

Penetration Test GreenOptic

Tester: **Daniele Gregori**

Penetration Testing & Ethical Hacking
Anno Accademico 2024/2025



TABLE OF CONTENTS

01



Obiettivo

02



Metodologia

03



Stato Attuale
della Sicurezza

04



Vulnerabilità
Critiche

05



Azioni
Correttive



01

Obiettivo



Obiettivo del Penetration Testing

- **Identificare le vulnerabilità** presenti nell'infrastruttura IT di GreenOptic.
- **Simulare attacchi reali** per valutare l'efficacia delle misure di sicurezza attualmente in uso.
- **Valutare il rischio di compromissione** dei dati sensibili e delle operazioni aziendali.
- **Proporre soluzioni pratiche** per mitigare i rischi identificati e migliorare la postura di sicurezza.
- **Rafforzare la resilienza del sistema** contro futuri attacchi informatici, proteggendo le informazioni critiche dell'azienda.





02

Metodologia



Framework Generale per il Penetration Testing (FGPT)



Tecniche Utilizzate

Analisi Manuale



Strumenti Automatici




Nessus
vulnerability scanner



Greenbone OpenVAS
Open Vulnerability Assessment Scanner

Architettura di Rete





Stato Attuale della Sicurezza

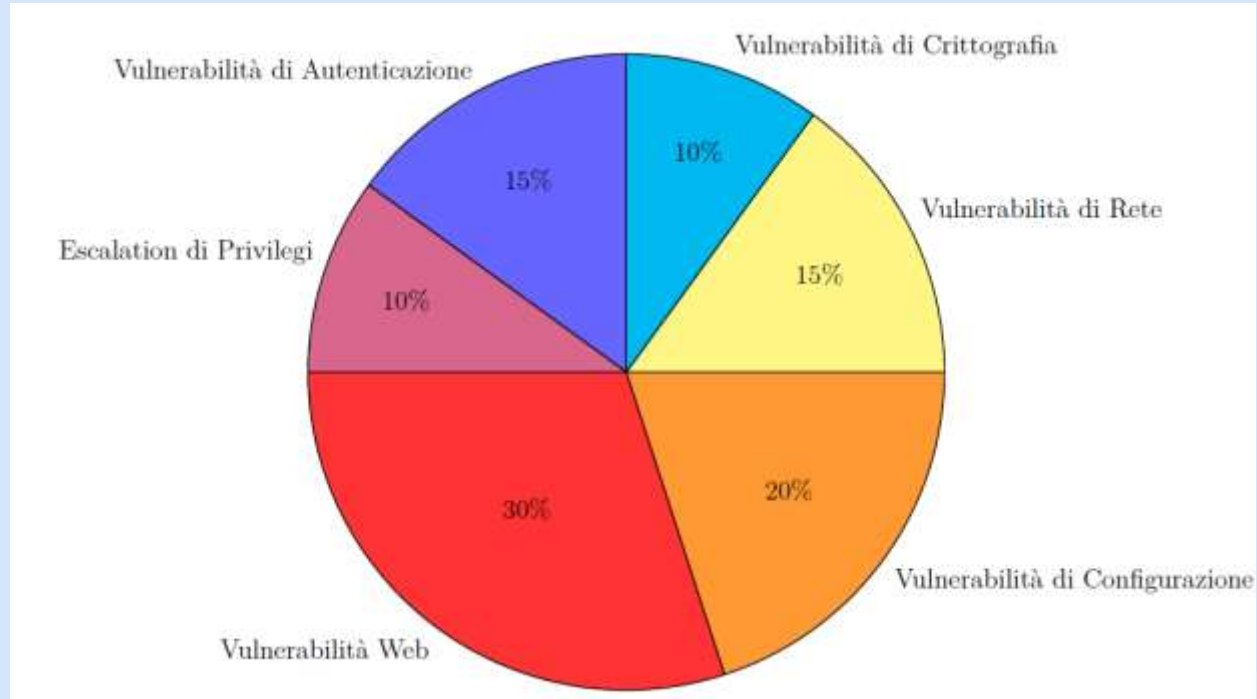
03



Vulnerabilità Rilevate

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

Macro-categorie






04



Vulnerabilità
Critiche



Vulnerabilità ad Alto Rischio (1)

Local File Inclusion (LFI)

- **Descrizione:** Manipolazione dell'URL per accedere a file sensibili presenti sul server.
- **Impatto:** Esposizione di file critici come configurazioni di sistema e credenziali di accesso, con possibile esfiltrazione di dati riservati.



Privilege Escalation

- **Descrizione:** Sfruttamento di vulnerabilità per ottenere privilegi amministrativi, consentendo il controllo completo del sistema.
- **Impatto:** Un attaccante potrebbe modificare, cancellare o rubare dati critici, compromettendo l'intero sistema aziendale.

Vulnerabilità di XSS (Cross-Site Scripting)

- **Descrizione:** Iniezione di codice malevolo in pagine web vulnerabili, eseguibile nel browser dell'utente.
- **Impatto:** Furto di credenziali, compromissione delle sessioni e manipolazione dei dati utente.



