Universitá degli studi di Salerno

Penetration Testing

The Planets: Earth

Report

Relatore
Prof. **Arcangelo Castiglione**

Candidato
Carmine D'Angelo
Matricola: 05225 00881

Anno Accademico 2021-2022

Indice

Capitolo 1

Executive Summary

Per il progetto di Penetration Testing è stato scelto di effettuare un processo di penetration testing etico sulla macchina virtuale The Planets: Earth, reperibile sulla piattaforma vulnhub al seguente link: https://www.vulnhub.com/entry/the-planets-earth,755/. Gli obiettivi da raggiungere sono i seguenti:

- Enumerare servizi e vulnerabilità presenti sulla macchina target

- Prendere possesso della macchina target;

- Prendere possesso del flag root_flag.txt;

- Instaurare una back-door.

L'attività di penetration testing sulla macchina target ha avuto inizio il 7/06/2022.
Questa tipologia di attacco rientra nella categoria di grey box testing, in quanto prima di iniziare il processo avevamo conoscenza soltanto del sistema operativo presente sulla macchina target. Non conoscevamo informazioni importanti come l'indirizzo IP e i vari servizi attivi. Durante la fase di penetration testing si seguirà anche l'ideologia di un white-hat hacker con l'obiettivo di scoprire , verificare e notificare vulnerabilità del sistema che attestino la sua fragilità; il tutto nel rispetto delle regole etiche. Si cercherà anche di fornire soluzioni da adoperare per mitigare gli eventuali problemi di sicurezza riscontrati. In questo report verranno illustrate tutte le vulnerabilità che sono state individuate durante il processo di penetration testing.

Capitolo 2

Engagement Highlights

L'attività di penetration testing che verrà eseguita ha un fine didattico quindi non è stata fatta nessuna contrattazione con il cliente. Saranno quindi utilizzati i tool che possono risultare più efficienti nella ricerca delle informazioni e nell'esecuzione dei task, senza che questi comportino particolari limitazioni. L'intero progetto ha seguito le fasi che sono state insegnate durante l'intero corso:

- Information Gatering & Target Discovery;
- Enumeration Target & Port Scanning;
- Vulnerability Mapping;
- Exploitation;
- Post-Exploitation (privilege escalation);
- Post-Exploitation (mantaining access).

Nella prima fase è stato utilizzato come tool di riferimento nmap, il cui output è stato messo a confronto con diversi altri tool come netdiscover e p0f.
Nella seconda fase è stato come tool per effettuare port scanning e enumeration è stato utilizzato nmap, mentre per osservare eventuali directory indicizzate è stato utilizzato il tool dirb.
Per il vulnerability mapping sono stati utilizzati i tool Nessun e OpenVass.
Per la la fase di exploitation, invece, è stato possibile ottenere un accesso alla macchina grazie al servizio web presente all'url https://terratest.earth.local/admin. Sfruttando l'accesso ottenuto alla macchina tramite il servizio precedentemente menzionato si è riuscito a svolgere privelege escalation sfruttando un file di reset password probabilmente lasciato per sbaglio da uno sviluppatore.
Infine si è tentato di installare una backdoor ma non ci si è riusciti per mancanza di exploit da sfruttare nel momento in cui è stato fatto penetration testing, si è tentato anche di installare una backdoor php ma non essendo installato sulla macchina target risulta inutilizzabile.

Capitolo 3

Vulnerability Report

L'analisi di The Planets: Earth ha portato alla luce diversi tipi di vulnerabilità, che saranno successivamente elencate. Tra le vulnerabilità più critiche riscontrate troviamo:

- Indicizzazione di file importanti come robot.txt .
- Indicizzazione del file testingnotes.txt probabilmente lasciato da uno sviluppatore in cui sono contenuti informazioni su quale algoritmo di cifratura si utilizza per le password e l'username dell'utente admin.
- Presenza della password dell'admin sulla home page.
- Problematica legata all'esecuzione di comandi remoti nella pagina dell'admin senza effettuare controlli efficaci.
- Presenza sulla macchina target del file reset_root che permette il reset della password dell'utente root.
- Presenza di software obsoleti sulla macchina che espongono la macchina a molte vulnerabilità conosciute o meno e possono portare un eventuale utente a ottenere il controllo remoto della macchina.

