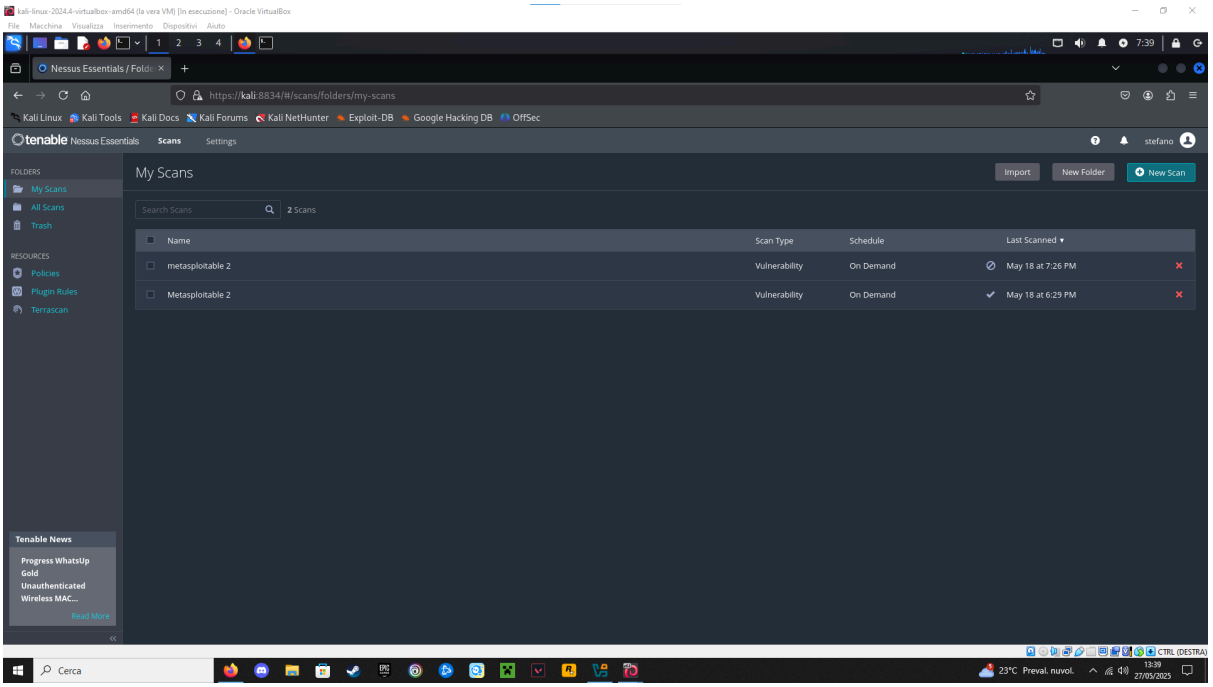
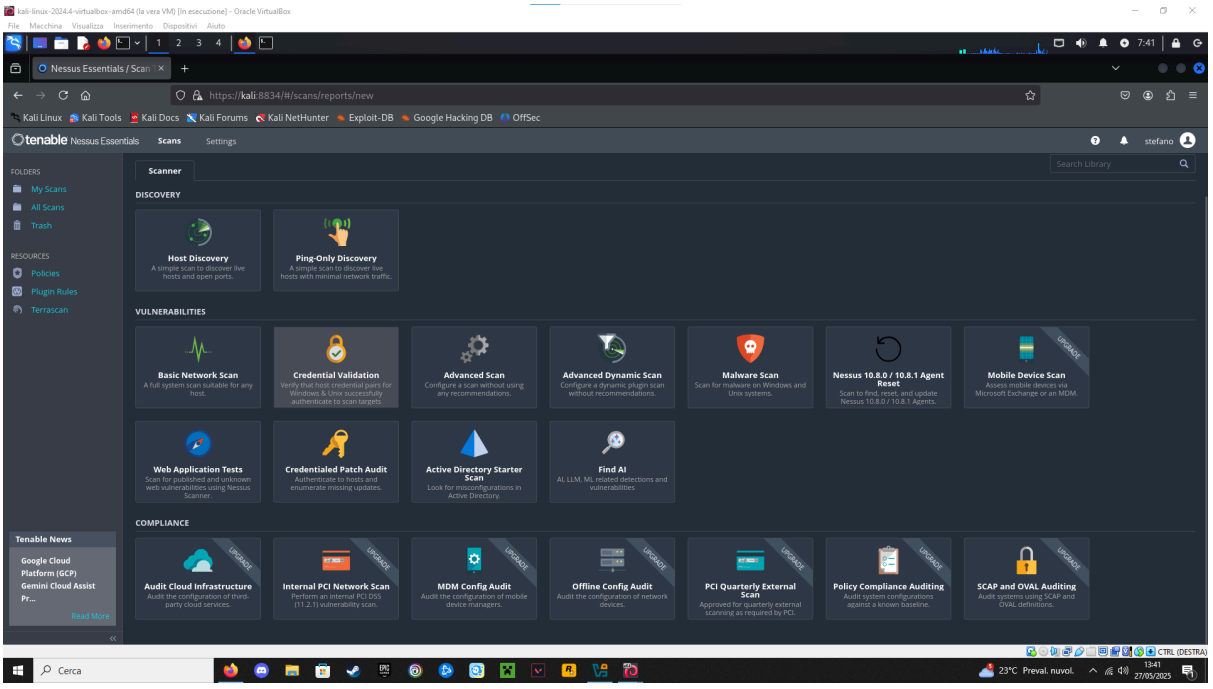
