
UNIVERSITÀ DEGLI STUDI DI SALERNO
**DIPARTIMENTO DI INFORMATICA**
DIPARTIMENTO DI ECCELLENZA

# Penetration Test Report

Caso di studio:

## GreenOptic: 1

*Team* *Email*

Daniele Gregori d.gregori1@studenti.unisa.it

Anno Accademico 2024/2025

# Indice

**1 Report Overview** **2**
1.1 Executive Summary . . . . . 2
1.2 Engagement Overview . . . . . 3

**2 Engagement Highlights** **3**

**3 Vulnerability Report** **6**
3.1 Descrizione delle Vulnerabilità . . . . . 6

**4 Remediation Report** **8**
4.1 Summary of Recommendations . . . . . 8

**5 Findings Summary** **11**

**6 Detailed Summary** **13**
6.1 High Risk . . . . . 13
6.2 Medium Risk . . . . . 17
6.3 Low Risk . . . . . 28
6.4 Informational . . . . . 30
6.5 Altre Vulnerabilità . . . . . 40

**7 Conclusioni** **44**

**Appendices** **46**

**A Risoluzione vulnerabilità SSL Medium Strength Cipher Suites Supported (SWEET32)** **46**

**B Webmin <= 1.994 Multiple Vulnerabilities: CVE-2021-32156 exploitation** **46**

**C Risoluzione vulnerabilità Local File Inclusion (LFI)** **48**

**D Tools** **50**

# 1 Report Overview

## 1.1 Executive Summary

Daniele Gregori è stato contattato dall'azienda denominata GreenOptic per un penetration test con l'obiettivo di identificare e valutare le vulnerabilità nella loro infrastruttura IT. Questo test è stato richiesto a seguito di un massiccio attacco informatico che ha colpito l'azienda, durante il quale sono stati esfiltrati oltre cinque milioni di record dei clienti, inclusi dati sulle carte di credito e informazioni bancarie.

Questo penetration test è stato redatto per l'esame di Penetration Testing and Ethical Hacking e l'approccio seguito è stato un **full black box penetration test**, simulando un attacco da parte di un attore malintenzionato esterno senza conoscenze preliminari sull'infrastruttura della GreenOptic.

Il report è strutturato per offrire una chiara visione delle scoperte fatte e delle raccomandazioni proposte per mitigare i rischi identificati. La **sezione Engagement Highlights [2]** introduce il contesto e gli obiettivi del test, fornendo una panoramica generale delle attività svolte e dei risultati ottenuti.

Successivamente, la **sezione Detailed Summary [6]** dettaglia le vulnerabilità individuate, categorizzate per livello di gravità, e descrive l'impatto potenziale di ciascuna di esse, insieme alle raccomandazioni per risolverle. Questo approccio permette di comprendere immediatamente quali siano le aree critiche che necessitano di interventi urgenti e quali miglioramenti possono essere implementati per rafforzare la sicurezza dell'infrastruttura.

Nell'**appendice [7]**, è possibile trovare dimostrazioni di exploitation e mitigazioni delle vulnerabilità ad alto rischio trovate tramite Nessus e OpenVAS.

Sono inoltre state illustrate nella **sezione Altre Vulnerabilità [6.5]** le vulnerabilità trovate tramite analisi manuale. Per ulteriori dettagli riguardanti le vulnerabilità individuate manualmente sul sistema e il loro sfruttamento, fare riferimento al documento **'Penetration Test Metodologia'** consegnato unitamente al presente documento.

Basandoci sui risultati della valutazione sono state trovate numerose vulnerabilità che confermano la debole postura di sicurezza dell'infrastruttura, la quale ha portato all'esfiltrazione precedentemente citata. Le vulnerabilità identificate rappresentano un rischio elevato per la sicurezza dell'organizzazione, in quanto potrebbero essere sfruttate per compromettere ulteriormente l'infrastruttura IT e causare gravi danni, inclusa la perdita di dati sensibili e l'interruzione delle operazioni aziendali. Le raccomandazioni fornite nella **sezione Remediation Report [4]** rafforzeranno le difese dell'infrastruttura IT di GreenOptic, riducendo significativamente la probabilità di successo di eventuali attacchi futuri e proteggendo al contempo la confidenzialità, l'integrità e la disponibilità dei dati aziendali.

### 1.2 Engagement Overview

Daniele Gregori ha condotto il penetration test a partire dall'11 Giugno 2024 sulla base del documento Request for Proposal (RFP). Durante l'incarico è stata posta particolare attenzione sui seguenti obiettivi:

- Ricerca di vulnerabilità dell'infrastruttura tramite sistemi manuali ed automatici.
- Verificare il livello di controllo della macchina che un attaccante può ottenere.
- Scoperta di vulnerabilità e complicazioni che potrebbero impattare la confidenzialità, integrità e disponibilità (CIA) dei sistemi informativi della GreenOptic.
- Assistere la GreenOptic nel miglioramento della loro postura di sicurezza.

## 2 Engagement Highlights

Il penetration test descritto in questo documento è stato condotto nell'ambito di un progetto universitario, seguendo le linee guida del **PCI Data Security Standard (PCI DSS)** [1] e senza alcuna limitazione imposta sull'ambito delle attività. Grazie a questa libertà, è stato possibile eseguire un'analisi completa e approfondita del sistema target, con l'obiettivo di identificare potenziali vulnerabilità e migliorare la sicurezza complessiva del sistema.

Data la natura del progetto, non è stato ritenuto necessario stabilire un canale di comunicazione formale tra Daniele Gregori e GreenOptic, né è presente un accordo di non divulgazione (NDA). Inoltre, Daniele Gregori ha avuto piena libertà nella scelta delle metodologia (Figura 2), dei tempi, degli strumenti (consultabili nella **sezione Tools [D]**) e delle tecniche utilizzate durante il test (consultabili nel documento **'Penetration Test Metodologia'**).

Per eseguire il test, è stata impiegata una macchina basata sul sistema operativo **Kali Linux**, una distribuzione specificamente progettata per il penetration testing. La macchina è stata collegata direttamente alla stessa rete locale del sistema target, consentendo di eseguire test in condizioni reali e di valutare l'efficacia delle misure di sicurezza implementate (Figura 1). Le attività di testing sono iniziate a Giugno 2024 e si sono svolte secondo le tempistiche stabilite dal progetto.

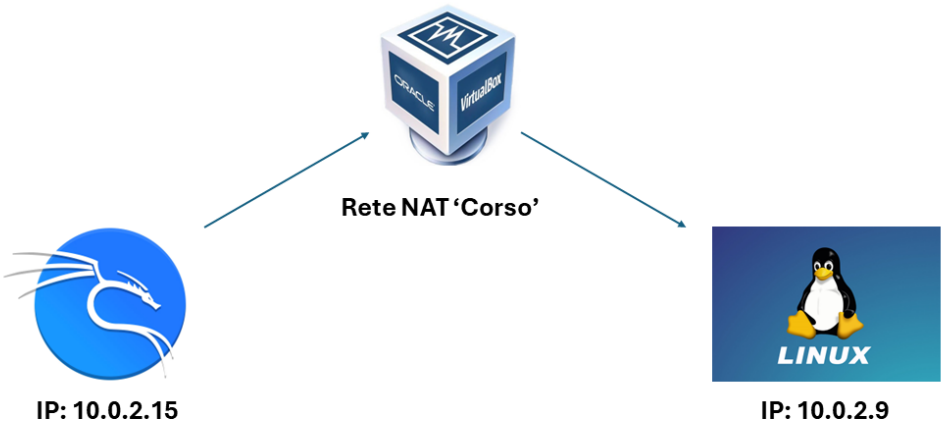


Figura 1: Architettura di rete

Durante il test, è stata installata una backdoor sul sistema target, al fine di garantire un accesso rapido e continuativo. Al termine del penetration test, la backdoor è stata completamente rimossa, ripristinando la piena integrità e sicurezza del sistema.

Il penetration test è stato condotto seguendo rigorosamente il **Framework Generale per il Penetration Testing (FGPT)** che fornisce un approccio strutturato e metodico per l'identificazione e l'analisi delle vulnerabilità. La Figura 2 illustra i vari passaggi del framework, che sono stati applicati in modo sequenziale per garantire un'analisi completa. Tutti i passaggi eseguiti possono essere consultati nel documento **Penetration Test Metodologia**, dove è riportata una descrizione dettagliata delle procedure utilizzate.


Figura 2: Framework Generale per il Penetration Testing

Il penetration test è stato condotto con estrema attenzione, garantendo che tutte le azioni fossero strettamente limitate all'ambito definito. Daniele Gregori conferma di non aver esfiltrato, modificato o cancellato alcun dato che non fosse esplicitamente incluso in questo rapporto.

Daniele Gregori rimane a disposizione di GreenOptic per ulteriori interventi volti a migliorare la sicurezza, proteggere i dipendenti e i clienti, e verificare l'efficacia delle tecniche di mitigazione implementate. Inoltre, Daniele Gregori può supportare GreenOptic nell'implementazione di strategie di sicurezza avanzate, assicurando che siano presenti diversi livelli di difesa. Siamo lieti di proseguire la collaborazione con GreenOptic per garantire la sicurezza delle sue operazioni future.

# 3 Vulnerability Report

Questa sezione funge da panoramica di alto livello della postura di sicurezza di GreenOptic. Un elenco dettagliato di tutte le vulnerabilità scoperte si trova nella **sezione Detailed Summary [6]**.

Di seguito è riportata una descrizione generale delle vulnerabilità individuate manualmente e il loro potenziale impatto.

## 3.1 Descrizione delle Vulnerabilità

- **Porte Aperte e Servizi Esposti**
  - **Descrizione**: La scansione del sistema ha rivelato che diverse porte sono aperte e che vi sono servizi attivi come FTP (porta 21), SSH (porta 22), DNS (porta 53) e Webmin (porta 10000). Ogni servizio esposto rappresenta una potenziale superficie di attacco, specialmente se non sono state implementate le migliori pratiche di sicurezza.
  - **Rischio**: La presenza di queste porte aperte potrebbe consentire a un attaccante di eseguire attacchi di brute force, sfruttare vulnerabilità note o raccogliere informazioni sul sistema per pianificare attacchi più sofisticati.
- **Server DNS Mal Configurato**
  - **Descrizione**: È stato scoperto che il server DNS era configurato in modo errato, permettendo un DNS zone transfer non autorizzato. Questo tipo di errore consente a un attaccante di ottenere una mappa dettagliata della struttura di rete interna, inclusi i nomi di dominio e i sottodomini utilizzati.
  - **Rischio**: Con queste informazioni, un attaccante può identificare nuovi obiettivi all'interno dell'infrastruttura aziendale, pianificando attacchi mirati contro i sistemi scoperti.
- **Vulnerabilità di Local File Inclusion (LFI)**
  - **Descrizione**: È stata individuata una vulnerabilità di tipo LFI nella pagina web dell'azienda. Questa vulnerabilità consente a un attaccante di manipolare i parametri dell'URL per accedere a file locali sul server, come i file di configurazione e persino file contenenti credenziali.
  - **Rischio**: La LFI può essere sfruttata per accedere a file sensibili, esfiltrare informazioni riservate e ottenere ulteriori credenziali che potrebbero permettere l'accesso a sistemi interni più critici.
- **Crack delle Password e Riutilizzo delle Credenziali**
  - **Descrizione**: Utilizzando le vulnerabilità trovate, sono state scoperte e decifrate diverse password. Queste credenziali sono state utilizzate per accedere a vari servizi come FTP, SSH e Webmin. Il problema del riutilizzo delle password è emerso

quando le stesse credenziali hanno permesso l'accesso a più servizi, amplificando l'esposizione al rischio.

  - **Rischio**: Se un attaccante riesce a compromettere una sola credenziale, potrebbe utilizzarla per ottenere accesso a una vasta gamma di servizi, ampliando l'entità dell'attacco.

