UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Magistrale in Informatica

CORSO DI PENETRATION TESTING
AND ETHICAL HACKING

De-ICE S1.140: Penetration Testing Report

STUDENTE

Lorenzo Criscuolo

Matricola: 0522501268

DOCENTE

Prof. **Arcangelo Castiglione**

Università degli studi di Salerno

Anno Accademico 2022-2023

Indice

CAPITOLO 1

Penetration Testing Report

1.1 Executive Summary

Al fine di realizzare il progetto del corso *Penetration Testing and Ethical Hacking* sono state svolte delle attività di Penetration Testing su una macchina virtuale vulnerabile chiamata **De-ICE S1.140**. Il fine ultimo di tutte le attività svolte è stato semplicemente didattico, con lo scopo di acquisire al meglio tutte le conoscenze fornite durante lo svolgimento del corso. Per l'esecuzione di tutte le attività è stata adottata una strategia di analisi *Black-Box*, quindi senza avere nessuna conoscenza pregressa sull'asset, e sono state realizzate all'interno di un'ambiente simulato con una connessione diretta con l'asset.
Durante le varie attività svolte sono state riscontrate diverse vulnerabilità che possono portare un malintenzionato ad ottenere documenti o file a cui non dovrebbe avere accesso e, nel caso peggiore, alla compromissione totale del sistema.

Lasciare il sistema in questo stato è un rischio **critico** e, per questa ragione, bisognerebbe correre subito ai ripari aggiornando il sistema, gli applicativi e nascondendo alcune informazioni **sensibili** per far tornare il sistema entro livelli di rischio *accettabili*.

1.2 Engagement Highlights

Essendo un progetto universitario nell'ambito del corso *Penetration Testing and Ethical hacking* ed essendo che l'ambiente su cui è effettuato l'intero processo è *virtualizzato*, non ci

sono **NDA** da rispettare e non ci sono vincoli sulle tecniche che è possibile utilizzare o sulle parti dell'asset da analizzare.

1.3 Vulnerability Report

Durante il processo sono state trovate varie vulnerabilità, aclune di queste con gravità **critica** e **alta**. Le principali sono le seguenti:

- *Information Leakage* (gravità **critica**): alcune informazioni importanti sono salvate in maniera non protetta fornendo ad un attaccante la possibilità di compromettere le password degli utenti e dell'amministratore;
- Sistema Operativo Deprecato (gravità **critica**): Il sistema operativo dell'asset non è più supportato e non riceverà più aggiornamenti di sicurezza. Pertanto, potrebbero presentarsi vulnerabilità che permettono ad attaccanti di ottenere pieno controllo della macchina;
- Versione deprecata di **ProFTPD** (gravità **critica**): la versione attuale di **ProFTPD** consente ad un malintenzionato di leggere e scrivere qualunque file presente nel sistema senza doversi autenticare, quindi potrebbe scrivere un codice malevolo e eseguirlo da remoto;
- Versione deprecata di **OpenSSL** (gravità **critica**): La versione di **OpenSSL** installata utilizza protocolli crittografici datati e vulnerabili, permettendo ad un attaccante di violare il traffico web verso il sistema. Inoltre, implementa una versione di *SSL* che è affetta dalla nota vulnerabilità **HeartBleed**, con la quale un attaccante potrebbe compromettere sessioni web e ottenere chiavi e password salvate nel server;
- Versione vulnerabile di **phpMyAdmin** (gravità **critica**): La versione di **phpMyAdmin** è vulnerabile ad un attacco che permette ad un malintenzionato di ottenere dati dal database senza dover autenticarsi;
- Utilizzo di password deboli (gravità **alta**): Per l'accesso al sistema, sono state utilizzate password deboli che possono essere facilmente indovinate o forzate da un attaccante;
- Utilizzo di protocolli crittografici deboli (gravità **medio-alta**): Le versioni di SSL e TLS utilizzate e supportate dal sistema sono deboli e non dovrebbero essere più supportate, visto che possono portare alla compromissione del traffico web;

- Server web *Apache* malconfigurato (gravità **media**): Il server web invia informazioni sensibili che potrebbero aiutare un attaccante contro il server web stesso e, inoltre, non utilizza un meccanismo di sicurezza che impedisce ad un attaccante di fare operazioni all'insaputa del client e reindirizzarlo verso pagine web maelvole;

- Utilizzo di una versione deprecata di **jQuery** (gravità **media**): Viene utilizzata una versione della libreria **jQuery** che è vulnerabile ad un attacco che permette ad un attaccante di rubare informazioni sensibili ai client che visitano una pagina con integrata quella libreria;

- Rilascio di timestamp sui pacchetti *TCP* (gravità **bassa**): Sui pacchetti che vengono inviati per instaurare connessioni viene aggiunto anche un *timestamp*, il quale può essere utilizzato per stabilire il tempo di operatività del sistema;

- Supportati protocolli deboli per *SSH* (gravità **bassa**): per le connessioni *SSH* è abilitato il supporto a protocolli di scambio di chiavi e di autenticazione che sono deboli e sfacilmente attaccabili;

- Invio dell'IP privato all'interno di richieste *HTTP* (gravità **bassa**): Quando viene effettuata una richiesta al server web, questo risponde aggiungendo anche l'indirizzo IP privato del sistema, fornendo ad un attaccante informazioni utili per quanto riguarda l'architettura di rete e lo spazio di indirizzamento dell'asset.

1.4 Remediation Report

Durante il processo eseguito, sono state trovate molte vulnerabilità tra cui alcune abbastanza importanti che potrebbero comportare la compromissione completa del sistema e di file e documenti all'interno, nonchè la compromissione dei dati dei visitatori del sito web. Per questa ragione, si forniscono i seguenti consigli per migliorare la sicurezza dell'asset con indirizzo *10.0.2.4*:

- Aggiornare il Sistema Operativo ad una versione più recente;

- Aggiornare la versione di **ProFTPD** ad una non vulnerabile;

- Aggiornare la versione installa di **OpenSSL**;

- Rimuovere le informazioni sensibili non correttamente protette;

- Aggiornare la versione di **phpMyAdmin** ad una più recente e non vulnerabile;
- Cambiare le credenziali di tutti gli utenti con alcune che siano molto più difficili da forzare e indovinare, magari utilizzando combinazioni di caratteri alfanumerici e speciali;
- Configurare il web server *Apache* in modo tale da aggiungere attributi di sicurezza nelle pagine e da non supportare più protocolli crittografici deprecati e facilmente compromissibili;
- Aggiornare la versione di **jQuery** utilizzata nelle pagine web;
- Rimuovere dai pacchetti *TCP* il campo *timestamp*;
- Configurare il servizio *SSH* in modo tale che non supporti protocolli crittografici deboli;
- Rimuovere dalle risposte del web server l'indirizzo IP privato del sistema.