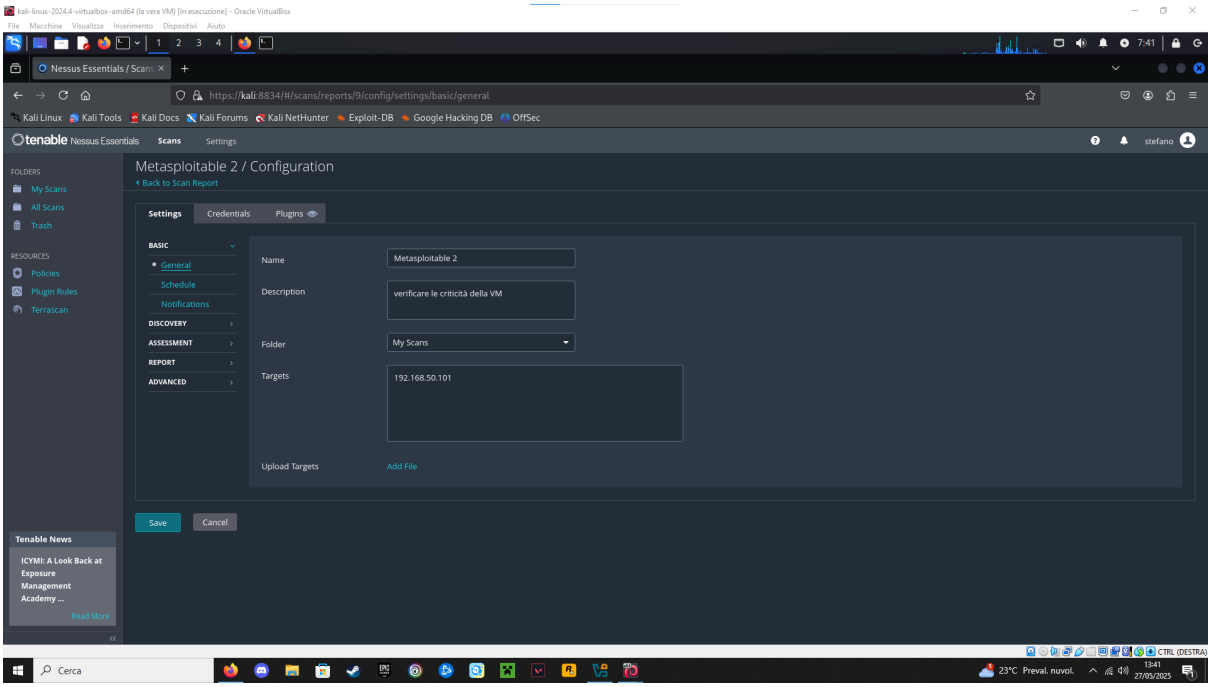


