UNIVERSITÀ DEGLI STUDI DI SALERNO

CORSO DI PENETRATION TESTING AND ETHICAL HACKING

Penetration Testing Report

Harry Potter: Fawkes

Prof:
Arcangelo Castiglione

Studente:
Simone MASULLO
Mat. 0522501369

ANNO ACCADEMICO 2023/2024

Indice

Elenco delle figure

Elenco delle tabelle

1. Executive Summary

Lo studente Simone Masullo ha condotto un'attività di Penetration Testing sull'asset Harry Potter: Fawkes [19] - disponibile su VulnHub - al fine di identificarne le vulnerabilità e le debolezze. L'asset analizzato consiste in un'unica macchina virtuale con indirizzo IP locale **10.0.2.10**. Oltre all'analisi della sicurezza delle versioni dei protocolli e degli applicativi presenti, sono state adottate tecniche ad hoc per l'analisi dell'applicazione web erogata attraverso la porta 80. Non è stata fornita alcuna informazione preventiva dal committente, dunque si è proceduto ad eseguire un'analisi di tipo black-box. L'attività di Penetration Testing condotta è stata avviata il giorno 28/05/2024 ed è terminata il giorno 06/07/2024. Come risultato dell'attività sono state trovate diverse vulnerabilità che comportano un **rischio alto** per la sicurezza dell'asset, valutato anche in base alla difficoltà nello sfruttamento delle vulnerabilità riscontrate. Il processo di Penetration Testing è culminato con l'acquisizione di privilegi di amministrazione sulla macchina virtuale. Nei capitoli successivi di questo documento verranno mostrate con maggiore dettaglio le vulnerabilità che affliggono l'asset. In genera-

le il rischio per la sicurezza dell'asset è **alto** ma, con l'adozione di opportune contromisure, è possibile rapidamente ottenere un buon livello di sicurezza. Un rapido elenco delle contromisure da adottare è presente di seguito, stipulato in ordine di quella che - secondo il parere del pentester - è l'urgenza di adozione (decrescente). Per maggiori dettagli si rimanda al capitolo 4 del presente documento. Le contromisure suggerite sono:

1. Utilizzo di funzioni sicure che impediscano attacchi di tipo *buffer overflow* all'interno degli applicativi, con maggiore attenzione a tutti quei programmi con cui un utente può interagire. Particolare riguardo va posto nei confronti dell'applicativo esposto tramite la porta 9898;

2. Utilizzo esclusivamente di *protocolli sicuri*, in particolare sostituzione del protocollo **FTP** erogato attraverso la porta 21 con la sua versione sicura che non trasmette i dati in chiaro: **SFTP**;

3. Aggiornamento del sistema operativo e della versione dell'applicativo **sudo** sulla macchina Fawkes;

4. Gestione dell'autenticazione per il protocollo FTP (o SFTP) sulla porta 21. In particolare è altamente sconsigliato abilitare l'accesso anonimo, ovvero consentire l'accesso alle risorse condvise senza richiedere preventivamente autenticazione dell'utente;

5. Maggiore protezione del file eseguibile relativo all'applicativo **server_hogwarts**, il quale è attualmente accessibile tramite il protocollo FTP. Un attaccante che entra in possesso di tale file binario può analizzarlo al fine di identificare vulnerabilità nel servizio esposto attraverso la porta 9898;

6. Aggiornamento generale delle versioni degli applicativi utilizzati, nonché dei sistemi operativi della macchina virtuale e del container in essa presente.

2. Engagement Highlights

In questo capitolo vengono presentate le regole di ingaggio stipulate con il committente dell'attività di Penetration Testing. L'asset in analisi è noto con il nome di "Harry Potter: Fawkes" ed è una macchina virtuale nata a scopo didattico presente sul sito web VulnHub [19].

2.1. Identificazione del committente

Il committente dell'attività di Penetration Testing è il prof. Arcangelo Castiglione dell'Università degli Studi di Salerno, con il quale la comunicazione avverrà via e-mail all'indirizzo "arcastiglione@unisa.it".

2.2. Accordo di non divulgazione

Nonostante la natura didattica dell'asset in analisi, si considera la presenza di un accordo di non divulgazione (**non disclosure agreement**). A seguito della stipula dell'accordo di riservatezza, il penetration tester si impegna a non divulgare informazioni sensibili

che possano compromettere la sicurezza dell'asset. Per informazioni sensibili si intendono tutte quelle informazioni, ottenute durante il processo di analisi condotto, che non siano già di pubblico dominio.

2.3. Informazioni preliminari

Nono sono state fornite informazioni preliminiari sull'asset target, dunque si procederà con un'analisi di tipo **black-box**.

2.4. Tecniche e strumenti consentiti

Trattandosi di una macchina nata a scopo didattico, è possibile eseguire qualsivoglia tipo di attività poiché essa non comporta criticità nel funzionamento del sistema. Naturalmente, non essendo l'asset caratterizzato da una componente umana, tutte le attività che riguardano questa sfera - come tecniche di social engineering - non possono essere praticate.