- **Privilege Escalation**
  - **Descrizione**: Sono stati scoperti exploit che consentono di elevare i privilegi di un utente normale fino a ottenere l'accesso come root (amministratore). Questi exploit sfruttano vulnerabilità conosciute nel sistema operativo o nei servizi in esecuzione.
  - **Rischio**: L'accesso come root dà all'attaccante un controllo totale sulla macchina, permettendogli di modificare, cancellare o rubare dati, installare backdoor, e compromettere ulteriormente altri sistemi collegati.

Di seguito, invece, è riportata una descrizione generale delle vulnerabilità riscontrate tramite strumenti automatici come: **Nessus** ed **OpenVAS**.

- **High Risk (Rischio Elevato)**: Queste vulnerabilità sono quelle con il rischio più alto, che possono essere sfruttate per causare danni gravi all'infrastruttura IT, come il furto di dati o il controllo remoto del sistema. Tra queste rientrano le vulnerabilità che consentono l'esecuzione di codice da remoto, l'escalation di privilegi, o attacchi di tipo cross-site scripting (XSS). Tali vulnerabilità richiedono una correzione immediata per evitare potenziali compromissioni.
- **Medium Risk (Rischio Medio)**: Le vulnerabilità di rischio medio rappresentano ancora una minaccia significativa, ma generalmente richiedono un attore più sofisticato o condizioni specifiche per essere sfruttate. Possono includere l'uso di certificati SSL non affidabili, cifrari deboli o malconfigurazioni che espongono il sistema a potenziali attacchi man-in-the-middle o di intercettazione delle comunicazioni.
- **Low Risk (Rischio Basso)**: Le vulnerabilità a basso rischio non rappresentano una minaccia immediata e spesso richiedono circostanze particolari o livelli di accesso elevati per essere sfruttate. Sono, tuttavia, importanti da correggere per migliorare la sicurezza complessiva del sistema ed evitare che piccole debolezze possano essere combinate per attacchi più sofisticati. Esempi includono la configurazione di cifrari più deboli nel protocollo SSH.
- **Informational**: Queste non sono vulnerabilità in senso stretto, ma piuttosto informazioni che potrebbero essere utilizzate da un attaccante per conoscere meglio il sistema target e pianificare attacchi futuri. Includono dettagli su versioni di software, configurazioni di rete e altre informazioni tecniche che possono esporre l'infrastruttura a rischi se non opportunamente gestite.

# 4 Remediation Report

## 4.1 Summary of Recommendations

Per migliorare la sicurezza dell'infrastruttura IT di GreenOptic e mitigare le vulnerabilità rilevate, si raccomanda di adottare il seguente insieme di misure di sicurezza. Ogni categoria mira a ridurre specifici rischi di sicurezza identificati durante il penetration test, fornendo raccomandazioni pratiche per migliorare la postura di sicurezza complessiva.

Si consiglia vivamente di affrontare e risolvere tempestivamente le vulnerabilità descritte nella **sezione Detailed Summary [6]**, procedendo in ordine di priorità a partire da quelle classificate come ad alto rischio, per poi passare a quelle a rischio medio e basso. Questa strategia permette di mitigare in modo efficace i potenziali danni, riducendo al minimo le minacce più critiche e garantendo una maggiore sicurezza complessiva del sistema.

- **Aggiornamento delle applicazioni e dei sistemi**
  - **Raccomandazione**: Aggiornare tutte le applicazioni e i sistemi vulnerabili alle ultime versioni disponibili. Le vulnerabilità di esecuzione di codice remoto (RCE), escalation dei privilegi e XSS possono essere mitigate implementando patch di sicurezza e aggiornamenti. Ad esempio, aggiornare Webmin alle versioni più recenti per eliminare le vulnerabilità di XSS e RCE.
  - **Azioni specifiche**: Si consiglia di automatizzare il processo di aggiornamento, configurando i sistemi per ricevere patch di sicurezza automaticamente, o eseguire aggiornamenti periodici.
  - **Benefici**: L'applicazione delle patch riduce significativamente i rischi legati allo sfruttamento di vulnerabilità note, assicurando che i sistemi siano protetti contro attacchi noti.
- **Rafforzare la configurazione del server**
  - **Raccomandazione**: Migliorare le configurazioni dei server per prevenire attacchi come quelli derivati da configurazioni errate di DNS, SSH, e servizi web. Disabilitare metodi HTTP pericolosi come TRACE e TRACK, e configurare correttamente le zone transfer DNS per limitare l'esposizione della rete interna.
  - **Azioni specifiche**: Implementare restrizioni di accesso ai servizi di rete, utilizzando regole di accesso basate sugli indirizzi IP e limitando i permessi agli utenti e ai sistemi di cui si ha bisogno.
  - **Benefici**: Configurazioni sicure dei server riducono l'esposizione a potenziali attacchi e prevengono la divulgazione di informazioni sensibili sulla rete.
- **Implementazione di crittografia robusta**
  - **Raccomandazione**: Sostituire gli algoritmi di crittografia deboli, come CBC o RC4, con cifrari più sicuri come AES-GCM o TLS 1.2 e superiori. Assicurarsi che tutte le comunicazioni critiche, inclusi i login e il trasferimento di dati, utilizzino HTTPS anziché HTTP.

  - **Azioni specifiche**: Verificare i certificati SSL per assicurarsi che siano firmati da un'autorità di certificazione riconosciuta e non autofirmati e migrare qualsiasi servizio web che utilizza HTTP a HTTPS, garantendo che le informazioni critiche siano sempre trasmesse in modo sicuro.
  - **Benefici**: L'utilizzo di crittografia avanzata protegge i dati in transito, riducendo il rischio di intercettazione e man-in-the-middle.

- **Gestione sicura delle credenziali**
  - **Raccomandazione**: Migliorare la gestione delle credenziali adottando politiche di password sicure e implementando l'autenticazione a più fattori (MFA). Evitare il riutilizzo delle credenziali su più servizi e assicurarsi che i file di configurazione non contengano credenziali in chiaro.
  - **Azioni specifiche**: Forzare la rotazione periodica delle password e vietare l'uso di password precedenti.
  - **Benefici**: Queste misure riducono il rischio di accesso non autorizzato e limitano l'impatto di eventuali compromissioni di credenziali.

- **Controllo degli accessi e gestione dei privilegi**
  - **Raccomandazione**: Implementare il principio del minimo privilegio, assicurandosi che gli utenti abbiano solo i diritti strettamente necessari. Monitorare l'utilizzo dei privilegi e correggere le vulnerabilità che permettono l'escalation dei privilegi.
  - **Azioni specifiche**: Configurare strumenti di monitoraggio che generino avvisi in caso di uso non autorizzato o sospetto di privilegi elevati.
  - **Benefici**: Ridurre i privilegi di esecuzione e monitorare costantemente le attività di sistema contribuisce a prevenire compromissioni complete dei sistemi.

- **Protezione contro gli attacchi XSS e CSRF**
  - **Raccomandazione**: Implementare header di sicurezza, come X-Frame-Options e Content-Security-Policy, e sanitizzare correttamente gli input utente per prevenire attacchi di tipo cross-site scripting (XSS) e cross-site request forgery (CSRF).
  - **Azioni specifiche**: Verificare tutte le pagine web e assicurarsi che gli input utente siano sempre validati e sanitizzati, riducendo così la possibilità di inserire script malevoli.
  - **Benefici**: Queste protezioni riducono il rischio che codice maligno venga eseguito nei browser degli utenti, proteggendo le sessioni e i dati sensibili.

- **Implementazione di un Processo di Gestione delle Vulnerabilità**
  - **Raccomandazione**: È fondamentale stabilire un processo continuo di gestione delle vulnerabilità che includa la scansione regolare dei sistemi per identifica-

re eventuali debolezze e la loro pronta correzione. Questo processo deve essere integrato nel ciclo di vita della gestione dei sistemi IT.

  - **Azioni specifiche**: Stabilire delle scansioni settimanali e mensili per la ricerca delle vulnerabilità, utilizzando strumenti automatizzati come Nessus o OpenVAS, e assicurarsi che i risultati siano esaminati e trattati con priorità alta.

- **Formazione e Sensibilizzazione del Personale**
  - **Raccomandazione**: Il personale è spesso il primo punto di contatto con le minacce alla sicurezza. È necessario che i dipendenti ricevano una formazione continua sulle migliori pratiche di sicurezza e sui rischi emergenti.
  - **Azioni specifiche**: Implementare un programma di formazione obbligatoria e periodica per tutto il personale, con un focus particolare sulla gestione delle password, il riconoscimento delle email di phishing e l'uso sicuro dei dispositivi aziendali.
- **Monitoraggio e Risposta agli Incidenti**
  - **Raccomandazione**: È essenziale disporre di un sistema di monitoraggio attivo e continuo delle attività di rete e dei sistemi per rilevare comportamenti anomali o sospetti. Devono essere stabilite chiare procedure di risposta agli incidenti.
  - **Azioni specifiche**: Implementare un Security Information and Event Management (SIEM) per il monitoraggio in tempo reale e definire procedure di risposta agli incidenti, con un team dedicato pronto a intervenire in caso di compromissione.

# 5 Findings Summary

In questa sezione viene fornita una panoramica visiva dei risultati emersi dal processo di penetration testing, attraverso una serie di grafici che sintetizzano in modo chiaro e immediato le vulnerabilità identificate.

L'analisi condotta mediante **strumenti automatici** ha rilevato un totale di **24 vulnerabilità**, distribuite come segue:

- **6 vulnerabilità ad alto rischio**
- **14 vulnerabilità a rischio medio**
- **4 vulnerabilità a basso rischio**
- **30 vulnerabilità di tipo informazionale**

Parallelamente, **l'analisi manuale** ha portato all'identificazione di ulteriori **10 vulnerabilità**. Queste si suddividono in:

- **5 vulnerabilità ad alto rischio**
- **5 vulnerabilità a rischio medio**

La combinazione tra analisi automatizzata e manuale ha garantito una copertura completa, individuando sia le vulnerabilità facilmente rilevabili dagli strumenti, sia quelle che richiedono una valutazione più approfondita e contestuale.

La tabella 1 mostra il numero totale di vulnerabilità individuate durante il penetration test categorizzate in base al livello di rischio. I livelli di rischio sono stati calcolati usando il 'Common Vulnerability Scoring System (CVSS)' versione 2 [2] e 3.1 [3].

Tabella 1: Distribuzione delle vulnerabilità per gravità

| Gravità | Info (0) | Low (0.1-3.9) | Medium (4.0-6.9) | High (7.0-10) |
|---|---|---|---|---|
| Numero Vulnerabilità | 30 | 4 | 19 | 11 |

Nel grafico 3 viene presentata una rappresentazione visiva delle vulnerabilità riscontrate, suddivise nelle principali macro-categorie. Questa suddivisione consente di comprendere rapidamente le aree maggiormente esposte e di individuare i settori che richiedono interventi prioritari.

