

L'esercizio di oggi consisteva nel usare nessus per fare una scansione verso metasploitable nella foto qui sotto è la pagina iniziale di nessus per fare una scansione dove si inserisce il nome(va bene qualsiasi nome) e il target (può essere più d'uno contemporaneamente)

or
in

Back to Scan Templates

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

metasploitable

Description

Folder

scansioni

Targets

192.168.49.102

Upload Targets

Add File

Dopo aver messo il nome e il target si imposta le porte tramite discovery e le vulnerabilità tramite assessment, dopo aver lanciato la scansione se procede tutto bene apparirà lo schermo come la foto sotto indicando le vulnerabilità trovato e quanto sono serie in questo caso la vulnerabilità è medium e il modo per risolvere questa è limitare la rete

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	MEDIUM	5.8		Network Time Protocol (NTP) Mode 6 Scanner	Misc.	1		
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	6		
<input type="checkbox"/>	MIXED	Web Server (Multiple Issues)	Web Servers	3		
<input type="checkbox"/>	INFO	HTTP (Multiple Issues)	Web Servers	7		
<input type="checkbox"/>	INFO	HTTP (Multiple Issues)	CGI abuses	2		
<input type="checkbox"/>	INFO	TLS (Multiple Issues)	General	2		
<input type="checkbox"/>	INFO	TLS (Multiple Issues)	Service detection	2		