UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INFORMATICA

Corso di Laurea in Sicurezza

CyberSploit: 2
Report

Relatore:
Prof.
Arcangelo Castiglione

Candidato:
Luigi Gallo
Mat. 0522501404

ANNO ACCADEMICO 2023-2024

CONTENTS

CHAPTER 1

EXECUTIVE SUMMARY

Il presente report documenta il processo di penetration testing etico condotto sulla macchina virtuale CyberSploit: 2, reperibile sulla piattaforma vulnhub al seguente link.

L'obiettivo del testing era di identificare vulnerabilità, ottenere il controllo della macchina e installare una backdoor.

L'attività di penetration testing è iniziata il 8 maggio 2024 e si è svolta secondo la metodologia black box, in quanto inizialmente non erano disponibili informazioni.

Nell'ambito del penetration testing condotto sulla macchina target, si adotterà un approccio etico ispirato ai principi dei white-hat hacker. L'obiettivo primario sarà quello di individuare, verificare e notificare le vulnerabilità del sistema che ne evidenziano la potenziale fragilità. Tale attività sarà condotta nel pieno rispetto delle regole etiche e professionali del settore.

Infine verranno proposte soluzioni per mitigare i potenziali problemi di sicurezza riscontrati.

CHAPTER 2

ENGAGEMENT HIGHLIGHTS

La presente relazione descrive un penetration testing condotto a scopo didattico sulla macchina target "CyberSploit: 2". Non essendo stata stipulata alcuna contrattazione con un cliente, la scelta degli strumenti è stata basata unicamente sull'efficienza e sulla capacità di superare le limitazioni tecniche riscontrate.
Il progetto ha seguito le fasi tipiche del penetration testing:

1. **Raccolta informazioni e scoperta del bersaglio:** In questa fase, è stato utilizzato lo strumento Nmap per identificare i servizi attivi e le vulnerabilità potenziali. L'output di Nmap è stato confrontato con altri strumenti come Netdiscover e P0f per ottenere una visione più completa della rete target.

2. **Enumerazione del bersaglio e scansione delle porte:** Nmap è stato nuovamente utilizzato per la scansione delle porte e l'enumerazione dei servizi attivi. Lo strumento Dirb è stato impiegato per individuare eventuali directory indicizzate.

3. **Mapping delle vulnerabilità:** Nessus e OpenVAS sono stati utilizzati per identificare le vulnerabilità presenti sulla macchina target.

4. **Exploitation:** È stato possibile ottenere l'accesso alla macchina target in due modi:

    - Sfruttando delle informazioni residue presenti all'URL "http://10.0.2.6" .
    - Effettuando il cracking della password dell'utente "centos" in quanto quest'ultima risulta essere molto debole.

5. **Post-Exploitation (escalation dei privilegi):** Una volta ottenuto l'accesso, è stato possibile elevare i privilegi sfruttando un container docker malevolo.

6. **Post-Exploitation (mantenimento dell'accesso):** Ottenuti i privilegi completi sulla macchina target, è stata installata una backdoor persistente che stabilisce una connessione "reverse TCP" verso la macchina kali ad ogni avvio del sistema.

CHAPTER 3

VULNERABILITY REPORT

L'analisi approfondita della macchina virtuale CyberSploit: 2 ha rivelato la presenza di diverse vulnerabilità di sicurezza, che saranno elencate in dettaglio nel seguito di questo report. Tra le più critiche e preoccupanti, si evidenziano:

- **Password SSH Debole per Utente Root:**
  È stata rilevata l'utilizzo di una password SSH estremamente debole per un utente con privilegi di root. Questo rappresenta un grave rischio per la sicurezza del sistema, in quanto un malintenzionato che ottiene questa password potrebbe acquisire il controllo completo del server.

- **Credenziali Esposte in Homepage:**
  È stata scoperta una homepage contenente le credenziali dell'utente "shailendra", protette da un algoritmo di cifratura debole. Questo rende le credenziali facilmente accessibili a chiunque abbia accesso alla homepage, esponendo l'utente a potenziali attacchi di autenticazione.

- **Creazione Arbitraria di Container Docker:**
  Il sistema permette a qualsiasi utente di creare nuovi container Docker in modo arbitrario. Questa configurazione insicura consente a utenti

malintenzionati di eseguire codice dannoso all'interno dei container, compromettendo la sicurezza del sistema e potenzialmente causando danni significativi.

- **Violazione della Confidenzialità con HTTP TRACE/TRACK Abilitato:**
  L'attivazione dei metodi HTTP TRACE e TRACK espone il sistema a violazioni delSono state identificate diverse vulnerabilità relative al protocollo SSH. Queste vulnerabilità espongono le comunicazioni SSH a potenziali attacchi di intercettazione e decrittazione, compromettendo la sicurezza e la riservatezza dei dati trasmessi.la confidenzialità. Un utente malintenzionato potrebbe sfruttare questa configurazione per accedere a informazioni sensibili a cui non dovrebbe avere accesso.

