

S5L4,

BENVENUTI LUIGI, 22/02/2024

### 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.

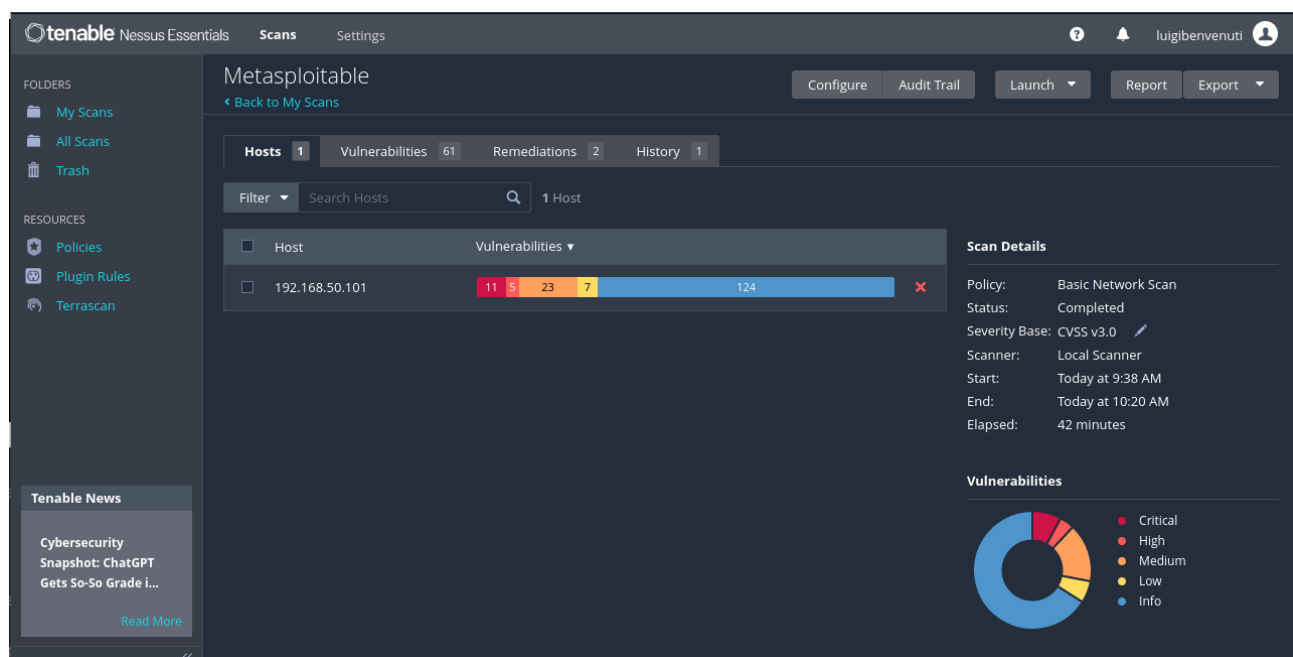
Gli obiettivi dell'esercizio sono:

- 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.

Una volta terminata l'installazione di Nessus, andiamo a sfruttarne le capacità di scansione verso la macchina Metasploitable, come precedentemente richiesto. Per fare ciò, selezioniamo la voce "Basic Network Scan", che ci fornisce una scansione con funzioni base di default, ed inseriamo come IP target quello della macchina Metasploitable.

Selezioniamo poi l'opzione <<port scan common ports>>, per andare a scansionare soltanto le porte più frequenti.

Il risultato della scansione è il seguente:



Scarichiamo il report in formato PDF utilizzando la funzione <<Report>> in alto a destra.

192.168.50.101



#### Vulnerabilities

Total: 106

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

Nella prima parte del report generato, ci vengono ricapitolate le vulnerabilità rilevate sulla macchina scansionata.

Vediamo nel dettaglio il significato di alcune voci:

- Severity: indica il grado di pericolosità di una vulnerabilità, ed ha 5 voci. Oltre a critical, high, medium e low, fornisce una voce info, che sta ad indicare che la macchina espone alcune possibili informazioni interessanti per un eventuale attaccante.
- CVSS: Common Vulnerability Scoring System, metodo standard di valutazione della gravità di una vulnerabilità.
- VPR score: Vulnerability Priority Rating, è uno score fornito direttamente da Nessus che consiglia un'indice di priorità nell'applicazione delle patch.
- Plugin: indica l'ID plugin di Nessus che ha scovato la vulnerabilità.
- Name: indica il nome della vulnerabilità rilevata.

Analizziamo una criticità per ogni severity, cercando di capirne il significato.

## 1- Critical

Prendiamo in esame la criticità con pericolosità Critical di nome “VNC Server Password password”;

Questa vulnerabilità ha CVSS 10, quindi massimo. Essa sta ad indicare che una virtual network computing app ha come password di accesso “password”, facilmente reperibile da un potenziale attaccante. Si potrebbe sfruttare la vulnerabilità per lanciare una shell e prendere il comando del server.

