UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Magistrale in Informatica

CORSO DI PENETRATION TESTING
AND ETHICAL HACKING

Gaara:
Penetration Testing Report

STUDENTE

Alessandro Aquino

Matricola: 0522501563

DOCENTE

Prof. **Arcangelo Castiglione**

Università degli studi di Salerno

Anno Accademico 2023-2024

Indice

CAPITOLO 1

Penetration Testing Report

1.1 Executive Summary

Al fine di realizzare il progetto del corso *Penetration Testing and Ethical Hacking* sono state svolte delle attività di Penetration Testing su una macchina virtuale vulnerabile chiamata **Gaara**. Il fine ultimo di tutte le attività svolte è stato semplicemente didattico, con lo scopo di acquisire al meglio tutte le conoscenze fornite durante lo svolgimento del corso. 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.txt;
- Instaurare una back-door.

L'attività di penetration testing sulla macchina target ha avuto inizio il 21/04/2023. Questa tipologia di attacco rientra nella categoria 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 e contrassegnare vulnerabilità del sistema che attestino la sua fragilità, fatto in modo etico. Si cercherà poi di fornire soluzioni da adoperare per mitigare i problemi

di sicurezza riscontrati. In questo report verranno illustrate tutte le vulnerabilità che sono state individuate durante il processo di penetration testing.

1.2 Engagement Highlights

Essendo un progetto universitario nell'ambito del corso *Penetration Testing and Ethical hacking* ed essendo che l'ambiente su cui è effettuato l'intero processo è *virtualizzato*, non ci sono **NDA** da rispettare e non ci sono vincoli sulle tecniche che è possibile utilizzare o sulle parti dell'asset da analizzare.

1.3 Vulnerability Report

Durante il processo sono state trovate varie vulnerabilità, alcune di queste con gravità **medium** e **low**. Le principali sono le seguenti:

- SSH Terrapin Prefix Truncation Weakness (gravità **media**): Il server SSH remoto è vulnerabile a una debolezza di troncamento del prefisso man-in-the-middle nota come Terrapin. Questo può consentire a un attaccante remoto man-in-the-middle di bypassare i controlli di integrità e degradare la sicurezza della connessione
- ICMP Timestamp Request Remote Date Disclosure (gravità **bassa**): L'host remoto risponde a una richiesta di timestamp ICMP. Questo consente a un attaccante di conoscere la data impostata sulla macchina target, il che può aiutare un attaccante remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo.

1.4 Remediation Report

Durante il processo eseguito, sono state trovate molte vulnerabilità tra cui alcune abbastanza importanti che potrebbero comportare la compromissione completa del sistema e di file e documenti all'interno, nonchè la compromissione dei dati dei visitatori del sito web. Per questa ragione, si forniscono i seguenti consigli per migliorare la sicurezza dell'asset:

- 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;
- Configurare il web server *Apache* in modo tale da aggiungere attributi di sicurezza nelle pagine e da non supportare più protocolli crittografici deprecati e facilmente compromissibili;
- Aggiornare la versione di **jQuery** utilizzata nelle pagine web;
- Configurare il servizio *SSH* in modo tale che non supporti protocolli crittografici deboli;

1.5 Findings Summary

Durante l'attività di penetration testing sono state individuate numerose vulnerabilità nella macchina target Gaara: Le vulnerabilità individuate vengono solitamente suddivise in quattro classi in base alla loro gravità nel mio caso specifico ho riscontrato solo vulnerabilità presenti in medium e low:

- 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.

