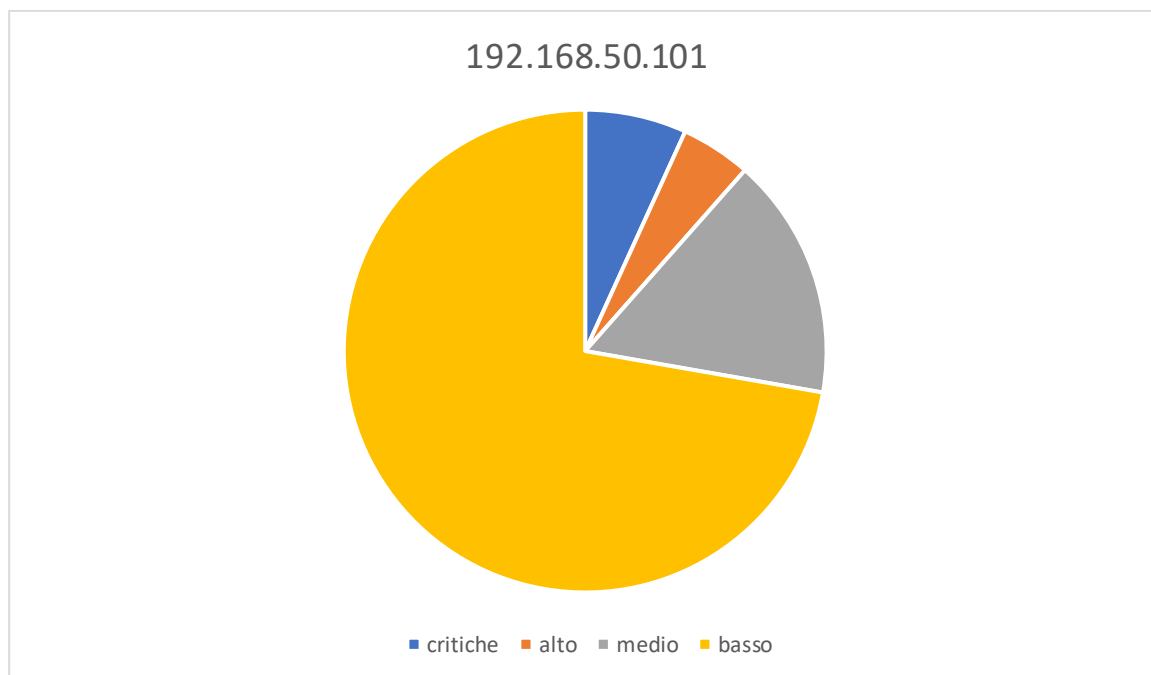


Report sulle Vulnerabilità – Metasploitable

La seguente analisi delle vulnerabilità è stata condotta sul sistema Metasploitable al fine di identificare le aree di rischio potenziale a fornire raccomandazioni per mitigare tali vulnerabilità.



Informazioni scansione

Inizio 26/08/2023 16:30:20

Fine 26/08/2023 16:34:15

Informazioni Host

Nome Host Metasploitable

IP 192.168.50.101

OS Linux Vulnerabilità **vsFTPd**
versione 2.3.4. Backdoor

Descrizione

La vulnerabilità CVE-2011-2523 è una backdoor presente nella versione 2.3.4. del server FTP vsftpd. Questa backdoor consente

ad un attaccante remoto di ottenere l'accesso al sistema senza le credenziali corrette. La backdoor è stata inserita nel codice sorgente del software e consente all'attaccante di eseguire comandi arbitrari con privilegi elevati(root) sul sistema compromesso.

Soluzione

Disabilita l'accesso FTP anonimo o limita l'accesso solo a utenti autorizzati.

Aggiornare vsftpd all'ultima versione.

```
not shown: 65535 closed tcp ports (conn refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.50.100
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
```

Fattore di rischio : Critico Vulnerabilità

Porta 25 e 5432 ssl-dh-params

Descrizione

Questa vulnerabilità consente a un attaccante di ricevere dati in chiaro utilizzando un attacco padding-oracle.

Soluzione

Assicurarsi di disabilitare ssl e utilizzare tls

```
25/tcp open smtp Postfix smtpd
|_ssl-date: 2023-08-24T18:52:55+00:00; +41s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
```

Fattore di rischio : Alto

Vulnerabilità

Porta 25 ssl-dh-params

Descrizione

Questa vulnerabilità riguarda l'Exchange di chiavi DH e potrebbe permettere a un attaccante di compromettere la confidenzialità e l'integrità dei dati.

Soluzione

Si consiglia di rinforzare l'uso di DH

```
25/tcp open smtp
| ssl-dh-params:
| VULNERABLE:
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
| State: VULNERABLE
| Transport Layer Security (TLS) services that use anonymous
| Diffie-Hellman key exchange only provide protection against passive
| eavesdropping, and are vulnerable to active man-in-the-middle attacks
| which could completely compromise the confidentiality and integrity
| of any data exchanged over the resulting session.
| Check results:
| ANONYMOUS DH GROUP 1
| Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: postfix builtin
| Modulus Length: 1024
| Generator Length: 8
| Public Key Length: 1024
| References:
| https://www.ietf.org/rfc/rfc2246.txt
```

Risoluzione prima vulnerabilità:

```
21/tcp open ftp          vsftpd 2.3.4
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.50.100
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPD 2.3.4 - secure, fast, stable
|_End of status
```

Spiegazione

Per mitigare questa vulnerabilità, è essenziale aggiornare il software vsftpd alla

versione più recente, che corregge questa vulnerabilità. Inoltre, è importante monitorare regolarmente i server FTP per rilevare eventuali attività sospette e adottare pratiche di sicurezza solide per proteggere i sistemi da intrusioni.

Inoltre è fondamentale tenere sempre aggiornati i software di sistema e le applicazioni per proteggere i sistemi da vulnerabilità conosciute e per garantire un ambiente di rete sicuro.

Seconda vulnerabilità :

```
25/tcp open smtp  
| smtp-vuln-cve2010-4344:  
|_ The SMTP server is not Exim: NOT VULNERABLE
```

Soluzione

Disabilitare SSL :

Verifica la configurazione del tuo server e assicurati che tutti i protocolli SSL siano disabilitati. SSL è considerato insicuro a causa di numerose vulnerabilità e dovrebbe essere evitato. Assicurati che solo i protocolli TLS siano abilitati.

Abilitare TLS con Parametri sicuri utilizzi le versioni più recenti dei protocolli TLS.

Terza vulnerabilità

```
25/tcp open smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
```

Soluzione

Rinforzare i parametri DH

Se il tuo server utilizza il protocollo DiffieHellman, assicurati che sia configurato con gruppi DH sufficientemente robusti. Evita l'uso di gruppi DH con lunghezza inferiore a 2048 bit.

