REPORT TECNICO

Destinato a tecnico “Mario”

Azienda “Struffoli”

Redatto da Andrea Sciattella

08/05/2024

INDICE

1. Traccia ..... Errore. Il segnalibro non è definito.
2. Sommario esecutivo 4
Panoramica risultati principali 4
3. Introduzione 5
Scopo del report e tools utilizzati 5
4. Risultati della scansione 6
Elenco vulnerabilità rilevate, CVSS e CVE 10
5. Conclusioni 11
Riassunto delle principali conclusioni e raccomandazioni 11

1. TRACCIA

Effettuare un Vulnerability Assessment con Nessus sulla macchina **Metasploitable** indicando come target solo le **porte comuni** (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo) A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

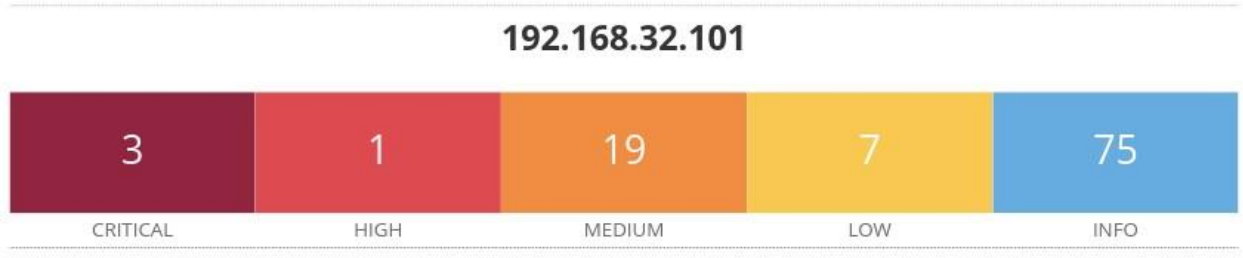
- Gli obiettivi dell'esercizio sono: **Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.**
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Consegna:

•Report PDF per «tecnico» Report tecnico è inteso come "quasi completo" che va ad indicare sia le porte che la vulnerabilità che la risoluzione, in modo da poter intervenire.

•Suggerimento: fare traduzione in italiano della descrizione e/o remediation.

2. SOMMARIO ESECUTIVO



INFORMAZIONI HOST:

Nome NetBIOS: "**METASPLOITABLE**";

Indirizzo IP: **192.168.32.101**;

Indirizzo MAC: **08:00:27:03:10:A4;**

OS: **Unix-Linux.**

Per questo vulnerabilities assesment abbiamo utilizzato Nessus, è un software proprietario di tipo Client-Server di scansione di tutti i tipi di vulnerabilità, uno dei migliori in questi ambiti.

La scansione effettuata, dalla durata di circa 20 minuti, è riuscita a rilevare 30 vulnerabilities, divise in 3 **CRITIC**, 1 **HIGH**, 19 **MEDIUM** e 7 **LOW** e 75 addizionali categorizzate in **INFO** visto la loro importanza quasi nulla.

Abbiamo scelto la modalità base di scanning, con un range ports da 1 a 1024.

La condizione dell'host si è rilevata immediatamente **critica** e assolutamente da risolvere tempestivamente per via delle CVE rivelate che possono portare all'exploit di reverse shell.

La maggior parte delle vulnerabilità rilevate può essere risolta immediatamente tramite l'applicazione di patch e aggiornamenti ai servizi retrodatati e obsoleti presenti nell'host "**METASPLOITABLE**".

3. INTRODUZIONE

PREMESSA: Questo report è stato compilato dopo ogni test del Vuln. Assesment, di conseguenza verranno esposte falle e problemi degli host presi di mira, **MANTENERE QUESTO DOCUMENTO CONFIDENZIALE**.

