto.	
Impatto: Un attaccante potrebbe sfruttare i metodi HTTP TRACE e TRACK usati per le funzioni di debug.	
Remediation suggerita: Disabilitare i metodi HTTP citati.	

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	
Porta: 53	CVSS: 6.5
Sinossi: Il name server remoto è affetto da una vulnerabilità DoS.	
Impatto: Un attaccante remoto con autenticazione potrebbe sfruttare questa vulnerabilità inviando una risposta parziale a una richiesta TSIG-signed per causare interruzione del server.	
Remediation suggerita: Aggiornare BIND alla versione 9.11.22, 9.16.6, 9.17.4 o successive.	

136808 - ISC BIND Denial of Service	
Porta: 53	CVSS: 5.9
Sinossi: Il name server remoto è affetto da una vulnerabilità di tipo assertion failure.	
Impatto: Un attaccante remoto senza autenticazione potrebbe sfruttare questa vulnerabilità tramite un messaggio elaborato su misura per causare l’interruzione del servizio.	
Remediation suggerita: Aggiornare alla versione più recente del servizio BIND installato.	

46803 - PHP expose_php Information Disclosure	
Porta: 80	CVSS: 5.0
Sinossi: La configurazione di PHP sull’host remoto permette la divulgazione di informazioni sensibili.	
Impatto: L'installazione di PHP sul server remoto è configurata in modo tale da consentire a un attaccante di accedere a informazioni potenzialmente sensibili tramite uno specifico URL. Tale URL attiva un Easter egg integrato in PHP.	
Remediation suggerita: Nel file di configurazione di PHP, php.ini, si consiglia di impostare il valore di 'expose_php' su 'Off' per disabilitare questo comportamento. È necessario riavviare il demone del server web affinché la modifica abbia effetto.	

57608 - SMB Signing not required	
Porta: 445	CVSS: 5.3
Sinossi: Il server remoto SMB non richiede autenticazione.	
Impatto: Un attaccante remoto non autenticato potrebbe effettuare attacchi man in the middle contro il server SMB.	
Remediation suggerita: Applicare la firma dei messaggi nella configurazione dell'host. Su Windows, questa impostazione si trova nella policy "Microsoft network server: Digitally sign communications (always)". Su Samba, l'impostazione corrispondente è "server signing".	

52611 - SMTP Service STARTTLS Plaintext Command Injection	
Porta: 25	CVSS: 4.0
Sinossi: Il servizio di email remoto consente immissioni di comandi in chiaro durante la negoziazione di un canale criptato.	
Impatto: Un attaccante remoto non autenticato potrebbe immettere comandi durante la fase in chiaro del protocollo che sarà eseguita durante la fase cifrata del protocollo. In questo modo l’attaccante potrebbe sottrarre la email o le credenziali SASL ad una vittima.	
Remediation suggerita: Contattare il vendor per aggiornamenti disponibili.	

90317 - SSH Weak Algorithms Supported	
Porta: 22	CVSS: 4.3
Sinossi: Il server remoto SSH è configurato per consentire algoritmi deboli di crittografia o nessun algoritmo.	
Impatto: I canali non risultano cifrati o hanno una cifratura debole.	
Remediation suggerita: Contattare il vendor o consultare la documentazione del prodotto per rimuovere i cifrari deboli.	

31705 - SSL Anonymous Cipher Suites Supported	
Porta: 25	CVSS: 5.9
Sinossi: Il servizio supporta l’utilizzo di cifrari SSL anonimi.	
Impatto: Non c’è modo di verificare l’identità dell’host remoto rendendo il servizio vulnerabile ad attacchi man in the middle.	
Remediation suggerita: Riconfigurare l’applicazione affetta, se possibile evitare l’uso di cifrari deboli.	

51192 - SSL Certificate Cannot Be Trusted	
Porta: 25, 5432	CVSS: 6.5
Sinossi: Il certificato SSL per questo servizio non è affidabile.	
Impatto: Host remoto vulnerabile ad attacchi man in the middle.	
Remediation suggerita: Comprare o generare un certificato SSL adeguato per questo servizio.	

15901 - SSL Certificate Expirya	
Porta: 25, 5432	CVSS: 5.3
Sinossi: Il certificato SSL del server remoto è scaduto.	
Impatto: Certificato SSL scaduto.	
Remediation suggerita: Comprare o generare una chiave SSL a sostituzione di quello scaduto.	

45411 - SSL Certificate with Wrong Hostname	
Porta: 25, 5432	CVSS: 5.3
Sinossi: Il certificato SSL per questo servizio è per un host diverso.	
Impatto: Certificato SSL con hostname sbagliato.	
Remediation suggerita: Comprare o generare un certificato SSL adeguato per questo servizio.	