- **Vulnerabilità ICMP Timestamp Reply Information Disclosure:**
  È stata rilevata la vulnerabilità "ICMP Timestamp Reply Information Disclosure". Questa vulnerabilità permette a un malintenzionato di estrarre informazioni dal dispositivo target inviando una semplice richiesta di timestamp ICMP. Le informazioni ottenute potrebbero essere utilizzate per pianificare attacchi mirati al sistema.

- **Vulnerabilità TCP Timestamps Information Disclosure:**
  È stata rilevata la vulnerabilità "TCP Timestamps Information Disclosure". Questa vulnerabilità apre la strada ad attacchi side-channel che permettono a un malintenzionato di ricavare informazioni come l'uptime e il sistema operativo della macchina target.

- **Vulnerabilità SSH:**
  Sono state identificate diverse vulnerabilità relative al protocollo SSH. Queste vulnerabilità espongono le comunicazioni SSH a potenziali attacchi di intercettazione e decrittazione, compromettendo la sicurezza e la riservatezza dei dati trasmessi.

CHAPTER 4

REMEDIATION REPORT

La macchina "CyberSploit: 2" possiede un livello di rischio elevato, quindi alla luce delle vulnerabilità elencate, si raccomanda di adottare le seguenti misure correttive:

- Cambiare immediatamente la password SSH dell'utente root con una password forte e complessa.
- Eliminare la homepage contenente le credenziali dell'utente "shailendra" o proteggerla con un algoritmo di cifratura robusto.
- Implementare controlli di accesso rigorosi per limitare la creazione di container Docker solo agli utenti autorizzati.
- Disabilitare i metodi HTTP TRACE e TRACK per prevenire accessi non autorizzati a informazioni sensibili.
- Aggiornare il firmware e i software del sistema per correggere le vulnerabilità ICMP e TCP Timestamps Information Disclosure.
- Applicare patch di sicurezza per le vulnerabilità SSH identificate e adottare pratiche di sicurezza rigorose per le connessioni SSH aggiornando OpenSSH all'ultima versione disponibile.

CHAPTER 5

FINDINGS SUMMARY

Durante l'attività di penetration testing sono state individuate numerose vulnerabilità nella macchina target. Le vulnerabilità sono state suddivise in quattro classi in base alla loro gravità:

- Le vulnerabilità classificate come **CRITICAL** rappresentano un rischio estremamente elevato per la sicurezza del sistema. Hanno il potenziale di causare danni ingenti e di consentire a un malintenzionato di ottenere un controllo completo o parziale del sistema.

- Le vulnerabilità classificate come **HIGH** rappresentano un rischio significativo per la sicurezza del sistema. Sebbene lo sfruttamento di queste vulnerabilità possa richiedere condizioni specifiche o competenze tecniche più elevate, l'impatto potenziale sul sistema può essere relativamente alto.

- Le vulnerabilità classificate come **MEDIUM** rappresentano un rischio moderato per la sicurezza del sistema. Sebbene lo sfruttamento di queste vulnerabilità possa richiedere condizioni specifiche o competenze tecniche elevate, l'impatto diretto sul sistema è generalmente limitato.

- Le vulnerabilità classificate come **LOW** rappresentano un rischio minimo

per la sicurezza del sistema. Hanno un impatto poco significativo e la loro probabilità di sfruttamento è bassa. Pertanto, non rappresentano una minaccia rilevante per il sistema nell'immediato.

- Le informazioni classificate come **INFO** non rappresentano vulnerabilità attive, bensì informazioni utili su configurazioni di software o pratiche che potrebbero potenzialmente esporre il sistema a vulnerabilità future.

Il seguente grafico mostra il numero di vulnerabilità individuate per ogni categoria:

Figure 5.1: Classificazione vulnerabilità.

Per fornire una panoramica completa e immediata della distribuzione delle vulnerabilità all'interno del sistema, viene presentato un grafico a torta. Questo strumento visivo consente di comprendere facilmente la proporzione di vulnerabilità appartenenti a ciascuna classe di gravità (CRITICAL, HIGH, MEDIUM, LOW).

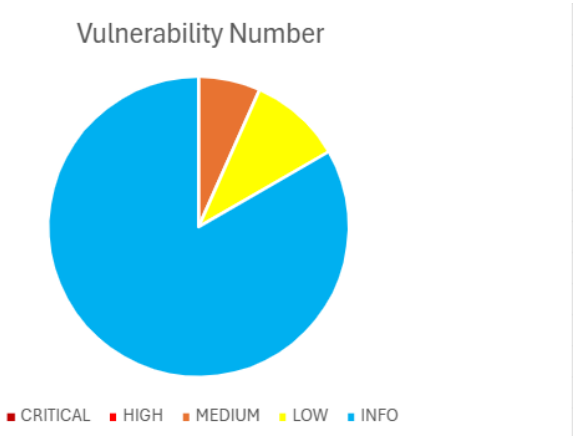

Figure 5.2: Grafico a torta delle vulnerabilità.