1.5 Findings Summary

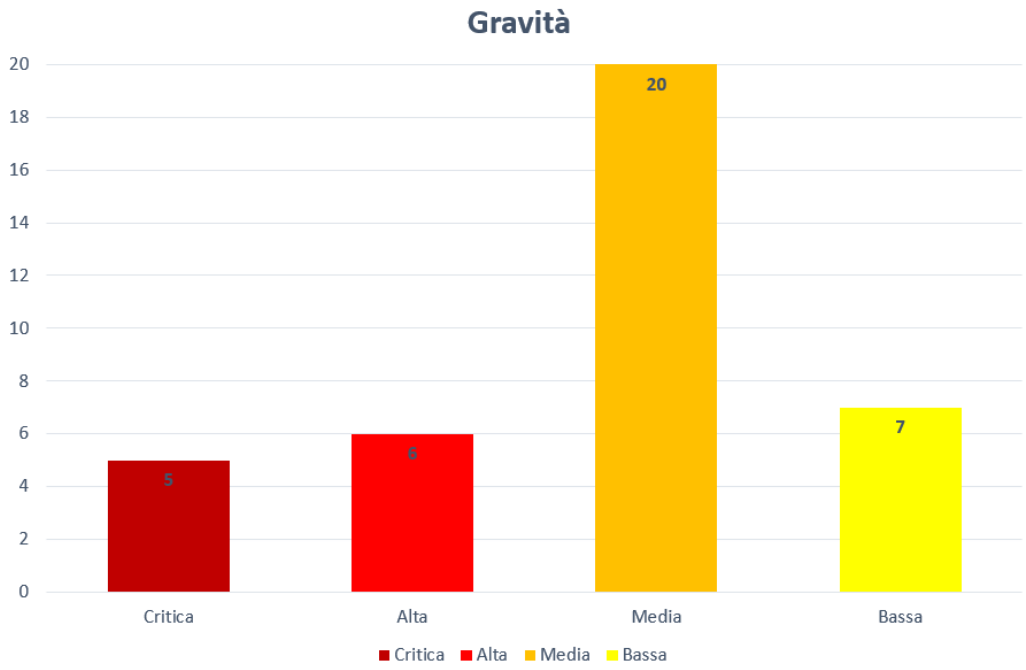

Figura 1.1: Ortogramma riassuntivo dei rilevamenti

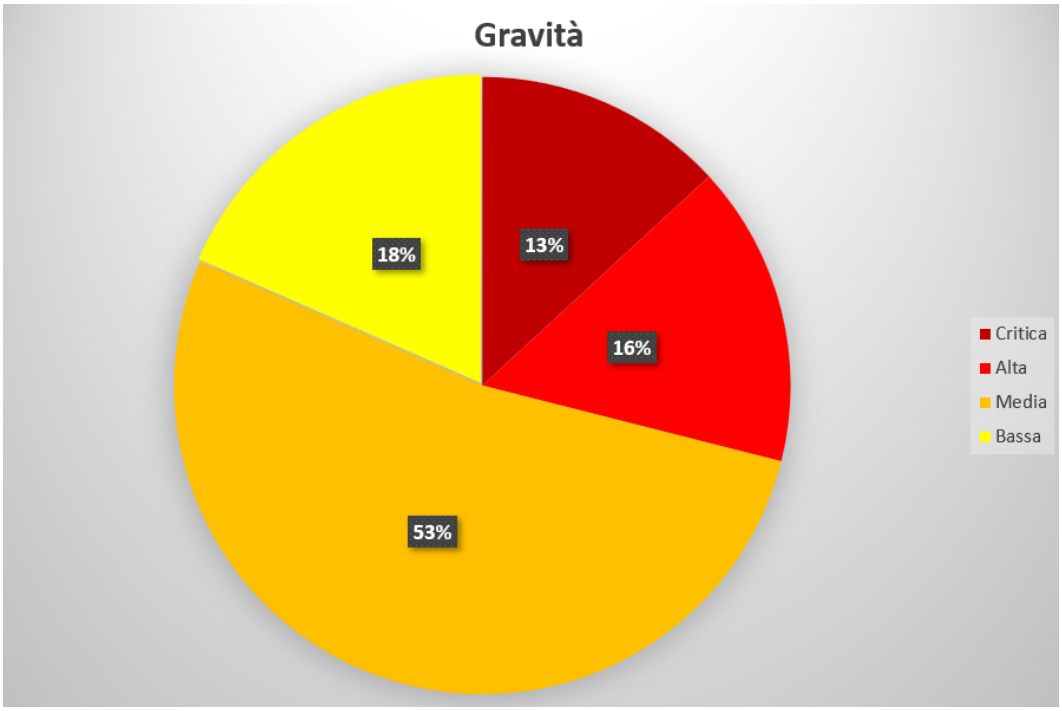

Figura 1.2: Aerogramma riassuntivo dei rilevamenti

1.6 Detailed Summary

Di seguito saranno elencate le varie vulnerabilità riscontrate manualmente, correlate di eventuale ID e rischi associati, e saranno indicati i documenti esaustivi nei quali consultare tutte le restanti vulnerabilità riscontrate grazie a tool di rilevazione automatica.