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

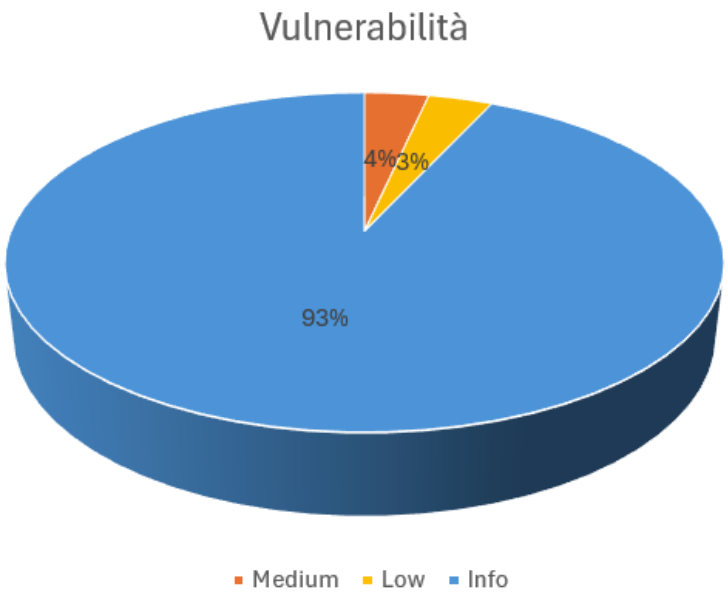

Figura 1.1: Grafico riassuntivo dei rilevamenti

1.6 Detailed Summary

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

1.6.1 Rilevamenti effettuati da *Nessus*

Titolo: HTTP Server Type and Version		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10107	
Sinossi: Un server web è in esecuzione sull'host remoto.		
Descrizione: Questo plugin tenta di determinare il tipo e la versione del server web remoto.		

Link: https://www.tenable.com/plugins/nessus/10107

Titolo: ICMP Timestamp Request Remote Date Disclosure		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
low	10114	2.1
Sinossi: È possibile determinare l'ora esatta impostata sull'host remoto.		
Descrizione: L'host remoto risponde a una richiesta di timestamp ICMP. Questo consente a un attaccante di conoscere la data impostata sulla macchina target, il che può aiutare un attaccante remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo.		
Soluzione: Filtrare le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita (14).		

Link: https://www.tenable.com/plugins/nessus/10114

Titolo: SSH Server Type and Version Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10267	
Sinossi: Un server SSH è in ascolto su questa porta.		
Descrizione: È possibile ottenere informazioni sul server SSH remoto inviando una richiesta di autenticazione vuota.		

Link: https://www.tenable.com/plugins/nessus/10267

Titolo: Traceroute Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10287	
Sinossi: È stato possibile ottenere informazioni di traceroute.		
Descrizione: Esegue un traceroute verso l'host remoto.		

Link: https://www.tenable.com/plugins/nessus/10287

Titolo: SSH Protocol Versions Supported		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	10881	
Sinossi: Un server SSH è in esecuzione sull'host remoto.		
Descrizione: Questo plugin determina le versioni del protocollo SSH supportate dal demone SSH remoto.		

Link: https://www.tenable.com/plugins/nessus/10881

Titolo: Target Credential Status by Authentication Protocol - No Credentials Provided		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	110723	
Sinossi: Nessus è stato in grado di trovare porte comuni utilizzate per i controlli locali, tuttavia, non sono state fornite credenziali nella politica di scansione.		
Descrizione: Nessus non è stato in grado di autenticarsi direttamente con successo al target remoto su un protocollo di autenticazione disponibile. Nessus è stato in grado di connettersi alla porta remota e identificare che il servizio in esecuzione sulla porta supporta un protocollo di autenticazione, ma Nessus non è riuscito ad autenticarsi al servizio remoto utilizzando le credenziali fornite. Potrebbe essersi verificato un errore di protocollo che ha impedito il tentativo di autenticazione o tutte le credenziali fornite per il protocollo di autenticazione potrebbero essere invalide. Vedi l'output del plugin per i dettagli dell'errore.		

Link: https://www.tenable.com/plugins/nessus/110723

Titolo: Nessus SYN scanner		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	11219	
Sinossi: È possibile determinare quali porte TCP sono aperte.		
Descrizione: Questo plugin è uno scanner di porte SYN 'half-open'. Dovrebbe essere ragionevolmente veloce anche contro un target con firewall.		
Soluzione: Proteggi il tuo target con un filtro IP.		

Link: https://www.tenable.com/plugins/nessus/11219

Titolo: OS Security Patch Assessment Not Available		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	117886	
Sinossi: La valutazione delle patch di sicurezza del sistema operativo non è disponibile.		
Descrizione: La valutazione delle patch di sicurezza del sistema operativo non è disponibile sull'host remoto.		

Link: https://www.tenable.com/plugins/nessus/117886

Titolo: OS Identification		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	11936	
Sinossi: È possibile indovinare il sistema operativo remoto.		
Descrizione: Utilizzando una combinazione di sonde remote (ad esempio, TCP/IP, SMB, HTTP, NTP, SNMP, ecc.), è possibile indovinare il nome del sistema operativo remoto in uso. È anche possibile talvolta indovinare la versione del sistema operativo.		

Link: https://www.tenable.com/plugins/nessus/11936

Titolo: SSH Password Authentication Accepted		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	149334	
Sinossi: Il server SSH sull'host remoto accetta l'autenticazione tramite password.		
Descrizione: Il server SSH sull'host remoto accetta l'autenticazione tramite password.		

Link: https://www.tenable.com/plugins/nessus/149334

Titolo: SSH SHA-1 HMAC Algorithms Enabled		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	153588	
Sinossi: Il server SSH remoto è configurato per abilitare gli algoritmi SHA-1 HMAC.		
Descrizione: Il server SSH remoto è configurato per abilitare gli algoritmi SHA-1 HMAC.		

Link: https://www.tenable.com/plugins/nessus/153588

Titolo: OpenSSH Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	181418	
Sinossi: È stato rilevato un server SSH basato su OpenSSH sull'host remoto.		
Descrizione: È stato rilevato un server SSH basato su OpenSSH sull'host remoto.		

Link: https://www.tenable.com/plugins/nessus/181418

Titolo: SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
medium	187315	5.9
Sinossi: Il server SSH remoto è vulnerabile a un attacco di troncamento del prefisso mitm.		
Descrizione: Il server SSH remoto è vulnerabile a una debolezza di troncamento del prefisso man-in-the-middle nota come Terrapin. Questo può consentire a un attaccante remoto man-in-the-middle di bypassare i controlli di integrità e degradare la sicurezza della connessione.		
Soluzione: Contattare il fornitore per un aggiornamento con le contromisure di scambio chiavi rigorose o disabilitare gli algoritmi interessati.		

Link: https://www.tenable.com/plugins/nessus/187315

Titolo: Nessus Scan Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	19506	
Sinossi: Questo plugin visualizza informazioni sulla scansione Nessus.		
Descrizione: Questo plugin visualizza, per ciascun host testato, informazioni sulla scansione stessa.		

Link: https://www.tenable.com/plugins/nessus/19506

Titolo: Service Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	22964	
Sinossi: Il servizio remoto potrebbe essere identificato.		
Descrizione: Nessus è stato in grado di identificare il servizio remoto tramite il suo banner o osservando il messaggio di errore che invia quando riceve una richiesta HTTP.		

Link: https://www.tenable.com/plugins/nessus/22964

Titolo: HyperText Transfer Protocol (HTTP) Information		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	24260	
Sinossi: Alcune informazioni sulla configurazione HTTP remota possono essere estratte.		
Descrizione: Questo test fornisce alcune informazioni sul protocollo HTTP remoto: la versione utilizzata, se HTTP Keep-Alive è abilitato, ecc.		

Link: https://www.tenable.com/plugins/nessus/24260

Titolo: TCP/IP Timestamps Supported		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	25220	
Sinossi: Il servizio remoto implementa i timestamp TCP.		
Descrizione: L'host remoto implementa i timestamp TCP, come definito da RFC1323. Un effetto collaterale di questa funzione è che a volte è possibile calcolare il tempo di attività dell'host remoto.		