Vediamo le specifiche della voce fornite da Nessus:

The screenshot displays the Nessus interface for a specific vulnerability. At the top, a tab labeled 'Vulnerabilities' shows a count of 61. The main header indicates a 'CRITICAL' severity for the 'VNC Server 'password' Password' vulnerability. The interface is divided into several sections: 'Description' explains that the VNC server is secured with a weak password, allowing an attacker to login and take control; 'Solution' advises securing the VNC service with a strong password; 'Output' shows a log entry: 'Nessus logged in using a password of "password".' and a table of hosts with port 5900/tcp/vnc open. On the right, 'Plugin Details' lists metadata like ID (61708), Version (\$Revision: 1.2 \$), and Type (remote). Below that, 'Risk Information' provides the Risk Factor (Critical), CVSS v2.0 Base Score (10.0), and CVSS v2.0 Vector (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C). At the bottom right, a section for 'Vulnerability Information' is partially visible.

Port	Hosts
5900 / tcp / vnc	192.168.50.101

## 2- High

Prendiamo in esame la criticità con pericolosità High di nome NFS Shares World Readable.

Si riferisce alla famiglia delle RPC (chiamate di procedura remota), ovvero la capacità di avviare un programma da un computer diverso da quello host. In particolare, un server NFS trasmette esportazioni di rete sensibili in maniera leggibile. Nessus consiglia di raffinare le restrizioni applicate allo sharing del file system in questione. Questa debolezza ha CVSS 7.5.

HIGH

NFS Shares World Readable

< >

Plugin Details

✎

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Solution

Place the appropriate restrictions on all NFS shares.

See Also

<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Output

The following shares have no access restrictions :

/ \*

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / tcp / rpc-nfs	192.168.50.101

Severity:

High

ID:

42256

Version:

1.12

Type:

remote

Family:

RPC

Published:

October 26, 2009

Modified:

February 21, 2024

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 7.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

### 3- Medium

Prendiamo in esame la criticità con pericolosità Medium di nome “HTTP TRACE/TRACK METHOD ALLOWED”. La vulnerabilità ha uno score 5.3 e riguarda l’abilitazione del metodo HTTP trace; esso consente di inviare al server un messaggio loopback per tracciare il path e fornire un meccanismo di debugging. Anche questa vulnerabilità è di tipo RPC. Il tool consiglia di disabilitare il metodo.

MEDIUM

HTTP TRACE / TRACK Methods Allowed

< >

Plugin Details

✎

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

See Also

<http://www.nessus.org/u7e979b5cb>  
<http://www.apacheweek.com/issues/03-01-24>  
<https://download.oracle.com/sunalerts/1000718.1.html>

Output

To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the `TraceEnable` more...

To see debug logs, please visit individual host

Severity:

Medium

ID:

11213

Version:

1.74

Type:

remote

Family:

Web Servers

Published:

January 23, 2003

Modified:

October 27, 2023

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 5.3

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 4.6

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Temporal Score: 3.7

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

#### 4- Low

Prendiamo in esame la criticità con pericolosità Low di nome “X Server Detection”. La vulnerabilità è della famiglia “Service detection” ed indica che sulla porta 6000 è attivo un servizio X11 in ascolto per la visualizzazione grafica di applicazioni da client remoto, ed il traffico non è cifrato. Il tool consiglia di restringere l’accesso alla suddetta porta.

LOWX Server Detection

**Description**

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

**Solution**

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

**Output**

```
X11 Version : 11.0
```

To see debug logs, please visit individual host

Port ▲	Hosts
6000 / tcp / x11	192.168.50.101

**Plugin Details**

Severity: Low  
ID: 10407  
Version: 1.38  
Type: remote  
Family: Service detection  
Published: May 12, 2000  
Modified: March 5, 2019

**Risk Information**

Risk Factor: Low  
CVSS v2.0 Base Score: 2.6  
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

#### 5- Info

Prendiamo infine in esame la criticità con pericolosità INFO di nome “Unknown Service Detection: Banner Retrieval”. Questa debolezza è relativa a delle informazioni esposte da un banner di uno script; il tool non ha rilevato a quale script esse possano far riferimento. Le informazioni esposte potrebbero comunque fare gola ad un aspirante intruso.

INFOUnknown Service Detection: Banner Retrieval

**Description**

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

**Output**

```
If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org :

Port      : 512
Type      : spontaneous
Banner    :
0x00:  01 57 68 65 72 65 20 61 72 65 20 79 6F 75 3F 0A   .Where are you?.
0x10:
```

To see debug logs, please visit individual host

Port ▲	Hosts
512 / tcp	192.168.50.101

**Plugin Details**

Severity: Info  
ID: 11154  
Version: 1.69  
Type: remote  
Family: Service detection  
Published: November 18, 2002  
Modified: July 26, 2022

**Risk Information**

Risk Factor: None