Nel panorama sempre più interconnesso e digitale del mondo odierno, la sicurezza informatica è diventata un pilastro fondamentale per garantire la protezione dei dati sensibili e dei sistemi critici. In questo contesto, la valutazione delle vulnerabilità rappresenta un'attività cruciale per identificare e mitigare le potenziali minacce che possono compromettere *l'integrità, la disponibilità e la riservatezza* (*CIA Triad*) delle risorse informatiche di un'organizzazione.

Il presente rapporto si propone di condurre un'analisi dettagliata delle vulnerabilità presenti nel sistema in esame, al fine di fornire una panoramica esaustiva sullo stato attuale della sicurezza informatica e suggerire le strategie più appropriate per migliorare la resilienza e protezione del sistema.

Attraverso una metodologia rigorosa e l'impiego delle più recenti tecniche di scansione e analisi, questo report mira a fornire una base solida per l'implementazione di misure preventive e correttive efficaci, allo scopo di ridurre il rischio di violazioni della sicurezza e proteggere il patrimonio informativo dell'organizzazione.

Specificatamente, è stato analizzato e scansionato un host molto problematico, piuttosto retrodatato e rimasto attivo per forza di cose.

In questo documento analizzeremo per filo e per segno ogni sua possibile “apertura all’esterno” e quindi potenziale accesso da parte di estranei nella vostra rete.

4. RISULTATI DELLA SCANSIONE

- 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness:

Sinossi:

Le chiavi host SSH remote sono deboli.

Descrizione:

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto ad un pacchettizzatore Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzare questo per impostare decifrare la sessione o impostare un Man In The Middle.

Soluzione:

Considera tutto il materiale crittografico generato sull'host remoto come prevedibile. In particolare, tutti gli SSH, Il materiale chiave SSL e OpenVPN dovrebbe essere rigenerato.

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score: 8.3 (CVSS2#E:F/RL:OF/RC:C)

BID: 29179

CVE: CVE-2008-0166

XREF: CWE:310

Plugin Output: tcp/22/ssh

- 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check):

Sinossi:

Il certificato SSL remoto utilizza una chiave debole.

Descrizione:

Il certificato remoto x509 sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

Il problema è dovuto ad un pacchettizzatore Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o realizzare un attacco man in the middle.

CVSS v2.0 Base Score: 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score: 8.3 (CVSS2#E:F/RL:OF/RC:C)

BID: 29179

CVE: CVE-2008-0166

XREF: CWE:310

Plugin Output: tcp/25/smtp

- 20007 - SSL Version 2 and 3 Protocol Detection:

Sinossi:

Il servizio remoto crittografa il traffico utilizzando un protocollo con debolezze note.

Descrizione:

Il servizio remoto accetta connessioni cifrate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono colpite da diversi difetti crittografici, tra cui:

- Un sistema di riempimento insicuro con cifrari CBC.

- Regimi insicuri di rinegoziazione e ripresa delle sessioni.

Un attaccante può sfruttare questi difetti per condurre attacchi man-in-the-middle o per decifrare le comunicazioni tra il servizio interessato e i clienti.

Anche se SSL/ TLS ha un mezzo sicuro per la scelta della versione più alta supportato del protocollo (così che queste versioni saranno utilizzate solo se il client o il server supportano nulla di meglio), molti browser web implementare questo in modo non sicuro che permette a un utente malintenzionato di declassare una connessione (come in POODLE).

Pertanto, si raccomanda di disabilitare completamente questi protocolli.

NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di applicazione trovata in PCI DSS v3.1, qualsiasi versione di SSL non soddisfa la definizione PCI SSC di 'forte crittografia.

Soluzione:

Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Usa invece TLS 1.2 (con suite di cifratura approvate) o superiori.

Risk Factor: Critical

CVSS v3.0 Base Score :9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score :10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information Published: 2005/10/12, Modified: 2022/04/04

Plugin Output: tcp/25/smtp

- 10205 - rlogin Service Detection:

Sinossi:

Il servizio rlogin è in esecuzione sull'host remoto.