Link: https://www.tenable.com/plugins/nessus/25220

Titolo: Ethernet Card Manufacturer Detection		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	35716	
Sinossi: Il produttore può essere identificato dall'OUI Ethernet.		
Descrizione: Ogni indirizzo MAC Ethernet inizia con un Identificatore Unico Organizzativo (OUI) a 24 bit. Questi OUI sono registrati dall'IEEE.		

Link: https://www.tenable.com/plugins/nessus/35716

Titolo: Backported Security Patch Detection (SSH)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	39520	
Sinossi: Le patch di sicurezza sono backportate.		
Descrizione: Le patch di sicurezza potrebbero essere state 'backportate' al server SSH remoto senza modificare il numero di versione.		

Link: https://www.tenable.com/plugins/nessus/39520

Titolo: Backported Security Patch Detection (WWW)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	39521	
Sinossi: Le patch di sicurezza sono backportate.		
Descrizione: Le patch di sicurezza potrebbero essere state 'backportate' al server HTTP remoto senza modificare il numero di versione.		

Link: https://www.tenable.com/plugins/nessus/39521

Titolo: HTTP Methods Allowed (per directory)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	43111	
Sinossi: Questo plugin determina quali metodi HTTP sono consentiti su varie directory CGI.		
Descrizione: Chiamando il metodo OPTIONS, è possibile determinare quali metodi HTTP sono consentiti su ogni directory.		

Link: https://www.tenable.com/plugins/nessus/43111

Titolo: Common Platform Enumeration (CPE)		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	45590	
Sinossi: È stato possibile enumerare i nomi CPE corrispondenti sul sistema remoto.		
Descrizione: Utilizzando le informazioni ottenute da una scansione Nessus, questo plugin riporta le corrispondenze CPE (Common Platform Enumeration) per vari prodotti hardware e software trovati su un host.		

Link: https://www.tenable.com/plugins/nessus/45590

Titolo: Apache HTTP Server Version		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	48204	
Sinossi: È possibile ottenere il numero di versione del server Apache HTTP remoto.		
Descrizione: L'host remoto esegue Apache HTTP Server, un server web open source. È stato possibile leggere il numero di versione dal banner.		

Link: https://www.tenable.com/plugins/nessus/48204

Titolo: Device Type		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	54615	
Sinossi: È possibile indovinare il tipo di dispositivo remoto.		
Descrizione: Basandosi sul sistema operativo remoto, è possibile determinare quale tipo di sistema remoto è (ad esempio: una stampante, un router, un computer generico, ecc).		

Link: https://www.tenable.com/plugins/nessus/54615

Titolo: Patch Report		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	66334	
Sinossi: L'host remoto è privo di diverse patch.		
Descrizione: L'host remoto è privo di una o più patch di sicurezza. Questo plugin elenca la versione più recente di ciascuna patch da installare per assicurarsi che l'host remoto sia aggiornato.		
Soluzione: Installare le patch elencate di seguito.		

Link: https://www.tenable.com/plugins/nessus/66334

Titolo: SSH Algorithms and Languages Supported		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	70657	
Sinossi: Un server SSH è in ascolto su questa porta.		
Descrizione: Questo script rileva quali algoritmi e linguaggi sono supportati dal servizio remoto per crittografare le comunicazioni.		

Link: https://www.tenable.com/plugins/nessus/70657

Titolo: Ethernet MAC Addresses		
Classe	**Nessus Plugin ID**	**CVSS v3 Base Score**
info	86420	
Sinossi: Questo plugin raccoglie indirizzi MAC da varie fonti e li consolida in un elenco.		
Descrizione: Questo plugin raccoglie indirizzi MAC rilevati sia da sonde remote dell'host (ad esempio, SNMP e Netbios) che dall'esecuzione di controlli locali (ad esempio, ifconfig). Successivamente consolida gli indirizzi MAC in un elenco unico, uniforme e univoco.		

Link: https://www.tenable.com/plugins/nessus/86420