Capitolo 4

Remediation Report

La macchina The Planets: Earth possiede un grado di rischio molto elevato, per cercare di mitigare questo fattore è possibile prendere le seguenti contromisure:

- Effettuare un aggiornamento di Apache alla versione 2.4.53 o successive.
- Effettuare un aggiornamento di OpenSSL 1.1.1 a OpenSSL 1.1.1o o successive.
- Togliere l'indicizzazione di file importanti come robot.txtx.
- Usare algoritmi di cifratura più sicuri come l'hashing.
- Effettuare dei controlli migliori sull'input che può inserire l'admin nella propria area.
- Migliorare l'attività dei programmatori, in particolare focalizzarsi sulla pericolosità di rimanere file di test sul server o la presenza di file che possono portare modifiche al sistema eseguibili da chiunque.
- Pianificare periodicamente un controllo della sicurezza al fine di valutare la sicurezza del sistema e la presenza di nuove vulnerabilità.
- Aggiornare continuamente i servizi utilizzati.

Capitolo 5

Findings Summary

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

- CRITICAL: vulnerabilità che possono avere un impatto elevato e che possono consentire ad un utente malintenzionato di ottenere un controllo completo o parziale del sistema.
- HIGH: vulnerabilità che richiedono determinati requisiti per poter essere sfruttate e hanno un impatto relativamente alto sul sistema.
- MEDIUM: vulnerabilità non semplici da sfruttare e che, nella maggior parte dei casi, non hanno un impatto diretto molto significativo.
- LOW: vulnerabilità che hanno un impatto poco significativo e che hanno una bassa probabilità di essere sfruttate e, pertanto, non rappresentano, nell'immediato, una minaccia rilevante per il sistema.
- INFO: non sono vulnerabilità ma sono informazioni su configurazioni di software che nel futuro potrebbero generare delle vulnerabilità.

La tabella seguente mostra il numero di vulnerabilità individuate per ogni categoria:

	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTALE
#**Vulnerabilità**	**8**	**2**	**7**	**0**	**47**	**64**

Tabella 5.1: Classificazione vulnerabilità

Di seguito è mostrato anche un grafico a torta per avere una visione più dettagliata sul numero di vulnerabilità presenti:

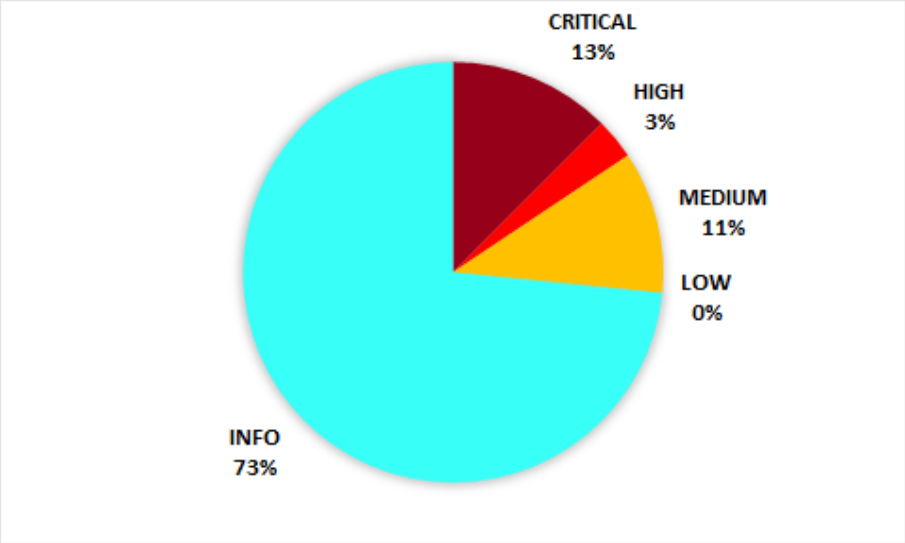

Figura 5.1: grafico a torta delle vulnerabilità

Capitolo 6

Detailed Summary

In questa sezione verranno elencate e descritte tutte le vulnerabilità riscontrate utilizzando il tool Nessus.

6.1 Vulnerabilità classificate: CRITICAL

Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	**CVE**
	CVE-2021-44790[1]
Descrizione: La versione di Apache httpd installata sull'host remoto è precedente alla 2.4.52. È quindi presente un difetto relativo a mod_lua. Una richiesta accuratamente impostata può causare un buffer overflow nel parser multipart di mod_lua. Al momento non si è a conoscenza di un exploit per la vulnerabilità anche se potrebbe essere possibile crearne uno.	
Soluzione: Eseguire l'upgrade ad Apache versione 2.4.52 o successiva.	

Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	**CVE**
	CVE-2021-44224[2] CVE-2021-44790[1]
Descrizione: La versione di Apache httpd installata sull'host remoto è uguale o maggiore di 2.4.7 e precedente a 2.4.52. Essa è, pertanto affetta da forward proxy. Un URI malizioso inviato a httpd configurato come proxy forward può causare un arresto anomalo o, per configurazioni che mescolano dichiarazioni proxy forward e reverse, può consentire che le richieste vengano indirizzate a un endpoint Unix Domain Socket questo porta alla falsificazione delle richieste lato server.	
Soluzione: Eseguire l'upgrade ad Apache versione 2.4.52 o successiva.	

Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	**CVE**
	CVE-2022-22719[3] CVE-2022-22720[4] CVE-2022-22721[5] CVE-2022-23943[6]
Descrizione: - mod_lua: uso di un valore non inizializzato di in r:parsebody, una richiesta settata accuratamente può causare una lettura in un'area di memoria casuale che potrebbe causare il crash del processo (CVE-2022-22719). - Vulnerabilità di smuggling di richieste HTTP in Apache HTTP Server 2.4.52 e precedenti. Apache HTTP Server 2.4.52 e versioni precedenti non riesce a chiudere la connessione in entrata quando si verificano errori che eliminano il corpo della richiesta, esponendo il server a HTTP Request Smuggling (CVE-2022-22720). - core: possibile overflow del buffer con il valore LimitXMLRequestBody molto grande o illimitato. Se LimitXMLRequestBody è impostato per consentire corpi di richiesta più grandi di 350 MB (predefinito su 1 M) su sistemi a 32 bit si verifica un overflow intero che in seguito provoca scritture in area di memoria non consentite (CVE-2022-22721) - mod_sed: lettura/scrittura oltre i limiti imposti. La vulnerabilità di scrittura in mod_sed di Apache HTTP Server consente a un utente malintenzionato di sovrascrivere la memoria heap con i dati eventualmente forniti dall'utente malintenzionato(CVE-2022-23943).	
Soluzione: Eseguire l'upgrade ad Apache versione 2.4.53 o successiva.	

OpenSSL 1.1.1 < 1.1.1o command injection	**CVE**
	CVE-2022-1292[7]
Descrizione: Lo script c_rehash non sanifica correttamente i metacaratteri della shell per impedire l'iniezione di comandi. Questo script in alcuni sistemi operativi viene eseguito automaticamente, su tali sistemi operativi, un utente malintenzionato potrebbe eseguire comandi arbitrari con i privilegi dello script. L'uso dello script c_rehash è considerato obsoleto e dovrebbe essere sostituito dallo strumento da riga di comando di rehash OpenSSL.	
Soluzione: Eseguire l'upgrade di OpenSSL alla versione 1.1.1o o successiva.	

6.2 Vulnerabilità classificate: HIGH

OpenSSL 1.1.1 < 1.1.1n forever loop	**CVE**
	CVE-2022-0778[8]
Descrizione: La funzione BN_mod_sqrt(), che calcola una radice quadrata modulare, contiene un bug che può causare un ciclo continuo per i moduli non primi. Questa funzione viene utilizzata durante l'analisi di certificati che contengono chiavi pubbliche creati tramite curve ellittiche. È possibile attivare il ciclo infinito creando un certificato con i parametri delle curve ellittiche non validi. Poiché l'analisi del certificato avviene prima della verifica della firma del certificato, qualsiasi processo che analizza un certificato fornito esternamente può quindi essere soggetto a un attacco Denial of Service.	
Soluzione: Eseguire l'upgrade di OpenSSL alla versione 1.1.1n o successiva.	

6.3 Vulnerabilità classificate: MEDIUM

HSTS Missing From HTTPS Server	**CVE**
	-
Descrizione: Il server Web remoto non applica HSTS, come definito da RFC 6797. HSTS è un'intestazione di risposta opzionale che può essere configurata sul server per indicare al browser di comunicare solo tramite HTTPS. La mancanza di HSTS consente attacchi di downgrade, attacchi man-in-the-middle che eliminano SSL e indebolisce le protezioni contro il dirottamento dei cookie.	
Soluzione: Configurare il server web remoto in modo da usare HSTS.	

