UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Magistrale in Informatica

CORSO DI PENETRATION TESTING
AND ETHICAL HACKING

Penetration Testing Report: *Momentum: 1*

STUDENTE

Vincenzo Emanuele Martone

DOCENTE

Prof. **Arcangelo Castiglione**

Anno Accademico 2022-2023

Indice

Elenco delle figure

CAPITOLO 1

Penetration Testing Report

1.1 Executive Summary

Per l'attività progettuale relativa al corso di *Penetration Testing and Ethical Hacking* è stato svolto un processo di *Penetration Testing* sulla macchina virtuale vulnerabile *by-design* '*Momentum: 1*', disponibile sulla piattaforma *VulnHub*. In assenza di particolari e specifiche informazioni relative all'asset da analizzare, è stato utilizzato un approccio di tipo *Black Box*. Per svolgere l'analisi è stato configurato un opportuno ambiente simulato che consente un'interazione con l'asset, permettendo di esaminarlo e di rilevarne le vulnerabilità. In particolare, le vulnerabilità rilevate possono portare all'ottenimento del pieno controllo del sistema da parte di un attaccante che può assumere il ruolo di amministratore. Risulta, altresì, possibile per un attaccante rubare dati sensibili degli utenti del sito *web*. Allo stato attuale, il livello di rischio complessivo associato all'asset risulta essere critico, tuttavia mediante alcuni accorgimenti, come la rimozione di dati sensibili dalle risorse pubbliche e l'implementazione di alcuni semplici controlli, è possibile abbassare sensibilmente il livello di rischio.

1.2 Engagement Highlights

Dal momento il processo di *Penetration Testing* è stato svolto in ambito accademico, non è stato necessario definire particolari regole di ingaggio.

1.3 Vulnerability Report

Nel corso del processo di *Penetration Testing* sono state rilevate diverse vulnerabilità sfruttabili per compromettere vari aspetti del sistema. Di seguito è riprotata una descrizione generale delle problematiche riscontrate:

- **[Severity: Alta] Information Leakage del *Web Server***: presenza di una password usata per la decifratura di dati sensibili, all'interno di risorse pubblicamente accessibili mediante il *Web Server*, che mette, altresì, a disposizione i dati sensibili cifrati. Tali dati rappresentano le credenziali di accesso di un utente del sistema;
- **[Severity: Alta] Information Leakage di un servizio in esecuzione all'interno del sistema**: presenza della password dell'amministratore del sistema nella memoria di un servizio accessibile anche da utenti non privilegiati;
- **[Severity: Media] Session Data Stealing**: possibilità di rubare i dati di sessione di un utente del *Web Server* mediante l'iniezione di codice all'interno di una pagina;
- **[Serverity: Media] Navigabilità delle directory del *Web Server***: possibilità di navigare le directory del *Web Server* mediante il *Web Browser* al fine di visualizzarne il contenuto;
- **[Severity: Media] Errata configurazione del *Web Server***: assenza di attributi di controllo all'interno delle risposte del *Web Server* volte alla protezione da alcuni tipi di attacchi noti. Il *Web Server* lascia, inoltre, trapelare informazioni sul sistema.
- **[Severity: Media] Utilizzo di una versione non aggiornata del *Web Server***;
- **[Severity: Bassa] Trapelamento del *timestamp* del sistema**: ottenimento di informazioni sul *timestamp* del sistema con eventuale possibilità di prevedere dati generati in maniera arbitraria dal sistema.

1.4 Remediation Report

Mediante vari accorgimenti risulta possibile rimuovere le vulnerabilità dal sistema evitando, in questo modo, tutti i rischi ad esse associate. Di seguito è riportata una descrizione generale delle operazioni consigliate:

- Rimozione delle informazioni sensibili dalle risorse messe a disposizione dal *Web Server*

- Implementazione di alcuni filtri per evitare l'iniezione di codice nelle pagine del sito *Web*;
- Riconfigurazione del *Web Server* al fine di impedire la navigazione delle directory e di impostare opportuni attributi di sicurezza;
- Aggiornamento del *Web Server* all'ultima versione stabile disponibile;
- Inibizione del trapelamento delle informazioni relative al *timestamp* del sistema.