2.5. Periodo di attività

L'attività di penetration testing è stata avviata il giorno 28 maggio 2024 e la sua terminazione è prevista entro e non oltre il giorno 10 luglio 2024. Tale scadenza è stata valutata tenendo conto del margine di tempo necessario alla valutazione della documentazione prodotta rispetto alla data in cui si intende sostenere la prova d'esame, fissata preventivamente dal committente.

2.6. Budget stimato

Trattandosi di un progetto in ambito universitario il cui unico scopo è quello di consentire al committente di valutare le abilità dello studente nell'utilizzo degli strumenti e delle tecniche introdotti durante il corso, l'attività di penetration testing non ha un budget di riferimento. Ogni eventuale spesa sostenuta durante lo svolgimento dell'attività sarà a carico del pentester.

2.7. Risultati attesi

In accordo con il committente, i documenti la cui consegna è prevista al termine dell'attività di penetration testing sono *nr. 1 Penetration Testing Report* conforme ad uno dei template analizzati durante il corso e *nr. 1 documento di replicabilità* allo scopo di fornire informazioni sugli strumenti utilizzati e di consentire ad un eventuale altro soggetto di replicare l'attività condotta ottenendo gli stessi risultati. I documenti elencati verranno consegnati in formato PDF, accompagnati da *nr. 1 presentazione digitale* - anch'essa in formato PDF - prodotta in merito all'attività di penetration testing svolta. Tutta la documentazione verrà consegnata al prof. Arcangelo Castiglione, tramite posta ordinaria, utilizzando account facenti parte dell'organizzazione UniSa.

2.8. Test plan

Il piano di testing seguito durante il processo di penetration testing effettuato, prevede diverse fasi:

1. **Information Gathering**: si cercherà di ottenere quante più informazioni possibili sull'asset in analisi;

2. T**arget Discovery**: si cercheranno eventuali informazioni aggiuntive che possano aiutare ad identificare tutte le risorse facenti parte dell'asset in analisi come macchine attive;

3. **Enumerating Target**: verrà eseguita allo scopo di ottenere maggiori informazioni sull'asset, sul sistema operativo delle macchine identificate, sulle versioni dei servizi erogati dalle diverse macchine facenti parte dell'asset;

4. **Vulnerability Mapping**: in questa fase verranno elencate le vulnerabilità ed i problemi di sicurezza identificati all'interno dell'asset in analisi, nonché le conseguenze di un eventuale sfruttamento di tali vulnerabilità da parte di attaccanti;

5. **Target Exploitation**: data la natura didattica dell'asset in analisi, la fase di target exploitation non richiede alcun accordo preliminare e verrà eseguita, senza alcuna limitazione su tecniche o strumenti adottati, allo scopo di simulare un attaccante che, scoperte le vulnerabilità che affliggono l'asset in

analisi, tenta di sfruttarle per ottenere accesso a risorse a cui non potrebbe normalmente accedere;

6. **Post-exploitation**: verranno adottate tecniche di post exploitation per poter effettuare **privilege escalation** e **mantenimento dell'accesso** tramite installazione di backdoor. Tutte le backdoor introdotte in questa fase verranno documentate e successivamente eliminate per non compromettere l'asset.

3. Vulnerability Report

In questo capitolo vengono riportate le vulnerabilità trovate e l'impatto che costituiscono sulla sicurezza dell'asset. Per un maggiore dettaglio si rimanda al capitolo 5. Di seguito le vulnerabilità che hanno concorso alla compromissione dell'asset in analisi:

- È presente una vulnerabilità nel software **server_hogwarts**, in esecuzione sulla porta 9898, che consente ad un utente malintenzionato di inserire input malevolo che può portare all'esecuzione di codice arbitrario sulla macchina che ospita tale server. Tale vulnerabilità è dovuta ad una debolezza nel codice che consente attacchi di tipo *buffer overflow*.

- Sono presenti due vulnerabilità nella versione dell'applicativo **sudo** sulla macchina target che consentono, ad un utente con accesso locale, di ottenere privilegi di amministratore (root).

- È presente una debolezza nella configurazione del protocollo FTP esposto tramite la porta 21 che consente a chiunque di accedere ai file condivisi senza necessità di autenticazione.

- È presente una vulnerabilità nella versione del protocollo SSH che consente ad un attaccante di bypassare i controlli di sicurezza.

- Il protocollo FTP utilizzato trasmette i dati in chiaro e ciò comporta che un utente che possa leggere il traffico di rete ha accesso ad informazioni sensibili degli utenti che interagiscono con tale protocollo.

- All'interno del sistema containerizzato che espone il servizio sulla porta 9898 è possibile eseguire qualsiasi operazione con privilegi di amministratore senza necessità di autenticazione.

- Sono state trovate le credenziali di accesso per uno degli utenti memorizzate in chiaro sul sistema target.

- È presente una vulnerabilità nella versione del protocollo SSH utilizzato che consente ad un attaccante di generare traffico malevolo al fine di causare denial of service (DOS).

- È presente una vulnerabilità nella versione del protocollo FTP utilizzato che consente ad un attaccante di generare traffico malevolo al fine di causare denial of service (DOS).

