UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INFORMATICA

Corso di **Penetration Testing and Ethical Hacking**

NoobBox-1:

Penetration Testing Report

ANNO ACCADEMICO 2022/2023

Docente:

Prof. Arcangelo Castiglione

Studente:

Hermann Senatore

Indice

1 Scopi e struttura del documento

Il **Penetration Testing Report** consiste in un resoconto, articolato in diversi livelli di dettaglio, sulle varie fasi del processo di Penetration Testing condotto sull'asset.

Tale documento è articolato in diverse sezioni. Ciascuna di queste si concentra su aspetti diversi. In particolare:

1. **Executive Summary**: in questa sezione viene svolta una sintesi dei risultati del processo e dello stato generale di sicurezza del sistema analizzato;

2. **Engagement Highlights**: in questa sezione vengono esplicitate le regole di ingaggio tra chi ha commissionato l'indagine ed il Penetration Tester, le metodologie e gli obiettivi dell'analisi;

3. **Vulnerability Report**: in questa sezione viene fornita una visione d'insieme delle problematiche di sicurezza di cui l'asset è affetto;

4. **Findings Summary**: in questa sezione vengono presentate con maggior livello di dettaglio le vulnerabilità riscontrate durante il processo di Penetration Testing;

5. **Remediation Report**: in questa sezione sono proposte eventuali soluzioni alle vulnerabilità ed alle debolezze descritte nella sezione precedente;

6. **Detailed Summary**: in questa sezione è presente una discussione approfondita sulle problematiche individuate in precedenza.

2 Executive Summary

Il processo di Penetration Testing che questo documento sommarizza è stato svolto su un asset *vulnerable by default* denominato **NoobBox-1** reperibile presso la piattaforma **VulnHub** all'indirizzo `https://www.vulnhub.com/entry/noobbox-1,664/`. Nato come sfida CTF, è stato utilizzato dall'autore del presente documento per prendere confidenza con i tool e le metodologie più utilizzate nel contesto del Penetration Testing.

Gli obiettivi che sono stati fissati e raggiunti in questo processo consistono sostanzialmente in:

- Identificazione ed enumerazione completa dei servizi presenti all'interno dell'asset;
- Rilevamento delle vulnerabilità e delle debolezze presenti all'interno dell'asset;
- Ottenere accesso privilegiato alla macchina;
- Provvedere all'installazione di software specializzato per permettere l'accesso persistente all'asset.

L'attività di Penetration Testing è stata condotta a partire dal giorno 22 maggio 2023 ed ha avuto una connotazione **grey box** poiché alcune informazioni sono reperibili direttamente dalla piattaforma VulnHub e che fungono da punto di partenza.

Il livello di rischio derivato dall'analisi è stato classificato come **Medio-Alto** perché sebbene non siano presenti vulnerabilità intrinseche dei servizi in esecuzione che siano direttamente sfruttabili, è stato comunque possibile ottenere accesso privilegiato alla macchina mediante **errori di configurazione** e pratiche di sicurezza **scorrette**.

Una volta applicate le migliorie e le correzioni descritte nella sezione denominata **Remediation Report**, il livello di rischio scenderebbe ad un livello tale da non permettere più l'accesso non autorizzato alla macchina.

3 Engagement Highlights

Poiché l'analisi descritta da questo documento consiste in un progetto di stampo accademico e l'asset considerato ha questo tipo di analisi come scopo dichiarato, non sono state definite delle limitazioni dal punto di vista legale o contrattuale.

In particolare, non sono presenti parti dell'asset che non sarebbero dovute essere analizzate così come non è stata imposta alcuna limitazione riguardo gli strumenti da utilizzare.

Inoltre, non è stato (ovviamente) previsto alcun accordo di non-divulgazione.

4 Vulnerability Report

In questa sezione viene proposta un'*overview* delle problematiche di sicurezza presenti sull'asset.

