Università degli Studi di Salerno

Penetration Testing Report

HACKSUDO: FOG

Triggiani Giulio: 0522501328 | Corso di PTEH | A.A. 2023/2024

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

Executive Summary

È stata condotta un'attività di Penetration Testing sulla macchina virtuale HACKSUDO: FOG, reperibile al seguente link: https://vulnhub.com/entry/hacksudo-fog,697/ [1]. Lo scopo è stato quello di analizzare lo stato di sicurezza del sistema e suggerire contromisure appropriate per mitigare o risolvere le vulnerabilità rilevate.

L'attività di Penetration Testing è stata condotta durante il corso di PTEH, da febbraio a maggio 2024. Le uniche informazioni che abbiamo a priori sono quelle presenti sul sito della macchina, essendo molte scarse si tratta di un testing di tipo black box.

Come risultato del testing sono emerse molte vulnerabilità ad alto rischio che hanno compromesso la macchina e non sono state implementate adeguate contromisure di sicurezza.

Il report contiene un'analisi dettagliata di tutte le vulnerabilità trovate durante lo svolgimento del testing, unitamente a tutte le contromisure per ovviare ai rischi a cui il sistema è esposto.

Engagement Highlights

L'attività di Penetration Testing è stata svolta nell'ambito di un progetto per il corso di Penetration Testing and Ethical Hacking (PTEH) erogato dall'Università degli Studi di Salerno. Le regole di ingaggio fanno seguito al regolamento del corso ed alle relative istruzioni e requisiti forniti dal docente per il superamento dell'esame finale.

Non sono state indicate, da parte del docente, particolari limitazioni sul tipo di analisi da effettuare e sulle metodologie da applicare, inoltre non sono state imposte limitazioni sui tools da utilizzare e sul tipo di testing da effettuare, infine non sono stati imposti limiti alla condivisione di informazioni relative all'asset analizzato, non si rende dunque necessaria la stipula di un accordo di non divulgazione.

Hacksudo: Fog è una macchina virtuale contenete una sfida CTF progettata per gli utenti del server Discord InfoSec Prep. Non vengono fornite ulteriori informazioni sulla macchina.

Il processo di Penetration Testing verrà eseguito in un ambiente virtualizzato all'interno di Virtual Box in cui saranno presenti solamente la macchina Kali per il Penetration Testing e l'asset da analizzare. Le due macchine saranno connesse attraverso una rete ad hoc.

L'obiettivo di questa attività di Penetration testing è quello di trovare tutte le vulnerabilità possibili all'interno dell'asset e possibilmente fornire per ciascuna di esse delle azioni correttive per migliorare la sicurezza collettiva della macchina.

Vulnerability Report

Nel Corso dell'attività di penetration testing sono state trovate varie vulnerabilità che espongono il sistema a notevoli rischi. Di seguito viene fornito un elenco sintetico di queste ultime.

- Apache Webserver presenta una vulnerabilità per la quale un attaccante potrebbe creare dei pacchetti ad hoc e sfruttando un errore chiamato buffer overflow eseguire del codice arbitrario nel sistema.
- OpenSSH presenta una vulnerabilità per la quale, in abbinamento con alcune estensioni presenti in OpenSSH permette ad attaccanti remoti di bypassare i controlli di integrità in modo da compromettere la connessione tra client e server causando il malfunzionamento o la disabilitazione completa di alcune funzionalità di sicurezza.
- OpenSHH presenta una vulnerabilità per la quale un utente malintenzionato potrebbe impiegare nomi di oggetti creati ad arte, all'interno della visualizzazione dell'avanzamento del server, per manipolare l'output del client per nascondere ad esempio il trasferimento di file dannosi.
- OpenSSH presenta una vulnerabilità per la quale un attaccate potrebbe aggirare le restrizioni di sicurezza attraverso il nome del file.
- CMS Made Simple è affetto da una vulnerabilità, denominata SQL Injection, che permette ad un attaccante remoto di eseguire comandi arbitrari sulla macchina.
- Il web server presenta delle cartelle che sono navigabili.
- La Web App risulta vulnerabile al Clickjacking mettendo a rischio le informazioni degli utenti e la navigazione di questi ultimi.
- La Web App presenta alcuni errori di cattiva programmazione che portano a problemi di sicurezza come commenti che suggeriscono come decodificare un file o dizionari con possibili password per utenti del sistema.

Remediation Report

La machina Hacksudo:fog possiede un grado di rischio molto elevato e numerose vulnerabilità. Di seguito vengono elencate alcune procedure per migliorare la sicurezza complessiva del sistema e mitigarne le vulnerabilità.