- È presente una vulnerabilità nella versione di Apache HTTP utilizzata che consente ad un utente di sfruttare una race condition al fine di manipolare un sistema di autenticazione per

ottenere accesso non legittimo con uno username diverso dal proprio.

- È presente una vulnerabilità nella versione di Apache HTTP utilizzata che consente ad un attaccante di generare traffico malevolo al fine di causare denial of service (DOS).

4. Remediation Report

Di seguito vengono suggerite alcune contromisure da adottare per mitigare i problemi riscontrati. Si specifica che le seguenti tecniche e mitigazioni non sono da sostituire ad un'ulteriore analisi approfondita delle vulnerabilità elencate e delle soluzioni ad esse. Il pentester incaricato dell'analisi resta disponibile a fornire supporto nell'attività di correzione delle vulnerabilità trovate.

4.1. Messa in sicurezza del software server_hogwarts

Il software in questione presenta errori di implementazione. In particolare non è presente un adeguato controllo della taglia dell'input dell'utente che comporta la possibilità per un attaccante di inserire una stringa malevola al fine di eseguire codice arbitrario. I rimedi da porre in atto per mitigare tale debolezza sono:

1. **controllo della taglia dell'input:** è importante evitare l'utilizzo di funzioni che non eseguano tale controllo, come **strcpy, gets, ...** È possibile sostituirle con funzioni che effettuino tale controllo come **strncpy, fgets, ...**;

2. **limitazione dell'input dell'utente:** piuttosto che consentire l'inserimento di stringhe arbitrarie, data la natura del software, sarebbe preferibile limitare l'input dell'utente alla scelta di opzioni presentate.

4.2. Autenticazione al server FTP

È sempre preferibile consentire l'accesso al server FTP previa autenticazione dell'utente. Per mitigare la debolezza riscontrata è dunque possibile disabilitare l'accesso anonimo.

4.3. Sostituzione del protocollo FTP

Piuttosto che utilizzare un protocollo FTP che non si preoccupa di garantire la confidenzialità della conversazione tra server e client, è preferibile utilizzare una versione sicura (SFTP) che utilizzi tecniche di cifratura.

4.4. Aggiornamento degli applicativi

È fondamentale tenere costantemente aggiornati gli applicativi presenti sul sistema in quanto gli sviluppatori rilasciano periodicamente patch al fine di mitigare le vulnerabilità in essi presenti. Si consiglia dunque l'immediato aggiornamento di software per i quali sono state riscontrate vulnerabilità (sudo, apache http, openssh, ...)

e non. Da tale lista non viene escluso il sistema operativo, anch'esso soggetto a vulnerabilità.

4.5. Miglioramento della politica di controllo degli accessi

Anche se ci si trova in un ambiente containerizzato, una politica di controllo degli accessi debole può comportare gravi rischi per la sicurezza dell'asset. In particolare, l'utente **harry** dell'ambiente containerizzato che espone il servizio sulla porta 9898, può sempre eseguire qualsiasi operazione come *super user* senza necessità di inserire la propria password. Tale possibilità è assolutamente da inibire.

4.6. Formazione del personale

Sono state trovate in un file liberamente accessibile le credenziali dell'utente **harry** per l'accesso al sistema containerizzato. È fondamentale formare il personale al fine di evitare comportamenti che possono mettere a rischio la sicurezza del sistema. In particolare, le credenziali di autenticazione di qualsiasi utente devono essere protette nel miglior modo possibile. Ciò implica l'adozione di tecniche crittografiche avanzate nei sistemi di memorizzazione delle credenziali, nonché una maggiore consapevolezza da parte dello staff.

4.7. Implementazione di sistemi di sicurezza avanzati

Sulla macchina target non sono presenti sistemi di sicurezza come firewall che possano prevenire attacchi di tipo Denial of Service (DOS) o il rilascio di informazioni sensibili. È stato infatti possibile effettuare scansioni sul sistema senza alcun problema da parte di un host presente sulla stessa rete. È generalmente preferibile configurare la rete - e nel caso specifico le interazioni che la macchina virtuale ha con essa - in modo che tra le risorse accessibili dall'esterno e quelle interne siano presenti strati di protezione.

5. Findings Summary

In questo capitolo vengono mostrati con dettaglio tutti i problemi di sicurezza identificati durante l'attività di penetration testing. Al fine di garantire una valutazione oggettiva e misurabile della gravità delle vulnerabilità viene adottato il **Common Vulnerability Scoring System (CVSS) 3.1**. La categorizzazione per *severity* è conforme a tale criterio di valutazione. Si precisa che la valutazione oggettiva delle vulnerabilità comporta una mancata contestualizzazione delle stesse: più vulnerabilità che non vengono considerate gravi dalle metriche utilizzate potrebbero comportare un rischio di sicurezza elevato per l'asset quando coesistenti nello stesso sistema.

5.1. Descrizione delle vulnerabilità riscontrate

In tabella 5.1 è presente la lista delle vulnerabilità identificate nell'asset.