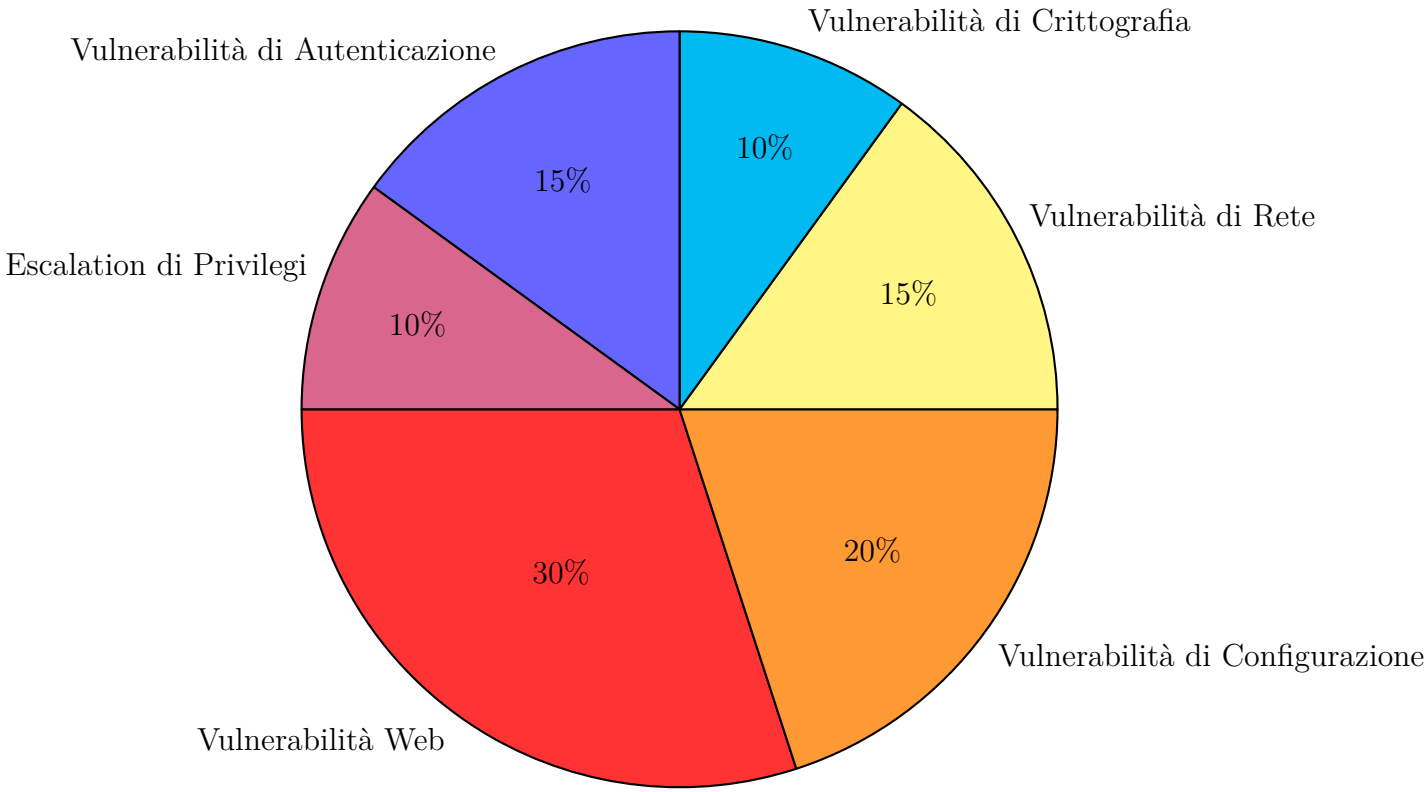


Figura 3: Sintesi delle vulnerabilità riscontrate per categoria

# 6 Detailed Summary

In questa sezione viene fornita una descrizione tecnica dettagliata delle vulnerabilità individuate durante l'analisi ordinate in base al livello di rischio. Ogni vulnerabilità è stata esaminata in modo approfondito, utilizzando un formato strutturato che permetta una comprensione completa e una gestione efficace delle problematiche emerse.

## 6.1 High Risk

| Webmin < 1.997 XSS Vulnerability | CVE<br>2022-36446 |
|---|---|
| HIGH | |
| **Descrizione:**<br>Webmin è vulnerabile a un attacco cross-site scripting (XSS), che consente a un attaccante di iniettare codice malevolo all'interno dell'interfaccia utente non protetta. Questo potrebbe risultare nell'esecuzione di codice arbitrario nei browser degli utenti. La vulnerabilità è presente nella versione 1.953 di Webmin. | |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe sfruttare questa vulnerabilità per compromettere le sessioni utente, rubare informazioni sensibili o manipolare i dati visualizzati. | |
| **Soluzione consigliata:**<br>Aggiornare Webmin alla versione 1.997 o successiva per eliminare questa vulnerabilità. | |
| **CVSS v3.1 Base Score:**<br>9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) | |
| **Metodo di rilevazione:**<br>OpenVAS | |
| **Riferimenti:**<br>`https://www.webmin.com/security.html`<br>`https://github.com/webmin/webmin/commit/13f7bf9621a82d93f1e9dbd838d1e2202021bde` | |

| | |
|---|---|
| Webmin <= 1.994 Multiple Vulnerabilities | CVE<br>2021-32156<br>2021-32157<br>2021-32158<br>2021-32159<br>2021-32160<br>2021-32161<br>2021-32162 |
| HIGH | |
| **Descrizione:**<br>Webmin è vulnerabile a molteplici attacchi, inclusi Cross-Site Request Forgery (CSRF) e Cross-Site Scripting (XSS).<br>Le vulnerabilità sono state riscontrate in diverse funzionalità, come Scheduled Cron Jobs, File Manager e Upload/Download. | |
| **Potenziale impatto aziendale:**<br>Gli attacchi XSS e CSRF potrebbero compromettere le sessioni utente, permettendo la manipolazione dei dati o<br>l'esecuzione di comandi non autorizzati. Consultare la **sezione Appendice [B]** per visionare un potenziale sfruttamento della vulnerabilità | |
| **Soluzione consigliata:**<br>Non è disponibile una soluzione ufficiale, ma si consiglia di disabilitare le funzionalità vulnerabili<br>o aggiornare a una versione più recente. | |
| **CVSS v3.1 Base Score:**<br>9.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N) | |
| **Metodo di rilevazione:**<br>OpenVAS | |
| **Riferimenti:**<br>`https://github.com/Mesh31911/CVE-2021-32156`<br>`https://github.com/Mesh31911/CVE-2021-32157`<br>`https://github.com/Mesh31911/CVE-2021-32158`<br>`https://github.com/Mesh31911/CVE-2021-32159`<br>`https://github.com/Mesh31911/CVE-2021-32160`<br>`https://github.com/Mesh31911/CVE-2021-32161`<br>`https://github.com/Mesh31911/CVE-2021-32162` | |

| Webmin <= 1.983 RCE Vulnerability | CVE<br>2020-35606 |
|---|---|
| HIGH | |
| **Descrizione:**<br>Webmin è vulnerabile a esecuzione di codice remoto (RCE). Un utente autenticato<br>per il modulo di aggiornamento pacchetti può eseguire comandi arbitrari con privilegi di root. | |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe ottenere l'accesso completo al sistema compromesso, eseguendo comandi con privilegi elevati. | |
| **Soluzione consigliata:**<br>Non è disponibile una soluzione ufficiale. Si consiglia di aggiornare<br>a una versione più recente o disabilitare le funzionalità vulnerabili. | |
| **CVSS v3.1 Base Score:**<br>8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | |
| **Metodo di rilevazione:**<br>OpenVAS | |
| **Riferimenti:**<br>`https://www.pentest.com.tr/exploits/Webmin-1962-PU-Escape-Bypass-Remote-Command-Execution.html` | |

| Webmin <= 1.991 Privilege Escalation | CVE<br>2022-30708 |
|---|---|
| HIGH | |
| **Descrizione:**<br>Un problema di escalation di privilegi in Webmin consente l'esecuzione di codice<br>remoto quando viene creato un utente manualmente, non tramite Virtualmin o Cloudmin. | |
| **Potenziale impatto aziendale:**<br>Un utente con privilegi limitati potrebbe elevare i propri privilegi, ottenendo il controllo completo del sistema. | |
| **Soluzione consigliata:**<br>Aggiornare Webmin alla versione 1.994 o successiva per mitigare la vulnerabilità. | |
| **CVSS v3.1 Base Score:**<br>8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | |
| **Metodo di rilevazione:**<br>OpenVAS | |
| **Riferimenti:**<br>`https://github.com/esp0xdeadbeef/rce_webmin`<br>`https://www.webmin.com/security.html` | |

| Webmin <= 1.984 Multiple Vulnerabilities | CVE<br>2022-0824<br>2022-0829 |
|---|---|
| HIGH | |
| **Descrizione:**<br>Webmin presenta vulnerabilità multiple che permettono l'esecuzione di codice remoto (RCE) e l'accesso non autorizzato.<br>L'accesso non autorizzato può avvenire attraverso un controllo di accesso improprio. | |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe ottenere l'accesso non autorizzato al sistema o eseguire comandi arbitrari, compromettendo la sicurezza del sistema. | |
| **Soluzione consigliata:**<br>Aggiornare Webmin alla versione 1.990 o successiva per eliminare le vulnerabilità. | |
| **CVSS v3.1 Base Score:**<br>8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | |
| **Metodo di rilevazione:**<br>OpenVAS | |
| **Riferimenti:**<br>`https://www.webmin.com/security.html`<br>`https://huntr.dev/bounties/d0049a96-de90-4b1a-9111-94de1044f295/`<br>`https://huntr.dev/bounties/f2d0389f-d7d1-4f34-9f9d-268b0a0da05e/` | |

| SSL Medium Strength Cipher Suites Supported (SWEET32) | CVE<br>2016-2183 |
|---|---|
| HIGH | |
| **Descrizione:**<br>L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia di media forza. Nessus considera<br>media forza qualsiasi crittografia che utilizzi chiavi di lunghezza pari ad almeno 64 bit e inferiore a 112 bit, oppure che<br>utilizza la suite di crittografia 3DES.<br>Si noti che è molto più facile aggirare la crittografia a media resistenza se l'aggressore si trova sulla stessa rete fisica. | |
| **Potenziale impatto aziendale:**<br>L'uso di cifrari di media sicurezza può permettere a un attaccante che si trova sulla stessa rete di intercettare le<br>comunicazioni crittografate, mettendo a rischio dati sensibili. Questo potrebbe comportare il furto di informazioni<br>riservate, compromettendo la reputazione dell'azienda e potenzialmente violando regolamentazioni sulla protezione dei dati. | |
| **Soluzione consigliata:**<br>Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari a media forza. Consultare mitigazione nella **sezione Appendice** [**A**]. | |
| **CVSS v3.1 Base Score:**<br>7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) | |
| **Metodo di rilevazione:**<br>Nessus | |
| **Riferimenti:**<br>`https://www.openssl.org/blog/blog/2016/08/24/sweet32/`<br>`https://sweet32.info` | |

