MODULO 3
TEST

Andrea Ferrantino

Traccia: Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

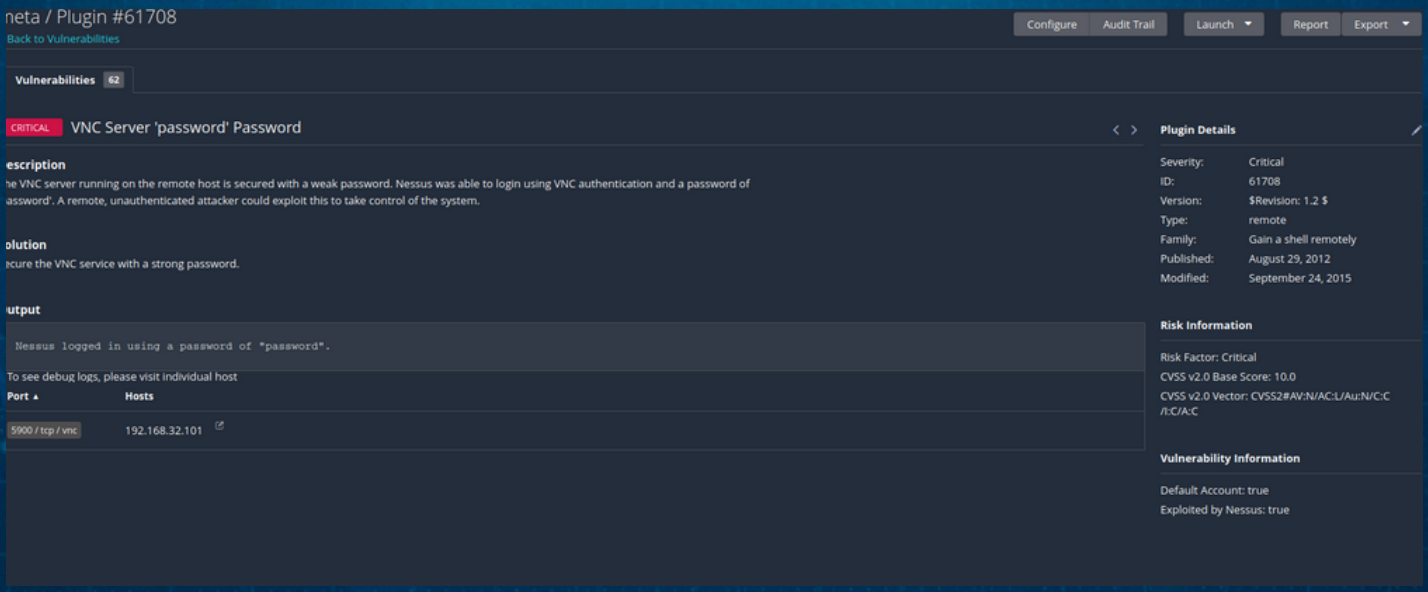
192.168.32.101

9	4	17	6	71
CRITICAL	HIGH	MEDIUM	LOW	INFO