entriamo su nessus attraverso “https://kali:8834” (dopo aver già attivato il servizio con “sudo systemctl start nessusd.service)

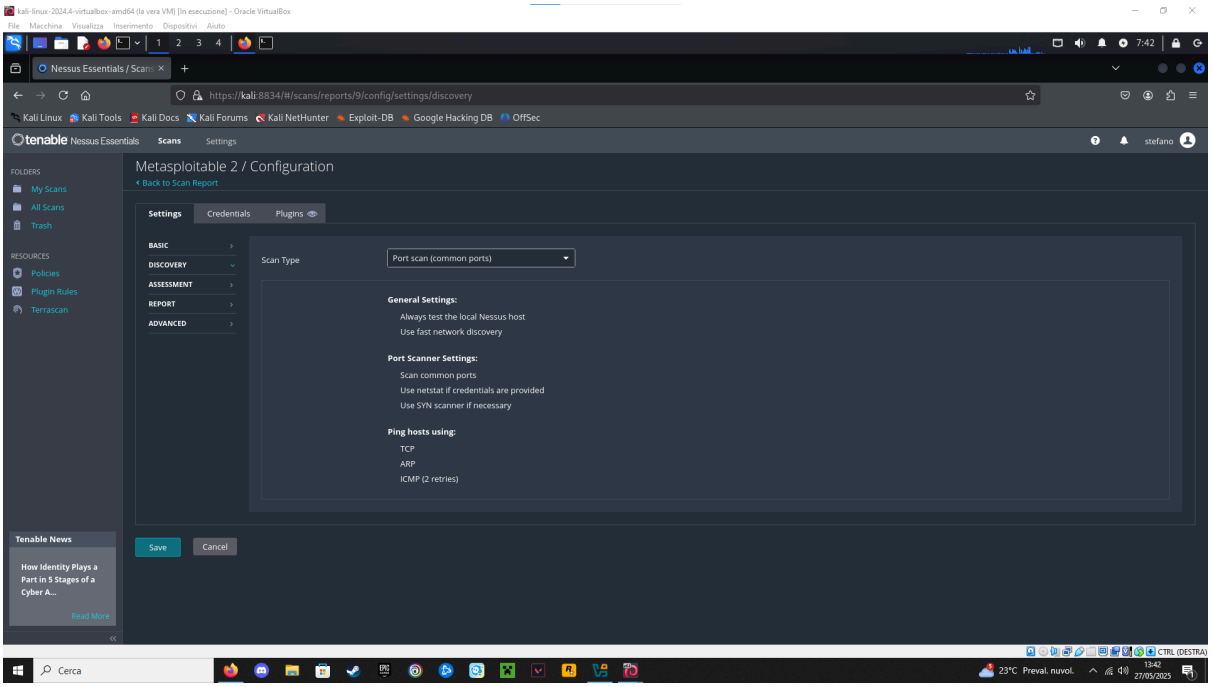
clicchiamo su “new scan”



useremo il tool classico “basic network scan”)

