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

Indice **i**

1 Penetration Testing Report **1**

1.1 Executive Summary 1

1.2 Engagement Highlights 1

1.3 Vulnerability Report 2

1.4 Remediation Report 3

1.5 Findings Summary 3

1.6 Detailed Summary 3

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 *critiche*.

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 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

1.5 Findings Summary

1.6 Detailed Summary