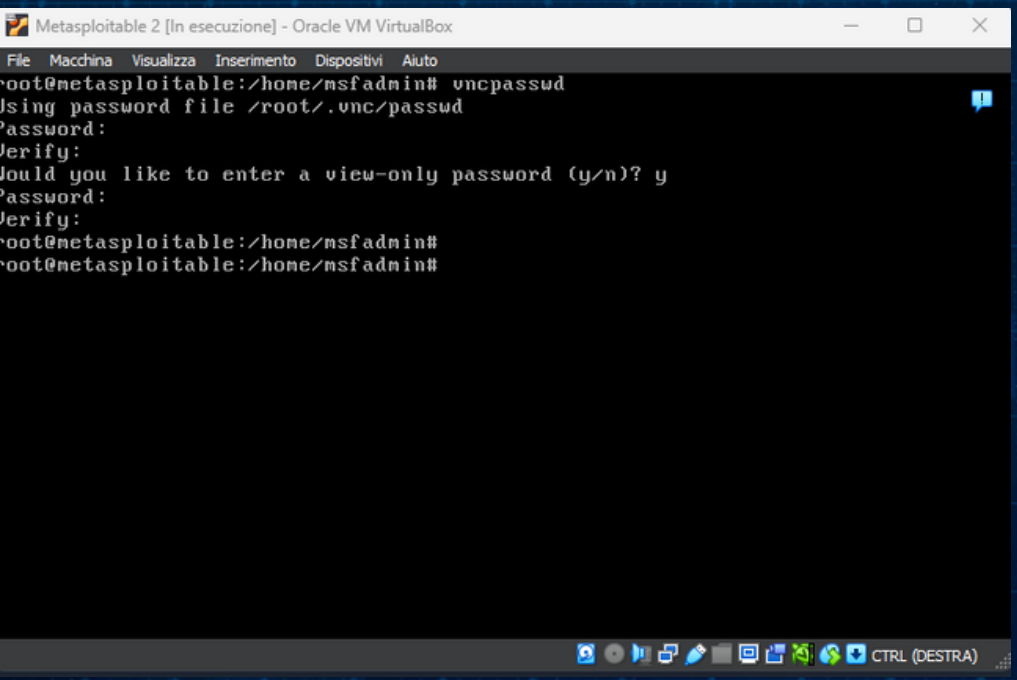
Vulnerabilities Total: 107

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

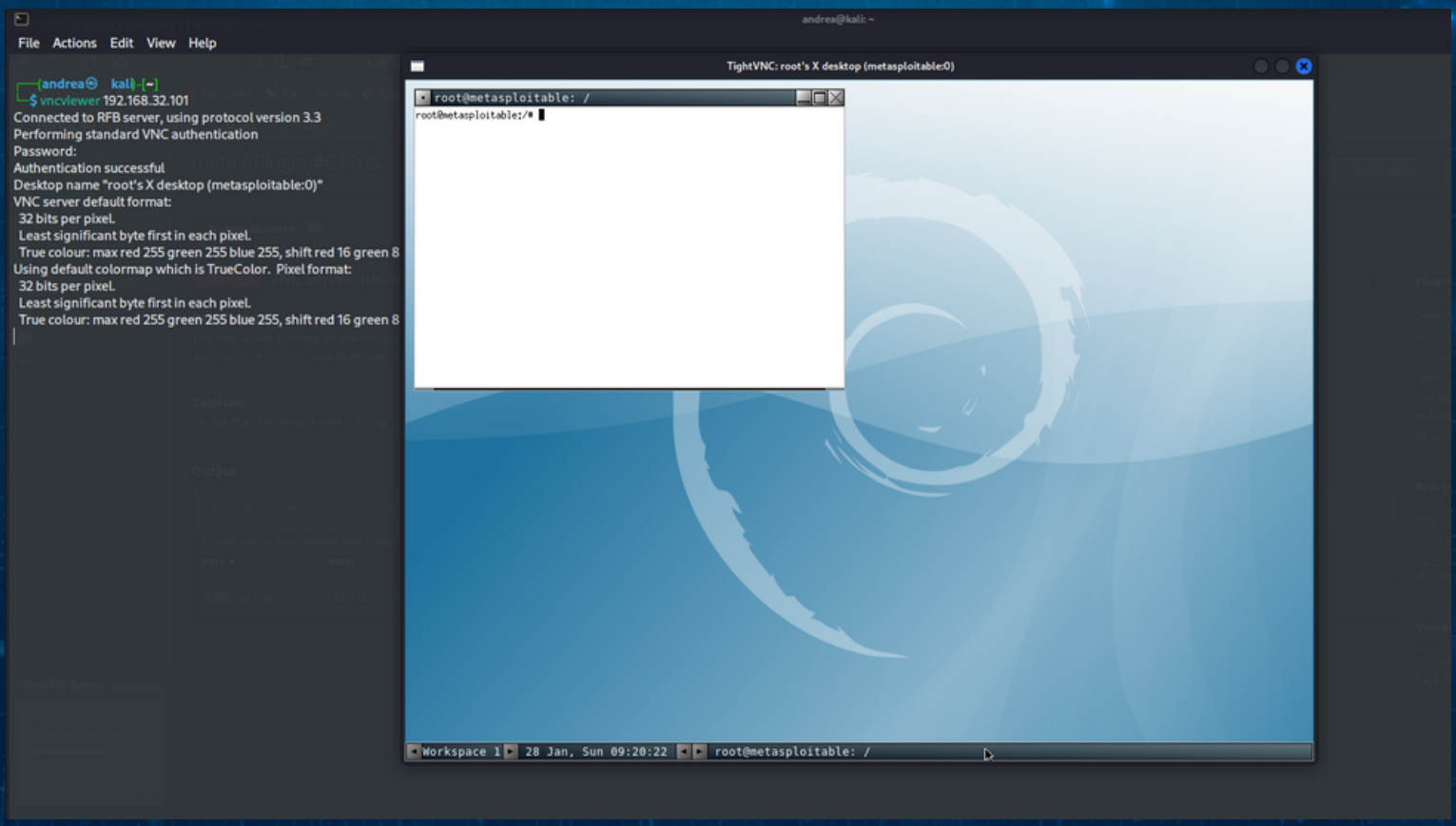
VNC SERVER



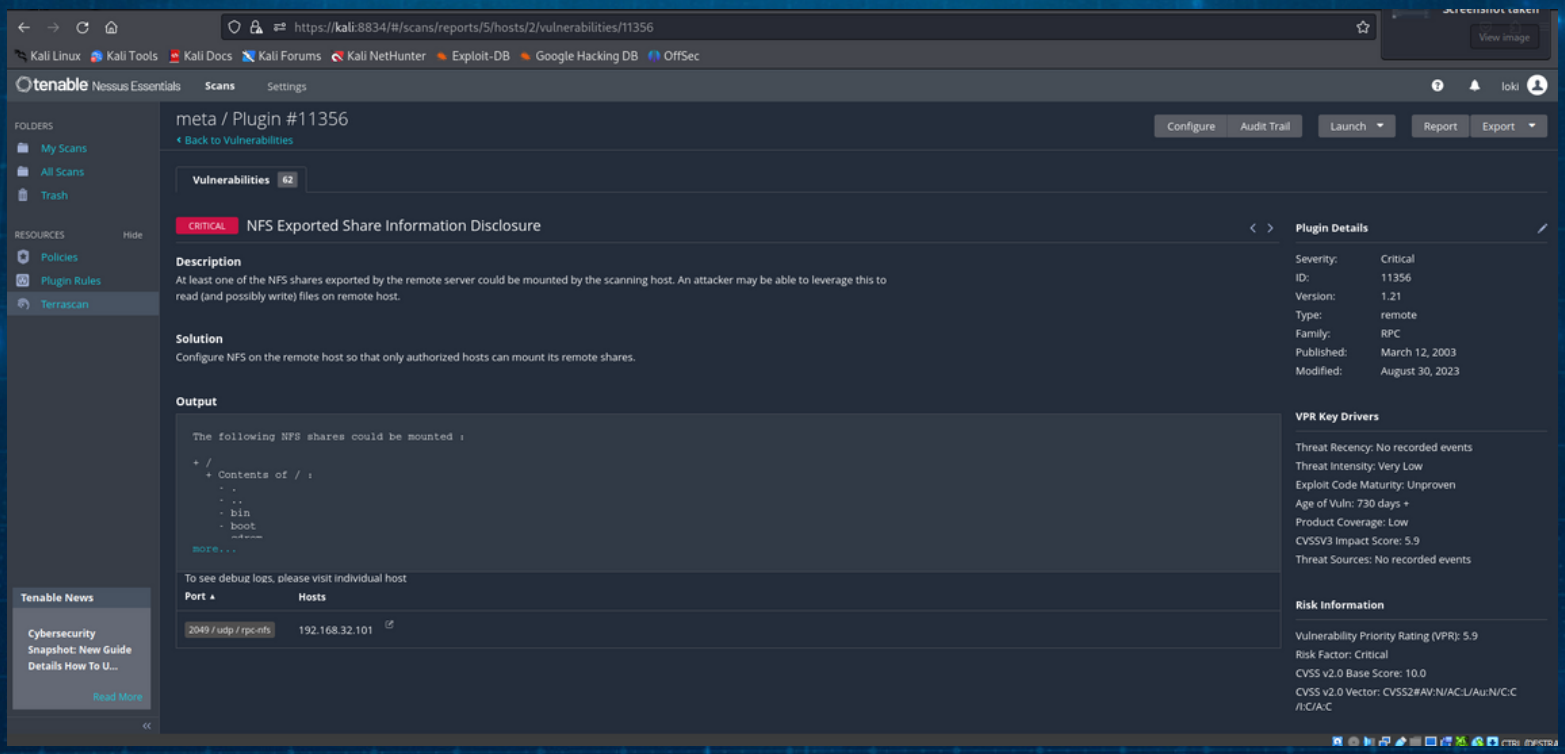
Per risolvere questa vulnerabilità lanciamo il comando “sudo su” dal terminale di metasploitable per ottenere i permessi di root,successivamente lanciamo “vnc passwd” inserendo la nuov password



