



S5/L4 - Assessment delle vulnerabilità



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.

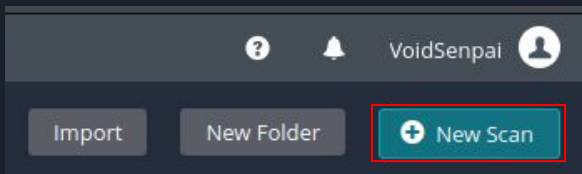


Nessus

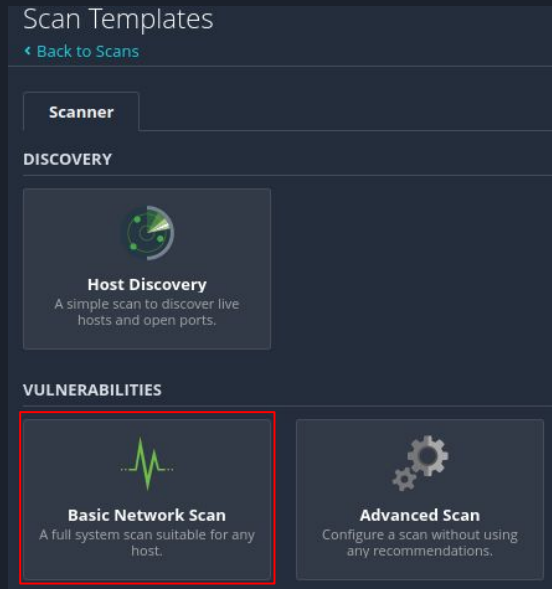
Nessus è un vulnerability scanner, ovvero uno strumento software automatizzato che esegue una scansione di un sistema o di una rete alla ricerca di vulnerabilità conosciute. Ora, vediamo come effettuare una scansione su un dispositivo utilizzando Meta come target e generiamo un breve rapporto su alcune vulnerabilità.

Nessus

Andiamo a cliccare su “New scan”.



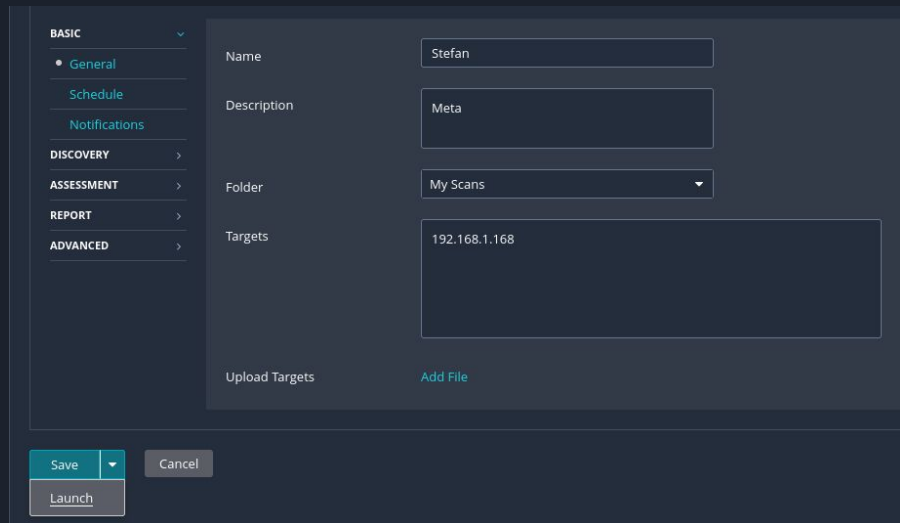
Fra le varie opzione scegliete “Basic Network Scan”.





Nessus

A questo punto basta inserire un Nome, una descrizione, in quale cartella salvare e per finire il/i target. Poi cliccare nel menu di “save” e cliccare “launch”.