CVE ID	**Descrizione della vulnerabilità**	**CVE Score**	**Severity**
CVE-2018-7566 [2]	Il kernel Linux 4.15 presenta un buffer overflow attraverso un'operazione di scrittura ioctl SNDRV_SEQ_IOCTL _SET_CLIENT_POOL su /dev/snd/seq da parte di un utente locale.	7.8	High

CVE-2018-8781 [3]	La funzione udl_fb_mmap in drivers/gpu/drm/udl/udl_fb.c nel kernel Linux versione 3.4 e fino alla 4.15 inclusa presenta una vulnerabilità di tipo integer-overflow che consente agli utenti locali con accesso al driver udldrmfb di ottenere autorizzazioni complete di lettura e scrittura sulle pagine fisiche del kernel, con conseguente esecuzione di codice nello spazio kernel.	7.8	High
CVE-2021-30047 [9]	VSFTPD 3.0.3 consente agli attaccanti di causare un denial of service a causa del numero limitato di connessioni consentite.	7.5	High

CVE-2019-0211 [4]	In Apache HTTP Server 2.4 release da 2.4.17 a 2.4.38, con evento MPM, worker o prefork, il codice in esecuzione in processi o thread figli con privilegi minori (compresi gli script eseguiti da un interprete di scripting in-process) potrebbe eseguire codice arbitrario con i privilegi del processo padre (solitamente root).	7.8	High
CVE-2019-0215 [5]	In Apache HTTP Server 2.4 release 2.4.37 e 2.4.38, un bug in mod_ssl quando si utilizzava la verifica del certificato client per-location con TLSv1.3 permetteva a un client di aggirare le restrizioni di controllo dell'accesso configurate.	7.5	High

CVE-2019-0217 [6]	In Apache HTTP Server 2.4 release 2.4.38 e precedenti, una race condition in mod_auth_digest durante l'esecuzione in un server threaded potrebbe consentire a un utente con credenziali valide di autenticarsi utilizzando un altro nome utente, aggirando le restrizioni di controllo degli accessi configurate.	7.5	High

CVE-2021-3156 [10]	Sudo prima della versione 1.9.5p2 contiene un errore off-by-one che può causare un buffer overflow basato su heap, che consente l'escalation dei privilegi a root tramite "sudoedit -s" e un argomento della riga di comando che termina con un singolo carattere backslash.	7.8	High

CVE-2023-22809 [11]	In Sudo prima della 1.9.12p2, la funzione sudoedit (alias -e) gestisce male gli argomenti extra passati nelle variabili d'ambiente fornite dall'utente (SUDO_EDITOR, VISUAL e EDITOR), consentendo a un attaccante locale di aggiungere voci arbitrarie all'elenco dei file da elaborare. Questo può portare all'escalation dei privilegi. Le versioni interessate sono dalla 1.8.0 alla 1.9.12.p1.	7.8	High
CVE-2023-48795 [12]	Il protocollo di trasporto SSH (OpenSSH 9.6) consente agli aggressori remoti di aggirare i controlli di integrità in modo che alcuni pacchetti vengano omessi.	5.9	Medium

CVE-2019-20908 [8]	È stato rilevato un problema in drivers/firmware/efi/efi.c nel kernel Linux precedente alla versione 5.4. Permessi di accesso errati per la variabile ACPI efivar_ssdt potrebbero essere utilizzati dagli aggressori per aggirare le restrizioni di lockdown o di avvio sicuro, alias CID-1957a85b0032.	6.7	Medium

CVE-2023-51384 [13]	In ssh-agent in OpenSSH prima della versione 9.6, alcuni vincoli di destinazione possono essere applicati in modo incompleto. Quando i vincoli di destinazione sono specificati durante l'aggiunta di chiavi private ospitate da PKCS#11, questi vincoli vengono applicati solo alla prima chiave, anche se un token PKCS#11 restituisce più chiavi.	5.5	Medium

CVE-2023-51385 [14]	In ssh in OpenSSH prima della versione 9.6, potrebbe verificarsi un'iniezione di comandi OS se il nome di un utente o di un host ha metacaratteri di shell e questo nome è referenziato da un token di espansione in determinate situazioni. Ad esempio, un repository Git non attendibile può avere un sottomodulo con metacaratteri di shell in un nome utente o host.	6.5	Medium

CVE-2019-0220 [7]	È stata riscontrata una vulnerabilità in Apache HTTP Server da 2.4.0 a 2.4.38. Quando il componente percorso di un URL di richiesta contiene più slash consecutivi ('/'), le direttive come LocationMatch e RewriteRule devono tenere conto dei duplicati nelle espressioni regolari, mentre altri aspetti dell'elaborazione del server li annullano implicitamente.	5.3	Medium
CVE-1999-0524 [1]	Informazioni ICMP come (1) netmask e (2) timestamp sono consentite da host arbitrari.	2.1	Low

Tabella 5.1: Riepilogo delle vulnerabilità identificate

5.2. Descrizione delle debolezze riscontrate

In tabella 5.2 sono presenti le debolezze identificate all'interno dell'asset.

CWE ID	**Descrizione della debolezza**
CWE-120 [15]	Copia di un buffer senza controllo della taglia dell'input ('Buffer Overflow')
CWE-256 [16]	Memorizzazione in chiaro di Password
CWE-284 [17]	Mancato controllo degli accessi
CWE-285 [18]	Mancata autorizzazione

Tabella 5.2: Riepilogo delle debolezze identificate

5.3. Suddivisione delle vulnerabilità per severity

In Figura 5.1 è presente un diagramma che mostra la suddivisione in gravità delle vulnerabilità riscontrate.