- Progettare un piano per risolvere le vulnerabilità a rischio critico, alto e medio, risolvendole in ordine decrescente di priorità.
- Implementare un ciclo di vita di sviluppo e manutenzione sicuro per l'applicazione web.
- Eseguire regolarmente controlli di sicurezza.
- Mantenere sempre aggiornati OpenSSH, Apache Webserver alle ultime versioni in modo da avere sempre a disposizione gli aggiornamenti di sicurezza più recenti ed eliminare le vulnerabilità che non dipendono in modo diretto dalla gestione del sistema.
- Modificare la configurazione del webserver per rendere le directory non navigabili.
- Modificare il comportamento della Web Application in modo da non rendere più possibile il Clickjacking.
- Aggiornare CMS Made Simple all'ultima versione disponibile in modo da non rendere più possibile l'SQL Injection.
- Applicare pratiche di buona programmazione non lasciando in giro informazioni o file che potrebbero compromettere la sicurezza della macchina.

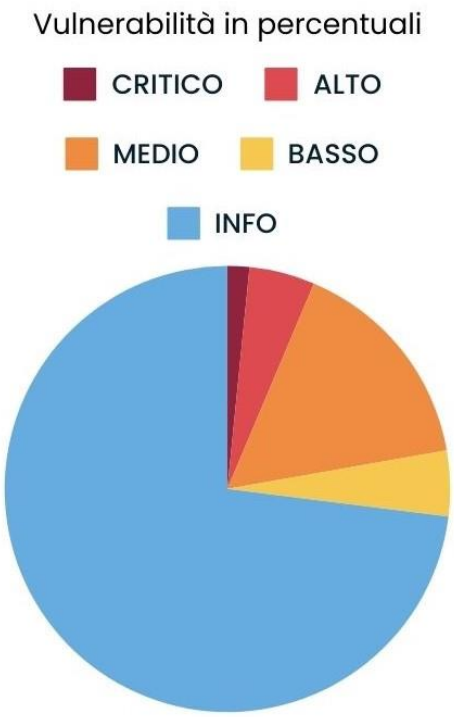
Findings Summary

Di seguito verrà fornita una panoramica generale sullo stato di sicurezza dell'asset analizzato, le vulnerabilità sono state suddivise in cinque classi di gravita.

10.0.2.7

CRITICO: 1	ALTO: 3	MEDIO: 10	BASSO: 3	INFO: 46

Di seguito dei grafici che mostrano le vulnerabilità.



Detailed Summary

Di seguito sono descritte in maniera dettagliata tutte le vulnerabilità trovate.

CVE-2021-44790 [2]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: critico

lDescrizione: Il corpo di una richiesta creato appositamente può causare un buffer overflow nel parser multipart (r:parsebody() chiamato da script Lua) di mod_lua. Questo problema riguarda Apache HTTP Server 2.4.51 e precedenti.

Rischi: Il buffer overflow può permettere ad un attaccante di modificare i puntatori del sistema e consentire la chiamata di funzioni contenenti codice arbitrario.

Mitigazione: Aggiornare Apache Webserver alla versione più recente.

CVE-2019-16905 [3]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: alto

Descrizione: OpenSSH da 7.7 a 8.x se il client o il server sono configurati per usare una chiave XMSS presenta un problema di integer overflow.

Rischi: Potrebbe portare alla corruzione della memoria e all'esecuzione di codice locale arbitrario.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

CVE-2021-41617 [4]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: alto

Descrizione: In OpenSSH dalla versione 6.2 alla 8.x, quando vengono usate alcune configurazioni non predefinite, consente privilege escalation poiché i gruppi supplementari non vengono inizializzati come previsto.

Rischi: Consente privilege escalation.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

CMS Made Simple < 2.2.10 – SQL Injection (CVE-2019-9053) [5]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: alto

Descrizione: In CMS Made Simple fino alla versione 2.2.8 è presente una vulnerabilità attraverso la quale sfruttando un URL modificato è possibile effettuare una SQL Injection non autenticata.

Rischi: SQL Injection non autenticata.

Mitigazione: Aggiornare CMS Made Simple alla versione più recente.

SSH Terrapin Prefix Truncation Weakness [6]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: Il server SSH remoto è vulnerabile ad un attacco man in the middle di troncamento del prefisso.

Rischi: Ciò può consentire ad un aggressore remoto di aggirare i controlli di integrità e di ridurre la sicurezza della connessione.

Mitigazione: Aggiornare SHH alla versione più recente.

Browsable Web Directories [7]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: Alcune directory del web server remoto sono navigabili.

Rischi: Directory navigabili espongono il web server alla fuoriuscita di informazioni sensibili

Mitigazione: Assicurarsi che le directory navigabili non contengano informazioni sensibili, utilizzare restrizioni d'accesso o disabilitare l'indicizzazione per le directory che le contengono.

ICMP Timestamp Request Remote Date Disclosure [8]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: Si può determinare l'ora esatta impostata sull'host remoto.

Rischi: Può essere utile ad un utente remoto male intenzionato non autenticato a superare protocolli di autenticazione basati sul tempo.

Mitigazione: Filtrare le richieste ICMP timestamp e le risposte ICMP timestamp in uscita.

Web Application Potentially Vulnerable to Clickjacking [9]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: Il server Web remoto potrebbe non riuscire a mitigare una classe di vulnerabilità delle applicazioni web.