## 6.2 Medium Risk

| SSL Certificate Cannot Be Trusted |
| --- |
| MEDIUM |
| **Descrizione:**<br>Il certificato SSL del server non può essere considerato affidabile. Questo può derivare dall'uso di un certificato autofirmato o da una catena di certificati incompleta o non valida. |
| **Potenziale impatto aziendale:**<br>Un certificato SSL non fidato riduce la capacità degli utenti di verificare l'identità del server, aumentando il rischio di attacchi man-in-the-middle. Ciò può minare la fiducia dei clienti e causare danni alla reputazione dell'azienda, oltre a potenziali perdite finanziarie. |
| **Soluzione consigliata:**<br>Acquistare o generare un certificato SSL corretto per questo servizio, firmato da un'autorità di certificazione riconosciuta. |
| **CVSS v3.1 Base Score:**<br>6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N) |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:**<br>`https://www.itu.int/rec/T-REC-X.509/en`<br>`https://en.wikipedia.org/wiki/X.509` |

| SSL Self-Signed Certificate |
| --- |
| MEDIUM |
| **Descrizione:**<br>La catena di certificati SSL del servizio termina in un certificato autofirmato non riconosciuto come affidabile. Questo annulla l'utilità dell'SSL, poiché un attaccante potrebbe facilmente effettuare un attacco man-in-the-middle. |
| **Potenziale impatto aziendale:**<br>Un certificato SSL autofirmato può permettere attacchi man-in-the-middle, soprattutto su host pubblici. Questo riduce la fiducia degli utenti nel sito web e può danneggiare la reputazione aziendale, portando a una perdita di clienti e problemi di conformità legale. |
| **Soluzione consigliata:**<br>Acquistare o generare un certificato SSL corretto per questo servizio, firmato da un'autorità di certificazione riconosciuta. |
| **CVSS v3.1 Base Score:**<br>6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N) |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:** `https://www.itu.int/rec/T-REC-X.509/en` |

| Webmin <= 1.995 XSS Vulnerability | CVE<br>2022-36880 |
|---|---|
| MEDIUM | |
| **Descrizione:**<br>Webmin è vulnerabile a un attacco cross-site scripting (XSS) nella versione 1.995 e precedenti. Un attaccante potrebbe inviare una email HTML contenente codice malevolo per catturare i cookie del browser della vittima. | |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe rubare credenziali di sessione e accedere ai dati riservati della vittima o manipolare le sessioni attive. | |
| **Soluzione consigliata:**<br>Poiché non è disponibile una soluzione ufficiale, si consiglia di aggiornare a una versione più recente o disabilitare le funzionalità vulnerabili. | |
| **CVSS v3.1 Base Score:**<br>6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N) | |
| **Metodo di rilevazione:**<br>OpenVAS | |
| **Riferimenti:**<br>`https://www.webmin.com/security.html` | |

| Webmin < 2.003 XSS Vulnerability | CVE<br>2022-3844 |
|---|---|
| MEDIUM | |
| **Descrizione:**<br>Webmin è vulnerabile a un attacco cross-site scripting (XSS) nella funzione<br>"xterm/index.cgi". Questa vulnerabilità permette a un attaccante di iniettare<br>codice JavaScript malevolo nell'interfaccia utente, eseguendolo nel contesto del browser della vittima. | |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe sfruttare questa vulnerabilità per rubare credenziali<br>o manipolare le informazioni visualizzate, compromettendo la sicurezza dell'utente. | |
| **Soluzione consigliata:**<br>Aggiornare Webmin alla versione 2.003 o successiva per eliminare questa vulnerabilità. | |
| **CVSS v3.1 Base Score:**<br>6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N) | |
| **Metodo di rilevazione:**<br>OpenVAS | |
| **Riferimenti:**<br>`https://github.com/webmin/webmin/compare/2.001...2.003` | |

| JQuery 1.2 < 3.5.0 Multiple XSS | CVE<br>2020-11022, CVE<br>2020-11023 |
|---|---|
| MEDIUM | |
| **Descrizione:**<br>La versione di JQuery installata sul server web remoto è vulnerabile a diverse vulnerabilità di cross-site scripting. | |
| **Potenziale impatto aziendale:**<br>L'utilizzo di versioni obsolete di JQuery può rendere il sito vulnerabile a exploit di sicurezza noti. Ciò potrebbe essere sfruttato per attacchi XSS, compromettendo la sicurezza del sito e causando perdite di dati o manipolazioni fraudolente. | |
| **Soluzione consigliata:**<br>Aggiornare JQuery alla versione 3.5.0 o successiva. | |
| **CVSS v3.1 Base Score:**<br>6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N) | |
| **Metodo di rilevazione:** Nessus | |
| **Riferimenti:**<br>`https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/`<br>`https://security.paloaltonetworks.com/PAN-SA-2020-0007` | |

| SSH Terrapin Prefix Truncation Weakness | CVE<br>2023-48795 |
|---|---|
| MEDIUM | |
| **Descrizione:**<br>Il server SSH remoto è vulnerabile a un attacco man-in-the-middle noto come Terrapin, che può consentire a un attaccante di bypassare i controlli di integrità e degradare la sicurezza della connessione. | |
| **Potenziale impatto aziendale:**<br>Può esporre l'azienda a potenziali attacchi MITM, compromettendo l'integrità delle connessioni SSH. Ciò può portare a intercettazioni e manipolazioni dei dati sensibili, con conseguenti rischi per la sicurezza e l'integrità operativa. | |
| **Soluzione consigliata:**<br>Contattare il fornitore per un aggiornamento che implementi contromisure rigorose per lo scambio di chiavi o disabilitare gli algoritmi interessati. | |
| **CVSS v3.1 Base Score:**<br>5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N) | |
| **Metodo di rilevazione:** Nessus | |
| **Riferimenti:**<br>`https://terrapin-attack.com/` | |

| SSL RC4 Cipher Suites Supported (Bar Mitzvah) | CVE<br>2013-2566, CVE<br>2015-2808 |
|---|---|
| MEDIUM | |
| **Descrizione:**<br>Il servizio remoto supporta l'uso del cifrario RC4, che è considerato insicuro a causa delle debolezze nella generazione del flusso di byte pseudo-casuale, riducendo la casualità. | |
| **Potenziale impatto aziendale:**<br>L'algoritmo RC4 è noto per le sue vulnerabilità. L'uso di RC4 nelle suite di crittografia SSL/TLS può portare a una decrittazione facilitata delle comunicazioni crittografate, mettendo a rischio informazioni riservate come credenziali, dati finanziari e altri dati sensibili. La compromissione dei dati potrebbe avere conseguenze legali e finanziarie per l'azienda. | |
| **Soluzione consigliata:**<br>Riconfigurare l'applicazione interessata per evitare l'uso di cifrari RC4, preferendo TLS 1.2 con suite di cifratura AES-GCM. | |
| **CVSS v3.1 Base Score:**<br>5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N) | |
| **Metodo di rilevazione:** Nessus | |
| **Riferimenti:**<br>`https://www.rc4nomore.com/`<br>`http://www.nessus.org/u?ac7327a0` | |

| Browsable Web Directories |
| --- |
| MEDIUM |
| **Descrizione:**<br>Alcune directory sul server web remoto sono navigabili. |
| **Potenziale impatto aziendale:**<br>Se le directory web sono accessibili pubblicamente, un attaccante potrebbe ottenere informazioni critiche sui file presenti nel server, come configurazioni o dati riservati. Ciò potrebbe esporre l'azienda a perdite di dati o a compromissioni del sistema. |
| **Soluzione consigliata:**<br>Assicurarsi che le directory navigabili non contengano informazioni riservate o risorse sensibili. Implementare restrizioni di accesso o disabilitare l'indicizzazione delle directory. |
| **CVSS v3.1 Base Score:**<br>5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:** `http://www.nessus.org/u?0a35179e` |

| HTTP TRACE / TRACK Methods Allowed | CVE<br>2003-1567 |
|---|---|
| MEDIUM | |
| **Descrizione:**<br>Il server web remoto supporta i metodi HTTP TRACE e/o TRACK, utilizzati per il debug delle connessioni web. | |
| **Potenziale impatto aziendale:**<br>L'abilitazione dei metodi TRACE e TRACK può facilitare attacchi di tipo cross-site scripting o man-in-the-middle. Ciò può portare a perdite di dati, danni alla reputazione e, se sfruttato in un attacco di vasta portata, può influire sulla fiducia degli utenti nei confronti del sistema. | |
| **Soluzione consigliata:**<br>Disabilitare i metodi HTTP TRACE e TRACK sul server web. | |
| **CVSS v3.1 Base Score:**<br>5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) | |
| **Metodo di rilevazione:** Nessus | |
| **Riferimenti:**<br>`http://www.nessus.org/u?e979b5cb`<br>`http://www.apacheweek.com/issues/03-01-24` | |

| DNS Server Zone Transfer Information Disclosure (AXFR) | CVE<br>1999-0532 |
|---|---|
| MEDIUM | |
| **Descrizione:**<br>Il name server remoto consente di eseguire zone transfer DNS. Uno zone transfer consente a un aggressore remoto di compilare istantaneamente un elenco di potenziali obiettivi. Inoltre, le aziende utilizzano spesso una convenzione di denominazione che può fornire indicazioni sull'applicazione principale di un server (ad esempio, proxy.example.com, payroll.example.com, b2b.example.com e così via). Per questo motivo, queste informazioni sono di grande utilità per un aggressore, che può utilizzarle per ottenere informazioni sulla topologia della rete e individuare nuovi obiettivi. | |
| **Potenziale impatto aziendale:**<br>Un trasferimento di zona DNS non limitato può rivelare informazioni sull'infrastruttura di rete dell'azienda, fornendo potenziali punti d'attacco agli hacker. Questo espone l'organizzazione a una gamma più ampia di attacchi mirati. | |
| **Soluzione consigliata:**<br>Limitare i trasferimenti di zona DNS solo ai server che ne hanno bisogno. | |
| **CVSS v2.0 Base Score:**<br>5.0 (CVSS2AV:N/AC:L/Au:N/C:P/I:N/A:N) | |
| **Metodo di rilevazione:** Nessus | |
| **Riferimenti:** `https://en.wikipedia.org/wiki/AXFR` | |

| Weak Key Exchange Algorithm(s) Supported (SSH) |
|---|
| MEDIUM |
| **Descrizione:**<br>Il server SSH supporta algoritmi di scambio chiavi deboli come diffie-hellman-group1-sha1<br>e diffie-hellman-group-exchange-sha1, che utilizzano chiavi a 1024-bit e SHA-1, vulnerabili a vari attacchi. |
| **Potenziale impatto aziendale:**<br>La compromissione delle chiavi durante lo scambio potrebbe portare alla decodifica<br>delle comunicazioni SSH e all'intercettazione dei dati sensibili. |
| **Soluzione consigliata:**<br>Disabilitare gli algoritmi di scambio chiavi deboli e abilitare algoritmi più sicuri,<br>come elliptic-curve Diffie-Hellman o Curve25519. |
| **CVSS v2 Base Score:**<br>5.0 (CVSS2AV:N/AC:L/Au:N/C:P/I:N/A:N) |
| **Metodo di rilevazione:**<br>OpenVAS |
| **Riferimenti:**<br>`https://weakdh.org/sysadmin.html` |

| FTP Unencrypted Cleartext Login |
|---|
| MEDIUM |
| **Descrizione:**<br>Il servizio FTP accetta login senza crittografia (in chiaro).<br>Questo permette a un attaccante di intercettare facilmente le credenziali durante una sessione FTP non protetta. |
| **Potenziale impatto aziendale:**<br>La compromissione delle credenziali di accesso potrebbe esporre i dati aziendali a furti e manomissioni. |
| **Soluzione consigliata:**<br>Abilitare l'uso di FTPS o forzare la connessione a passare attraverso l'autenticazione TLS. |
| **CVSS v2 Base Score:**<br>4.8 (CVSS2AV:A/AC:L/Au:N/C:P/I:P/A:N) |
| **Metodo di rilevazione:**<br>OpenVAS |

| Web Application Potentially Vulnerable to Clickjacking |
| --- |
| MEDIUM |
| **Descrizione:**<br>Il server web remoto non imposta l'intestazione X-Frame-Options o l'intestazione Content-Security-Policy 'frame-ancestors' in tutte le risposte. Questo potrebbe esporre il sito a un attacco di clickjacking o ad un attacco UI redress, in cui un aggressore può indurre un utente a cliccare su un'area della pagina vulnerabile diversa da quella che l'utente percepisce.<br>Questo può portare l'utente a eseguire transazioni fraudolente o dannose. |
| **Potenziale impatto aziendale:**<br>La vulnerabilità al clickjacking può permettere a un attaccante di indurre l'utente a compiere azioni non desiderate, come l'approvazione di transazioni o l'esecuzione di comandi non intenzionali. Questo può danneggiare la fiducia degli utenti e provocare conseguenze legali, soprattutto se l'attacco porta a violazioni della sicurezza o a transazioni fraudolente. |
| **Soluzione consigliata:**<br>Configurare il server web per restituire un'intestazione X-Frame-Options o Content-Security-Policy non permissiva per tutte le risorse richieste. |
| **CVSS v2 Base Score:**<br>4.3 (CVSS2AV:N/AC:M/Au:N/C:N/I:P/A:N) |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:**<br>`https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet`<br>`https://en.wikipedia.org/wiki/Clickjacking` |

| Weak Encryption Algorithm(s) Supported (SSH) |
|---|
| MEDIUM |
| **Descrizione:**<br>Il server SSH supporta algoritmi di crittografia deboli come 3des-cbc, aes128-cbc,<br>aes192-cbc e aes256-cbc, che utilizzano modalità CBC, vulnerabili a vari tipi di attacchi. |
| **Potenziale impatto aziendale:**<br>L'uso di algoritmi deboli potrebbe compromettere la riservatezza delle comunicazioni crittografate, esponendo dati sensibili a potenziali attacchi. |
| **Soluzione consigliata:**<br>Disabilitare gli algoritmi di crittografia deboli e abilitare algoritmi più robusti come AES-GCM. |
| **CVSS v2 Base Score:**<br>4.3 (CVSS2AV:N/AC:M/Au:N/C:P/I:N/A:N) |
| **Metodo di rilevazione:**<br>OpenVAS |
| **Riferimenti:**<br>`https://www.rfc-editor.org/rfc/rfc4253` |