In particolare, le problematiche appartengono alle categorie di:

- Information disclosure;
- Obsolescenza del software utilizzato dall'asset;
- Errori di configurazione e cattive pratiche di sicurezza;

4.1 Information Disclosure

Alcune informazioni sensibili che possono essere ricollegate a meccanismi di funzionamento interni all'asset sono **pubblicamente accessibili**. In particolare, visitando il sito web offerto dall'asset all'URL `/img.jpg` è possibile rinvenire la password dell'utente amministratore di **Wordpress**. Inoltre, lo username di quest'ultimo è enumerabile mediante scansioni automatiche. Entrambi questi aspetti consentono immediatamente l'accesso non autorizzato all'asset.

4.2 Obsolescenza del software utilizzato nell'asset

Alcune componenti dell'asset sono ormai **obsolete**. In particolare, il server web **Apache httpd** è aggiornato alla versione **2.4.38**, rilasciata il **22 gennaio 2019**. Questa versione del software risulta essere afflitta da alcune vulnerabilita. Sebbene nessuna di queste sia risultata sfruttabile per ottenere l'accesso alla macchina, l'obsolescenza dei software, sia nel caso di `httpd2` che di qualunque altro software rende sempre più probabile la compromissione dell'asset man mano che passa il tempo.

4.3 Cattive pratiche di sicurezza

L'utente della macchina locale possiede **lo stesso username** dell'utente che amministra il sito web creato con **Wordpress**. Una situazione del genere semplifica notevolmente il processo di enumerazione dell'asset, che può condurre alla sua compromissione. A peggiorare la situazione è stata la constatazione di un **riuso** della password per i due account. Una situazione del genere consente ad un attaccante di accedere ai file personali dell'utente locale dell'asset.

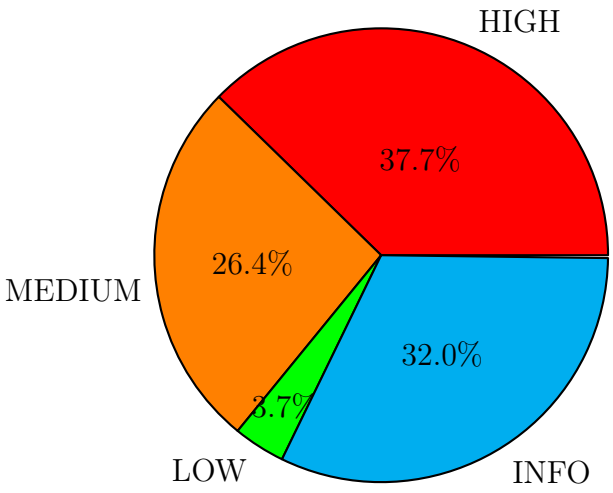
È stata inoltre rilevata la possibilità per l'utente locale di eseguire software con privilegi **ingiustamente elevati**. Quest'ultimo aspetto, in caso di accesso non autorizzato, permette di effettuare **Privilege Escalation**.

5 Findings Summary

In questa sezione viene proposta una panoramica dei risultati della fase di **Vulnerability Assessment**, che si propone di rilevare le vulnerabilità di cui l'asset è affetto. Siccome per eseguire la ricerca delle vulnerabilità è stato utilizzato più di un tool, il conto delle vulnerabilità non includerà più volte una vulnerabilità già riscontrata una volta. Il totale tra vulnerabilità riscontrate ed informazioni ammonta a **53**. Nessuna delle vulnerabilità di livello alto si è rivelata sfruttabile.

Seguono dei diagrammi che forniscono una più chiara ripartizione dei rilevamenti.

Livello di Rischio	HIGH	MEDIUM	LOW	INFO
# vulnerabilità	20	14	2	17



6 Remediation Report

In questa sezione verranno presentate delle strategie per risolvere o mitigare le problematiche di sicurezza emerse durante il processo svolto e documentate nella Sezione 4.