1.6.1 Information Leakage

- **Descrizione**: Informazioni sensibili non sono state protette adeguatamente o sono state inserite in risorse accessibili da utenti non autorizzati. Le informazioni trovate sono le seguenti:
  - Nella discussione **Login Attacks** presente nel forum (*10.0.2.4/forum*) è presente la password di **mbrown** per l'accesso alla pagina personale del forum e alla mail;
  - Nell'account webmail di **mbrown** presente all'indirizzo *10.0.2.4/webmail* è stata trovata una mail nella casella *In Arrivo* che contiene le credenziali in chiaro dell'utente **root** del servizio **phpMyAdmin**;
  - Nello script che si trova al percorso */opt/backup.sh* è presente l'opzione `-pass pass:<PASSWORD>` con la password specificata in chiaro;

  - Nella cartella *.ssh* dell'utente **mbrown**, è presente un file *downloadkey* che è una copia della chiave privata di tale utente, però con permessi di lettura anche ad altri utenti.

- **Rischi associati**: La presenza di queste informazioni permette la compromissione dell'utente **mbrown**, di tutti i database presenti in **phpMyAdmin** e dell'intero sistema, permettendo ad un attaccante di effettuare il login prima come utente **suoder** (in particolare l'utente **swillard**) e, successivamente come utente **root**.

- **Soluzione**:

  - Cancellare il thread **Login Attacks** dal forum;
  - Cancellare la mail contenente la password dell'utente **root** di **phpMyAdmin** e non usare questo metodo per scambiare informazioni sensibili;
  - Utilizzare come password un file `.key` protetto da password;
  - Rimuovere il file */home/mbrown/.ssh/downloadkey* o specificare dei permessi adeguati in modo da renderlo leggibile solo all'utente **mbrown**

- **ID di riferimento**: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor;

- **Riferimenti**: `https://cwe.mitre.org/data/definitions/200.html`.

1.6.2 Impiego di password deboli

- **Descrizione**: Per accedere al sistema e ai servizi vengono utilizzate le stesse password o, in ogni caso, password facilmente compromissibili;

- **Rischi associati**: Un attaccante potrebbe entrare in possesso degli hash delle password e tramite strumenti di *Offline Password Cracking* come `john` o `hashcat` potrebbe riuscire a forzare tramite con successo le password degli utenti tramite attacco a dizionario, compromettendo il sistema;

- **Soluzione**: Utilizzare password diverse per ogni servizio e impiegare dei requisiti di password più stringenti, come combinazioni di caratteri alfanumerici e caratteri speciali (anche combinazioni di maiuscole e minuscole) specificando anche una lunghezza minima;

- **ID di riferimento**: CWE-1391: Use of Weak Credentials, CWE-521: Weak Password Requirements
- **Riferimenti**: `https://cwe.mitre.org/data/definitions/1391.html`,`https://cwe.mitre.org/data/definitions/521.html`.

1.6.3 Rilevamenti effettuati da *Nessus*

Con il tool *Nessus* sono stati generati due report, entrambi posti nella cartella *Report* e con il nome **De-ICE_scan_nessus.pdf** e **De-ICE_scan_nessus_web.pdf**.

1.6.4 Rilevamenti effettuati da *OpenVAS*

Con il tool *OpenVAS* è stato generato un solo report, posto nella cartella *Report* e con il nome **De-ICE_scan_openvas.pdf**.

1.6.5 Rilevamenti effettuati da *OWASP ZAP*

Con il tool *OWASP ZAP* è stato generato un solo report, posto nella cartella *Report* e con il nome **De-ICE-ZAP-Report.html**.

1.6.6 Rilevamenti effettuati da *Paros*

Con il tool *Paros* è stato generato un solo report, posto nella cartella *Report* e con il nome **paros-report.htm**.

1.6.7 Rilevamenti effettuati da *Nikto*

Con il tool *Nikto* è stato generato un solo report, posto nella cartella *Report* e con il nome **nikto-report.html**.

Bibliografia

Siti Web consultati

- CWE-200 – `https://cwe.mitre.org/data/definitions/200.html`
- CWE-521 – `https://cwe.mitre.org/data/definitions/521.html`
- CWE-1391 – `https://cwe.mitre.org/data/definitions/1391.html`