

18.05.2025



# VULNERABILITY ASSESSMENT

SCANSIONE FINALE  
FABIO MUNGIOVÌ

# SCANSIONE FINALE

## METASPLOITABLE 2

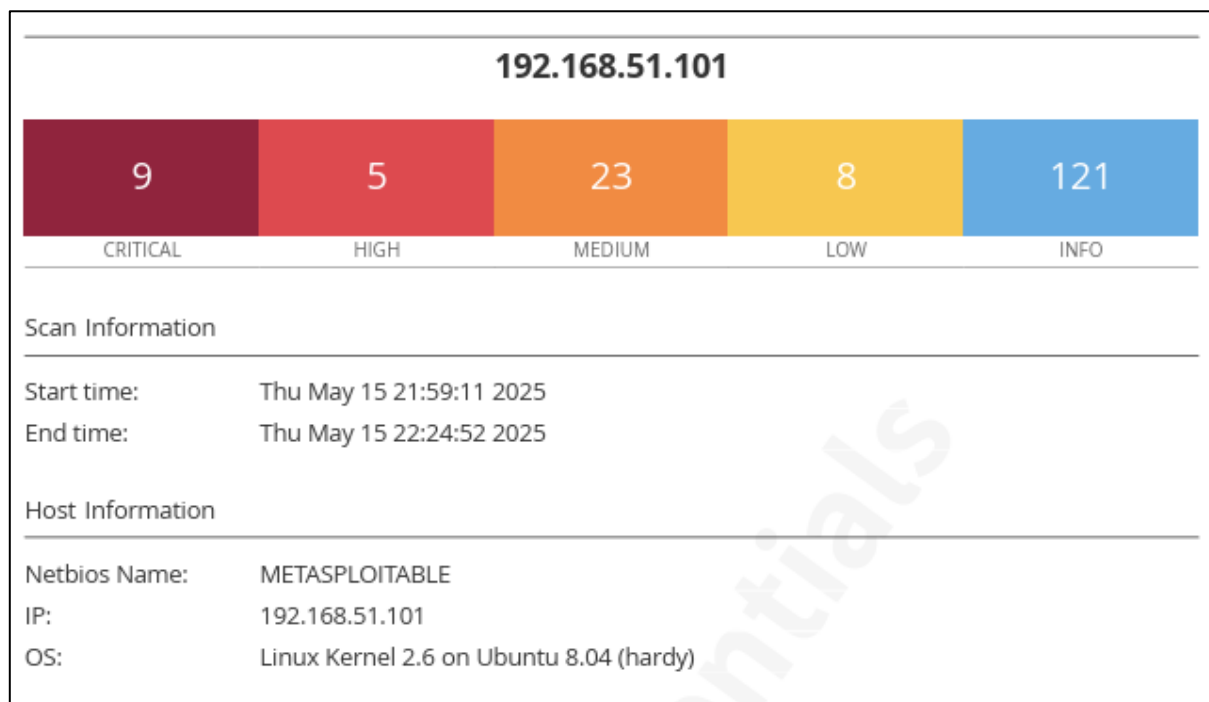
### INDICE

SOMMARIO.....	2
SCANSIONE INIZIALE.....	2
SCANSIONE FINALE.....	3
CONCLUSIONI.....	4

## SOMMARIO

In questo report verranno mostrati i risultati della scansione effettuata a valle delle azioni di mitigazione sulle vulnerabilità riscontrate con la prima scansione, a conferma dell'efficacia delle azioni compiute.