89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	
Porta: 25	CVSS: 5.9
Sinossi: L’host remoto potrebbe essere affetto da una vulnerabilità che permette ad un attaccante remoto di decriptare il traffico TLS catturato.	
Impatto: Un attaccante man in the middle può sfruttare questa vulnerabilità per decriptare la connessione TLS utilizzando traffico catturato in precedenza e una crittografia debole, insieme a una serie di connessioni appositamente predisposte a un server SSLv2 che utilizza la stessa chiave privata.	
Remediation suggerita: Disabilitare SSLv2 ed esportare le suite di crittografia di livello 1. Assicurarsi che le chiavi private non vengano utilizzate da nessuna parte con software server che supporti connessioni SSLv2.	

5821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	
Porta: 25, 5432	CVSS: 5.9
Sinossi: Il servizio remoto supporta l’uso del cifrario RC4.	
Impatto: Un attaccante è in grado di ottenere molti cyphertext e potrebbe derivare il plaintext.	
Remediation suggerita: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrari RC4. Valutare l'utilizzo di TLS 1.2 con suite AES-GCM, a seconda del supporto del browser e del server web.	

57582 - SSL Self-Signed Certificate	
Porta: 25, 5432	CVSS: 6.5
Sinossi: La catena dei certificati SSL per questo servizio finisce in un certificato auto-firmato non riconosciuto.	
Impatto: Chiunque potrebbe effettuare un attacco man in the middle sull’host remoto.	
Remediation suggerita: Comprare o generare un certificato SSL adeguato per questo servizio.	

26928 - SSL Weak Cipher Suites Supported	
Porta: 25	CVSS: 5.3
Sinossi: Il server remoto supporta l’uso di cifrari SSL deboli.	
Impatto: Vulnerabilità facile da sfruttare se l’attaccante si trova sulla stessa rete della macchina.	
Remediation suggerita: Riconfigurare l’applicazione afflitta, se possibile evitare l’uso di cifrari deboli.	

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	
Porta: 25	CVSS: 4.3
Sinossi: Il server remoto supporta l’utilizzo di un set di cifrari deboli.	
Impatto: Un attaccante man in the middle può effettuare il downgrade della sessione per utilizzare i cifrari EXPORT_RSA.	
Remediation suggerita: Riconfigurare il servizio per rimuovere il supporto degli EXPORT_RSA.	

104743 - TLS Version 1.0 Protocol Detection	
Porta: 25, 5432	CVSS: 6.5
Sinossi: Il servizio remoto cripta il traffico utilizzando una versione più vecchia di TLS.	
Impatto: Dal 31/03/2020 i dispositivi non abilitati a TLS 1.2 o superiore non funzioneranno correttamente con la maggior parte dei browser e dei vendor.	
Remediation suggerita: Abilitare il supporto per TLS 1.2 e 1.3 e disattivare TLS 1.0.	

57640 - Web Application Information Disclosure	
Porta: 80	CVSS: 5.0
Sinossi: L’applicazione web remota rivela informazioni sui path.	
Impatto: Rivelare questo tipo di informazioni potrebbe aiutare un attaccante ad eseguire attacchi mirati verso le applicazioni e i loro back-end.	
Remediation suggerita: Filtrare i messaggi di errore che contengono informazioni sui path.	

85582 - Web Application Potentially Vulnerable to Clickjacking	
Porta: 80	CVSS: 4.3
Sinossi: Il web server remoto potrebbe non mitigare una classe di vulnerabilità verso le web app.	
Impatto: Un attaccante potrebbe ingannare un utente facendogli cliccare un’area della pagina vulnerabile diversa da come l’utente la percepisce. Questo può risultare in tentativi fraudolenti o transazioni malevole.	
Remediation suggerita: Restituire a schermo l'intestazione HTTP X-Frame-Options o Content-Security-Policy (con la direttiva 'frame-ancestors') nella risposta della pagina. Questo impedisce che il contenuto della pagina venga visualizzato da un altro sito tramite i tag HTML frame o iframe.	

11229 - Web Server info.php / phpinfo.php Detection	
Porta: 80	CVSS: 5.3
Sinossi: Il web server remoto contiene uno script PHP vulnerabile a un attacco di esposizione informazioni.	
Impatto: Un attaccante può ricavare un gran numero di informazioni riguardo il web server.	
Remediation suggerita: Rimuovere i file affetti.	

11229 - Web Server info.php / phpinfo.php Detection	
Porta: 80	CVSS: 5.3
Sinossi: Il web server remoto contiene uno script PHP vulnerabile a un attacco di esposizione informazioni.	
Impatto: Un attaccante può ricavare un gran numero di informazioni riguardo il web server.	
Remediation suggerita: Rimuovere i file affetti.	

51425 - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	
Porta: 80	CVSS: 4.3
Sinossi: Il web server remoto hosta uno script PHP soggetto ad attacchi XSS.	
Impatto: Un attaccante potrebbe sfruttare la vulnerabilità immettendo codice HTML o script nel browser di un utente per essere eseguito nel contesto di sicurezza del sito implicato.	
Remediation suggerita: Aggiornare a phpMyAdmin 3.4.0-beta1 o versioni succcessive.	

