

Relazione Scan Target Metasploitable e Scan Ports tramite il Software Nessus Essentials

Nessus Essentials: è un Software Scanner semplice da utilizzare, ma allo stesso tempo potente, usato per coprire reti estese

- Utilizziamo Nessus per la scansione avanzata sul **Target METASPLOITABLE2:**
- Nella seguente immagine andremo a nominare il target: **Metasploitable2**
- Scrivo nella scheda **Targets** l'indirizzo IP della VM Matasploitable2: **192.168.1.28**

Metasploitable2 / Configuration

[Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Metasploitable2

Description:

Folder: My Scans

Targets: 192.168.1.28

Upload Targets [Add File](#)

Save Cancel

Nel seguente passaggio ed immagine, vado ad inserire le porte da scansionare, in TCP, come ad esempio: **range 21-3389:**

- Scrivo nella scheda **Port scan range: 21-3389**, così che Nessus effettui lo scan tra la porta 21 e la porta 3389

Metasploitable2 / Configuration

[Back to Scan Report](#)

Settings | Credentials | Plugins

BASIC

DISCOVERY

- Host Discovery
- Port Scanning
- Service Discovery
- Identity

Ports

☐ Consider unscanned ports as closed

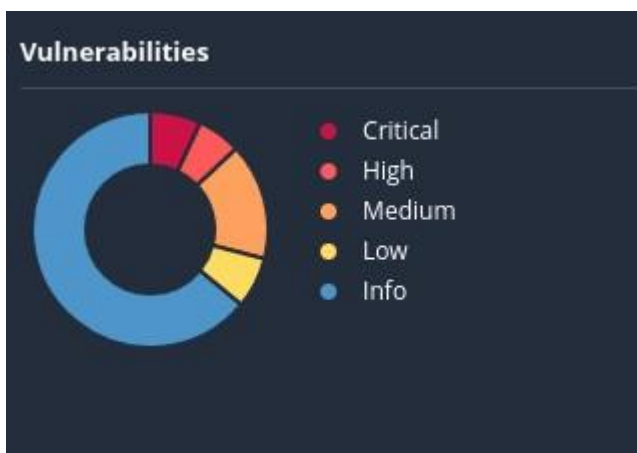
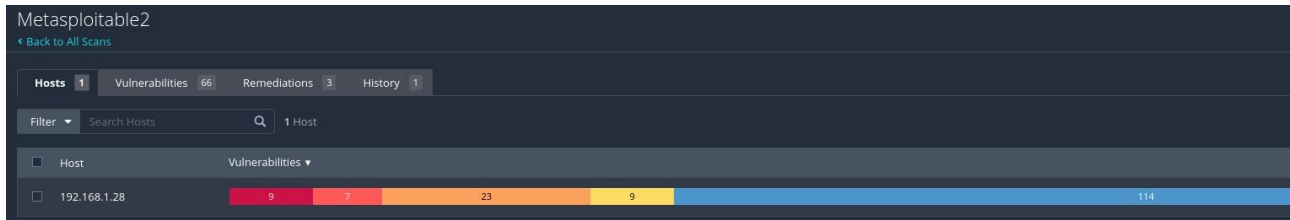
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.

Port scan range: 21-3389

Specifies the range of ports to be scanned.

Nel seguente passaggio ed immagine, possiamo vedere il risultato finale della scansione con i relativi colori che identificano i livelli di vulnerabilità:

- **Critical**
- **High**
- **Medium**
- **Low**
- **Info**



Nel seguente passaggio, dopo aver illustrato precedentemente i vari livelli di vulnerabilità, identificati con i vari colori, in ultimo, potremmo vedere i consigli che ci illustra **Nessus Essentials**, chiamate **Actions** per riparare e correggere le vulnerabilità:

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Analisi dei livelli di vulnerabilità

Per l'analisi dei vari livelli di vulnerabilità, tramite il Report finale creato da **Nessus Essentials**, come da seguente immagine, devo cliccare sul numero identificativo in **blu (PLUGIN)**, dove, posso vedere successivamente, la descrizione della vulnerabilità:

- **CRITICAL**

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **HIGH**

HIGH	8.6	5.2	0.0234	136769	ISC BIND Service Downgrade / Reflected DoS
------	-----	-----	--------	--------	--

- **MEDIUM**

MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
--------	-----	-----	--------	--------	--

- **LOW**

LOW	3.7	3.6	0.5961	70658	SSH Server CBC Mode Ciphers Enabled
-----	-----	-----	--------	-------	-------------------------------------

1. Analisi del livello di vulnerabilità: **Critical**

Apache Tomcat AJP Connector Request Injection (Ghostcat)

CRITICAL

Nessus Plugin ID 134862

Information

Dependencies

Dependents

Changelog

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

See Also

<http://www.nessus.org/u?8ebe6246>

<http://www.nessus.org/u?4e287adb>

<http://www.nessus.org/u?cbc3d54e>

<https://access.redhat.com/security/cve/CVE-2020-1745>

<https://access.redhat.com/solutions/4851251>

<http://www.nessus.org/u?dd218234>

<http://www.nessus.org/u?dd772531>

<http://www.nessus.org/u?2a01d6bf>

<http://www.nessus.org/u?3b5af27e>

<http://www.nessus.org/u?9dab109f>

<http://www.nessus.org/u?5eafcf70>

2. Analisi del livello di vulnerabilità: **High**

ISC BIND Service Downgrade / Reflected DoS

HIGH

Nessus Plugin ID 136769

Information

Dependencies

Dependents

Changelog

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

See Also

<https://kb.isc.org/docs/cve-2020-8816>

3. Analisi del livello di vulnerabilità: **Medium**

ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

MEDIUM Nessus Plugin ID 139915

Information

Dependencies

Dependents

Changelog

Synopsis

The remote name server is affected by a denial of service vulnerability.

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

See Also

<https://kb.isc.org/docs/cve-2020-8622>

4. Analisi del livello di vulnerabilità: **Low**

SSH Server CBC Mode Ciphers Enabled

LOW Nessus Plugin ID 70658

Information

Dependencies

Dependents

Changelog

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.