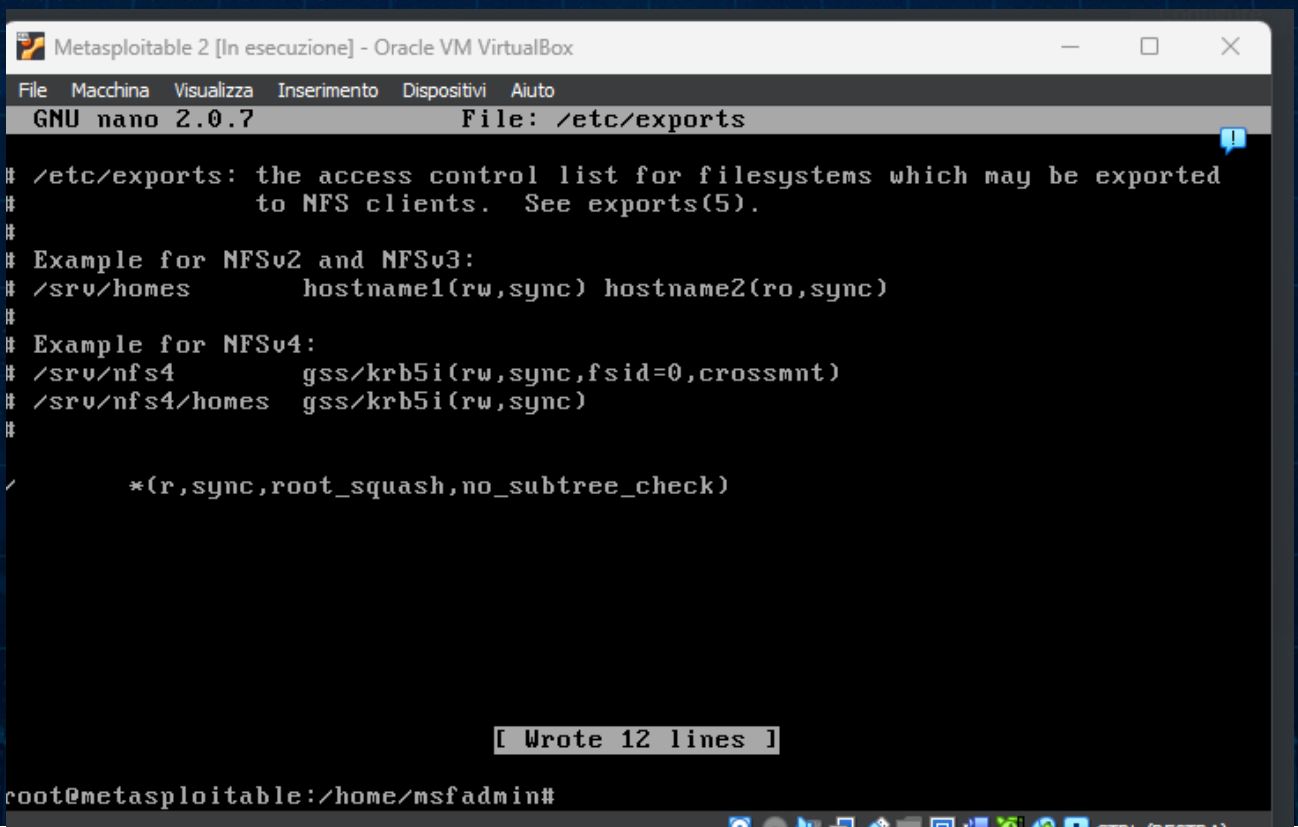
In seguito controlliamo che sia andato tutto a buon fine digitando nel terminale di kali “vncviewer 192.168.32.101”.