## 6.3 Low Risk

| SSH Server CBC Mode Ciphers Enabled | CVE<br>2008-5161 |
|---|---|
| LOW | |
| **Descrizione:**<br>Il server SSH remoto è configurato per supportare la crittografia con Cipher Block Chaining (CBC),<br>che può consentire a un attaccante di recuperare il testo in chiaro dal messaggio cifrato. | |
| **Potenziale impatto aziendale:**<br>L'abilitazione di cifrari CBC nell'SSH espone il sistema a vulnerabilità che possono portare alla<br>decifrazione del traffico crittografato. Un attaccante potrebbe intercettare comunicazioni e accedere<br>a dati sensibili, compromettendo la sicurezza aziendale e portando a possibili perdite di dati o accessi non autorizzati. | |
| **Soluzione consigliata:**<br>Contattare il fornitore o consultare la documentazione del prodotto per disabilitare la crittografia CBC<br>e abilitare la crittografia CTR o GCM. | |
| **CVSS v3.1 Base Score:**<br>3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N) | |
| **Metodo di rilevazione:** Nessus | |
| **Riferimenti:** `http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161` | |

| SSH Weak Key Exchange Algorithms Enabled |
|---|
| LOW |
| **Descrizione:**<br>Il server SSH remoto è configurato per consentire l'uso di algoritmi di scambio chiavi considerati deboli, come diffie-hellman-group1-sha1. |
| **Potenziale impatto aziendale:**<br>L'utilizzo di algoritmi di scambio chiavi deboli può esporre le comunicazioni SSH a un attaccante, che potrebbe decifrare il traffico e ottenere accesso non autorizzato al sistema. Questo rischio aumenta la probabilità di accessi non autorizzati, compromissione dei dati sensibili e potenziali violazioni di conformità alle normative sulla sicurezza. |
| **Soluzione consigliata:**<br>Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi deboli di scambio chiavi. |
| **CVSS v3.1 Base Score:**<br>3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N) |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:** `https://datatracker.ietf.org/doc/html/rfc9142` |

| ICMP Timestamp Request Remote Date Disclosure | CVE<br>1999-0524 |
|---|---|
| LOW | |
| **Descrizione:**<br>Il sistema remoto risponde a una richiesta di timestamp ICMP. Questo consente a un attaccante di conoscere l'ora impostata sulla macchina bersaglio, il che può aiutare un attaccante remoto e non autenticato a eludere i protocolli di autenticazione time-based. | |
| **Potenziale impatto aziendale:**<br>Sebbene a basso rischio, la divulgazione dell'orario del server può aiutare un attaccante a sincronizzare attacchi di tipo replay o a sfruttare debolezze nei protocolli di autenticazione basati sull'ora. Questo potrebbe influenzare la sicurezza complessiva dell'infrastruttura IT. | |
| **Soluzione consigliata:**<br>Filtrare le richieste ICMP timestamp (13) e le risposte ICMP timestamp (14). | |
| **CVSS v2 Base Score:**<br>2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N) | |
| **Metodo di rilevazione: Nessus** | |
| **Riferimenti:**<br>`http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524`<br>`http://cwe.mitre.org/data/definitions/200` | |

| Weak MAC Algorithm(s) Supported (SSH) |
|---|
| LOW |
| **Descrizione:**<br>Il server SSH supporta algoritmi di Message Authentication Code (MAC) deboli, come umac-64-etm@openssh.com e umac-64@openssh.com, che utilizzano chiavi di dimensione ridotta o insicure, aumentando la probabilità di attacchi crittografici. |
| **Potenziale impatto aziendale:**<br>Gli algoritmi MAC deboli possono essere sfruttati per intercettare o alterare i messaggi SSH, compromettendo la sicurezza delle comunicazioni. |
| **Soluzione consigliata:**<br>Disabilitare gli algoritmi MAC deboli e abilitare algoritmi più robusti, come SHA-256 o SHA-512 per le comunicazioni SSH. |
| **CVSS v2 Base Score:**<br>2.6 (CVSS2AV:N/AC:H/Au:N/C:P/I:N/A:N) |
| **Metodo di rilevazione:**<br>OpenVAS |
| **Riferimenti:**<br>`https://www.rfc-editor.org/rfc/rfc6668` |

## 6.4 Informational

| Apache Banner Linux Distribution Disclosure |
|---|
| INFO |
| **Descrizione:**<br>Il nome della distribuzione Linux in esecuzione sull'host remoto è stato rilevato dall'intestazione banner del server web Apache. |
| **Soluzione consigliata:**<br>Modificare il file 'httpd.conf' impostando la direttiva 'ServerTokens Prod' e riavviare Apache per evitare di mostrare queste informazioni. |
| **Metodo di rilevazione:** Nessus |

| Apache HTTP Server Version |
| --- |
| INFO |
| **Descrizione:**<br>È possibile ottenere il numero di versione del server Apache HTTP remoto.<br>Questo potrebbe aiutare un attaccante a identificare vulnerabilità specifiche della versione in uso. |
| **Metodo di rilevazione:** Nessus |

| Backported Security Patch Detection (FTP) |
| --- |
| INFO |
| **Descrizione:**<br>Le patch di sicurezza potrebbero essere state 'backportate' sul server FTP remoto senza modificare il numero di versione. |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:** `https://access.redhat.com/security/updates/backporting/?sc_cid=3093` |

| Backported Security Patch Detection (PHP) |
| --- |
| INFO |
| **Descrizione:**<br>Le patch di sicurezza potrebbero essere state 'backportate' sul server PHP remoto senza modificare il numero di versione. |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:** `https://access.redhat.com/security/updates/backporting/?sc_cid=3093` |

| Backported Security Patch Detection (SSH) |
| --- |
| INFO |
| **Descrizione:**<br>Le patch di sicurezza potrebbero essere state 'backportate' sul server SSH remoto senza modificare il numero di versione. |
| **Metodo di rilevazione:** Nessus |

| Backported Security Patch Detection (WWW) |
| --- |
| INFO |
| **Descrizione:**<br>Le patch di sicurezza potrebbero essere state 'backportate' sul server HTTP remoto senza modificare il numero di versione. |
| **Metodo di rilevazione:** Nessus |

| Common Platform Enumeration (CPE) |
| --- |
| INFO |
| **Descrizione:**<br>È stato possibile enumerare i CPE per vari prodotti hardware e software trovati sull' host.<br>I seguenti CPE di applicazioni sono stati riscontrati sul sistema remoto:<br>cpe:/a:apache:http_server:2.4.6 -> Apache Software Foundation Apache HTTP Server<br>cpe:/a:isc:bind:9.11.4-p2-redhat-9.11.4-16.p2.el7_8.6 -> ISC BIND<br>cpe:/a:isc:bind:9.11.4:P2 -> ISC BIND<br>cpe:/a:jquery:jquery:3.2.1 -> jQuery<br>cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH<br>cpe:/a:php:php:5.4.16 -> PHP PHP<br>cpe:/a:webmin:webmin:1.953 -> Webmin |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:**<br>`http://cpe.mitre.org/`<br>`https://nvd.nist.gov/products/cpe` |

| SSH Weak MAC Algorithms Enabled |
| --- |
| INFO |
| **Descrizione:**<br>Il server SSH remoto è configurato per consentire l'uso di algoritmi MAC considerati deboli, come HMAC-MD5 e HMAC-SHA1. |
| **Soluzione consigliata:**<br>Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi MAC deboli e abilitare algoritmi MAC più forti come HMAC-SHA2. |
| **Metodo di rilevazione:** Nessus |

| DNS Server BIND version Directive Remote Version Detection |
| --- |
| INFO |
| **Descrizione:**<br>Il sistema remoto esegue BIND o un altro server DNS che riporta il numero di versione quando riceve una richiesta speciale per il testo 'version.bind' nel dominio 'chaos'. |
| **Soluzione consigliata:**<br>È possibile nascondere il numero di versione di BIND utilizzando la direttiva 'version' nella sezione 'options' di named.conf. |
| **Metodo di rilevazione:** Nessus |

| DNS Server Detection |
| --- |
| INFO |
| **Descrizione:**<br>Il servizio remoto è un server DNS (Domain Name System), che fornisce una mappatura tra nomi host e indirizzi IP. |
| **Soluzione consigliata:**<br>Disabilitare questo servizio se non necessario o limitare l'accesso solo agli host interni se il servizio è disponibile esternamente. |
| **Metodo di rilevazione:** Nessus |

| DNS Server hostname.bind Map Hostname Disclosure |
| --- |
| INFO |
| **Descrizione:**<br>Il server DNS rivela il nome dell'host remoto quando viene interrogato per 'hostname.bind' nel dominio CHAOS. |
| **Soluzione consigliata:**<br>È possibile disabilitare questa funzionalità. Consultare la documentazione del fornitore per più informazioni. |
| **Metodo di rilevazione:** Nessus |

| Deprecated SSLv2 Connection Attempts |
| --- |
| INFO |
| **Descrizione:**<br>Questo plugin enumera e segnala tutte le connessioni SSLv2 tentate come parte della scansione. Questo protocollo è proibito dal 2011 a causa di vulnerabilità di sicurezza e la maggior parte delle librerie SSL principali non supportano più questa funzionalità. |
| **Metodo di rilevazione:** Nessus |

| Device Type |
| --- |
| INFO |
| **Descrizione:**<br>Basandosi sul sistema operativo remoto, è possibile determinare il tipo di sistema remoto (es. un computer generico, una stampante, un router, ecc.). |
| **Metodo di rilevazione:** Nessus |

| Embedded Web Server Detection |
| --- |
| INFO |
| **Descrizione:**<br>Il server web remoto è incorporato e non può ospitare CGIs forniti dagli utenti. La scansione CGI sarà disabilitata su questo server. |
| **Metodo di rilevazione:** Nessus |

| Ethernet Card Manufacturer Detection |
| --- |
| INFO |
| **Descrizione:**<br>Ogni indirizzo MAC ethernet inizia con un identificatore univoco (OUI) registrato dall'IEEE, il che consente di determinare il produttore della scheda ethernet. |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:**<br>`https://standards.ieee.org/faqs/regauth.html` |

| Ethernet MAC Addresses |
| --- |
| INFO |
| **Descrizione:**<br>Questo plugin raccoglie gli indirizzi MAC scoperti da varie fonti e li consolida in un elenco univoco e uniforme. |
| **Metodo di rilevazione:** Nessus |

| External URLs |
| --- |
| INFO |
| **Descrizione:**<br>Nessus ha raccolto link HREF verso siti esterni scansionando il server web remoto. |
| **Metodo di rilevazione:** Nessus |

| FTP Server Detection |
| --- |
| INFO |
| **Descrizione:**<br>È possibile ottenere il banner del server FTP remoto connettendosi a una porta remota. |
| **Metodo di rilevazione:** Nessus |