6.1 Remediation per Information Disclosure

1. **Eliminare** il file `img.jpg` dalla root del web server per evitare di divulgare la password dell'amministratore di **Wordpress**;

2. Installare e configurare il plugin di Wordpress **Stop User Enumeration** per contrastare tool di enumerazione automatica [1];

3. Aggiornare il profilo dell'amministratore di **Wordpress** ed utilizzare un **Display Name** diverso dallo username.

6.2 Remediation per Obsolescenza del software

La strategia più semplice (ma anche la migliore!) per risolvere le criticità appartenenti a questa categoria consiste nell'applicare in maniera frequente le **patch dei vendor** dei vari software in esecuzione, con una particolare attenzione ad **Apache httpd**. Tale processo può essere svolto sia **manualmente** che **automaticamente**, utilizzando sistemi di scheduling dei task come ad esempio `cron` nei momenti in cui tipicamente il traffico verso il sito web è minore.

6.3 Remediation per Cattive pratiche di sicurezza

1. Modificare lo username dell'utente della macchina locale (o quello dell'admin di Wordpress) per far sì che non siano identici e contrastare il processo di enumerazione;

2. Ripetere lo stesso procedimento descritto al punto precedente per le **password** dei due account;

3. Eliminare dal file `/etc/sudoers` la possibilità per l'utente `noobbox` di eseguire il comando `vim` come utente `root`.

7 Detailed Summary

In questa sezione vengono fornite informazioni dettagliate sulle vulnerabilità e sulle debolezze di cui l'asset è affetto che sono state riscontrate durante il processo di Penetration Testing nella fase di **Vulnerability Mapping**.

Per assolvere a tale compito, sono stati utilizzati in particolare tre tools:

1. **Nessus**;
2. **OpenVAS**;
3. **LinPEAS**, utilizzato per ottenere informazioni utili alla **Privilege Escalation** ma che ha permesso di rilevare vulnerabilità che affliggono, tra gli altri, il tool `sudo`.

7.1 Nessus

Un resoconto dettagliato delle vulnerabilità rilevate dal tool **Nessus** è allegato al presente documento ed è presente al percorso `extra/Nessus-Scan.pdf`. Si noti che tale tool ha prodotto **due falsi positivi**, di cui è stato discusso nella documentazione del processo. In particolare, le vulnerabilità etichettate come:

- 42423 - CGI Generic SSI Injection (HTTP headers);
- 57640 - Web Application Information Disclosure

sono falsi positivi e come tali **non sono stati considerati nel conteggio finale delle vulnerabilità**

7.2 OpenVAS

Parimenti, un resoconto dettagliato delle vulnerabilità rilevate dal tool **OpenVAS** è allegato al presente documento ed è presente al percorso `extra/OpenVAS-Scan.pdf`.

7.3 LinPEAS

Poiché tale tool non fornisce un output strutturato, sono di seguito riportate informazioni dettagliate sulla natura delle vulnerabilità rilevate.

7.3.1 CVE-2019-13272

- **Descrizione:** nelle versioni del Kernel Linux precedenti alla 5.1.17, la funzione `ptrace_link()` all'interno del file `kernel/ptrace.c` gestisce male le credenziali di un processo che intende sfruttare il meccanismo delle relazioni `ptrace`. In determinati scenari, tipicamente quando sussiste una relazione padre-figlio, la situazione potrebbe essere sfruttata da un utente locale per ottenere **accesso root**.
- **Livello di Impatto**: HIGH;
- **Punteggio CVSS v3**: 7.8;
- **Riferimento**: [2]
- **Contromisura**: effettuare un aggiornamento software, in particolare del **kernel**.

