UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INFORMATICA

Laurea Magistrale in Informatica

Corso di Penetration Testing And Ethical Hacking

Penetration Testing Report - Proxima Centauri

Matteo Della Rocca

ANNO ACCADEMICO 2023/2024

Indice

CAPITOLO 1

Executive Summary

L'attività di penetration testing del professionista Matteo Della Rocca, commissionata dal corso di Penetration Testing and Ethical Hacking nell'anno 2024, è stata condotta per evidenziare gli aspetti critici del sistema "Proxima Centauri" dell'azienda Vulnhub, con lo scopo di studiare difese efficaci contro potenziali attacchi. L'attività è stata portata avanti per un mese, con data di inizio 24/05/2024.
Gli obiettivi principali erano:

- Identificare, analizzare, sfruttare e documentare il maggior numero possibile di vulnerabilità.
- Ottenere accesso non autorizzato ai file critici, come user.txt e root.txt.

1.0.1 Metodologia utilizzata

Il test è stato effettuato utilizzando una metodologia **full black box**, poiché non sono stati forniti dettagli sull'implementazione dell'asset né risultati di testing precedenti. È stata effettuata un'analisi approfondita delle configurazioni di sicurezza, utilizzando strumenti specifici per la rilevazione delle vulnerabilità e tecniche di exploit per verificarne la reale possibilità di compromissione.

1.0.2 Principali risultati

I risultati ottenuti hanno rivelato svariate vulnerabilità, alcune delle quali critiche, dovute principalmente a:

- Mancanza di aggiornamenti del sistema;
- Presenza di password deboli;
- Sistema di autenticazione web debole;

1.0.3 Rischi e impatto delle vulnerabilità

Le vulnerabilità identificate possono portare a una compromissione totale della triade CIA (Confidentiality, Integrity, and Availability) del sistema. Il rischio di essere compromessi è molto alto, con potenziali impatti significativi sulla sicurezza e l'operatività.

1.0.4 Raccomandazioni generali

Si raccomanda di:

- Applicare tempestivamente le patch e gli aggiornamenti ai sistemi vulnerabili;
- Implementare politiche di autenticazione più rigorose;
- Effettuare regolari test di sicurezza per monitorare e migliorare continuamente la postura di sicurezza.

CAPITOLO 2

Engagement Highlights

Durante il mese di testing, che si è svolto senza restrizioni riguardo alle tecniche e agli strumenti utilizzati, è stato impiegato un computer con sistema operativo Kali Linux. Questa scelta è stata motivata dalla vasta gamma di strumenti disponibili nella suite di Kali Linux, ideali per verificare la sicurezza del sistema, individuare vulnerabilità e suggerire possibili soluzioni per mitigarle. Inoltre, non è stato imposto alcun limite riguardo ai potenziali danni che potrebbero derivare dall'attività di testing.
Durante il processo di testing della sicurezza dell'applicativo web hostato, è stato seguito un framework generico articolato nelle seguenti fasi:

1. **Target Discovery**: Identificazione dell'indirizzo IP della macchina target.
   - Tool usati: arp-scan, ping
2. **Enumerating Target e Port Scanning**: Utilizzo di Nmap per la scansione delle porte, dei servizi e la raccolta di informazioni sul target.
   - Tool usato: nmap
3. **Vulnerability Mapping**:
   - Utilizzo di strumenti come Nessus, OpenVAS, wafw00f, Whatweb, Gobuster per identificare vulnerabilità e analizzare la configurazione dell'applicativo web.

- Analisi manuale delle pagine web raggiungibili e ricerca di vulnerabilità specifiche utilizzando Exploit-DB.

4. **Target Exploitation**:
   - Sfruttamento di una vulnerabilità nota (CVE-2020-29607), con descrizione delle fasi di sfruttamento, requisiti e conseguenze del successo dell'exploit.
   - Acquisizione di file sensibili come user.txt.
5. **Post Exploitation**:
   - Escalation dei privilegi attraverso la ricerca di eseguibili con SUID settato, esplorazione dei permessi sudo e valutazione delle capabilities.
   - Acquisizione della bandierina root.txt per dimostrare l'ottenimento del controllo completo sulla macchina.
   - Mantenimento dell'accesso attraverso l'implementazione di un backdoor SSH e l'utilizzo di Systemd come backdoor.

CAPITOLO 3

Vulnerability Report

L'analisi dell'asset Proxima Centauri ha identificato diverse vulnerabilità critiche, elencate di seguito:

- Il file robots.txt è indicizzato, rivelando la struttura del sito e le direttive di accesso;
- L'autenticazione dell'amministratore avviene attraverso un singolo parametro password, potenzialmente vulnerabile ad attacchi di forza bruta;
- Il CMS utilizzato presenta una vulnerabilità di file upload, permettendo il caricamento di file malevoli. Molte estensioni sono controllate ma altre ad esempio *phar* no;
- Sulla pagina /planet/travel è presente un commento che fornisce indizi sulla gestione delle porte chiuse del firewall, mettendo a rischio la configurazione di sicurezza;
- Il backup di MySQL contiene informazioni sensibili non correttamente cifrate con permessi di lettura corretti, esponendo i dati a possibili accessi non autorizzati;
- Sono presenti eseguibili con capabilities ingiustamente assegnate, potenzialmente consentendo operazioni non autorizzate o accessi impropri.

CAPITOLO 4

Remediation Report

L'analisi delle vulnerabilità dell'asset Proxima Centauri ha identificato i seguenti punti critici che necessitano di azioni immediate di remediation:

- **Indicizzazione di robots.txt**:
  - Il file robots.txt è indicizzato, rivelando la struttura del sito e le direttive di accesso.
  - Azioni di remediation:
    * Rivedere e aggiornare il contenuto del file robots.txt per limitare l'esposizione delle informazioni sensibili.
    * Implementare direttive di accesso più restrittive per proteggere le risorse critiche.
- **Autenticazione dell'amministratore tramite parametro password**:
  - L'autenticazione dell'amministratore avviene tramite un singolo parametro password, vulnerabile ad attacchi di forza bruta.
  - Azioni di remediation:
    * Implementare un sistema di autenticazione più robusto e multifattoriale..

- **Vulnerabilità di file upload sul CMS utilizzato**:
  - Il CMS utilizzato presenta una vulnerabilità di file upload, permettendo il caricamento di file malevoli.
  - Azioni di remediation:
    * Applicare un filtro rigoroso sui tipi di file consentiti per il caricamento per prevenire l'esecuzione di script dannosi.
- **Commento nella pagina /planet/travel**:
  - Sulla pagina /planet/travel è presente un commento che fornisce indizi sulla gestione delle porte chiuse del firewall, mettendo a rischio la configurazione di sicurezza.
  - Azioni di remediation:
    * Rimuovere o proteggere il commento per evitare la divulgazione di informazioni sensibili sulla configurazione del firewall.
- **Backup di MySQL con permessi di lettura non corretti**:
  - Il backup di MySQL contiene informazioni sensibili ma non ha i permessi di lettura corretti, esponendo i dati a possibili accessi non autorizzati.
  - Azioni di remediation:
    * Aggiornare e correggere i permessi del backup di MySQL per garantire che solo gli utenti autorizzati possano accedere ai dati sensibili.
    * Implementare controlli regolari sui permessi per prevenire futuri errori di configurazione.
- **Eseguibili con capabilities ingiustamente assegnate**:
  - Sono presenti eseguibili con capabilities ingiustamente date, potenzialmente consentendo operazioni non autorizzate o accessi impropriati.
  - Azioni di remediation:
    * Rivedere e limitare le capabilities assegnate agli eseguibili, assicurando che siano congruenti con le necessità funzionali dell'applicazione.
    * Implementare un controllo regolare delle capabilities per rilevare e correggere anomalie.

CAPITOLO 5

Findings Summary

Durante l'attività di penetration testing sulla macchina target "Proxima Centauri", sono state identificate numerose vulnerabilità classificate in base alla loro gravità, utilizzando come riferimento il CVSS 3.0 o, se non disponibile, il CVSS 2.0:

1. **Alto**:
    - Rischi elevati, con vulnerabilità potenzialmente gravi per il sistema [CVSS ≥ 7]
2. **Medio**:
    - Rischio medi, con vulnerabilità che possono avere un impatto significativo sul sistema [$4 \leq$ CVSS < 7]
3. **Basso**:
    - Rischi bassi e vulnerabilità poco gravi [CVSS < 4]

Nota: Le vulnerabilità di tipo "Info" elencate da Nessus non sono state menzionate nel report poiché non rappresentano rischi diretti significativi per il sistema durante il penetration testing, focalizzato invece su vulnerabilità che consentono accessi non autorizzati o compromettono la sicurezza.

5.0.1 Vulnerabilità rilevate da Nessus

Figura 5.1: Fonte: report generato da Nessus

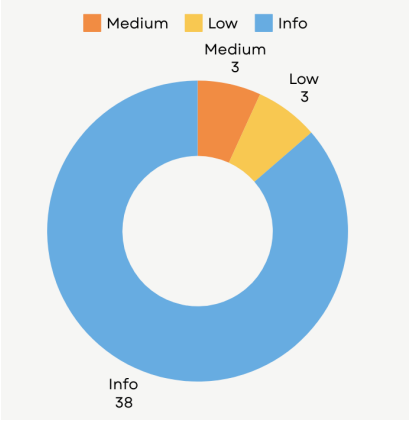

Figura 5.2: Grafico a torta relativo alle vulnerabilià trovate da Nessus

5.0.2 Vulnerabilità rilevate da OpenVas

Host	High	Medium	Low	Log	False Positive
10.0.2.8	0	2	3	0	0
Total: 1	0	2	3	0	0

Figura 5.3: Fonte: report pdf generato da OpenVas

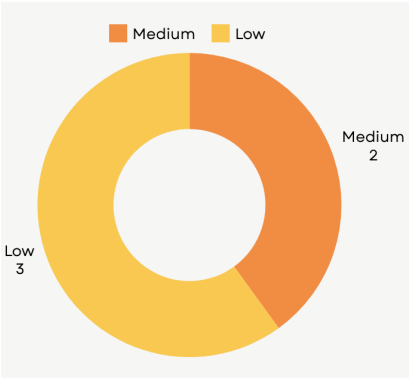

Figura 5.4: Grafico a torta relativo alle vulnerabilià trovate da OpenVAS

CAPITOLO 6

Detailed Summary

6.1 Nessus

6.1.1 Vulnerabilità classificate con rischio Medio

Directory Web esplorabili	
CVE	-
Punteggio (CVSS)	5.3
Rischio	Medio
Descrizione	Alcune directory sul server web remoto sono navigabili. Ciò può permettere a un attaccante di visualizzare o scaricare file riservati.
Soluzione	Assicurarsi che le directory navigabili non perdano informazioni riservate o non diano accesso a risorse sensibili. Inoltre, utilizzare restrizioni di accesso o disabilitare l'indicizzazione delle directory.
Metodo di detection	Tramite il tool Nessus

Applicazione web potenzialmente vulnerabile al clickjacking	
CVE	.
Punteggio (CVSS)	4.3
Rischio	Medio
Descrizione	Il server SSH remoto è vulnerabile a un attacco di truncamento del prefisso man-in-the-middle conosciuto come Terrapin. Ciò può permettere a un attaccante remoto di bypassare i controlli di integrità e degradare la sicurezza della connessione.
Soluzione	Contattare il fornitore per un aggiornamento con le contromisure di scambio chiavi rigorose o disabilitare gli algoritmi interessati.
Riferimenti	• CWE:693 (`https://cwe.mitre.org/data/definitions/693.html`)
Metodo di detection	Tramite il tool Nessus

SSH Terrapin Prefix Truncation Weakness	
CVE	CVE-2023-48795
Punteggio (CVSS)	5.9
Rischio	Medio
Descrizione	Il server SSH remoto è vulnerabile a un attacco di truncamento del prefisso man-in-the-middle conosciuto come Terrapin. Ciò può permettere a un attaccante remoto di bypassare i controlli di integrità e degradare la sicurezza della connessione.

Limitazione plugin	Da tenere presente che il plugin controlla solo i server SSH remoti che supportano ChaCha20-Poly1305 o CBC con Encrypt-then-MAC e non supportano le rigorose contromisure per lo scambio di chiavi.
Soluzione	Contattare il fornitore per un aggiornamento con le contromisure di scambio chiavi rigorose o disabilitare gli algoritmi interessati.
Riferimenti	• CVE-2023-48795
Metodo di detection	Tramite il tool Nessus

6.1.2 Vulnerabilità classificate con rischio basso

ICMP Timestamp Request Remote Date Disclosure	
CVE	CVE-1999-0524
Punteggio (CVSS)	2.1
Rischio	Basso
Descrizione	È possibile determinare l'ora esatta impostata sull'host remoto rispondendo a una richiesta di timestamp ICMP. Ciò può assistere un attaccante remoto non autenticato nel bypassare i protocolli di autenticazione basati sul tempo.
Soluzione	Filtrare le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita (14).
Riferimenti	• CVE-1999-0524 (`https://nvd.nist.gov/vuln/detail/CVE-1999-0524`) • CWE:200 (`https://cwe.mitre.org/data/definitions/200.html`)

Metodo di detection	Tramite il tool Nessus

Il server Web consente il completamento automatico della password	
CVE	-
Punteggio (CVSS)	-
Rischio	Basso
Descrizione	Il server web remoto contiene almeno un campo di tipo 'password' in un form HTML dove l'attributo 'autocomplete' non è impostato su 'off'. Ciò può portare alla perdita di riservatezza se gli utenti utilizzano un host condiviso o se il loro computer viene compromesso.
Soluzione	Aggiungere l'attributo 'autocomplete=off' a questi campi per impedire ai browser di memorizzare le credenziali.
Metodo di detection	Tramite il tool Nessus

Il server Web trasmette credenziali in chiaro	
CVE	-
Punteggio (CVSS)	2.6
Rischio	Basso
Descrizione	Il server web remoto trasmette credenziali in chiaro attraverso campi di tipo 'password' in form HTML. Un attaccante che intercetta il traffico può ottenere le credenziali degli utenti.
Soluzione	Assicurarsi che ogni form sensibile trasmetta il contenuto tramite HTTPS.

Riferimenti	• CWE:522 (https://cwe.mitre.org/data/definitions/522.html) • CWE:523 (https://cwe.mitre.org/data/definitions/523.html) • CWE:718 (https://cwe.mitre.org/data/definitions/718.html) • CWE:724 (https://cwe.mitre.org/data/definitions/724.html) • CWE:928 (https://cwe.mitre.org/data/definitions/928.html) • CWE:930 (https://cwe.mitre.org/data/definitions/930.html)
Metodo di detection	Tramite il tool Nessus

6.2 OpenVas

6.2.1 Vulnerabilità classificate con rischio medio

NVT: Attributo 'HttpOnly' mancante per i cookie (HTTP)	
CVE	CVE-2023-48795
Punteggio (CVSS)	5.0
Rischio	Medio
Descrizione	Il server web HTTP remoto / l'applicazione non imposta l'attributo 'HttpOnly' per uno o più cookie HTTP inviati. Il cookie: Set-Cookie: PHPSESSID=***sostituito***; path=/ è/sono privi dell'attributo "HttpOnly".

Limitazione plugin	Da tenere presente che il plugin controlla solo i server SSH remoti che supportano ChaCha20-Poly1305 o CBC con Encrypt-then-MAC e non supportano le rigorose contromisure per lo scambio di chiavi.
Soluzione	• Impostare l'attributo 'HttpOnly' per ogni cookie di sessione • Valutare/effettuare una propria valutazione dell'impatto sulla sicurezza del server web/applicazione e creare un'override per questo risultato se non ne esiste uno
Riferimenti	• `https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6` • `https://owasp.org/www-community/HttpOnly` • `https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0,02)`
Metodo di detection	Tramite il tool OpenVas

Trasmissione non crittografata di informazioni sensibili via HTTP	
CVE	-
Punteggio (CVSS)	4.8
Rischio	Medio
Descrizione	L'host o l'applicazione trasmette informazioni sensibili (come username e password) in chiaro tramite HTTP.

Soluzione	• Assicurarsi che i dati sensibili siano trasmessi tramite connessione crittografata SSL/TLS. • Implementare un meccanismo di reindirizzamento automatico degli utenti verso la connessione SSL/TLS sicura prima di consentire l'inserimento di informazioni sensibili nelle funzioni menzionate.
Riferimenti	• `https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management` • `https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure` • `https://cwe.mitre.org/data/definitions/319.html`
Metodo di detection	Tramite il tool OpenVas

6.2.2 Vulnerabilità classificate con rischio basso

Divulgazione delle Informazioni tramite Timestamp TCP	
CVE	-
Punteggio (CVSS)	-
Rischio	Basso
Descrizione	L'host remoto implementa i timestamp TCP e pertanto consente di calcolare il tempo di attività.

Soluzione	Per disabilitare i timestamp TCP su Linux, aggiungere la linea 'net.ipv4.tcp_timestamps = 0' a /etc/sysctl.conf. Eseguire 'sysctl -p' per applicare le impostazioni durante l'esecuzione.
Riferimenti	• `https://datatracker.ietf.org/doc/html/rfc1323` • `https://datatracker.ietf.org/doc/html/rfc7323` • `https://www.fortiguard.com/psirt/FG-IR-16-090`
Metodo di detection	Tramite il tool OpenVas

Supporto a algoritmi MAC deboli (SSH)	
CVE	-
Punteggio (CVSS)	-
Rischio	Basso
Descrizione	Il server SSH remoto è configurato per consentire/supportare algoritmi MAC deboli. Il server SSH remoto supporta i seguenti algoritmi MAC deboli da client a server e da server a client: • umac-64-etm@openssh.com • umac-64@openssh.com

Soluzione	• Disabilitare i segnalati algoritmi MAC deboli. – Algoritmi basati su MD5 – Algoritmi basati su 96-bit – Algoritmi basati su 64-bit
Riferimenti	• `https://www.rfc-editor.org/rfc/rfc6668` • `https://www.rfc-editor.org/rfc/rfc4253#section-6.4`
Metodo di detection	Tramite il tool OpenVas

Divulgazione di Informazioni di Risposta agli ICMP Timestamp	
CVE	CVE-1999-0524
Punteggio (CVSS)	2.1
Rischio	Basso
Descrizione	L'host remoto ha risposto a una richiesta di timestamp ICMP.
Soluzione	• Disabilitare completamente il supporto per gli ICMP timestamp sull'host remoto • Proteggere l'host remoto con un firewall e bloccare i pacchetti ICMP che attraversano il firewall in entrambe le direzioni (completamente o solo per reti non attendibili)

Riferimenti	• https://datatracker.ietf.org/doc/html/rfc792 • https://datatracker.ietf.org/doc/html/rfc2780
Metodo di detection	Tramite il tool OpenVas

6.3 Analisi manuale

6.3.1 Vulnerabilità classificate con rischio alto

CVE-2020–29607	
CVE	CVE-2020-296074
Punteggio (CVSS)	7.2
Rischio	Alto
Descrizione	Una vulnerabilità di bypass delle restrizioni di caricamento file nella Pluck CMS prima della versione 4.7.13 consente a un utente con privilegi di amministratore di ottenere accesso all'host attraverso la funzionalità "gestione file", con il potenziale rischio di esecuzione remota di codice.
Soluzione	• Aggiornare il CMS Pluck alle versioni successive
Exploit utilizzato	https://www.exploit-db.com/exploits/49909

Riferimenti	• `https://nvd.nist.gov/vuln/detail/CVE-2020-29607` • CWE-434 (`https://cwe.mitre.org/data/definitions/434.html`)
Metodo di detection	Tramite analisi manuale

Autenticazione del sito vulnerabile ad attacchi di forza bruta	
CVE	-
Punteggio (CVSS)	-
Rischio	Alto
Descrizione	L'applicazione web ospitata nell'asset utilizza solo una password per l'autenticazione dell'amministratore
Soluzione	• Implementare misure di sicurezza come il blocco temporaneo dell'account dopo tentativi falliti oppure usare autenticazione a più livelli
Metodo di detection	Tramite analisi manuale

Esposizione di informazioni sulla configurazione del firewall	
CVE	-
Punteggio (CVSS)	-
Rischio	Alto

Descrizione	Sulla pagina /planet/travel è presente un commento che fornisce indizi sulla gestione delle porte chiuse del firewall, mettendo a rischio la configurazione di sicurezza. Questa esposizione di informazioni critiche potrebbe essere sfruttata da attaccanti per pianificare e condurre attacchi mirati al sistema.
Soluzione	• Modificare o rimuovere il commento o le informazioni sensibili dalla pagina /planet/travel che forniscono dettagli sulla gestione delle porte chiuse del firewall.
Riferimenti	CWE-200 (`https://cwe.mitre.org/data/definitions/200.html`)
Metodo di detection	Analisi manuale

Eseguibili con capabilities assegnate in modo non adeguato	
CVE	-
Punteggio (CVSS)	-
Rischio	Alto
Descrizione	L'eseguibile in /home/proxima/proximaCentauriA/perl ha capabilities (capacità speciali) assegnate in modo non adeguato. Questo potrebbe consentire all'eseguibile di eseguire operazioni per le quali non ha le autorizzazioni appropriate, aumentando il rischio di accessi impropri o di compromissione del sistema.

Soluzione	• Rimuovere tutte le capabilities non necessarie o non appropriate per il corretto funzionamento dell'applicazione. • Implementare controlli regolari per monitorare e validare le capabilities assegnate agli eseguibili critici nel sistema.
Riferimenti	CWE-250 (`https://cwe.mitre.org/data/definitions/250.html`)
Metodo di detection	Tramite analisi manuale

Password nel database non cifrata nel mysql.bak	
CVE	-
Punteggio (CVSS)	-
Rischio	Alto
Descrizione	Nel file di backup mysql.bak, le password sono memorizzate in chiaro, senza cifratura. Questo rappresenta un grave rischio per la sicurezza poiché chiunque abbia accesso al file di backup può leggere le password e potenzialmente ottenere accessi non autorizzati ai database e ad altre risorse critiche.
Soluzione	• Cifrare tutte le password nel database utilizzando algoritmi di cifratura robusti. • Implementare meccanismi di hashing sicuri per le password
Riferimenti	CWE-256 (`https://cwe.mitre.org/data/definitions/256.html`)
Metodo di detection	Tramite analisi manuale

6.3.2 Vulnerabilità classificate con rischio medio

Indicizzazione del file robots.txt	
CVE	-
Punteggio (CVSS)	-
Rischio	Medio
Descrizione	Il file robots.txt è indicizzato, rivelando la struttura del sito e le direttive di accesso. Questo può essere sfruttato dagli attaccanti per comprendere la topologia del sito e potenzialmente identificare vulnerabilità o punti di accesso critici.
Soluzione	• Impostare le direttive nel file robots.txt in modo da non esporre informazioni sensibili sulla struttura del sito.
Riferimenti	OWASP Information Disclosure: `https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A5-Security_Misconfiguration.html`
Metodo di detection	Tramite analisi manuale