5.4. Vulnerability breakdown

In questa sezione le vulnerabilità sono suddivise per risorsa interessata. In particolare, sono considerate risorse differenti il container che espone il servizio sulla porta 9898 e la macchina virtuale con

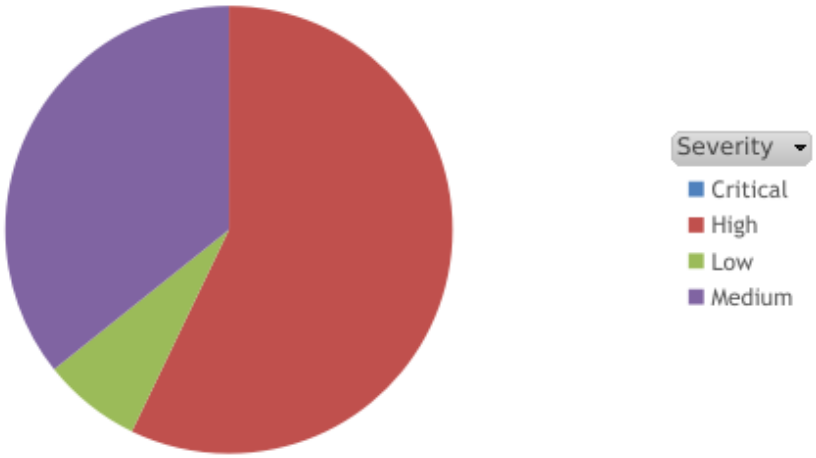

Figura 5.1: Diagramma delle vulnerabilità

hostname Fawkes. Nonostante il container sia ospitato sulla macchina virtuale Fawkes, dunque non è propriamente una risorsa separata, è stato considerato utile fornire una separazione dei due ambienti per consentire una più semplice identificazione e mitigazione dei problemi.

5.4.1. Vulnerabilità del container

Il container è affetto dalle vulnerabilità in tabella 5.3 (per la visualizzazione dettagliata delle vulnerabilità si rimanda alla tabella 5.1 o alle relative schede tecniche presentate al capitolo 6).

Inoltre presenta i seguenti problemi:

- l'utente **harry** ha accesso a tutti i comandi in qualità di super user senza richiesta di autenticazione;
- è presente un file contenente le credenziali dell'utente **harry**;

CVE-ID	Componente
CVE-2021-3156 [10]	sudo
CVE-2023-22809 [11]	sudo
CVE-2021-30047 [9]	ftp
CVE-2023-48795 [12]	OpenSSH
CVE-2023-51384 [13]	OpenSSH
CVE-2023-51385 [14]	OpenSSH
CVE-1999-0524 [1]	Politica di filtraggio

Tabella 5.3: Tabella delle vulnerabilità del container

- il servizio esposto attraverso la porta 21 non fa utilizzo di crittografia, è dunque possibile visualizzare i dati trasmessi in chiaro;

5.4.2. Vulnerabilità di Fawkes

L'host Fawkes è affetto dalle vulnerabilità in tabella 5.4.

5.5. Valutazione dei rischi

Nella seguente sezione viene presentata una lista di rischi per la sicurezza dell'asset. Ad ognuno dei rischi viene attribuito un punteggio da 1 a 4 indicante la gravità del rischio ed un valore da A ad E indicante la frequenza del rischio. La frequenza del rischio tiene conto della facilità con cui un attaccante riesce a sfruttare la relativa vulnerabilità. La legenda contenente il significato di tali

CVE-ID	Componente
CVE-2018-7566 [2]	OS Kernel
CVE-2018-8781 [3]	OS
CVE-2019-0211 [4]	Apache HTTP
CVE-2019-0215 [5]	Apache HTTP
CVE-2019-0217 [6]	Apache HTTP
CVE-2021-3156 [10]	sudo
CVE-2023-22809 [11]	sudo
CVE-2023-48795 [12]	OpenSSH
CVE-2019-20908 [8]	OS
CVE-2023-51384 [13]	OpenSSH
CVE-2023-51385 [14]	OpenSSH
CVE-2019-0220 [7]	Apache HTTP
CVE-1999-0524 [1]	Politica di filtraggio

Tabella 5.4: Tabella delle vulnerabilità di Fawkes

punteggi è presente, assieme alla matrice dei rischi (**Hazard Risk Assessment Matrix**) in Figura 5.2.