Rischi: Il server Web remoto non imposta un'intestazione di risposta X-Frame-Options o un'intestazione di risposta Content-Security-Policy "frame-ancestors" in tutte le risposte di contenuto. Ciò potrebbe esporre il sito ad un attacco di clickjacking o UI redress, in cui un aggressore può indurre un utente a fare clic su un'area della pagina vulnerabile diversa da quella che l'utente percepisce come pagina. Questo può portare l'utente a eseguire transazioni fraudolente o dannose.

Mitigazione: Restituire l'intestazione http X-Frame_Options o Content-Security-Policy con la risposta della pagina. Questo impedisce che il contenuto della pagina venga reso ad un altro sito quando si utilizzano i tag HTML frame o iframe.

CVE-2023-48795 [10]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: Il protocollo di trasporto SSH con alcune estensioni OpenSSH, prima della versione 9,6, consente ad aggressori remoti di bypassare i controlli di integrità ed omettere alcuni pacchetti. Accade poiché il protocollo SSH Binary Packet Protocol (BPP), implementato da queste estensioni, gestisce male la fase di handshake e l'uso di numeri di sequenza.

Rischi: Il client e il server potrebbero ritrovarsi con una connessione per la quale alcune funzionalità di sicurezza sono state disabilitate.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

CVE-2019-6111 [11]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: Il server scp sceglie quali file/directory inviare al client; tuttavia, il client esegue una convalida sommaria del nome dell'oggetto restituito.

Rischi: Un server scp dannoso potrebbe sovrascrivere file arbitrari nella directory di destinazione, se viene eseguita un'operazione ricorsiva il server può manipolare anche le sottodirectory.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

CVE-2019-6110 [12]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: A causa dell'accettazione e della visualizzazione di output stdrr arbitrario da parte del server.

Rischi: Un server dannoso o un attaccante MITM potrebbe manipolare l'output del client per nascondere file dannosi trasferiti.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

CVE-2019-6109 [13]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: A causa della mancata codifica dei caratteri nella visualizzazione dell'avanzamento, un attaccante MITM potrebbe impiegare nomi di oggetti creati ad hoc per manipolare l'output del client.

Rischi: Un attaccante potrebbe usare questo problema per nascondere file dannosi trasferiti al sistema.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

CVE-2020-14145 [14]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: Da OpenSSH 5.7 a 8.4 è presente una discrepanza nella negoziazione dell'algoritmo che porta ad una perdita di informazioni.

Rischi: Consente ad attaccanti MITM di colpire i tentativi di connessione iniziali.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

CVE-2016-20012 [15]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: medio

Descrizione: OpenSSH fino alla versione 8.7 consente ad attaccanti remoti di verificare una combinazione di nome utente e password sia nota ad un server SSH

Rischi: Consente il fuzzing della password.

Mitigazione: Aggiornare OpenSSH alla versione più recente.

Web Server Allows Password Auto-Completion [16]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: basso

Descrizione: Il Web server permette l'auto completamento delle password.

Rischi: I campi con l'auto completamento portano ad una perdita di riservatezza per gli utenti che ne fanno uso.

Mitigazione: Aggiungere l'attributo "autocomplete=off" ai campi che fanno uso di auto completamento delle password per impedirlo.

Web Server Transmits Cleartext Credentials [17]

Host: Hacksudo: Fog (10.0.2.7)

Rischio: basso

Descrizione: Il server Web remoto potrebbe trasmettere le credenziali in chiaro.

Rischi: Un attaccante che intercetta il traffico tra il Web browser e il server potrebbe ottenere le credenziali di utenti validi.

Mitigazione: Assicurarsi di trasmettere informazioni sensibili tramite HTTPS.

CVE-2018-20685 [18]
Host: Hacksudo: Fog (10.0.2.7)
Rischio: basso
Descrizione: Consente a server SSH remoti di aggirare le restrizioni di accesso previste tramite il nome del file.
Rischi: Un attaccante potrebbe modificare i permessi della directory di destinazione lato client.
Mitigazione: Aggiornare OpenSSH alla versione più recente.

References

[1] V. Waghmare, "VulnHub," [Online]. Available: https://vulnhub.com/entry/hacksudo-fog,697/.

[2] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-44790.

[3] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-16905.

[4] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-41617.

[5] D. Scanu, "Exploit Databese," [Online]. Available: https://www.exploit-db.com/exploits/46635.

[6] Nessus, "Tenable," [Online]. Available: https://www.tenable.com/products/nessus.

[7] Nessus, "Tenable," [Online]. Available: https://www.tenable.com/products/nessus.

[8] Nessus, "Tenable," [Online]. Available: https://www.tenable.com/products/nessus.

[9] Nessus, "Tenable," [Online]. Available: https://www.tenable.com/products/nessus.

[10] Nist, "NVD Nistt," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-48795.

[11] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-6111.

[12] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-6110.

[13] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-6109.

[14] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-14145.

[15] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-20012.

[16] Nessus, "Tenable," [Online]. Available: https://www.tenable.com/products/nessus.

[17] Nessus, "Tenable," [Online]. Available: https://www.tenable.com/products/nessus.

[18] Nist, "NVD Nist," [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-20685.