Vulnerabilità ad Alto Rischio (2)

Remote Command Execution (RCE)

- **Descrizione:** Sfruttamento di vulnerabilità che permette a un attaccante di eseguire comandi da remoto con privilegi elevati.
- **Impatto:** Un attaccante può ottenere accesso completo al sistema e compromettere l'integrità dell'infrastruttura aziendale.



Uso di HTTP anziché HTTPS

- **Descrizione:** Comunicazioni non crittografate su HTTP, che espongono dati sensibili a intercettazioni.
- **Impatto:** Un attaccante può intercettare informazioni sensibili come credenziali e dati finanziari, aumentando il rischio di attacchi man-in-the-middle.

SSL Medium Strength Cipher Suites Supported (SWEET32)

- **Descrizione:** Uso di cifrari SSL di media forza che offrono protezione insufficiente.
- **Impatto:** Un attaccante sulla stessa rete può sfruttare la debole crittografia per intercettare le comunicazioni crittografate, con possibili furti di informazioni riservate.

Vulnerabilità ad Alto Rischio (3)

Vulnerabilità CSRF (Cross-Site Request Forgery)



- **Descrizione:** Esecuzione non autorizzata di azioni tramite l'utente autenticato, sfruttando sessioni attive.
- **Impatto:** Un attaccante può eseguire azioni malevole senza il consenso dell'utente, con possibile compromissione delle operazioni aziendali.

Riuso di Credenziali per Più Servizi

- **Descrizione:** Le stesse credenziali (username e password) vengono utilizzate su diversi servizi come FTP, SSH e Webmin.
- **Impatto:** Se una credenziale viene compromessa, l'attaccante può ottenere accesso a più servizi, ampliando il danno e aumentando l'esposizione dell'intera infrastruttura.



Azioni Correttive

05

Rimedi Proposti (1)

Aggiornamento delle Applicazioni e Sistemi

- **Descrizione:** Installare patch di sicurezza e aggiornamenti per tutte le applicazioni e sistemi vulnerabili.
- **Impatto:** Riduzione delle vulnerabilità legate a Remote Code Execution (RCE), XSS e Privilege Escalation.

Rafforzare la Configurazione del Server

- **Descrizione:** Implementare configurazioni più sicure per DNS, SSH e Webmin.
- **Impatto:** Miglioramento della sicurezza delle comunicazioni e riduzione del rischio di attacchi man-in-the-middle.

Implementazione di Crittografia Robusta

- **Descrizione:** Sostituire cifrari deboli come RC4 e CBC con cifrari più sicuri (AES-GCM o TLS 1.2+) e forzare l'uso di HTTPS per tutte le comunicazioni.
- **Impatto:** Protezione avanzata dei dati in transito, riducendo il rischio di intercettazioni.



Rimedi Proposti (2)



Migliorare la Gestione delle Credenziali

- **Descrizione:** Adottare l'autenticazione a più fattori ed evitare il riutilizzo delle credenziali su più servizi.
 - **Impatto:** Riduzione del rischio di compromissione delle credenziali e accessi non autorizzati.

Controllo degli Accessi e Privilegi

- **Descrizione:** Applicare il principio del minimo privilegio per gli utenti e monitorare l'uso dei privilegi elevati.
- **Impatto:** Limitazione dei danni in caso di compromissione e riduzione del rischio di privilege escalation.

Protezione Contro XSS e CSRF

- **Descrizione:** Implementare header di sicurezza come X-Frame-Options e Content-Security-Policy e sanitizzare correttamente gli input dell'utente.
- **Impatto:** Riduzione del rischio che codice malevolo venga eseguito nei browser degli utenti.

Rimedi Proposti (3)

Processo di Gestione delle Vulnerabilità

- **Descrizione:** Stabilire un processo continuo di scansione e gestione delle vulnerabilità per identificare e correggere tempestivamente eventuali debolezze.
- **Impatto:** Riduzione delle esposizioni a nuove vulnerabilità e mantenimento della sicurezza nel tempo.

Monitoraggio e Risposta agli Incidenti

- **Descrizione:** Implementare sistemi di monitoraggio attivo (SIEM) per rilevare comportamenti sospetti e attacchi in corso.
- **Impatto:** Miglioramento della reattività aziendale in caso di attacco e minimizzazione dei danni.

Formazione e Sensibilizzazione del Personale

- **Descrizione:** Implementare un programma di formazione continua per il personale sulle migliori pratiche di sicurezza.
- **Impatto:** Miglioramento della consapevolezza del personale e riduzione del rischio di attacchi basati su errori umani.



A stylized blue frame with a thick border. On the left and right sides, there are orange arrows pointing outwards. At the top center, there is a small orange oval with a white dot inside. On the left and right sides, there are orange curved lines with dots at their ends. At the bottom center, there is an orange zigzag line.

**GRAZIE PER
L'ATTENZIONE**