HTTP TRACE / TRACK Methods Allowed	**CVE**
	CVE-2003-1567[9] CVE-2004-2320[10] CVE-2010-0386[11]
Descrizione: Il server web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP utilizzati per eseguire il debug delle connessioni al server web.	
Soluzione: Disabilitare i metodi HTTP Trace/ Track	

OpenSSL 1.1.1 < 1.1.1m Vulnerability	**CVE**
	CVE-2021-4160[12]
Descrizione: Esiste un carry propagation bug in MIPS32 e MIPS64. Molti algoritmi EC sono interessati da questo bug, comprese alcune EC predefinite di TLS 1.3. L'impatto non è stato analizzato, perché i prerequisiti per l'attacco sono considerati improbabili e includono il riutilizzo delle chiavi private. Gli attacchi contro RSA e DSA a seguito di questo difetto sarebbero molto difficili da eseguire e non si ritiene probabile. Gli attacchi contro DH sono considerati semplicemente fattibili (sebbene molto difficili) perché la maggior parte del lavoro necessario per dedurre informazioni su una chiave privata può essere eseguita offline. La quantità di risorse necessarie per un simile attacco sarebbe significativa. Tuttavia, affinché un attacco a TLS sia significativo, il server dovrebbe condividere la chiave privata DH tra più client, cosa che non è più un'opzione.	
Soluzione: Aggiorna OpenSSL alla versione 1.1.1m o successive.	

Cerificato SSL non attendibile	**CVE**
	-
Descrizione: Il certificato X.509 del server non può essere considerato attendibile.	
Soluzione: Comprare o aggiornare il certificato SSL	

OpenSSL 1.1.1 < 1.1.1m Vulnerability	**CVE**
	CVE-2021-4160[12]
Descrizione: Esiste un carry propagation bug in MIPS32 e MIPS64. Molti algoritmi EC sono interessati da questo bug, comprese alcune EC predefinite di TLS 1.3. L'impatto non è stato analizzato, perché i prerequisiti per l'attacco sono considerati improbabili e includono il riutilizzo delle chiavi private. Gli attacchi contro RSA e DSA a seguito di questo difetto sarebbero molto difficili da eseguire e non si ritiene probabile. Gli attacchi contro DH sono considerati semplicemente fattibili (sebbene molto difficili) perché la maggior parte del lavoro necessario per dedurre informazioni su una chiave privata può essere eseguita offline. La quantità di risorse necessarie per un simile attacco sarebbe significativa. Tuttavia, affinché un attacco a TLS sia significativo, il server dovrebbe condividere la chiave privata DH tra più client, cosa che non è più un'opzione.	
Soluzione: Aggiorna OpenSSL alla versione 1.1.1m o successive.	

Certificato SSL autofirmato	CVE
	-
Descrizione: La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se l'host remoto è un host pubblico in produzione, ciò annulla l'uso di SSL poiché chiunque potrebbe stabilire un attacco man-in-themiddle contro l'host remoto.	
Soluzione: Comprare o aggiornare il certificato SSL	

6.4 Vulnerabilità classificate: INFO

Apache HTTP Server Version	CVE
	-
Descrizione: Il server remoto utilizza come host Apache HTTP Server, è possibile leggere la versione del server.	

Common Platform Enumeration (CPE)	CVE
	-
Descrizione: È possibile enumerare i nomi CPE corrispondenti sul sistema remoto.	

Device Type	CVE
	-
Descrizione: È possibile indovinare il sistema operativo della macchina target.	

Ethernet Card Manufacturer Detection	CVE
	-
Descrizione: Ogni indirizzo MAC Ethernet inizia con un Organizationally Unique Identifier (OUI) di 24 bit. Questi OUI sono registrati da IEEE.	

Ethernet MAC Addresses	CVE
	-
Descrizione: Questo plugin raccoglie gli indirizzi MAC scoperti sia dal rilevamento remoto dell'host (ad es. SNMP e Netbios) sia dall'esecuzione di controlli locali (ad es. ifconfig). Quindi consolida gli indirizzi MAC in un elenco unico, univoco e uniforme.	

HTTP Server Type and Version	CVE
	-
Descrizione: È possibile determinare il tipo e la versione del server remoto.	