| HTTP Methods Allowed (per directory) |
| --- |
| INFO |
| **Descrizione:**<br>Chiamando il metodo OPTIONS, è possibile determinare quali metodi HTTP sono consentiti per ogni cartella. |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:**<br>`http://www.nessus.org/u?d9c03a9a`<br>`https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)` |

| HTTP Server Type and Version |
| --- |
| INFO |
| **Descrizione:**<br>Un web server è in esecuzione sull'host remoto. |
| **Metodo di rilevazione:** Nessus |

| Host Fully Qualified Domain Name (FQDN) Resolution |
| --- |
| INFO |
| **Descrizione:**<br>È stato possibile risolvere il nome di dominio completo (FQDN) dell'host remoto. |
| **Metodo di rilevazione:** Nessus |

| HyperText Transfer Protocol (HTTP) Information |
| --- |
| INFO |
| **Descrizione:**<br>Questo test fornisce alcune informazioni sulla configurazione HTTP remota - la versione utilizzata, se Keep-Alive è abilitato, ecc. |
| **Metodo di rilevazione:** Nessus |

| Inconsistent Hostname and IP Address |
| --- |
| INFO |
| **Descrizione:**<br>Il nome dell'host remoto non è coerente con le informazioni DNS. Questo può derivare da una configurazione errata del DNS inverso o dall'uso di un file host sul sistema di scansione. |
| **Soluzione consigliata:**<br>Correggere il DNS inverso o il file host per garantire la coerenza delle informazioni DNS. |
| **Metodo di rilevazione:** Nessus |

| JQuery Detection |
| --- |
| INFO |
| **Descrizione:**<br>Il server web remoto utilizza JQuery. Questa informazione potrebbe essere utile per identificare vulnerabilità specifiche legate alla versione rilevata. |
| **Metodo di rilevazione:** Nessus |

| Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header |
|---|
| INFO |
| **Descrizione:**<br>Il server web remoto non imposta o imposta in modo permissivo l'intestazione Content-Security-Policy (CSP) frame-ancestors nelle risposte HTTP. Questo potrebbe esporre il sito a vulnerabilità di clickjacking e altre minacce alla sicurezza. |
| **Soluzione consigliata:**<br>Configurare il server per impostare un'intestazione CSP non permissiva nelle risposte HTTP. |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:**<br>`https://www.w3.org/TR/CSP2/`<br>`https://content-security-policy.com/` |

| Missing or Permissive X-Frame-Options HTTP Response Header |
|---|
| INFO |
| **Descrizione:**<br>Il server web remoto non imposta o imposta in modo permissivo l'intestazione X-Frame-Options nelle risposte HTTP. Questo potrebbe esporre il sito a vulnerabilità di clickjacking e altre minacce alla sicurezza. |
| **Soluzione consigliata:**<br>Configurare il server per impostare un'intestazione X-Frame-Options non permissiva nelle risposte HTTP. |
| **Metodo di rilevazione:** Nessus |
| **Riferimenti:**<br>`http://www.nessus.org/u?399b1f56` |

| Nessus SYN Scanner |
| --- |
| INFO |
| **Descrizione:**<br>È possibile determinare quali porte TCP sono aperte. |
| **Soluzione consigliata:**<br>Proteggere il target con un filtro IP per limitare l'accesso alle porte aperte. |
| **Metodo di rilevazione:** Nessus |

| OS Identification |
| --- |
| INFO |
| **Descrizione:**<br>Utilizzando una combinazione di probe remoti, è possibile indovinare il nome e, a volte, la versione del sistema operativo in uso sull'host remoto.<br>Questa identificazione potrebbe aiutare a determinare eventuali vulnerabilità specifiche della piattaforma. |
| **Metodo di rilevazione:** Nessus |

| OpenSSH Detection |
| --- |
| INFO |
| **Descrizione:**<br>Un server SSH basato su OpenSSH è stato rilevato sull'host remoto.<br>Questa informazione è utile per determinare il software in esecuzione sul target e può essere utilizzata per identificare potenziali vulnerabilità. |
| **Metodo di rilevazione:** Nessus |

| PHP Version Detection |
|---|
| INFO |
| **Descrizione:**<br>Nessus è stato in grado di determinare la versione di PHP in esecuzione sul server web remoto. Questa informazione potrebbe essere utilizzata per identificare vulnerabilità legate alla versione specifica rilevata. |
| **Metodo di rilevazione:** Nessus |

## 6.5 Altre Vulnerabilità

| Local File Inclusion (LFI) |
|---|
| HIGH |
| **Descrizione:**<br>La vulnerabilità di Local File Inclusion (LFI) si verifica quando un'applicazione web consente a un attaccante di includere file locali presenti sul server tramite input non adeguatamente sanitizzato. Questo permette all'attaccante di accedere a file sensibili, come configurazioni di sistema o informazioni riservate, sfruttando parametri vulnerabili. |
| **Potenziale impatto aziendale:**<br>Un attaccante può esfiltrare dati sensibili dal server, accedere a informazioni riservate come credenziali o chiavi di accesso, e compromettere la sicurezza dell'intera infrastruttura. |
| **Soluzione consigliata:**<br>È fondamentale sanitizzare correttamente tutti i parametri dell'input utente per evitare inclusioni non autorizzate di file e restringere l'accesso ai file del server solo a quelli strettamente necessari per l'applicazione. Consultare la **sezione Appendice [C]** per una mitigazione da noi consigliata. |
| **CVSS v3.0 Base Score:**<br>8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L) |
| **Metodo di rilevazione:**<br>LFI può essere rilevata utilizzando strumenti di sicurezza come Burp Suite o manualmente tramite ispezione dei parametri dell'applicazione. |
| **Riferimenti:**<br>`https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion`<br>`https://cwe.mitre.org/data/definitions/98.html` |

| Privilege Escalation tramite PwnKit | CVE<br>2021-4034 |
|---|---|
| HIGH | |
| **Descrizione:**<br>La vulnerabilità PwnKit si trova in pkexec, uno strumento utilizzato su sistemi Linux per eseguire comandi con privilegi elevati. L'exploit sfrutta una out-of-bounds write, che permette l'introduzione di variabili d'ambiente non sicure nell'ambiente di esecuzione di pkexec, consentendo a un utente non autorizzato di ottenere privilegi di root senza autenticazione corretta. | |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe ottenere il controllo completo del sistema come utente root, eseguendo comandi critici, modificando configurazioni di sistema e compromettendo la sicurezza dell'intera rete aziendale. | |
| **Soluzione consigliata:**<br>Aggiornare il pacchetto polkit alla versione più recente che include la patch per CVE-2021-4034 e limitare l'accesso a pkexec agli utenti con autorizzazioni appropriate. | |
| **CVSS v3.1 Base Score:**<br>7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | |
| **Metodo di rilevazione:**<br>L'esecuzione di controlli su pkexec tramite strumenti di auditing della sicurezza come LinPEAS può individuare questa vulnerabilità. | |
| **Riferimenti:**<br>`https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034`<br>`https://access.redhat.com/security/cve/CVE-2021-4034` | |

| Privilege Escalation tramite Sudo Baron Samedit | CVE<br>2021-3156 |
|---|---|
| HIGH | |
| **Descrizione:**<br>La vulnerabilità nel comando `sudo` consente a un utente di ottenere privilegi elevati senza una corretta autenticazione, sfruttando un heap buffer overflow. L'attacco permette l'esecuzione di comandi come root. | |
| **Potenziale impatto aziendale:**<br>Un utente malintenzionato potrebbe sfruttare questa vulnerabilità per ottenere accesso completo al sistema, eseguendo comandi di root senza l'autenticazione necessaria, compromettendo la sicurezza del sistema e dei dati aziendali. | |
| **Soluzione consigliata:**<br>Aggiornare il pacchetto `sudo` all'ultima versione che contiene la patch per CVE-2021-3156 e monitorare l'accesso agli strumenti amministrativi. | |
| **CVSS v3.1 Base Score:**<br>7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | |
| **Metodo di rilevazione:**<br>Utilizzare strumenti come `sudo` e `LinPEAS` per controllare le versioni vulnerabili del comando sudo e identificare possibili exploit. | |
| **Riferimenti:**<br>`https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156`<br>`https://www.sudo.ws/alerts/unescape_overflow.html` | |

| Uso di HTTP e non di HTTPS |
|---|
| HIGH |
| **Descrizione:**<br>L'utilizzo del protocollo HTTP anziché HTTPS espone il traffico di rete a rischi di intercettazione e attacchi man-in-the-middle. HTTP trasmette i dati in chiaro, consentendo a un attaccante di intercettare credenziali, sessioni utente e altre informazioni sensibili durante la trasmissione. |
| **Potenziale impatto aziendale:**<br>Un attaccante può intercettare e manipolare il traffico non crittografato, rubando credenziali, informazioni sensibili e potenzialmente compromettendo l'integrità dei dati aziendali. Questo può portare a furti di identità, violazioni di dati o accesso non autorizzato a risorse aziendali. |
| **Soluzione consigliata:**<br>Abilitare HTTPS per tutte le comunicazioni sensibili, utilizzando certificati SSL/TLS validi. Assicurarsi che tutte le pagine web, soprattutto quelle di login, trasmettano i dati in modo crittografato e che non sia possibile accedere tramite HTTP. |
| **Metodo di rilevazione:**<br>Analisi delle configurazioni del server e strumenti di auditing. |
| **Riferimenti:**<br>`https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration`<br>`https://www.ssllabs.com/ssltest/` |

| Riuso di credenziali per più servizi |
|---|
| HIGH |
| **Descrizione:**<br>Il riuso di credenziali, come nome utente e password, su più servizi rappresenta un rischio significativo per la sicurezza. Se un attaccante compromette un servizio, può utilizzare le stesse credenziali per accedere ad altri servizi, compromettendo l'integrità di interi sistemi aziendali. |
| **Potenziale impatto aziendale:**<br>Un attaccante che ottiene le credenziali di un servizio potrebbe facilmente compromettere altri sistemi aziendali utilizzando le stesse credenziali, aumentando il rischio di accessi non autorizzati e furto di dati sensibili su scala più ampia. |
| **Soluzione consigliata:**<br>Implementare politiche di password uniche per ogni servizio, utilizzare un gestore di password sicuro e adottare l'autenticazione multifattore (MFA) per ridurre il rischio di compromissione delle credenziali. |
| **Metodo di rilevazione:**<br>Manuale. |
| **Riferimenti:**<br>`https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication` |

| Credenziali database MariaDB esposte in PHP config files |
|---|
| MEDIUM |
| **Descrizione:**<br>Le credenziali del database MariaDB (nome utente e password) sono memorizzate in chiaro nei file di configurazione PHP. Questo espone il sistema a rischi, poiché se un attaccante riesce ad accedere ai file di configurazione, può ottenere facilmente le credenziali e accedere al database in modo non autorizzato. |
| **Potenziale impatto aziendale:**<br>Un attaccante che riesce a ottenere le credenziali può accedere al database, esfiltrare o manipolare dati sensibili, compromettere la continuità operativa dell'azienda e alterare informazioni critiche. |
| **Soluzione consigliata:**<br>Evitare di memorizzare le credenziali del database in chiaro nei file di configurazione. Utilizzare metodi più sicuri come variabili d'ambiente, file esterni con permessi di accesso limitati o servizi di gestione sicura delle credenziali. |
| **Metodo di rilevazione:**<br>Ispezionare i file di configurazione PHP e verificare la presenza di credenziali archiviate in chiaro. Utilizzare strumenti di auditing del codice o di sicurezza per automatizzare il controllo. |
| **Riferimenti:**<br>`https://mariadb.com/kb/en/securing-mariadb/` |