1. **R1**: accesso ai file condivisi tramite protocollo FTP. (4A);
2. **R2:** attacco denial-of-service al protocollo FTP, relativo a CVE-2021-30047 (3D);
3. **R3:** attacco di tipo buffer overflow al kernel Linux, relativo a CVE-2018-7566 (1D);
4. **R4:** attacco di tipo integer-overflow al kernel Linux, relativo a CVE-2018-8781 (1D);
5. **R5:** attacco al server HTTP, relativo a CVE-2019-0211 (1E);
6. **R6:** attacco al server HTTP, relativo a CVE-2019-0215 (3D);
7. **R7:** attacco al server HTTP, relativo a CVE-2019-0218 (2E);
8. **R8:** identity spoofing tramite autenticazione con username differente da quello per il quale un utente è autorizzato, relativo a CVE-2019-0217 (2E);
9. **R9:** privilege escalation sfruttando la vulnerabilità di sudo, relativa a CVE-2021-3156 (1B);
10. **R10:** privilege escalation sfruttando la vulnerabilità di sudo, relativa a CVE-2023-22809 (1D);

11. **R11:** omissione di pacchetti in transtio tramite il protocollo SSH, relativo a CVE-2023-48795 (3D);

12. **R12:** bypass delle restrizioni di secure boot, relativo a CVE-2019-20908 (4D):

13. **R13:** sfruttamento di errati vincoli di destinazione in OpenSSH, relativo a CVE-2023-51384 (3E);

14. **R14:** command injection tramite OpenSSH, relativo a CVE-2023-51385 (2D);

15. **R15:** manipolazione dell'input in una richiesta http per causare comportamento inaspettato, relativo a CVE-2019-0220 (3E);

16. **R16:** invio di messaggi ICMP arbitrari, relativo a CVE-1999-0524 (4B);

17. **R17:** rilascio di informazioni sensibili tramite l'analisi del traffico FTP (3A);

18. **R18:** invio di input arbitrario al server in esecuzione sulla porta 9898 per l'esecuzione di codice remoto (2B);

Occorrenza	1 - Catastrofico	2 - Critico	3 - Serio	4 - Minore
A) Frequente	0	0	1	1
B) Probabile	1	1	0	1
C) Occasionale	0	0	0	0
D) Remoto	3	1	3	1
E) Improbabile	1	2	2	0

Figura 5.2: Hazard Risk Assessment matrix

6. Detailed Summary

Nel seguente capitolo sono presenti schede per ogni vulnerabilità identificata. La suddivisione in sezioni prende in considerazione il livello di gravità assegnato dal CVSS 3.1.

Linux Kernel buffer overflow via SNDRV_SEQ_IOCTL_SET_CLIENT_POOL	**CVE-2018-7566**
CVSS Severity: High (Base score: 7.8)	
Descrizione: Il kernel Linux 4.15 presenta un buffer overflow attraverso un'operazione di scrittura dell'ioctl SNDRV_SEQ_IOCTL_SET_CLIENT_POOL operazione di scrittura ioctl su /dev/snd/seq da parte di un utente locale.	
Impatto: Sfruttando questa vulnerabilità è possibile ridirigere il flusso di esecuzione del codice per ottenere l'esecuzione di codice arbitrario.	
Soluzione: Aggiornare la versione del kernel installato.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.1: Scheda tecnica di CVE-2018-7566

Integer-overflow in udl_fb_mmap	**CVE-2018-8781**
CVSS Severity: High (Base score: 7.8)	
Descrizione: La funzione udl_fb_mmap in drivers/gpu/drm/udl/udl_fb.c nel kernel Linux versione 3.4 e fino alla 4.15 inclusa presenta una vulnerabilità di tipo integer-overflow che consente agli utenti locali con accesso al driver udldrmfb di ottenere autorizzazioni complete di lettura e scrittura sulle pagine fisiche del kernel, con conseguente esecuzione di codice nello spazio kernel.	
Impatto: Sfruttando questa vulnerabilità è possibile eseguire codice arbitrario nello spazio riservato al kernel.	
Soluzione: Aggiornare la versione del kernel installato.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.2: Scheda tecnica di CVE-2018-8781

DoS in vsftpd v3.0.3	**CVE-2021-30047**
CVSS Severity: High (Base score: 7.5)	
Descrizione: VSFTPD 3.0.3 consente agli aggressori di causare un denial of service a causa del numero limitato di connessioni consentite.	
Impatto: Sfruttando questa vulnerabilità è possibile causare un denial of service al servizio che sfrutta FTP.	
Soluzione: Aggiornare la versione di vsftpd.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.3: Scheda tecnica di CVE-2021-30047

Apache HTTP server command injection	**CVE-2019-0211**
CVSS Severity: High (Base score: 7.8)	
Descrizione: In Apache HTTP Server 2.4 dalla release 2.4.17 alla 2.4.38, con evento MPM, worker o prefork, il codice in esecuzione in processi o thread figli con privilegi minori (compresi gli script eseguiti da un interprete di scripting in-process) potrebbe eseguire codice arbitrario con i privilegi del processo padre (solitamente root). I sistemi non Unix non sono interessati.	
Impatto: Sfruttando questa vulnerabilità è possibile causare remote command injection. Tali comandi vengono eseguiti con i permessi associati al processo httpd. Avendo l'asset in esecuzione un sistema Unix non è necessario porre rimedio a questa vulnerabilità.	
Soluzione: Non necessaria	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.4: Scheda tecnica di CVE-2019-0211

Apache HTTP bypass dei controlli	CVE-2019-0215
CVSS Severity: High (Base score: 7.5)	
Descrizione: In Apache HTTP Server 2.4 nelle release 2.4.37 e 2.4.38, un bug in mod_ssl quando si utilizzava la verifica del certificato client per-location con TLSv1.3 permetteva a un client di aggirare le restrizioni di controllo dell'accesso configurate.	
Impatto: Un attaccante può aggirare le politiche di controllo degli accessi alle risorse HTTP tramite l'utilizzo di certificati contraffatti.	
Soluzione: Aggiornare la versione di Apache httpd.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.5: Scheda tecnica di CVE-2019-0215

Apache HTTP race condition	**CVE-2019-0217**
CVSS Severity: High (Base score: 7.5)	
Descrizione: In Apache HTTP Server 2.4 release 2.4.38 e precedenti, una race condition in mod_auth_digest durante l'esecuzione in un server threaded poteva consentire a un utente con credenziali valide di autenticarsi utilizzando un altro nome utente, aggirando le restrizioni di controllo dell'accesso configurate.	
Impatto: Un attaccante può autenticarsi, tramite pagine di login di una risorse HTTP, con nome utente arbitrario, se in possesso di un account legittimo.	
Soluzione: Non necessaria in quanto la risorsa web non fornisce meccanismi di autenticazione tramite login. Se tale funzionamento dovesse cambiare è necessario aggiornare la versione di Apache httpd.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.6: Scheda tecnica di CVE-2019-0217

Privilege escalation tramite sudo	**CVE-2021-3156**
CVSS Severity: High (Base score: 7.8)	
Descrizione: Sudo prima della versione 1.9.5p2 contiene un errore off-by-one che può causare un buffer overflow basato su heap, che consente l'escalation dei privilegi a root tramite "sudoedit -s" e un argomento della riga di comando che termina con un singolo carattere backslash.	
Impatto: Un utente che non abbia i permessi di root può effettuare privilege escalation verticale sfruttando un attacco buffer overflow.	
Soluzione: Aggiornare la versione di sudo.	
Metodo di detection: Vulnerabilità individuata tramite il tool linux-smart-enumeration v4.14nw .	

Figura 6.7: Scheda tecnica di CVE-2021-3156

Privilege escalation tramite sudo	**CVE-2023-22809**
CVSS Severity: High (Base score: 7.8)	
Descrizione: In Sudo prima della 1.9.12p2, la funzione sudoedit (alias -e) gestisce male gli argomenti extra passati nelle variabili d'ambiente fornite dall'utente (SUDO_EDITOR, VISUAL e EDITOR), consentendo a un aggressore locale di aggiungere voci arbitrarie all'elenco dei file da elaborare. Le versioni interessate sono dalla 1.8.0 alla 1.9.12.p1.	
Impatto: Un utente che non abbia i permessi di root può effettuare privilege escalation verticale sfruttando la modifica delle variabili d'ambiente.	
Soluzione: Aggiornare la versione di sudo.	
Metodo di detection: Vulnerabilità individuata tramite il tool linux-smart-enumeration v4.14nw .	

Figura 6.8: Scheda tecnica di CVE-2023-22809

Terrapin attack	**CVE-2023-48795**
CVSS Severity: Medium (Base score: 5.9)	
Descrizione: Il protocollo SSH con alcune estensioni OpenSSH, presenti in OpenSSH prima della versione 9.6, consente agli aggressori remoti di bypassare i controlli di integrità in modo tale che alcuni pacchetti vengano omessi (dal messaggio di negoziazione dell'estensione), alias un attacco Terrapin. Questo accade perch é il protocollo SSH Binary Packet Protocol (BPP), implementato da queste estensioni, gestisce male la fase di handshake e l'uso dei numeri di sequenza.	
Impatto: La connessione instaurata tra client e server aggira i controlli di sicurezza previsti.	
Soluzione: Aggiornare la versione di openssh.	
Metodo di detection: Vulnerabilità individuata tramite il tool nessus v10.7.4 .	

Figura 6.9: Scheda tecnica di CVE-2023-48795

Secure boot bypass	**CVE-2019-20908**
CVSS Severity: Medium (Base score: 6.7)	
Descrizione: È stato rilevato un problema in drivers/firmware/efi/efi.c nel kernel Linux precedente alla versione 5.4. Permessi di accesso errati per la variabile ACPI efivar_ssdt potrebbero essere utilizzati dagli aggressori per aggirare le restrizioni di lockdown o di avvio sicuro, alias CID-1957a85b0032.	
Impatto: Un utente malintenzionato può aggirare le regole di secure boot del sistema.	
Soluzione: Aggiornare la versione del kernel.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.10: Scheda tecnica di CVE-2019-20908

OpenSSH constraint bypass	**CVE-2023-51384**
CVSS Severity: Medium (Base score: 5.5)	
Descrizione: In ssh-agent in OpenSSH prima di 9.6, alcuni vincoli di destinazione possono essere applicati in modo incompleto. Quando i vincoli di destinazione sono specificati durante l'aggiunta di chiavi private ospitate da PKCS#11, questi vincoli vengono applicati solo alla prima chiave, anche se un token PKCS#11 restituisce più chiavi.	
Impatto: Un utente malintenzionato può aggirare i controlli su alcuni token PKCS#11.	
Soluzione: Aggiornare la versione di OpenSSH.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.11: Scheda tecnica di CVE-2023-51384