The screenshot shows the Nessus configuration interface with a sidebar on the left and a main form area on the right. The sidebar has a 'BASIC' section expanded, showing 'General' (selected), 'Schedule', and 'Notifications'. Below these are 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED' sections, each with a right-pointing arrow. The main form area contains the following fields:

- Name:** A text input field containing 'Stefan'.
- Description:** A text input field containing 'Meta'.
- Folder:** A dropdown menu showing 'My Scans'.
- Targets:** A large text area containing '192.168.1.168'.
- Upload Targets:** A label with a blue 'Add File' link next to it.

At the bottom of the interface, there is a 'Save' button with a dropdown arrow, a 'Cancel' button, and a 'Launch' button.

Nessus

Dopo aver completato questa procedura, possiamo visualizzare un elenco delle vulnerabilità, ognuna classificata con un livello di pericolo che può essere 'Info', 'Low', 'Medium', 'High', o 'Critical'. Le vulnerabilità classificate come 'Critical' sono quelle che dovremmo risolvere prioritariamente.

Filter ▾

Search Vulnerabilities 🔍


73 Vulnerabilities

<input type="checkbox"/> Sev ▾	CVSS ▾	VPR ▾	Name ▲	Family ▲	Count ▾	⌕	✎
<input type="checkbox"/> CRITICAL	10.0 *		NFS Exported S...	RPC	1	⌕	✎
<input type="checkbox"/> CRITICAL	10.0		Unix Operating ...	General	1	⌕	✎
<input type="checkbox"/> CRITICAL	10.0 *		UnrealIRCd Bac...	Backdoors	1	⌕	✎
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'pas...	Gain a shell remotely	1	⌕	✎
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 a...	Service detection	2	⌕	✎
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Back...	Backdoors	1	⌕	✎
<input type="checkbox"/> MIXED	DNS (Multi...	DNS	5	⌕	✎
<input type="checkbox"/> MIXED	Apache To...	Web Servers	4	⌕	✎
<input type="checkbox"/> CRITICAL	SSL (Multip...	Gain a shell remotely	3	⌕	✎
<input type="checkbox"/> HIGH	7.5		NFS Shares Wor...	RPC	1	⌕	✎

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0 ✎
Scanner: Local Scanner
Start: Today at 1:27 PM
End: Today at 1:49 PM
Elapsed: 23 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Nessus

In questo caso, abbiamo identificato una password piuttosto debole, e attraverso una simulazione di attacco, Nessus è riuscito a penetrare facilmente. La soluzione consigliata sarebbe quindi di utilizzare una password robusta, composta da almeno 12 caratteri.

CRITICAL VNC Server 'password' Password

< >

Plugin Details

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution
Secure the VNC service with a strong password.

Output
Nessus logged in using a password of "password".
To see debug logs, please visit individual host

Port **Hosts**

5900 / tcp / vnc 192.168.1.168

Plugin Details

Severity: Critical

ID: 61708

Version: \$Revision: 1.2 \$

Type: remote

Family: Gain a shell remotely

Published: August 29, 2012

Modified: September 24, 2015

Risk Information
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C /I:C/A:C

Nessus

In questo caso, abbiamo un dispositivo remoto che potrebbe essere facilmente attaccato, aumentando il rischio di perdita, rimozione o modifica dei file da parte di un black hat. Per prevenire questo problema, è sufficiente modificare il dispositivo in modo tale che siano autorizzati solo i dispositivi da noi desiderati.

CRITICAL NFS Exported Share Information Disclosure

< >

Plugin Details

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :  
  
+ /  
+ Contents of / :  
- .  
- ..  
- bin  
- ----
```

Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C
/I:C/A:C



Nessus

In questo caso, abbiamo un protocollo con una versione non aggiornata, che potrebbe essere vulnerabile ad attacchi di exploit. La soluzione consigliata è aggiornare il protocollo ed eliminare la versione obsoleta.

MEDIUM

TLS Version 1.0 Protocol Detection

< >

Plugin Details

✎

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern Implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Severity: Medium

ID: 104743

Version: 1.10

Type: remote

Family: Service detection

Published: November 22, 2017

Modified: April 19, 2023

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N