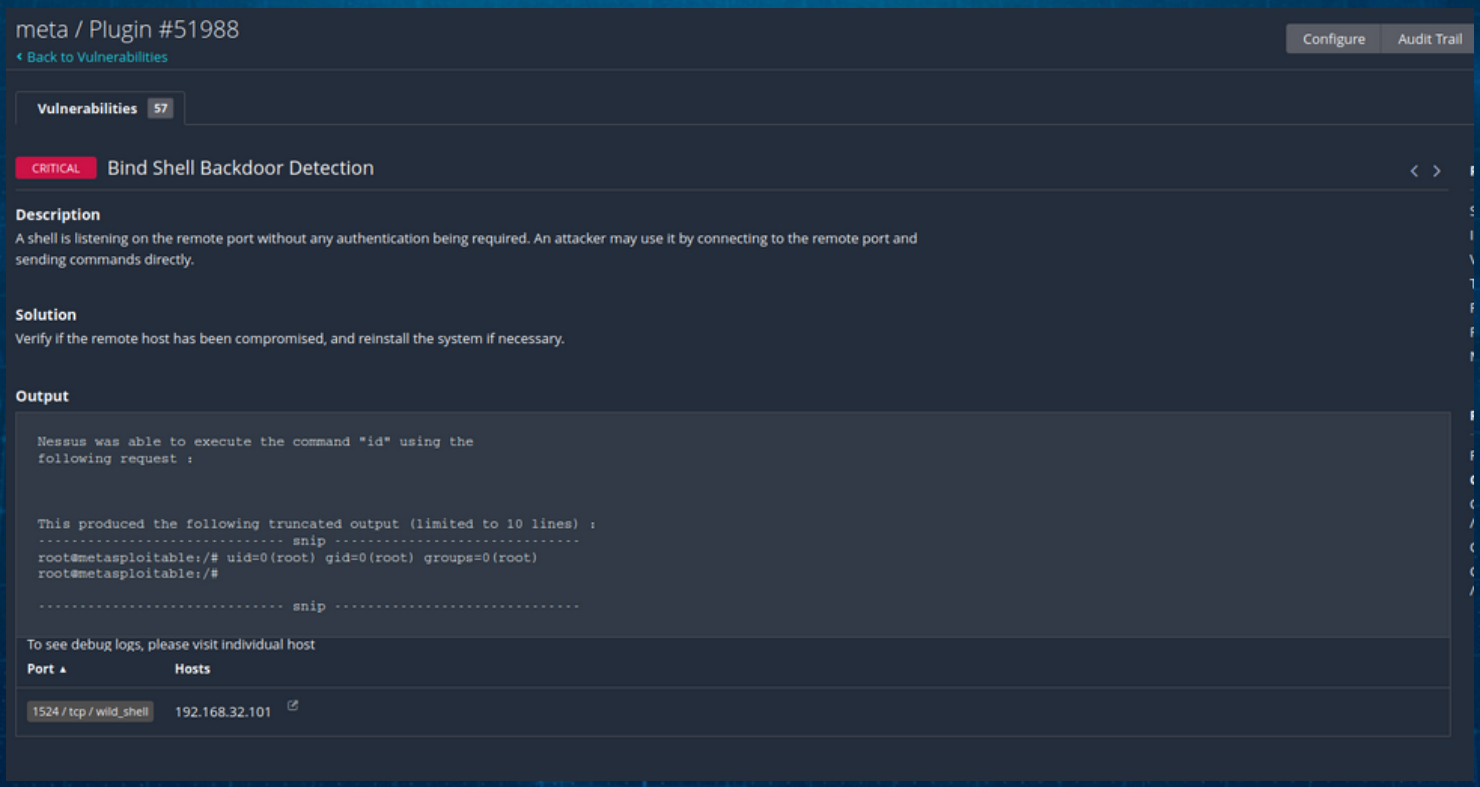
NFS EXPORTED SHARE INFORMATION DISCLOSURE



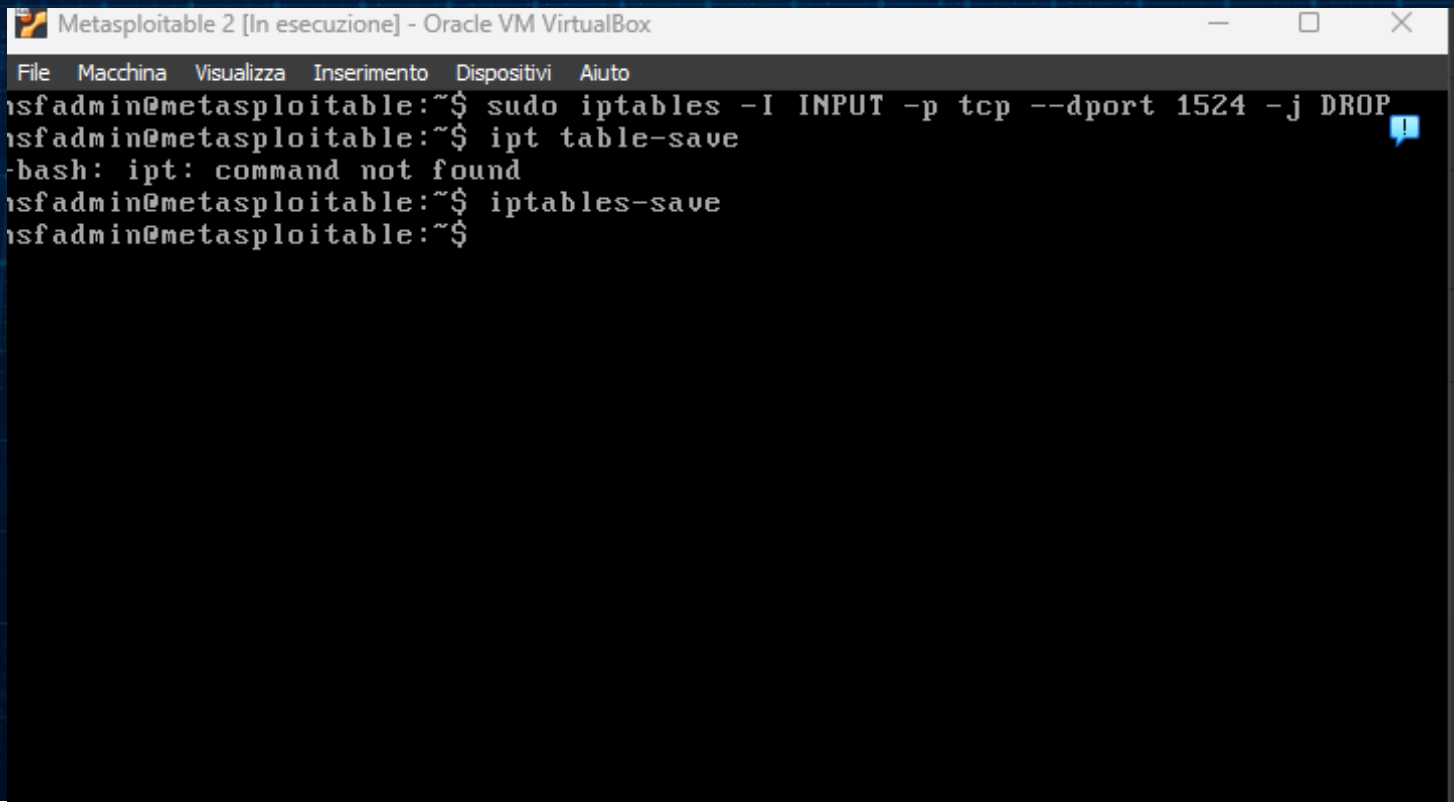
Per risolvere questa vulnerabilità andiamo a modificare il file con il seguente comando “sudo nano /etc/exports” cancellando parte del contenuto come screen qui sotto



BIND SHELL BACKDOOR DETECTION



Per risolvere questa vulnerabilità andiamo su metasploitable e modifichiamo la regola del firewall con il seguente comando: “iptables -I INPUT -p tcp --dport (numero porta) -j DROP” salvando successivamente la regola con “iptables-save”



Quindi notiamo che facendo un altra scan da nessus le vulnerabiltà elencate sono risolte: