Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing Report

64Base: 1.0.1

Marco Calenda | Corso di PTEH | A.A. 2022/23

Indice

1 Executive Summary

Il seguente documento descrive il progetto del corso di **Penetration Testing & Ethical Hacking** riguardante l'esecuzione di un'attività di Penetration Testing sulla macchina target nota come **64BASE: 1.0.1** [1]. L'obiettivo di questa attività è valutare la sicurezza della macchina target, individuare eventuali vulnerabilità e proporre contromisure efficaci per mitigare i rischi identificati. Per l'analisi, è stato adottato un approccio di tipo *Black Box*, poiché non si disponeva di informazioni dettagliate sulla macchina target né sulla struttura di rete circostante. Inoltre, va sottolineato che il test è stato eseguito all'interno della stessa rete locale della macchina target, simulando l'azione di un potenziale attaccante che abbia accesso a tale rete.

Le vulnerabilità riscontrate potrebbero consentire a un utente malevolo di acquisire il pieno controllo della macchina, causando danni significativi al sistema e mettendo a rischio i dati e gli utenti che usufruiscono dei servizi erogati dalla macchina. In altre parole, le debolezze individuate potrebbero compromettere l'integrità, la disponibilità e la confidenzialità del sistema. **Ciò implica che il livello di sicurezza della macchina è da considerarsi basso e il rischio di compromissione risulti essere elevato.**

Al fine di aumentare la sicurezza del sistema, diventa essenziale intervenire attivamente, apportando modifiche al sistema stesso al fine di eliminare le vulnerabilità rilevate. Nelle sezioni successive di questo documento, verranno presentate in dettaglio le vulnerabilità individuate, seguite dalle contromisure da adottare per affrontare efficacemente ciascuna problematica identificata.

2 Engagement Highlights

Considerando il contesto accademico del progetto, le regole che guidano l'attività di Penetration Testing non sono state definite in dettaglio, poiché l'attività non rientra in alcun accordo di non divulgazione (NDA). In particolare, non sono state poste restrizioni riguardanti gli strumenti e le tecniche utilizzabili, purché l'attività si mantenga entro i limiti della rete NAT creata appositamente per l'analisi della macchina target. Non sono stabiliti vincoli temporali o di costi. Ciononostante, è stato previsto che l'analisi, nonché la redazione dei documenti, richieda un tempo stimato di completamento pari a 20 giorni lavorativi. Le tecniche e gli strumenti utilizzati nel corso dell'attività sono descritti nel documento **Penetration Testing Summary** in allegato a questo.

L'obiettivo principale di questa attività è limitato all'analisi della macchina target. Pertanto, è espressamente vietato acquisire informazioni mediante l'utilizzo di metodologie di Intelligence, ed è altresì proibito coinvolgere altre persone nel processo di analisi. Durante l'analisi, eventuali vulnerabilità gravi identificate non verranno segnalate immediatamente bensí saranno comunicate alla conclusione dell'intero processo di analisi. Questo poiché la macchina target non offre servizi accessibili pubblicamente, quindi, non è necessario notificare prontamente le vulnerabilità più gravi riscontrate.

3 Vulnerability Report

Tramite tool automatici quali **Nessus**, **OpenVas** e **OWASP Zap** sono state rilevate vulnerabilità critiche, in particolare, la versione del sistema operativo Debian installato sulla macchina ha raggiunto la End of Life (EOF), quindi, essa non è più supportata dagli aggiornamenti di sicurezza. Altre vulnerabilità risultano avere un livello medio/basso di rischio e riguardano le seguenti aree:

- Libreria JQuery vulnerabile ad attacchi di tipo Cross-Site Scripting (XSS).
- Pagine web protette da Basic Access Authentication trasmettono credenziali in chiaro su un canale HTTP non sicuro.
- Assenza di token anti-CSRF.
- Assenza di Header anti-Clickjacking.
- Assenza di Header CSP.
- Directory navigabili.

Dall'analisi manuale invece sono state riscontrate vulnerabilità critiche che hanno permesso di prendere il controllo dell'asset e di ottenere i privilegi di root. In particolare, tramite una pagina dell'applicazione web, sono possibili attacchi di *Command Injection* che permettono l'esecuzione di comandi bash sulla macchina target. Inoltre, sull'asset è presente ed accessibile ad utenti non root la chiava privata RSA per un collegamento SSH come root sulla macchina. Infine, i permessi di alcuni utenti permettono di utilizzare un exploiit che sfrutta una versione non aggiornata e vulnerabile del comando sudo per effettuare Privilege Escalation ed ottenere l'accesso come root.

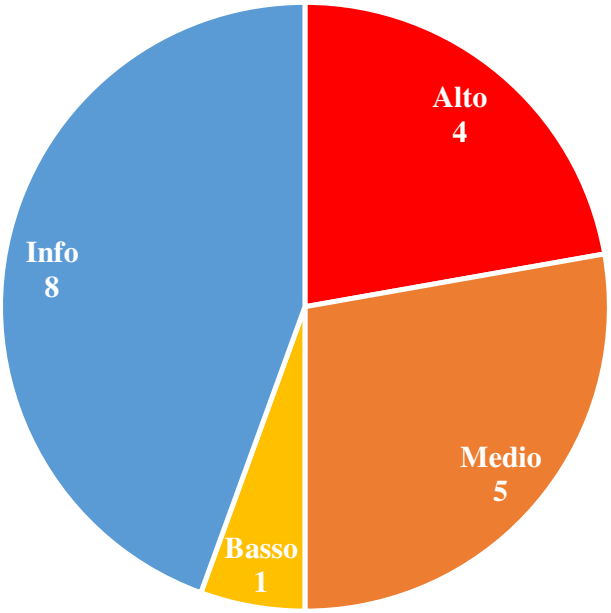
4 Remediation Report

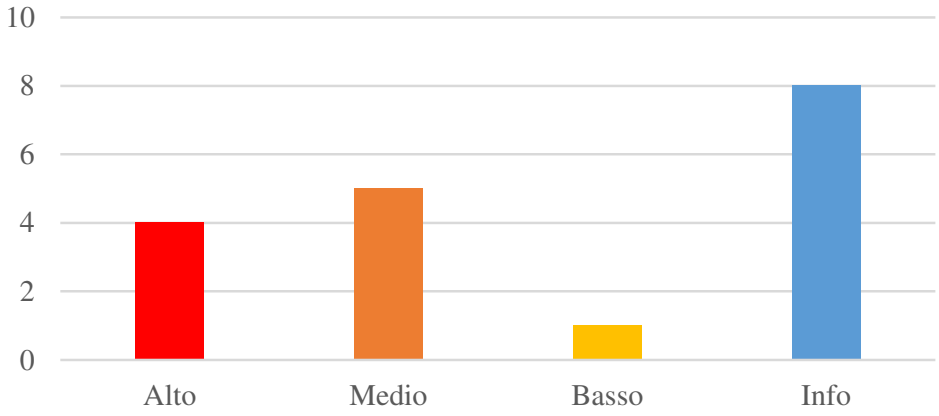
Viste le vulnerabilità identificate durante il Penetration Testing, presenteremo una serie di misure per potenziare la sicurezza del sistema e mitigare i potenziali rischi di attacco all'asset. Queste misure sono di seguito elencate in ordine di importanza, partendo dalla più urgente e procedendo verso le meno critiche:

- Aggiornare Debian ad una versione `>= 10`.
- Modificare il file `/Imperial-Class/BountyHunter/login.php` al fine di rimuovere comandi diretti al sistema operativo ed evitare attacchi di Command Injection.
- Modificare il file `/admin/flag5.jpeg` rimuovendo la chiava RSA codificata in Base64 all'interno dei metadata o consentendo l'accesso al solo utente root.
- Aggiornare sudo ad una versione `>= 1.8.28`.
- Aggiornare la libreria JQuery utilizzata dall'applicazione web ad una versione `>= 3.5.0`.
- Trasmettere le credenziali di autenticazione della pagina `/admin` tramite un canale HTTPS.
- Implementare tutte le possibili protezioni sul server web per prevenire attacchi basati sul web, come *Clickjacking* e *Cross-Site Request Forgery (CSRF)*.

5 Findings Summary

I seguenti grafici mostrano il numero di vulnerabilità presenti sulla macchina target in base della loro gravità:





6 Detailed Summary

6.1 Alto

Alto (CVSS 10.0)
La versione del sistema operativo ha raggiunto la End of Life (EOL)

Descrizione La versione del sistema operativo Debian presente sull'asset ha raggiunto la EOL.
CPE: `cpe:/o:debian:debian_linux:8`
Data EOL: `30/06/2020`

Rischio Una versione EOL di un sistema operativo non é più supportata dagli aggiornamenti di sicurezza rilasciati dal fornitore. Di conseguenza, il software potrebbe contenere molteplici vulnerabilità non corrette che potrebbero essere sfruttate da un attaccante per comprometterne la sicurezza.

Soluzione Aggiornare il sistema operativo sull'host remoto ad una versione che sia ancora supportata e che riceva aggiornamenti di sicurezza dal fornitore. In particolare, é necessario aggiornare il sistema operativo Debian ad una versione `>= 10`.

Alto
Command Injection attraverso la web application

Descrizione Mediante il file `/Imperial-Class/BountyHunter/login.php` accessibile tramite l'applicazione web, sono possibili attacchi di *Command Injection*. In particolare, il parametro HTTP `'c'` passato tramite richiesta GET esegue codice Bash sul server.

Rischio Un utente malevolo potrebbe sfruttare questa vulnerabilità per stampare informazioni riservate, caricare file sul server ed ottenere il controllo della macchina, ad esempio, tramite una TCP reverse shell.

Soluzione Il miglior approccio per evitare un attacco di *Command Injection* consiste nel negare l'esecuzione diretta di comandi del sistema operativo per mezzo del codice del layer applicativo. Qualora questo fosse inevitabile, é fondamentale modificare la logica del file `/Imperial-Class/BountyHunter/login.php` inserendo forti controlli volti a sanificare l'input fornito dall'utente.

Alto

Chiave privata RSA facilmente accessibile

Descrizione Sulla macchina è presente nella cartella `var/www/html/admin` l'immagine `flag5.jpeg` la quale sezione commento dei metadati contiene una chiave privata RSA. La chiave é utilizzata per una connessione SSH come root ed é accessibile a qualsiasi utente. La chiave é crittografata tramite l'algoritmo AES-128-CBC con una *passphrase* – quest'ultima, però, risulta essere molto debole e la cifratura é facilmente superabile tramite approcci di brute force.

Rischio Un utente malevolo che ha accesso alla macchina potrebbe sfruttare questa vulnerabilità per instaurare una connessione SSH come utente root ottenendo il pieno controllo della macchina.

Soluzione Per evitare connessioni SSH con privilegi elevati è necessario eliminare o modificare i permessi del file `flag5.jpeg` affinché possa essere acceduto solo da utente root. E' inoltre altamente consigliato crittografare la chiave RSA con una passphrase con una lunghezza maggiore di `20` caratteri alfanumerici e simboli.

Alto (CVSS: 8.8) - CVE-2019-14287 [2]

Bypass di sicurezza tramite versione vulnerabile di sudo

Descrizione L'utente 64Base può lanciare una bash come qualsiasi utente ad eccezione di root. Nelle versione di sudo `1.8.10p3` installata sulla macchina, un account sudoer con permesso di eseguire un comando come qualsiasi utente ("Runas ALL") può eludere la blacklist di politiche invocando sudo con un ID utente manipolato.

Rischio Un utente malevolo che ottiene l'accesso come 64Base può lanciare una bash come utente root malgrado questo sia esplicitamente negato nelle regole imposte nel file `/etc/sudoers`. In particolare, quando si esegue `sudo -u [id] /bin/bash`, il comando non controlla l'esistenza dello user ID specificato e, passando l'ID `-1`, questo restituisce 0 che é l'ID dell'utente root.

Soluzione E' necessario aggiornare sudo ad una versione `>= 1.8.28`.

6.2 Medio

Medio (CVSS: 6.1) - CVE-2020-11022 [3]
Versione di JQuery vulnerabile a Cross-Site Scripting (XSS)

Descrizione La versione di JQuery ospitata sul server web remoto è compresa tra la `1.2` e la `3.5.0`. Tali versioni sono affette da diverse vulnerabilità di tipo *Cross-Site Scripting (XSS)*.

Rischio Un aggressore potrebbe sfruttare tale vulnerabilità per inserire codice dannoso su una pagina web al fine di raccogliere, manipolare o reindirizzare informazioni sensibili, nonché alterare il comportamento delle pagine.

Soluzione Per evitare attacchi di tipo XSS é necessario aggiornare la liberia JQuery ad una versione `>= 3.5.0`.

Medio (CVSS: 5.3) - CWE-548 [4]
Directory navigabili

Descrizione Alcune directory sono liberamente navigabili tramite browser per visualizzarne il contenuto.

Rischio L'elenco delle directory potrebbe rivelare script nascosti, file di inclusione, file di origine di backup, ecc., ai quali si potrebbe accedere per leggere informazioni sensibili.

Soluzione Disabilitare la navigazione delle directory o, qualora questa fosse necessaria, assicurarsi che i file elencati non comportino rischi.

Medio (CVSS: 4.8) - CWE-319 [5]
Trasmissioni di credenziali su canali HTTP non sicuri

Descrizione L'applicazione web trasmette informazioni sensibili (come nomi utente e password) in chiaro tramite *Basic Access Authentication* che consiste in una richiesta HTTP contenente nell'header la codifica Base64 di nome utente e password concatenati. Le pagine vulnerabili risultano essere `/admin` e `/Imperial-Class`.

Rischio In questa situazione, un aggressore potrebbe sfruttare la vulnerabilità per eseguire un attacco *man-in-the-middle*, compromettendo o intercettando la comunicazione HTTP tra il client e il server e ottenendo così accesso a dati sensibili come nomi utente e password.

Soluzione Imporre la trasmissione di dati sensibili tramite una connessione crittografata SSL/TLS. Inoltre, assicurarsi che l'applicazione reindirizzi tutti gli utenti verso la connessione sicura prima di consentire l'inserimento di dati sensibili nelle funzioni menzionate.

Medio (CVSS: 4.3) - CWE-693 [6]
Assenza di Header anti-clickjacking

Descrizione Il web server non imposta un header di risposta X-Frame-Options né un header di risposta Content-Security-Policy 'frame-ancestors' nelle risposte HTTP.

Rischio Potenzialmente il sito é esposto ad attacchi di clickjacking o di ridirezione dell'interfaccia utente (UI redress), in cui un aggressore può ingannare l'utente facendogli fare clic su una parte della pagina vulnerabile che è diversa da quella che l'utente percepisce come parte della pagina. Questo può portare l'utente a compiere transazioni fraudolente o malintenzionate.

Soluzione Risulta importante restituire un header HTTP X-Frame-Options o un header Content-Security-Policy con la direttiva 'frame-ancestors' nella risposta della pagina. Questo impedisce che il contenuto della pagina venga caricato da un altro sito quando si utilizzano i tag HTML *frame* o *iframe*.

Medio (CVSS: 4.3) - CWE-352 [7]
Assenza di token anti Cross-Site Request Forgery (CSRF)

Descrizione L'applicazione web non effettua una verifica adeguata sul se una richiesta sia valida ed inviata in maniera legittima dall'utente che l'ha generata.

Rischio Sono possibili attacchi di tipo CSRF nel quale un utente autenticato viene ingannato nel cliccare su un link inviando automaticamente una richiesta senza il consenso dell'utente.

Soluzione Aggiornare l'applicazione includendo il supporto per i token anti-CSRF in qualsiasi form disponibile in una sessione autenticata. La maggior parte dei framework web offre soluzioni integrate o dispone di plugin che possono essere utilizzati per aggiungere facilmente questi token a qualsiasi form.

6.3 Basso

Basso (CVSS: 3.1) - CWE-1021 [8]
Assenza di Header Content Security Policy (CSP)

Descrizione Il web server non imposta un header CSP nelle risposte HTTP che garantirebbe un ulteriore strato di sicurezza. CSP fornisce un insieme di header HTTP standard che consentono di dichiarare le fonti approvate di contenuti che i browser sono autorizzati a caricare nelle pagine web.

Rischio La presenza di un header CSP aiuta a rilevare e mitigare determinati tipi di attacchi, tra cui XSS e attacchi di *Data Injection*.

Soluzione Assicurarsi che web server sia configurato per impostare l'header CSP correttamente.

6.4 Info

Le vulnerabilità di livello info sono state individuate dagli strumenti di scansione automatica, tuttavia, queste non verranno segnalate poiché non sono considerate rilevanti per potenziali attacchi. Esse si riferiscono principalmente alla possibilità di ottenere informazioni sulle versioni dei servizi esposti, e.g., Apache, HTTP.

Riferimenti bibliografici

[1] 3mrgnc3. (2016) 64base: 1.0.1 vulnhub. [Online]. Available: https://www.vulnhub.com/entry/64base-101,173 3

[2] CVE-2019-14287. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14287 9

[3] CVE-2020-11022. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022 10

[4] CWE-548. [Online]. Available: https://cwe.mitre.org/data/definitions/548 10

[5] CWE-319. [Online]. Available: https://cwe.mitre.org/data/definitions/319 11

[6] CWE-693. [Online]. Available: https://cwe.mitre.org/data/definitions/693 11

[7] CWE-352. [Online]. Available: https://cwe.mitre.org/data/definitions/352 12

[8] CWE-1021. [Online]. Available: https://cwe.mitre.org/data/definitions/1021 12