36083 - phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)	
Porta: 80	CVSS: 5.0
Sinossi: Il web server remoto hosta uno script PHP soggetto a diverse problematiche.	
Impatto: Un attaccante remoto senza autenticazione potrebbe far uso di questa vulnerabilità per leggere file malevoli, possibilmente da host di terze parti, oppure per immettere header HTTP malevoli nelle risposte inviate agli utenti di terze parti.	
Remediation suggerita: Aggiornare a phpMyAdmin 3.1.3.1 o applicare le patch citate nella project's advisory.	

49142 - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)	
Porta: 80	CVSS: 4.3
Sinossi: Il web server remoto contiene una applicazione PHP con vulnerabilità XSS.	
Impatto: Un attaccante remoto può sfruttare la vulnerabilità ingannando un utente ad eseguire codice malevolo.	
Remediation suggerita: Aggiornare a phpMyAdmin 3.3.7 o successive.	

Low

10114 - ICMP Timestamp Request Remote Date Disclosure	
Porta: /	CVSS: 2.1
Sinossi: È possibile determinare l’ora esatta sull’host remoto.	
Impatto: L'host remoto rivela l'orario di sistema tramite ICMP, facilitando attacchi contro autenticazioni basate sul tempo.	
Remediation suggerita: Filtrare le richieste ICMP timestamp (13) e le risposte ICMP timestamp in uscita (14).	

70658 - SSH Server CBC Mode Ciphers Enabled	
Porta: 22	CVSS: 3.7
Sinossi: Il server SSH è configurato per usare il cipher block chaining.	
Impatto: Un attaccante può recuperare il messaggio in chiaro dal messaggio cifrato.	
Remediation suggerita: Contattare il vendor o consultare la documentazione del prodotto per disattivare la modalità CBC e attivare la modalità CTR o GCM per la criptazione.	

153953 - SSH Weak Key Exchange Algorithms Enabled	
Porta: 22	CVSS: 3.0
Sinossi: Il server SSH è configurato per permettere algoritmi di scambio di chiavi deboli.	
Impatto: La criptazione è debole e non sicura.	
Remediation suggerita: Contattare il vendor o consultare la documentazione del prodotto per disabilitare gli algoritmi deboli.	

71049 - SSH Weak MAC Algorithms Enabled	
Porta: 22	CVSS: 2.6
Sinossi: Il server remoto SSH è configurato per permettere algoritmi MD5 e MAC 96-bit.	
Impatto: La criptazione è debole e non sicura.	
Remediation suggerita: Contattare il vendor o consultare la documentazione del prodotto per disabilitare MD5 e MAC 96-bit.	

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	
Porta: 25	CVSS: 3.7
Sinossi: L’host remoto supporta un set di cifrari deboli.	
Impatto: Un attaccante man in the middle può essere in grado di effettuare un downgrade della sessione per usare EXPORT_DHE.	
Remediation suggerita: Riconfigurare il servizio affinché rimuova i cifrari EXPORT_DHE.	

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	
Porta: 25, 5432	CVSS: 3.4
Sinossi: È possibile ottenere informazioni sensibili dal server remoto con i servizi SSL/TLS abilitati.	
Impatto: Gli attaccanti MitM (Man-in-the-Middle) possono decifrare un singolo byte di un testo cifrato con un massimo di 256 tentativi, se riescono a forzare un'applicazione vittima a inviare ripetutamente gli stessi dati tramite nuove connessioni SSL 3.0.	
Remediation suggerita: Disattivare SSLv3.	

42057 - Web Server Allows Password Auto-Completion	
Porta: 80	CVSS: /
Sinossi: L’attributo di auto-completamento non è disattivato nei campi della password.	
Impatto: Sebbene questo non rappresenti un rischio per il server web in sé, significa comunque che gli utenti che utilizzano i moduli interessati potrebbero avere le proprie credenziali salvate nei browser. Questo potrebbe a sua volta comportare una perdita di riservatezza, nel caso in cui utilizzino un computer condiviso o se la loro macchina venga compromessa in futuro.	
Remediation suggerita: Aggiungere l’attributo “autocomplete=off” a questi campi per non far memorizzare le credenziali ai browser.	

26194 - Web Server Transmits Cleartext Credentials	
Porta: 80	CVSS: 2.6
Sinossi: Il server remoto potrebbe trasmettere credenziali in chiaro.	
Impatto: Un attaccante in ascolto può ottenere le credenziali degli utenti.	
Remediation suggerita: Assicurarsi che ogni informazione sensibile venga trasmessa tramite HTTPS.	

10407 - X Server Detection	
Porta: 6000	CVSS: 2.6
Sinossi: Un server X11 è in ascolto sull’host remoto.	
Impatto: Il traffico sul server X11 non è cifrato, quindi un attaccante può intercettare la connessione.	
Remediation suggerita: Limitare l’accesso alla porta interessata.	