| Monitoraggio di rete tramite Wireshark da parte di un utente con privilegi minimi |
|---|
| MEDIUM |
| **Descrizione:**<br>Permettere a un utente con privilegi minimi di utilizzare strumenti di monitoraggio di rete come Wireshark è estremamente rischioso. Questi strumenti consentono di catturare pacchetti di rete in transito, che possono contenere dati sensibili come credenziali, informazioni personali o traffico amministrativo. Un utente non autorizzato potrebbe sfruttare questa capacità per monitorare e compromettere le comunicazioni all'interno della rete aziendale. |
| **Potenziale impatto aziendale:**<br>L'uso non autorizzato di Wireshark da parte di utenti con privilegi limitati può portare alla compromissione di informazioni sensibili, come credenziali di amministratori o dati trasmessi non crittografati. Questo potrebbe permettere all'attaccante di eseguire attacchi di tipo man-in-the-middle o accedere a risorse riservate. |
| **Soluzione consigliata:**<br>Limitare l'accesso agli strumenti di monitoraggio di rete solo agli amministratori di sistema o agli utenti con privilegi appropriati. Assicurarsi che i permessi di rete e le autorizzazioni dei gruppi siano correttamente configurati, impedendo a utenti con accesso limitato di catturare il traffico di rete. |
| **Metodo di rilevazione:**<br>Analisi delle politiche di accesso agli strumenti di monitoraggio di rete. |
| **Riferimenti:**<br>`https://wiki.wireshark.org/CaptureSetup/CapturePrivileges` |

| Cross-Site Scripting (XSS) su phpBB tramite BBCode |
|---|
| MEDIUM |
| **Descrizione:**<br>La vulnerabilità di Cross-Site Scripting (XSS) in phpBB consente di creare un BBCode personalizzato che esegue codice JavaScript malevolo nel browser degli utenti. Questo può avvenire quando gli utenti visualizzano il post compromesso nel forum, sfruttando il BBCode per iniettare il codice. |
| **Potenziale impatto aziendale:**<br>Un attaccante può ottenere il controllo del browser delle vittime, eseguire comandi remoti, rubare informazioni sensibili come cookie o credenziali e compromettere la sicurezza degli utenti e del sistema. |
| **Soluzione consigliata:**<br>Aggiornare phpBB all'ultima versione disponibile, implementare filtri di input per validare i dati del BBCode e impedire l'iniezione di codice JavaScript, ed educare gli utenti a riconoscere contenuti sospetti. |
| **Metodo di rilevazione:**<br>Verificare la possibilità di iniettare codice JavaScript tramite BBCode su phpBB utilizzando strumenti di analisi di vulnerabilità XSS come Burp Suite o OWASP ZAP. |
| **Riferimenti:**<br>`https://owasp.org/www-community/attacks/xss/` |

| Uso di funzione hash debole |
| --- |
| MEDIUM |
| **Descrizione:**<br>L'uso di funzioni hash deboli, come MD5 o SHA-1, compromette la sicurezza dei dati. Tali funzioni sono vulnerabili a collisioni, che consentono a un attaccante di generare due input diversi con lo stesso hash. Ciò può portare a violazioni di integrità e compromissioni di sicurezza in sistemi di autenticazione, firma digitale e archiviazione di password. |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe sfruttare le collisioni hash per bypassare controlli di sicurezza, manipolare dati firmati digitalmente o decifrare password archiviate, compromettendo così l'integrità e la confidenzialità dei dati aziendali. |
| **Soluzione consigliata:**<br>Sostituire le funzioni hash deboli con algoritmi più sicuri come SHA-256, SHA-3 o bcrypt per l'archiviazione di password e l'integrità dei dati. |
| **Metodo di rilevazione:**<br>Analisi del codice sorgente, strumenti di auditing della sicurezza come Nessus o OpenVAS per rilevare l'uso di hash deboli nei sistemi. |
| **Riferimenti:**<br>`https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure`<br>`https://cwe.mitre.org/data/definitions/328.html` |

| SMTP utilizza il metodo di autenticazione 'PLAIN' |
| --- |
| MEDIUM |
| **Descrizione:**<br>Il metodo di autenticazione 'PLAIN' nel protocollo SMTP trasmette le credenziali (nome utente e password) in chiaro, senza crittografia. Ciò consente a un attaccante di intercettare facilmente le credenziali durante la trasmissione, specialmente se la connessione non è protetta da TLS. |
| **Potenziale impatto aziendale:**<br>Un attaccante potrebbe intercettare le credenziali SMTP non crittografate, compromettendo gli account e utilizzandoli per inviare email non autorizzate, esfiltrare informazioni o accedere a risorse aziendali tramite i servizi di posta elettronica. |
| **Soluzione consigliata:**<br>Abilitare TLS per proteggere le comunicazioni SMTP, evitando che le credenziali vengano trasmesse in chiaro. Utilizzare metodi di autenticazione sicuri come CRAM-MD5 o OAuth2 per garantire una protezione crittografica durante la trasmissione dei dati sensibili. |
| **Metodo di rilevazione:**<br>Utilizzo di Wireshark per monitorare le trasmissioni SMTP. |
| **Riferimenti:**<br>`https://tools.ietf.org/html/rfc3207`<br>`https://tools.ietf.org/html/rfc4954` |

# 7 Conclusioni

In seguito al penetration test eseguito sull'infrastruttura IT di GreenOptic, è emerso che l'organizzazione presenta diverse vulnerabilità critiche che potrebbero essere sfruttate da attaccanti malintenzionati per compromettere la confidenzialità, l'integrità e la disponibilità dei dati aziendali. In particolare, sono state riscontrate debolezze nel processo di gestione delle credenziali, nell'utilizzo di protocolli non sicuri e nella configurazione dei server, che rappresentano un rischio elevato per l'organizzazione. Le raccomandazioni presentate, se implementate correttamente, permetteranno di rafforzare la sicurezza generale dell'infrastruttura IT, riducendo la probabilità di attacchi futuri e migliorando la resilienza contro minacce potenziali. La gestione continua delle vulnerabilità e la formazione del personale saranno fattori chiave per garantire una protezione efficace e duratura.

Questo report fornisce una guida dettagliata su come affrontare le problematiche riscontrate e migliorare la postura di sicurezza di GreenOptic, contribuendo a prevenire ulteriori compromissioni e proteggere i dati sensibili dell'azienda.

# Riferimenti bibliografici

[1] PCI. *Information Supplement: Penetration Testing Guidance*. https://listings.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

[2] First. *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. https://www.first.org/cvss/v2/guide.

[3] First. *Common Vulnerability Scoring System v3.1: Specification Document*. https://www.first.org/cvss/v3.1/specification-document.

[4] Ilia Ross. *PCI Compliance*. https://www.virtualmin.com/docs/security/pci-compliance/#webmin-configuration.

[5] OWASP. *File Upload Cheat Sheet*. https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html.

# Appendices

## A Risoluzione vulnerabilità SSL Medium Strength Cipher Suites Supported (SWEET32)

La vulnerabilità SWEET32 si manifesta sulla porta 10000, collegata al software Webmin. Per risolvere questa criticità, abbiamo seguito le raccomandazioni fornite da Virtualmin [4].

**Configurazione Webmin** (Figura 4) La procedura per risolvere la vulnerabilità prevede l'adeguamento delle impostazioni SSL di Webmin. Ecco i passaggi principali:

- Accedere all'interfaccia principale di Webmin e dal pannello di navigazione a sinistra, seguire il percorso:: **Webmin** -> **Webmin Configuration** -> **SSL Encryption**.
- Nella sezione **SSL protocol versions to reject**, selezionare tutti i protocolli. Questo permette di abilitare esclusivamente il protocollo TLSv1.3, che offre maggiore sicurezza.
- Abilitare l'opzione **Only strong PCI-compliant ciphers**.
- Salvare le modifiche per applicare la nuova configurazione.

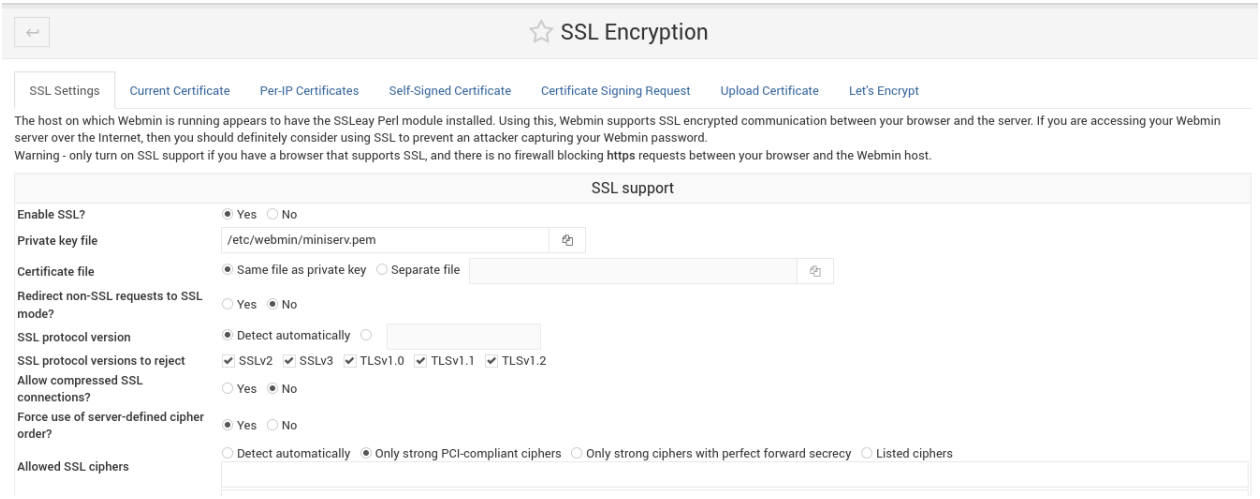


Figura 4: Configurazione SSL di Webmin per mitigare SWEET32

## B Webmin <= 1.994 Multiple Vulnerabilities: CVE-2021-32156 exploitation

Questa vulnerabilità di Webmin consente un attacco di tipo Cross-site request forgery (CSRF) per ottenere una Remote Command Execution (RCE). L'exploit sfrutta la possibilità di creare un Cron Job tramite Webmin, inducendo un amministratore loggato ad eseguire un file HTML creato ad hoc.

L'exploit disponibile su GitHub, purtroppo, non era pienamente funzionante e abbiamo dovuto modificarlo per garantire il suo corretto utilizzo.

All'avvio dello script vengono richieste le seguenti informazioni:

- **Path di Webmin**: Percorso web di Webmin.
- **Indirizzo IP dell'attaccant**e: Necessario per instaurare una reverse shell.
- **Porta di ascolto**: La porta sulla quale il sistema attaccante ascolterà la connessione in entrata.
- **Tipo di comando per la reverse shell**: La scelta del comando dipende dal linguaggio presente sul sistema bersaglio (ad esempio Bash, Python, PHP).

Nel nostro caso, sapendo che il sistema bersaglio supportava PHP, abbiamo optato per una reverse shell in PHP. Lo script genera un file chiamato `CSRF_POC.html`, che è stato poi eseguito dopo aver effettuato l'accesso a Webmin con credenziali di amministratore (root).

Una volta aperto il file `CSRF_POC.html` siamo riusciti a creare ed eseguire il cron job che ha permesso l'attivazione della reverse shell, ottenendo così accesso completo alla shell con privilegi di root sul sistema bersaglio (Figura 5).