1.5 Findings Summary

Di seguito sono riportati i grafici relativi alle vulnerabilità identificate in rapporto alla severity. In particolare, l'aerogramma illustrato nella figura 1.1 ne mostra la percentuale, mentre l'ortogramma mostrato nella figura 1.2 ne mostra il numero.

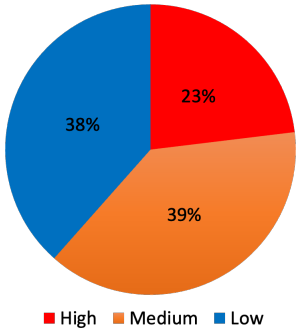

Figura 1.1: Aerogramma delle vulnerabilità rilevate

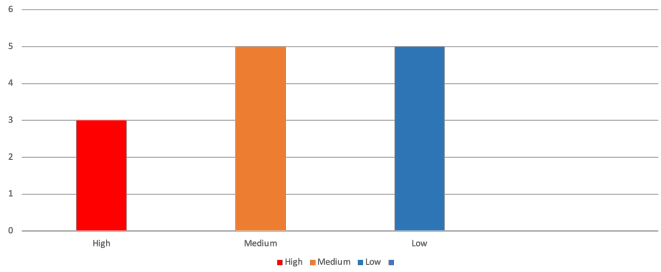

Figura 1.2: Ortogramma delle vulnerabilità rilevate

1.6 Detailed Summary

Le vulnerabilità discusse sono state rilevate sia mediante l'utilizzo di specifici *tool* che mediante tecniche di ricerca manuale. Complessivamente sono state rilevate 13 vulnerabilità e c'è stato un *End of Life Detection* del *Web Server*.

1.6.1 Vulnerabilità rilevate mediante i tool

OpenVAS

OpenVAS ha rilevato le seguenti due vulnerabilità di severity *low*:

- **ICMP Timestamp Reply Information Disclosure**;
- **TCP Timestamps Information Disclosure**.

Un report esaustivo relativo a tali vulnerabilità è riportato nel file *'openvas-report.pdf'* reperibile nella directory *'tools_output'*.

Nessus

Nessus ha rilevato le seguenti due vulnerabilità di severity media:

- **Browsable Web Directories**;
- **Web Application Potentially Vulnerable to Clickjacking**.

Un report esaustivo relativo a tali vulnerabilità è riportato nel file *'nessus-web-all-ports-complex-report.pdf'* reperibile nella directory *'tools_output'*. A tal proposito è doveroso sottolineare che *Nessus* ha rilevato due falsi positivi: *CGI Generic SSI Injection (HTTP headers)* e *Web Application Information Disclosure* che risulta opportuno ignorare nel corso della consultazione del report.

OWASP ZAP

OWASP ZAP ha rilevato tre vulnerabilità aventi severity media e due vulnerabilità aventi severity low:

- **Content Security Policy (CSP) Header Not Set**;
- **Directory Browsing**;
- **Missing Anti-clickjacking Header**;
- **Server Leaks Version Information via "Server" HTTP Response Header Field**;
- **X-Content-Type-Options Header Missing**.

Un report esaustivo relativo a tali vulnerabilità è riportato nel file *'zap-report.html'* reperibile nella directory *'tools_output'*.

Nikto 2

Nikto 2 ha rilevato diverse vulnerabilità senza, tuttavia, fornire un livello di severity associato. Per alcune di queste vulnerabilità è stato, tuttavia, fornita la relativa *CVE* che ha consentito l'identificazione della severity. Le vulnerabilità in questione sono le seguenti:

- **The anti-clickjacking X-Frame-Options header is not present** : questa vulnerabilità è stata rilevata anche da altri tool che hanno assegnato una severity media;
- **The X-Content-Type-Options header is not set**: questa vulnerabilità è stata rilevata anche da altri tool che hanno assegnato una severity bassa;
- **Server may leak inodes via ETags (CVE-2003-1418)**: consultando il sito del *NIST*, emerge che tale vulnerabilità ha una severity media [1];

Il report delle vulnerabilità di *Nikto* è riportato nel file *'nikto2-report.html'* reperibile nella directory *'tools_output'*. Tra le vulnerabilità rilevate è possibile osservare una *End Of Life detection* relativo alla versione di *Apache 2.2.34*.

