Università degli Studi di Salerno

Penetration Testing Report

FIRST BLOOD: 1

Benedetto Sommese | Corso di PTEH | A.A. 2020/2021

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

Capitolo 1: Executive Summary

Per l'attività progettuale di Penetration Testing è stato condotto un tipico processo di penetration testing sulla macchina target "First Blood: 1", reperita su VulnHub al seguente link:

- https://www.vulnhub.com/entry/firstblood-1,564/

Tutte le attività sono state svolte in modo da simulare le possibili azioni di un attaccante. Gli obiettivi da raggiungere durante questo processo sono i seguenti:

- rilevare i servizi offerti dall'asset target;
- determinare la presenza di vulnerabilità sull'asset target;
- ottenere il controllo della macchina target;
- elevare i permessi fino a raggiungere i permessi di root;
- istallare una backdoor, in modo da avere un accesso persistente sulla macchina target.

Durante questo processo sono state rilevate due vulnerabilità di livello critico, due vulnerabilità di livello alto, una vulnerabilità di livello medio e una vulnerabilità di livello basso.

Questo documento contiene un'analisi delle vulnerabilità riscontrate e una serie di soluzioni da adoperare per mitigare gli eventuali problemi di sicurezza riscontrati. Tutto ciò verrà illustrato nel dettaglio.

Capitolo 2: Vulnerability Report

Durante l'analisi della macchina in questione sono state trovate alcune vulnerabilità che la espongono ad attacchi da parte di utenti malintenzionati. Ecco un elenco delle vulnerabilità rilevate:

1. vulnerabilità del servizio nginx che potrebbe portare all'arresto totale della risorsa, in modo da renderla completamente non disponibile;
2. vulnerabilità del servizio SSH che potrebbe permettere l'enumerazione degli utenti;
3. vulnerabilità che permette di calcolare il timestamp e di calcolare il tempo di attività dell'host;
4. possibilità di recuperare credenziali di accesso all'interno di file e pagine Web.
5. utilizzo di password deboli che permettono di effettuare l'accesso tramite attacchi online di forza bruta (servizio SSH aperto sulla porta 60022);
6. facoltà per alcuni utenti di poter di eseguire comandi di sistema con i permessi di altri utenti o dell'utente root. Questo consente di ottenere il controllo totale della macchina.

Capitolo 3: Remediation Report

Per porre rimedio alle vulnerabilità riscontrate durante l'attività di Penetration Testing dovrebbero essere messe in atto le seguenti strategie:

1. aggiornare la versione di nginx;
2. aggiornare la versione di OpenSSH;
3. disabilitare il TCP timestamp;
4. rimuovere le credenziali di accesso all'interno di file e all'interno delle pagine Web poiché qualunque malintenzionato potrebbe recuperarle.
5. utilizzare password complesse poiché la macchina permette l'accesso remoto tramite SSH;
6. non permettere ad utenti di eseguire comandi di sistema con i permessi di altri utenti o con i permessi dell'utente root, in modo da evitare l'elevazione di privilegi.

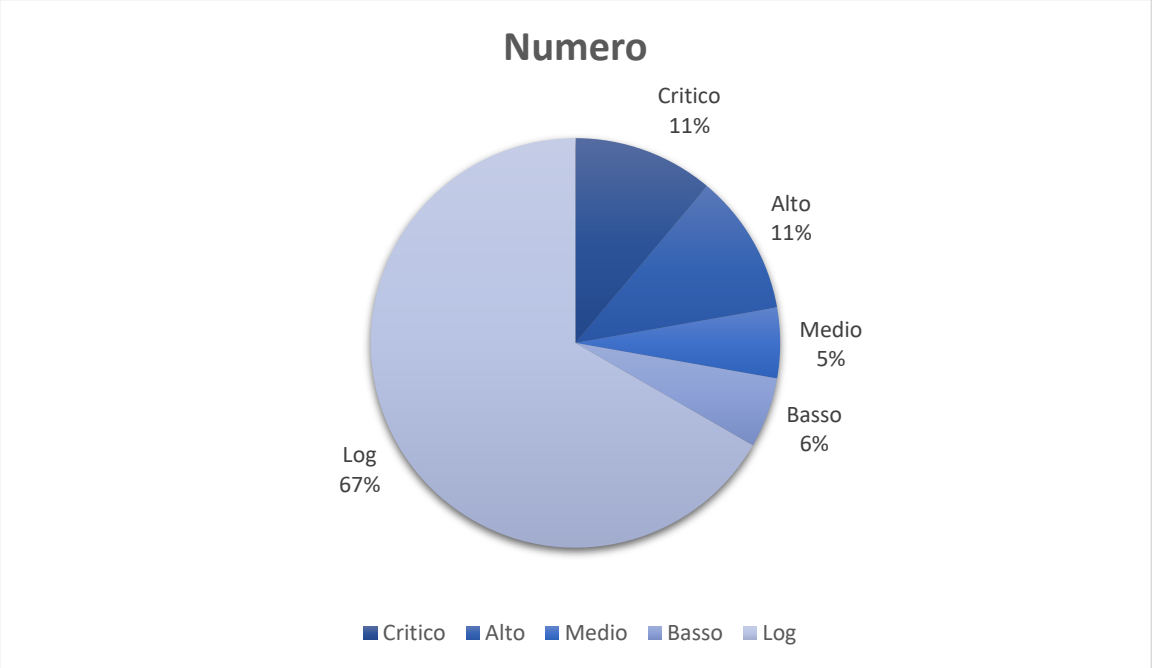
Capitolo 4: Findings Summary

All'interno di questa sezione mostreremo maggiori informazioni riguardo le vulnerabilità riscontrate presenti sulla macchina target. Tali vulnerabilità sono state trovate tramite una scansione manuale e una scansione automatica dell'asset. Queste vulnerabilità verranno valutate seguendo la seguente scala di valori, la quale indica il livello di rischio associato a ciascuna vulnerabilità:

- critico, per vulnerabilità che dovrebbero essere sistemate immediatamente in quanto rappresentano un pericolo serio per la sicurezza del sistema. Infatti, tipicamente lo sfruttamento di queste vulnerabilità non richiede tecniche avanzate o delle particolari conoscenze;
- alto, per vulnerabilità che dovrebbero essere risolte al più presto in quanto mettono il sistema in pericolo. Questo tipo di vulnerabilità sono più difficili da sfruttare rispetto al tipo precedente;
- medio, per le vulnerabilità che dovrebbero essere affrontate tempestivamente. Detto ciò, questo tipo di vulnerabilità è più difficile da sfruttare;
- basso, per vulnerabilità che possono essere affrontate in un secondo momento poiché potrebbero non rappresentare una seria minaccia;
- log, per vulnerabilità che non rappresentano una minaccia per la macchina target.

La scansione sull'asset ha prodotto i seguenti risultati:

Hostname	Critico	Alto	Medio	Basso	None
First Blood: 1	2	2	1	1	12



Capitolo 5: Detailed Summary

All'interno di questa sezione verranno riportate nel dettaglio tutte le vulnerabilità riscontrate.

4.1: Servizio nginx 1.14.0

All'interno di questo paragrafo andiamo a dettagliare la vulnerabilità rilevata relativa al servizio nginx.

CVE-2018-16843	
Criticità	Alta
Versioni coinvolte	Nginx before 1.15.6 and 1.14.1
Descrizione	Questa vulnerabilità è dovuta all'implementazione di HTTP/2 e potrebbe consentire un consumo eccessivo della memoria, portando all'arresto totale della risorsa, in modo da renderla completamente non disponibile
Soluzione	Aggiornare la versione di nginx
Link riferimento	https://www.cvedetails.com/cve/CVE-2018-16843/

4.2: Servizio OpenSSH 7.6p1

All'interno di questo paragrafo andiamo a dettagliare la vulnerabilità rilevata relativa al servizio OpenSSH.

CVE-2018-15473	
Criticità	Media
Versioni coinvolte	OpenSSH 2.3 < 7.7
Descrizione	Questa vulnerabilità permette di effettuare l'enumerazione degli utenti
Soluzione	Aggiornare la versione di OpenSSH
Link riferimento	https://www.exploit-db.com/exploits/45233

4.3: TCP Timestamp

All'interno di questo paragrafo andiamo a dettagliare la vulnerabilità rilevata relativa al TCP Timestamp.

CVE-2018-15473	
Criticità	Bassa
Descrizione	Questa vulnerabilità permette di calcolare il timestamp e di calcolare il tempo di attività dell'host
Soluzione	Disabilitare il TCP Timestamp
Link riferimento	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.80091

4.4: Recupero credenziali di accesso

All'interno di questo paragrafo andiamo a dettagliare la vulnerabilità rilevata relativa alle credenziali di accesso presenti all'interno di file di testo o pagine Web.

Recupero credenziali di accesso all'interno di file o pagine Web	
Criticità	Critica
Descrizione	Questa vulnerabilità permette a qualunque malintenzionato di recuperare credenziali di accesso all'interno di file di testo e pagine Web. Queste credenziali possono essere utilizzate per accedere al sistema da remoto utilizzando il servizio SSH
Soluzione	Rimuovere le credenziali da accesso dalle pagine Web e dai file di testo

4.5: Utilizzo di password deboli

All'interno di questo paragrafo andiamo a dettagliare la vulnerabilità rilevata relativa all'utilizzo di password deboli da parte di alcuni utenti della macchina target.

Utilizzo di password deboli per l'accesso al sistema	
Criticità	Critica
Descrizione	Questa vulnerabilità permette ad un malintenzionato di forzare l'accesso alla macchina target utilizzando un attacco di forza bruta
Soluzione	Utilizzare password difficili da indovinare

4.6: Esecuzione comandi di sistema con altri privilegi

All'interno di questo paragrafo andiamo a dettagliare la vulnerabilità rilevata relativa alla facoltà da parte di alcuni utenti di poter eseguire comandi di sistema utilizzando privilegi di altri utenti

Esecuzione comandi di sistema con privilegi di altri utenti	
Criticità	Alta
Descrizione	Questa vulnerabilità permette ad alcuni utenti di poter eseguire comandi di sistema utilizzando privilegi di altri utenti. Nel dettaglio, l'utente "sly" è capace di eseguire il comando ftp come root e tale comando può essere utilizzato per ottenere una root shell. Inoltre, l'utente "blood", utilizzando i privilegi dell'utente "sly", è capace di eseguire il comando cat su un file di testo di cui "sly" è proprietario, al cui interno è presente la password in chiaro
Soluzione	Non permettere agli utenti l'esecuzione di comandi di sistema con i privilegi di altri utenti