OpenSSH improper handling of special characters	**CVE-2023-51385**
CVSS Severity: Medium (Base score: 6.5)	
Descrizione: In ssh in OpenSSH prima della versione 9.6, l'iniezione di comandi OS potrebbe verificarsi se un nome utente o un nome host contiene metacaratteri di shell e questo nome è referenziato da un token di espansione in determinate situazioni. Ad esempio, un repository Git non attendibile può avere un sottomodulo con metacaratteri di shell nel nome utente o nel nome host.	
Impatto: Una connessione SSH ad un host con caratteri speciali può comportare l'esecuzione di comandi da remoto.	
Soluzione: Aggiornare la versione di OpenSSH.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.12: Scheda tecnica di CVE-2023-51385

LocationMatch security bypass	**CVE-2019-0220**
CVSS Severity: Medium (Base score: 5.3)	
Descrizione: È stata rilevata una vulnerabilità in Apache HTTP Server da 2.4.0 a 2.4.38. Quando il componente percorso di un URL di richiesta contiene più caratteri slash consecutivi ('/'), le direttive come LocationMatch e RewriteRule devono tenere conto dei duplicati nelle espressioni regolari, mentre altri aspetti dell'elaborazione del server li annullano implicitamente.	
Impatto: Una utente malintenzionato può accedere a risorse protette tramite regole di pattern matching inserendo un numero arbitrario di caratteri '/'.	
Soluzione: Aggiornare la versione di Apache httpd.	
Metodo di detection: Vulnerabilità individuata manualmente attraverso una query su https://cve.mitre.org/	

Figura 6.13: Scheda tecnica di CVE-2019-0220

ICMP data allowed from arbitrary hosts	**CVE-1999-0524**
CVSS Severity: Low (Base score: 2.1)	
Descrizione: Le informazioni ICMP come (1) netmask e (2) timestamp sono consentite da host arbitrari.	
Impatto: Una utente malintenzionato può manipolare le informazioni sulla netmask e sul timestamp del sistema inviando pacchetti ICMP.	
Soluzione: Inserire politiche di filtraggio.	
Metodo di detection: Vulnerabilità individuata tramite il tool nessus v10.7.4 .	

Figura 6.14: Scheda tecnica di CVE-1999-0524

Bibliografia

[1] National Institute of Standards and Technology. *CVE-1999-0524*. 1999. URL: https://nvd.nist.gov/vuln/detail/CVE-1999-0524.

[2] National Institute of Standards and Technology. *CVE-2018-7566*. 2018. URL: https://nvd.nist.gov/vuln/detail/CVE-2018-7566.

[3] National Institute of Standards and Technology. *CVE-2018-8781*. 2018. URL: https://nvd.nist.gov/vuln/detail/CVE-2018-8781.

[4] National Institute of Standards and Technology. *CVE-2019-0211*. 2019. URL: https://nvd.nist.gov/vuln/detail/CVE-2019-0211.

[5] National Institute of Standards and Technology. *CVE-2019-0215*. 2019. URL: https://nvd.nist.gov/vuln/detail/CVE-2019-0215.

[6] National Institute of Standards and Technology. *CVE-2019-0217*. 2019. URL: https://nvd.nist.gov/vuln/detail/CVE-2019-0217.

[7] National Institute of Standards and Technology. *CVE-2019-0220*. 2019. URL: https://nvd.nist.gov/vuln/detail/CVE-2019-0220.

[8] National Institute of Standards and Technology. *CVE-2019-20908*. 2019. URL: https://nvd.nist.gov/vuln/detail/CVE-2019-20908.

[9] National Institute of Standards and Technology. *CVE-2021-30047*. 2021. URL: https://nvd.nist.gov/vuln/detail/CVE-2021-30047.

[10] National Institute of Standards and Technology. *CVE-2021-3156*. 2021. URL: https://nvd.nist.gov/vuln/detail/CVE-2021-3156.

[11] National Institute of Standards and Technology. *CVE-2023-22809*. 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-22809.

[12] National Institute of Standards and Technology. *CVE-2023-48795*. 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-48795.

[13] National Institute of Standards and Technology. *CVE-2023-51384*. 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-51384.

[14] National Institute of Standards and Technology. *CVE-2023-51385*. 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-51385.

[15] National Institute of Standards and Technology. *CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')*. N/A. URL: https://nvd.nist.gov/vuln/detail/CWE-120.

[16] National Institute of Standards and Technology. *CWE-256: Plaintext Storage of a Password*. N/A. URL: https://nvd.nist.gov/vuln/detail/CWE-256.

[17] National Institute of Standards and Technology. *CWE-284: Improper Access Control*. N/A. URL: https://nvd.nist.gov/vuln/detail/CWE-284.

[18] National Institute of Standards and Technology. *CWE-285: Improper Authorization*. N/A. URL: https://nvd.nist.gov/vuln/detail/CWE-285.

[19] Mansoor R. *Harry Potter: Fawkes*. URL: https://www.vulnhub.com/entry/harrypotter-fawkes,686/.