Descrizione:

Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile in quanto i dati vengono scambiati tra il client e il server rlogin in chiaro. Un utente man-in-the-middle malintenzionato può sfruttare questa situazione per sniffare login e password.

Inoltre, potrebbe consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'indovinare il numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (compreso l'hijacking ARP su una rete locale), allora potrebbe essere possibile ignorare l'autenticazione.

Infine, rlogin è un modo semplice per trasformare l'accesso in scrittura ai file in accessi completi tramite i file .rhosts o rhosts.equiv.

Soluzione:

Commentare la riga “login” in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare il servizio e utilizzare invece SSH.

Fattore di rischio: Alto

Punteggio base CVSS v2.0: 7,5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE: CVE-1999-0651

Sfruttabile con: Metasploit (vero)

Informazioni sul plugin Pubblicato: 1999/08/30, Modificato: 2022/04/11

Uscita del plugin: tcp/513/rlogin

- 11213 - HTTP TRACE / TRACK Methods Allowed:

Sinossi:

Le funzioni di debug sono abilitate sul server web remoto.

Descrizione:

Il server Web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi HTTP che vengono utilizzati per eseguire il debug delle connessioni al server web.

Soluzione:

Disattivare questi metodi HTTP. Per ulteriori informazioni, consultare l'output del plugin.

Fattore di rischio: Medio

Punteggio base CVSS v3.0: 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Punteggio temporale CVSS v3.0: 4.6 (CVSS:3.0/E:U/RL:O/RC:C)

Punteggio base CVSS v2.0: 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Punteggio temporale CVSS v2.0: 3.7 (CVSS2#E:U/RL:OF/RC:C)

BID: 9506

BID: 9561

BID: 11604

BID: 33374

BID: 37995

CVE: CVE-2003-1567

CVE: CVE-2004-2320

CVE: CVE-2010-0386

XREF: CERT:288308

XREF: CERT:867593

XREF: CWE:16

XREF: CWE:200

Informazioni sui plugin Pubblicato: 2003/01/23, Modificato: 2024/04/09

Uscita del plugin: tcp/80/www

5. CONCLUSIONI

Arrivati alla fine possiamo trarre che in primo luogo, è fondamentale agire tempestivamente per affrontare le **tre vulnerabilità critiche** individuate.

Queste sono le più gravi e potrebbero essere sfruttate da attaccanti per ottenere accesso non autorizzato ai sistemi, eseguire codice dannoso o compromettere l'intero ambiente IT. La priorità dovrebbe essere data alla risoluzione di queste vulnerabilità, implementando le correzioni o le contromisure appropriate il più rapidamente possibile per ridurre al minimo il rischio.

Successivamente ci possiamo occupare della **vulnerabilità di livello alto** che richiede attenzione immediata, sebbene potenzialmente meno grave rispetto alle critiche.

Questo tipo di vulnerabilità potrebbe ancora essere sfruttato da attaccanti per ottenere accesso non autorizzato o compromettere la sicurezza del sistema.

Pertanto, è consigliabile trattare questa vulnerabilità con urgenza, applicando le necessarie misure correttive.

Infine, la **vulnerabilità di livello medio**, sebbene meno critica, non dovrebbe essere trascurata. Anche se il suo impatto potrebbe essere meno grave rispetto alle altre, potrebbe comunque rappresentare una potenziale minaccia per la sicurezza.

È importante pianificare e programmare la risoluzione di questa vulnerabilità in modo da mantenere un ambiente IT sicuro e resiliente nel lungo termine.

In conclusione, il report di Vulnerability Assessment evidenzia la necessità di adottare misure immediate per affrontare le vulnerabilità critiche e alte, insieme a un piano per mitigare la vulnerabilità di livello medio.

Agendo tempestivamente per correggere queste vulnerabilità, andremo a ridurre significativamente il rischio di violazioni della sicurezza e si proteggeranno i sistemi e i dati aziendali da potenziali minacce che potrebbero causare migliaia e migliaia di Euro in danni e materiali sovrascritti, eliminati o sequestrati.