7.3.2 CVE-2019-18634

- **Descrizione:** nelle versioni di `sudo` precedenti alla 1.8.26, l'opzione `pwfeedback` (utilizzata per far apparire degli asterischi mentre si sta digitando la password ad un prompt di `sudo`) attivabile all'interno del file `/etc/sudoers` permetteva ad un attaccante di veicolare un attacco di **stack based buffer overflow** mediante l'utilizzo di una stringa di caratteri molto lunga.
- **Livello di Impatto**: HIGH;
- **Punteggio CVSS v3**: 7.8;
- **Riferimento**: [3]

- **Contromisura**: effettuare un aggiornamento software, in particolare del pacchetto **sudo**.

7.3.3 CVE-2021-22555

- **Descrizione:** nelle versioni del Kernel Linux a partire dalla 2.6.19-rc1 è stato rilevato un **heap-out-of-bound write** nel file `net/netfilter/x_tables.c`, tramite il quale è possibile veicolare un attacco di **Denial of Service** usando la tecnica dell'**heap based memory corruption**.
- **Livello di Impatto**: HIGH;
- **Punteggio CVSS v3**: 7.8;
- **Riferimento**: [4]
- **Contromisura**: effettuare un aggiornamento software, in particolare del **kernel**.

7.4 Altre debolezze e criticità

Oltre alle vulnerabilità rilevate dai tool prima menzionati, l'asset è affetto da ulteriori debolezze ed errori di configurazione che possono portare ad accessi non autorizzati e **privilege escalation**.

7.4.1 Disclosure della password di Wordpress

- **Descrizione**: alla pagina `http://192.168.64.21/img.jpg` è possibile visualizzare una password che può essere ricondotta facilmente a quella dell'amministratore di wordpress;
- **Rischi e potenziali attacchi**: in combinazione con la debolezza che riguarda l'enumerabilità degli utenti di Wordpress già rilevata da **Nessus**, tale debolezza può essere utilizzata per impersonare l'amministratore di **Wordpress**;
- **Contromisura**: eliminare il file `img.jpg` dal web server.

7.4.2 Riuso degli username e delle password

- **Descrizione**: sia l'utente locale dell'asset che l'admin di Wordpress condividono la stessa coppia di credenziali.
- **Rischi e potenziali attacchi**: nel caso un attaccante riesca ad entrare in possesso delle credenziali di un account, ha automaticamente compresso anche l'altro;
- **Contromisura**: cambiare nome utente e password ad uno dei due account.

7.4.3 Esecuzione di `vim` come root

- **Descrizione**: tale politica di sicurezza scorretta è stata rilevata sia manualmente andando ad analizzare il file `/etc/sudoers` che mediante **LinPEAS**. La configurazione corrente del tool `sudo` non permette all'utente `noobbox` di eseguire alcun comando come root, ad eccezione del comando

`vim`. Anche in questo modo è comunque possibile ottenere una shell di root.

- **Rischi e potenziali attacchi**: l'esecuzione dell'editor `vim` supporta l'esecuzione di un "comando" dell'editor subito dopo il suo avvio. Mediante la command line `vim -c ':!<cmd>'` è possibile eseguire il comando di shell `<cmd>` all'apertura dell'editor. Usando `sudo vim -c ':!/bin/bash'` viene aperta una **shell di root**.

- **Contromisura**: inibire anche l'accesso al comando `vim` andando a modificare il file `/etc/sudoers` ed eliminare le righe che recitano:

```
User noobbox may run the following commands on N00bBox:
    (ALL : ALL) /usr/bin/vim
```

Riferimenti bibliografici

[1] *Stop User Enumeration - Plugin WordPress*. https://it.wordpress.org/plugins/stop-user-enumeration/. URL consultato l'8 giugno 2023.

[2] *CVE-2019-13272*. https://nvd.nist.gov/vuln/detail/cve-2019-13272. URL consultato l'8 giugno 2023.

[3] *CVE-2019-18634*. https://nvd.nist.gov/vuln/detail/cve-2019-18634. URL consultato l'8 giugno 2023.

[4] *CVE-2019-13272*. https://nvd.nist.gov/vuln/detail/cve-2021-22555. URL consultato l'8 giugno 2023.