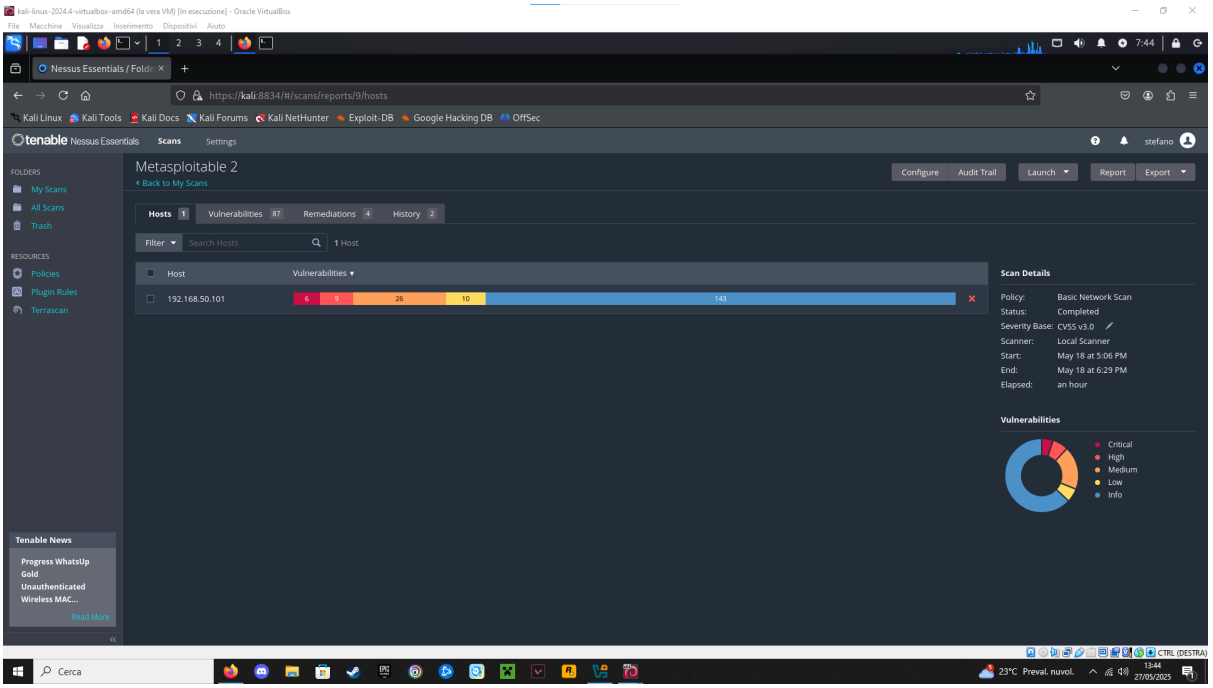


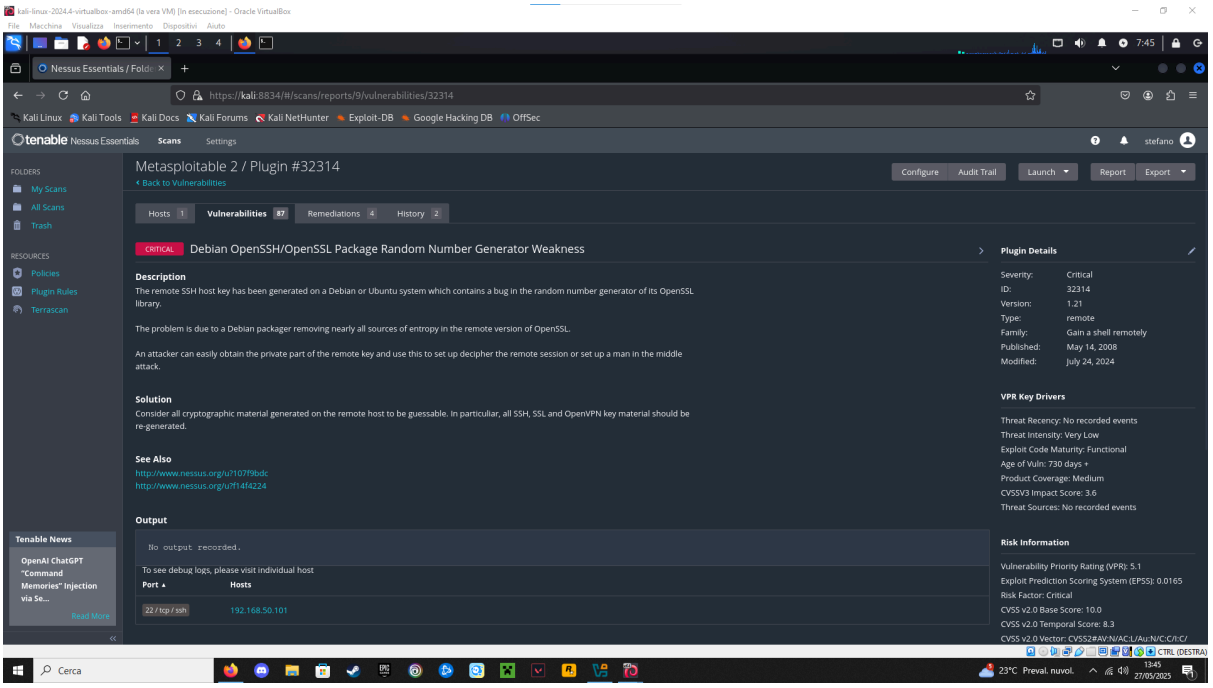
configurazione della sezione “general”



configurazione della sezione “discovery” solo le porte comuni

Dopo aver configurato tutto , nessus ci darà le vulnerabilità





ci indicherà ogni possibile causa e soluzione e starà a noi risolvere nei migliori dei modi mitigando le vulnerabilità

192.168.50.101

9	9	31	8	93
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 150

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.9439	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	8.9	0.9447	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	5.9	0.0172	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	0.8167	19704	TWiki 'rev' Parameter Arbitrary Command Execution

report fatto appositamente da nessus per mettere in risalto le vulnerabilità critiche dalle più alle più basse.