UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Penetration Testing and Ethical Hacking

Penetration Testing Report: Devel

STUDENTE

Esposito Francesco

Anno Accademico 2024-2025

Indice

CAPITOLO 1

Penetration Testing Report

1.1 Executive Summary

Per l'attività progettuale relativa al corso di *Penetration Testing and Ethical Hacking* è stato svolto un processo di *Penetration Testing* sulla macchina virtuale vulnerabile by-design *'Devel'*, disponibile sulla piattaforma *Hack The Box*. In assenza di particolari e specifiche informazioni relative all'asset da analizzare, è stato utilizzato un approccio di tipo *Black Box*. Per svolgere l'analisi è stato configurato un opportuno ambiente simulato che consente un'interazione con l'asset, permettendo di esaminarlo e rilevarne le vulnerabilità. In particolare, le vulnerabilità rilevate possono portare all'ottenimento del pieno controllo del sistema da parte di un attaccante che può assumere il ruolo di amministratore. Allo stato attuale, il livello complessivo associato all'asset risulta essere critico, tuttavia mediante alcuni accorgimenti, come la disabilitazione dell'accesso anonimo al servizio *FTP* e l'implementazione di alcuni semplici controlli, è possibile abbassare sensibilmente il livello di rischio.

1.2 Engagement Highlights

Dal momento che il processo di Penetration Testing è stato svolto in un contesto puramente didattico, non è stato necessario definire particolari regole di ingaggio.

1.3 Vulnerability Report

Nel corso del processo di Penetration Testing sono state rilevate diverse vulnerabilità sfruttabili per compromettere vari aspetti del sistema. di seguito è riportata una descrizione generale delle problematiche riscontrate:

Nel corso del processo di Penetration Testing sono state individuate diverse vulnerabilità che possono compromettere la sicurezza e l'integrità dell'infrastruttura. Di seguito è riportata una descrizione sintetica delle principali criticità riscontrate:

- **[Severity: Alta] Remote Code Execution tramite file upload non controllato**: è stato possibile caricare file potenzialmente pericolosi all'interno della directory web del server, con conseguente possibilità di esecuzione arbitraria di codice da remoto;
- **[Severity: Alta] FTP connesso a directory web con permessi di scrittura**: la configurazione errata consente a un attaccante remoto di caricare file direttamente accessibili via web, aumentando esponenzialmente il rischio di compromissione;
- **[Severity: Media] Accesso anonimo abilitato su servizio FTP**: la presenza dell'accesso anonimo su un servizio FTP espone il sistema a potenziali accessi non autorizzati a dati sensibili;
- **[Severity: Media] Utilizzo di un Web Server obsoleto e non aggiornato**: il server in uso risulta essere in end-of-life e privo degli aggiornamenti di sicurezza necessari, lasciando il sistema esposto a vulnerabilità note;
- **[Serverity: Media] Navigabilità delle directory del Web Server**: possibilità di navigare le directory del Web Server mediante il servizio *FTP* al fine di visualizzarne il contenuto.

- **[Severity: Bassa] Trapelamento del timestamp del sistema**: ottenimento di informazioni sul timestamp del sistema con eventuale possibilità di prevedere dati generati in maniera arbitraria dal sistema.

1.4 Remediation Report

Mediante vari accorgimenti risulta possibile rimuovere le vulnerabilità dal sistema evitando, in questo modo, tutti i rischi ad esse associate. Di seguito è riportata una descrizione generale delle operazioni consigliate:

- Disabilitazione dell'accesso anonimo al servizio *FTP* per prevenire accessi non autorizzati;
- Separazione tra l'area *FTP* e la directory esposta dal Web Server, con rimozione dei permessi di scrittura non necessari;
- Applicazione di controlli stringenti su file caricati dagli utenti al fine di impedire l'esecuzione remota di codice non autorizzato;
- Aggiornamento del Web Server all'ultima versione stabile supportata, con sostituzione delle versioni in *end-of-life*;
- Revisione delle policy di accesso e dei permessi sui file e directory critici del sistema.

1.5 Findings Summary

Di seguito sono riportati i grafici alle vulnerabilità indicare in rapporto alla severity. In particolare, l'aerogramma illustrato nella **figura 1.1** ne mostra la percentuale, mentre l'ortogramma mostrato nella **figura 1.2** ne mostra il numero.

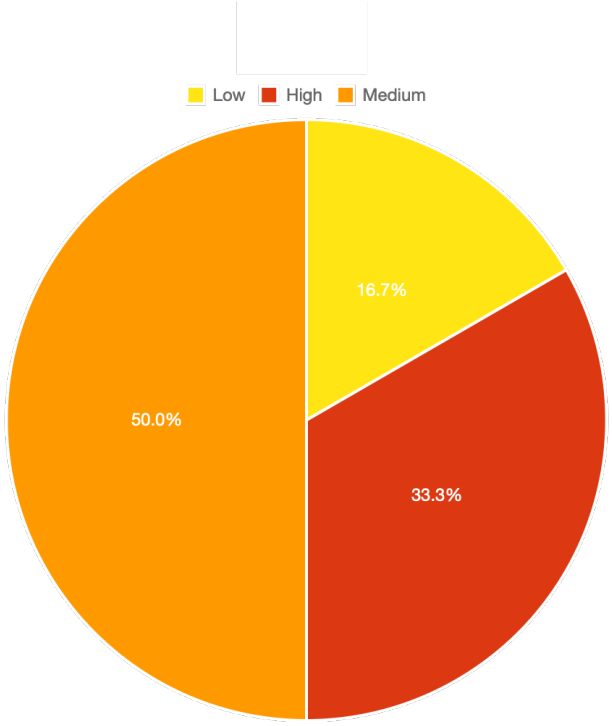

Figura 1.1: Aerogramma delle vulnerabilità rilevate

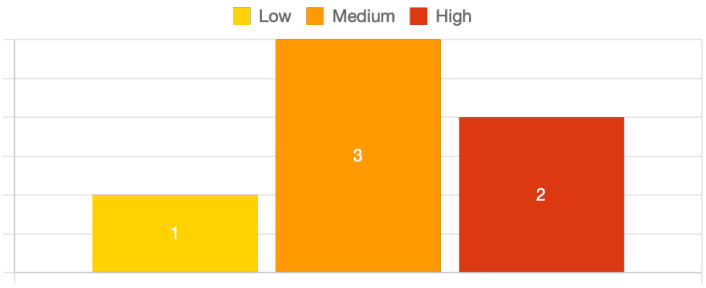

Figura 1.2: Ortogramma delle vulnerabilità rilevate

1.6 Detailed Summary

Le vulnerabilità discusse sono state rilevate sia mediante l'utilizzo di specifici tool che mediante tecniche di ricerca manuale. Complessivamente sono state rilevate 13 vulnerabilità e c'è stato un *End of Life Detection* del Web Server.

1.6.1 Vulnerabilità rilevate mediante tool

OpenVAS

OpenVAS ha rilevato le seguenti vulnerabilità:

- **TCP Timestamps Information Disclosure**, severity bassa;
- **ICMP Timestamp Reply Information Disclosure (CVE-1999- 0524)**, severity bassa;
- **Microsoft ASP.NET Information Disclosure (CVE-2010-3332)**, severity media;
- **Microsoft IIS Default Welcome Page Information Disclosure**, severity media;
- **Anonymous FTP Login Reporting (CVE-1999-0497)**, severity media;
- **FTP Unencrypted Cleartext Login**, severity media;
- **Microsoft HTTP.sys RCE Vulnerability (CVE-2015-1635)**, severity alta.

Nessus

Nessus ha rilevato le seguenti vulnerabilità:

- **ICMP Timestamp Request Remote Date Disclosure**, severity bassa;
- **MS12-0743: Vulnerabilites in Microsft IIS Could Allow Information Disclosure (2733829) (uncredentialed check)**, severity media;
- **Unsupported Web Server Detection**, severity alta.