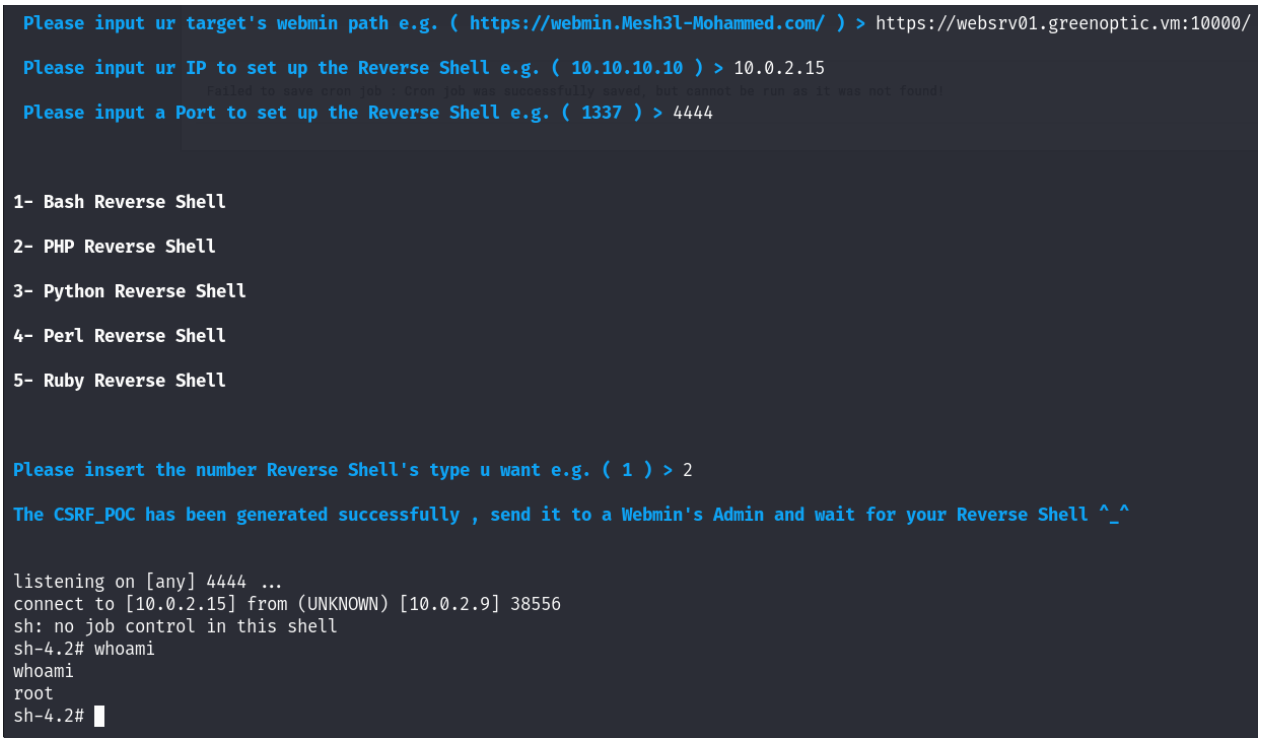


Figura 5: Sfruttamento di Webmin per ottenere una shell root

Per mitigare il rischio associato a vulnerabilità come la CVE-2021-32156, oltre all'aggiornamento di Webmin all'ultima versione disponibile, è fondamentale educare i dipendenti, specialmente quelli con privilegi elevati, sull'importanza di non aprire file o URL sospetti.

Gli attacchi di tipo CSRF e altre forme di social engineering possono spesso essere prevenuti attraverso la formazione e la consapevolezza degli utenti sui rischi legati a comportamenti non sicuri.

# C Risoluzione vulnerabilità Local File Inclusion (LFI)

Per mitigare la vulnerabilità di Local File Inclusion (LFI) riscontrata, è stato modificato il file PHP vulnerabile situato nel percorso **/var/www/html/account/index.php**. Di seguito, illustreremo le modifiche apportate al codice per garantire una gestione sicura dell'inclusione di file.

Listing 1: File PHP vulnerabile

```
<?php
$file = $_GET['include'];
require_once($file);
?>
```

Questa implementazione non effettua alcun tipo di validazione sull'input proveniente dall'utente, rendendo il sistema vulnerabile a attacchi di tipo Local File Inclusion, che possono permettere a un attaccante di includere file critici del sistema, come */etc/passwd*, o di eseguire codice arbitrario. Le modifiche apportate al codice sono state implementate in conformità con le linee guida descritte nella *OWASP File Upload Cheat Sheet* [5], che riducono sensibilmente il rischio di LFI:

Listing 2: File PHP modificato

```
<?php
if (empty($_GET['include'])) {
    header('Location: index.php?include=cookiewarning');
    die();
}

$allowed_files = array('cookiewarning', 'header', 'footer', 'login');

$file = basename($_GET['include']);

if (in_array($file, $allowed_files)) {
    require_once("includes/" . $file . ".php");
} else {
    echo "File non valido!";
    die();
}
?>
```

Per prevenire l'inclusione di file non autorizzati, sono state apportate le seguenti modifiche:

- **basename($_GET['include'])**: La funzione `basename` estrae solo il nome del file dall'input dell'utente, eliminando eventuali tentativi di attacco di directory traversal, come l'uso di `../` per accedere a directory superiori.
- **Whitelist ($allowed_files)**: È stata introdotta una whitelist di file consentiti per l'inclusione. In questo esempio, solo file specifici come `cookiewarning`, `header`, `footer` e `login` possono essere inclusi. Questa lista può essere estesa in base alle esigenze del progetto, garantendo un controllo rigido sui file inclusi.
- **Inclusione da una directory sicura**: Tutti i file vengono inclusi da una directory dedicata e sicura (`includes/`), riducendo ulteriormente il rischio di accesso a file non autorizzati o sensibili.
- **Gestione degli errori**: Se l'utente tenta di includere un file che non è presente nella whitelist, il sistema restituisce un messaggio di errore ("File non valido!") senza eseguire alcun codice. Questo impedisce il verificarsi di comportamenti imprevisti e limita la superficie di attacco.

Dopo aver apportato le modifiche, è stato necessario riavviare il server Apache per rendere effettivi i cambiamenti. Il comando utilizzato è stato il seguente:

Listing 3: Riavvio di Apache

```
service httpd restart
```

Le modifiche apportate hanno mitigato con successo la vulnerabilità LFI, come illustrato nella Figura 6.

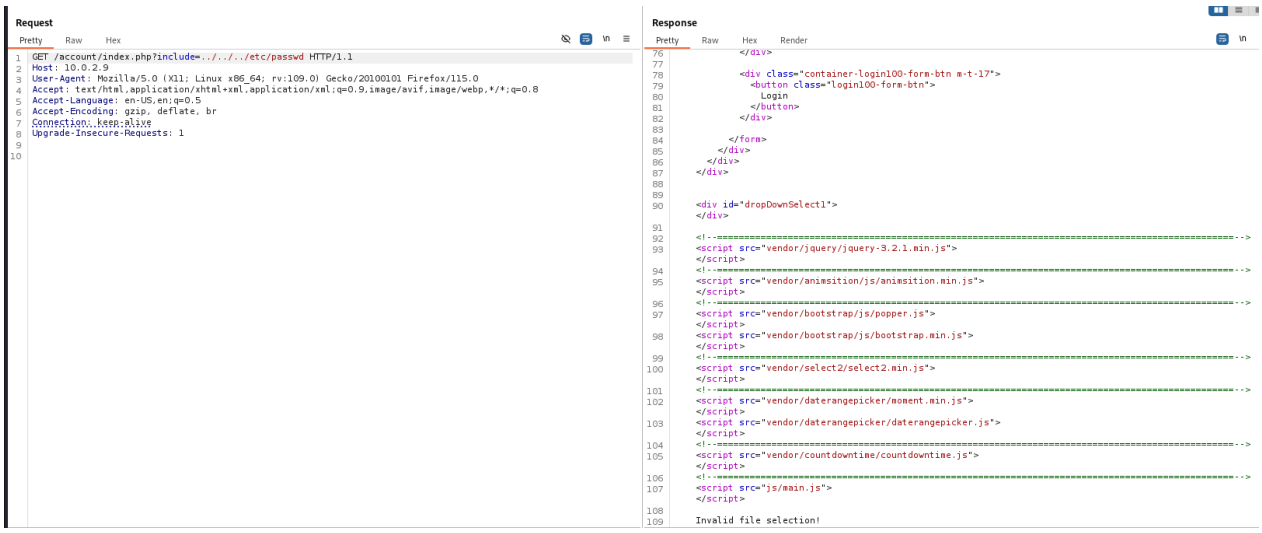


Figura 6: Mitigazione della vulnerabilità LFI

# D Tools

| Tool | Descrizione |
|---|---|
| Netdiscover | Strumento di rilevamento IP utilizzato per scoprire gli indirizzi IP all'interno di una rete locale, utile per la fase iniziale di scoperta del target. |
| Nmap | Strumento potente per la scansione delle porte aperte, per l'individuazione dei servizi in esecuzione e per il rilevamento del sistema operativo (OS Fingerprinting). |
| Arp-scan | Utilizzato per scansionare la rete e identificare dispositivi connessi tramite il protocollo ARP, spesso per confermare l'indirizzo IP target. |
| Hping3 | Generatore di pacchetti utilizzato per inviare pacchetti ICMP o TCP al fine di testare la disponibilità di un host, spesso in sostituzione o in aggiunta al comando ping. |
| p0f | Strumento di fingerprinting passivo, utilizzato per identificare il sistema operativo e altri dettagli di rete analizzando pacchetti di rete in transito. |
| SpiderFoot | Strumento di intelligence automatizzata per la raccolta di informazioni su target, utile per confermare porte e servizi aperti. |
| Unicornscan | Strumento veloce per la scansione delle porte UDP, utilizzato per identificare servizi UDP attivi su una macchina target. |
| Nessus | Scanner di vulnerabilità automatizzato, utilizzato per rilevare vulnerabilità note nei servizi e nei sistemi operativi. |
| OpenVAS | Scanner di vulnerabilità open source, simile a Nessus, utilizzato per identificare debolezze nel sistema target. |
| Burp Suite | Strumento di analisi e testing delle applicazioni web, utilizzato per intercettare, modificare e testare le richieste HTTP alla ricerca di vulnerabilità. |
| Hydra | Strumento di brute force che tenta combinazioni di username e password su servizi di autenticazione come SSH e HTTP per accedere illegalmente. |
| Gobuster | Strumento di brute-forcing per enumerare directory e file nascosti su server web, spesso utilizzato per scoprire percorsi non pubblicizzati. |
| Foremost | Strumento di recupero file, utilizzato nell'analisi forense per estrarre file cancellati o nascosti da immagini disco. |

| Tool | Descrizione |
|---|---|
| Scalpel | Simile a Foremost, questo strumento è utilizzato per il file carving, cioè l'estrazione di file cancellati o corrotti da immagini forensi. |
| Wireshark | Strumento di analisi dei pacchetti di rete, utilizzato per catturare e analizzare il traffico di rete alla ricerca di credenziali o altri dati sensibili. |
| John the Ripper | Strumento di cracking di password che cerca di decifrare hash di password utilizzando attacchi di brute force o dizionario. |
| LinEnum | Strumento di enumerazione automatizzata delle configurazioni di sistema su Linux, usato per trovare potenziali vie di privilege escalation. |
| Linux Exploit Suggester | Strumento che analizza il sistema e suggerisce exploit locali basati sulla versione del kernel e sulle vulnerabilità conosciute. |
| Linux Exploit Suggester 2 | Versione aggiornata di Linux Exploit Suggester, con una base di dati di vulnerabilità estesa e aggiornata per suggerire exploit locali. |
| MSFvenom | Parte della suite Metasploit, utilizzato per generare payload personalizzati come reverse shell e altri strumenti per l'attacco. |
| Metasploit | Piattaforma di exploit ampiamente utilizzata per eseguire e gestire exploit, post-exploitation, e privilege escalation. |
| BeEF | Browser Exploitation Framework, strumento per eseguire attacchi avanzati contro browser compromessi, sfruttando vulnerabilità XSS e altre tecniche. |
| LinPEAS | Strumento per l'enumerazione di potenziali vie di privilege escalation su sistemi Linux, spesso utilizzato in fase di post-exploitation. |
| Dig | Strumento per interrogazioni DNS, utilizzato per l'enumerazione di host e per eseguire trasferimenti di zona DNS in caso di errata configurazione. |