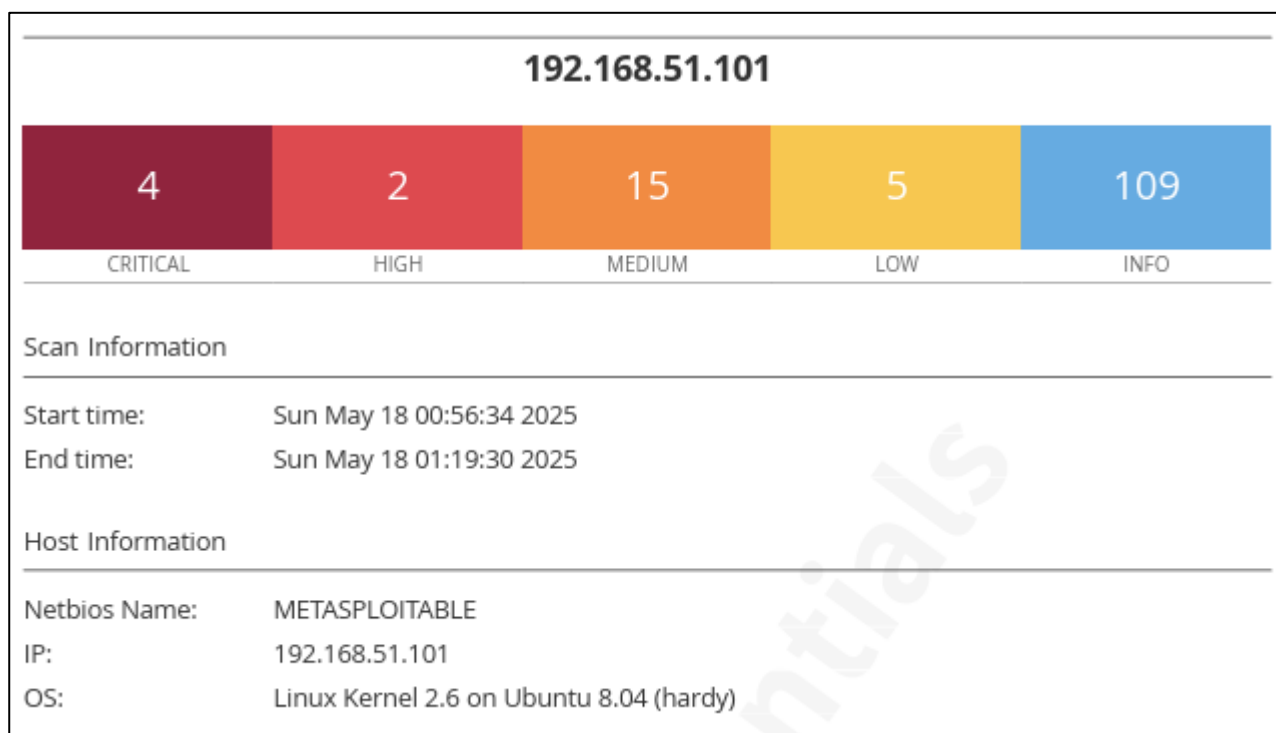
## SCANSIONE INIZIALE



*In evidenza le vulnerabilità mitigate*

<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲
<input type="checkbox"/> CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General
<input type="checkbox"/> CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/> CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Inje...	Web Servers
<input type="checkbox"/> CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection
<input type="checkbox"/> CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/> CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/> HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General
<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC
<input type="checkbox"/> MIXED	...	...	...	15 SSL (Multiple Issues)	General
<input type="checkbox"/> MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS

## SCANSIONE FINALE



Come si nota dall'immagine il numero di vulnerabilità, nella seconda scansione, si è abbassato.  
Sono state risolte più di 5 vulnerabilità in quanto alcune di queste impattavano su più porte.

Nell'immagine in basso la schermata dei risultati direttamente dal tool Nessus, che evidenzia l'assenza delle vulnerabilità prese in atto in precedenza.

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲
<input type="checkbox"/>	CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General
<input type="checkbox"/>	CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/>	HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General
<input type="checkbox"/>	MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS
<input type="checkbox"/>	MIXED	...	...	...	7 SSL (Multiple Issues)	General
<input type="checkbox"/>	MIXED	...	...	...	6 SSH (Multiple Issues)	Misc.
<input type="checkbox"/>	MIXED	...	...	...	3 DNS (Multiple Issues)	DNS

## CONCLUSIONI

Visti i risultati positivi possiamo ritenere ampiamente efficaci le azioni di mitigazione intraprese sulle vulnerabilità.

I processi e i servizi che esponevano a rischi sono stati contenuti, ma lasciando comunque al sistema host la possibilità di usufruire di servizi simili che possano sostituire quelli bloccati.