Host Fully Qualified Domain Name (FQDN) Resolution	**CVE**
	-
Descrizione: È possibile risalire al nome del server remoto.	

HyperText Transfer Protocol (HTTP) Information	**CVE**
	-
Descrizione: È possibile risalire a diverse informazioni sulla configurazione del protocollo HTTP.	

ICMP Timestamp Request Remote Date Disclosure	**CVE**
	CVE-1999-0524[13]
Descrizione: L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un utente malintenzionato di conoscere la data impostata sul computer preso di mira, il che può aiutare un utente malintenzionato remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo.	
Soluzione: Filtra le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita (14).	

Inconsistent Hostname and IP Address	**CVE**
	-
Descrizione: Il nome dell'host remoto non combacia con le informazioni del DNS.	

SYN scanner	**CVE**
	-
Descrizione: È possibile determinare quale porte TCP sono aperte.	
Soluzione: Applicare un filtro IP sulla macchina.	

OS Identification	**CVE**
	-
Descrizione: È possibile determinare il sistema operativo della macchina target.	

OpenSSL Version Detection	**CVE**
	-
Descrizione: È possibile determinare la versione di OpenSSl.	

SSH Password Authentication Accepted	**CVE**
	-
Descrizione: Il server SSH sull'host remoto accetta l'autenticazione via password.	

SSH Protocol Versions Supported	**CVE**
	-
Descrizione: È possibile determinare la versione di SSH utilizzata.	

SSH SHA-1 HMAC Algorithms Enabled	**CVE**
	-
Descrizione: Il server remoto SSH è configurato per utilizzare l'algoritmo SHA-1 HMAC.	

SSL / TLS Versions Supported	**CVE**
	-
Descrizione: Il server remoto utilizza SSL/TLS per criptare le comunicazioni.	

SSL Cipher Block Chaining Cipher Suites Supported	**CVE**
	-
Descrizione: Il servizio remoto supporta l'uso di crittografie SSL Cipher Block Chaining, che combinano i blocchi precedenti con quelli successivi.	

SSL Perfect Forward Secrecy Cipher Suites Supported	**CVE**
	-
Descrizione: Il servizio remoto supporta l'uso di crittografie SSL Perfect Forward Secrecy, che mantengono la riservatezza anche in caso di furto della chiave.	

TLS Version 1.2 Protocol Detection	**CVE**
	-
Descrizione: Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.2.	

TLS Version 1.3 Protocol Detection	**CVE**
	-
Descrizione: Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.3.	

Bibliografia

[1] CVE Details, "Vulnerability details : CVE-2021-44790." https://nvd.nist.gov/vuln/detail/CVE-2021-44790.

[2] CVE Details, "Vulnerability details : CVE-2021-44224." https://nvd.nist.gov/vuln/detail/CVE-2021-44224.

[3] CVE Details, "Vulnerability details : CVE-2022-22719." https://nvd.nist.gov/vuln/detail/CVE-2022-22719.

[4] CVE Details, "Vulnerability details : CVE-2022-22720." https://nvd.nist.gov/vuln/detail/CVE-2022-22720.

[5] CVE Details, "Vulnerability details : CVE-2022-22721." https://nvd.nist.gov/vuln/detail/CVE-2022-22721.

[6] CVE Details, "Vulnerability details : CVE-2022-23943." https://nvd.nist.gov/vuln/detail/CVE-2022-23943.

[7] CVE Details, "Vulnerability details : CVE-2022-1292." https://nvd.nist.gov/vuln/detail/CVE-2022-1292.

[8] CVE Details, "Vulnerability details : CVE-2022-0778." https://nvd.nist.gov/vuln/detail/CVE-2022-0778.

[9] CVE Details, "Vulnerability details : CVE-2003-1567." https://nvd.nist.gov/vuln/detail/CVE-2003-1567.

[10] CVE Details, "Vulnerability details : CVE-2004-2320." https://nvd.nist.gov/vuln/detail/CVE-2004-2320.

[11] CVE Details, "Vulnerability details : CVE-2010-0386." https://nvd.nist.gov/vuln/detail/CVE-2010-0386.

[12] CVE Details, "Vulnerability details : CVE-2021-4160." https://nvd.nist.gov/vuln/detail/CVE-2021-4160.

[13] CVE Details, "Vulnerability details : CVE-1999-0524." https://nvd.nist.gov/vuln/detail/CVE-1999-0524.