Paros Proxy

Paros Proxy ha rilevato quattro vulnerabilità di cui due aventi severity media ed una avente severity bassa. Le vulnerabilità in questione sono le seguenti:

- **Directory browsing**;
- **Cross site scripting**;
- **Private IP disclosure**.

Un report esaustivo relativo a tali vulnerabilità è riportato nel file *'paros-report.htm'* reperibile nella directory *'tools_output'*. A tal proposito è doveroso sottolineare che *Paros Proxy* ha rilevato un falso positivi: *Lotus Domino default files*, che che risulta opportuno ignorare nel corso della consultazione del report.

1.6.2 Vulnerabilità rilevate mediante le tecniche manuali

Le vulnerabilità aventi severity più elevata sono state rilevate mediante tecniche manuali di esplorazione dei servizi della macchina target. Di seguito è riportato un report dettagliato di tali vulnerabilità.

Presenza di una password nel sorgente di una pagina *Web*

- **Descrizione**: all'interno del file *'main.js'* presente sul *Web Server* è presente un commento contenente delle operazioni di decifratura che fa uso della password in chiaro *'SecretPassphraseMomentum'*;
- **Modalità di individuazione**: la vulnerabilità è stata individuata durante un'operazione di *browsing* delle directory del *Web Server*;
- **Rischi associati**: tale password può essere utilizzata per decifrare i dati inviati dal *Web Server*. In particolare è possibile decifrare il contenuto di un cookie;
- **Severity**: Alta;
- **CWE di riferimento**: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor);
- **Soluzione**: rimuovere il commento dallo script *'main.js'*;
- **Riferimenti**: https://cwe.mitre.org/data/definitions/200.html

Presenza di un cookie cifrato contenente la password di accesso al servizio *SSH*

- **Descrizione**: quando l'utente visita la pagina *'<WEB_SERVER_IP>/opus-details.php'*, il *Web Server* gli invia un cookie che può essere decifrato con la password presente all'interno dello script *'main.js'*;
- **Modalità di individuazione**: la vulnerabilità è stata individuata durante la ricerca di un dato da decifrare con la password presente all'interno dello script *'main.js'*;
- **Rischi associati**: la decifratura di tale cookie porta alla scoperta di una stringa che rappresenta la password di accesso dell'utente *'auxerre'* al servizio *SSH* del sistema;
- **Severity**: Alta;
- **CWE di riferimento**: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor);
- **Soluzione**: rimuovere il cookie contenente la password di accesso al servizio *SSH* e cifrarlo con una password non reperibile;
- **Riferimenti**: https://cwe.mitre.org/data/definitions/200.html

Presenza della password dell'utente *root* all'interno dello storage di *Redis*

- **Descrizione**: all'interno dello storage del *key-value store 'Redis'* è presente una chiave chiamata *'rootkey'* alla quale è associata la password dell'utente *root*;
- **Modalità di individuazione**: la vulnerabilità è stata individuata durante la ricerca di un metodo per effettuare la *privilege escalation* all'interno del sistema, dopo aver effettuato l'accesso con l'utente *'auxerre'*;
- **Rischi associati**: l'utilizzo di tale password permette ad un utente non privilegiato di accedere all'account *root*, ottenendo, in questo modo, i massimi privilegi all'interno del sistema;
- **Severity**: Alta;
- **CWE di riferimento**: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor);
- **Soluzione**: rimuovere la chiave *'rootpass'* all'interno dello storage di *Redis*;
- **Riferimenti**: https://cwe.mitre.org/data/definitions/200.html

Bibliografia

[1] "Cve-2003-1418 detail." (Citato a pagina 5)