CHAPTER 6

DETAILED SUMMARY

In questa sezione saranno elencate e descritte in modo dettagliato e preciso tutte le vulnerabilità riscontrate durante l'analisi del sistema.

Medium (CVSS: 5.8) **NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled**
Summary Il server web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP utilizzati per il debug delle connessioni al server web.
Quality of Detection: 99
Vulnerability Detection Result Il server web ha abilitato il seguente metodo HTTP: TRACE.
Impact Un malintenzionato potrebbe sfruttare questa debolezza per ingannare i tuoi legittimi utenti web e carpire le loro credenziali.
Solution: **Solution type:** Mitigazione Gruppi MODP a 1024 bit / algoritmi KEX primi: In alternativa, utilizzare in generale l'algoritmo Diffie-Hellmann a curva ellittica, ad esempio Curve 25519.

Medium (CVSS: 5.3) **NVT: Weak Encryption Algorithm(s) Supported (SSH)**
Riepilogo Il server SSH remoto supporta algoritmi di crittografia deboli. Gli algoritmi di crittografia deboli sono vulnerabili a tentativi di decifrazione e non sono sicuri per l'uso nelle comunicazioni SSH.
Qualità del rilevamento: 80
Risultato del rilevamento della vulnerabilità Il server SSH supporta algoritmi di crittografia deboli.
Impatto Un malintenzionato potrebbe utilizzare attacchi di forza bruta o altri metodi per decifrare il traffico SSH protetto con algoritmi deboli. Ciò potrebbe consentire loro di intercettare dati sensibili o impersonare utenti autorizzati.
Soluzione: **Tipo di soluzione:** Mitigazione Disabilitare l'uso di algoritmi di crittografia deboli sul server SSH. Consultare la documentazione del tuo server SSH per istruzioni specifiche.

Low (CVSS: 3.7)

NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) edit

Riepilogo

Il server SSH remoto supporta algoritmi deboli per lo scambio di chiavi (KEX). Gli algoritmi KEX deboli sono vulnerabili a tecniche di cracking e non sono sicuri per l'uso nelle connessioni SSH.

Qualità del rilevamento: 80

Risultato del rilevamento della vulnerabilità

Il server SSH supporta algoritmi KEX deboli.

Impatto

Un malintenzionato potrebbe sfruttare la debolezza degli algoritmi KEX per compromettere la segretezza della chiave di sessione SSH. Ciò consentirebbe loro di decifrare il traffico SSH protetto e potenzialmente impersonare utenti autorizzati.

Soluzione:

Tipo di soluzione: Mitigazione

Disabilitare l'uso di algoritmi KEX deboli sul server SSH. Consultare la documentazione del tuo server SSH per istruzioni specifiche. In generale, si consiglia di utilizzare algoritmi KEX basati su curve ellittiche, come Curve 25519, per una maggiore sicurezza.

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Riepilogo

Il server remoto abilita le opzioni del timestamp TCP. I timestamp TCP possono essere utilizzati da un malintenzionato per approsmare il tempo di attività del sistema, potenzialmente fornendo informazioni utili per ulteriori attacchi.

Qualità del rilevamento: 80

Risultato del rilevamento della vulnerabilità

Il server remoto consente le opzioni del timestamp TCP.

Impatto

Un malintenzionato potrebbe sfruttare la divulgazione del timestamp TCP per stimare il tempo di attività del sistema. Questo, combinato con altre tecniche di fingerprinting del sistema, potrebbe aiutare l'attaccante a identificare il software in uso e potenzialmente trovare vulnerabilità note associate a quel software.

Soluzione:

Tipo di soluzione: Mitigazione

Disabilitare le opzioni del timestamp TCP sul server. Consultare la documentazione del tuo sistema operativo per istruzioni specifiche.

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Riepilogo

Il server remoto abilita le opzioni del timestamp TCP. I timestamp TCP possono essere utilizzati da un malintenzionato per approsmare il tempo di attività del sistema, potenzialmente fornendo informazioni utili per ulteriori attacchi.

Qualità del rilevamento: 80

Risultato del rilevamento della vulnerabilità

Il server remoto consente le opzioni del timestamp TCP.

Impatto

Un malintenzionato potrebbe sfruttare la divulgazione del timestamp TCP per stimare il tempo di attività del sistema. Questo, combinato con altre tecniche di fingerprinting del sistema, potrebbe aiutare l'attaccante a identificare il software in uso e potenzialmente trovare vulnerabilità note associate a quel software.

Soluzione:

Tipo di soluzione: Mitigazione

Disabilitare le opzioni del timestamp TCP sul server. Consultare la documentazione del tuo sistema operativo per istruzioni specifiche.

LIST OF FIGURES