Nikto2

Nikto 2 ha rilevato diverse vulnerabilità, tuttavia, senza fornire un livello di severity associato. Le vulnerabilità sono le seguenti:

- **The anti-clickjacking X-Frame-Options header is not present**: questa vulnerabilità è stata rilevata anche da altri tool che hanno assegnato una severity media;

- **The X-Content-Type-Options header is not set**: questa vulnerabilità è stata rilevata anche da altri tool che hanno assegnato una severity bassa;
- **Presenza dell'header X-Powered-By: ASP.NET**: rivela dettagli sull'infrastruttura tecnologica utilizzata;

OWASP ZAP

OWASP ZAP ha rilevato le seguenti vulnerabilità web:

- **Content Security Policy (CSP) Header not set**, severity media;
- **Missing Anti-clickjacking Header**, severity media;
- **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**, severity bassa;
- **Server Leaks Information via "Server" HTTP Response Header Field**, severity bassa;
- **X-Content-Type-Options Header Missing**, severity bassa;

1.6.2 Vulnerabilità rilevate mediante tecniche manuali

Le vulnerabilità a severity più alta sono state scoperte con tecniche manuali attraverso l'esplorazione dei servizi sulla macchina target. Di seguito è riportato un rapporto dettagliato delle criticità rilevate:

Remote Code Execution tramite caricamento non controllato di file

- **Descrizione**: il servizio di upload rende disponibile una directory web con permessi scrittura, permettendo il caricamento di file potenzialmente pericolosi; tali file vengono automaticamente processati dal Web Server;
- **Modalità di individuazione**: test manuale di upload con file di tipo script in directory accessibile via web;
- **Rischi associati**: esecuzione arbitraria di codice da remoto, compromissione completa del sistema;

- **Severity**: Alta;
- **CWE di riferimento**:
  - CWE-434 – Unrestricted Upload of File with Dangerous Type;
  - CWE-94 – Improper Control of Generation of Code ('Code Injection').
- **Soluzione**: isolare l'area di upload fuori dal document-root.

Riferimenti: CWE-434(https://cwe.mitre.org/data/definitions/434.html)

***FTP* con accesso anonimo e scrittura in directory web**

- **Descrizione**: il servizio *FTP* consente l'accesso anonimo e permette di scrivere direttamente nella directory servita dal Web Server;
- **Modalità di individuazione**: accesso *FTP* senza credenziali, verifica della directory corrente e test di scrittura di file;
- **Rischi associati**: caricamento arbitrario di file web-accessibili con possibile Remote Code Execution;
- **Severity**: Alta;
- **CWE di riferimento**:
  - CWE-732 – Incorrect Permission Assignment for Critical Resource;
  - CWE-284 – Improper Access Control.
- **Soluzione**: disabilitare l'accesso anonimo su *FTP*, garantire che permessi di scrittura siano assegnati solo ad utenti autorizzati.

Riferimenti:

- CWE-732(https://cwe.mitre.org/data/definitions/732.html);
- CWE-284(https://cwe.mitre.org/data/definitions/284.html).

Web Server obsoleto, non aggiornato

- **Descrizione**: il server *HTTP* utilizzato è una versione obsoleta, priva di patch e aggiornata per vulnerabilità note;
- **Modalità di individuazione**: fingerprint tramite banner HTTP e ricerca versione nei registri;
- **Rischi associati**: esposizione a exploit noti, mancanza di difesa dagli attacchi comuni ;
- **Severity**: Medio-Alta;
- **CWE di riferimento**:
  - CWE-1104 – Use of Unmaintained Third Party Components;
  - CWE-937 – Use of Out-of-date Software.
- **Soluzione**: aggiornare il web server all'ultima release.

Riferimenti:

- CWE-1104(https://cwe.mitre.org/data/definitions/1104.html);