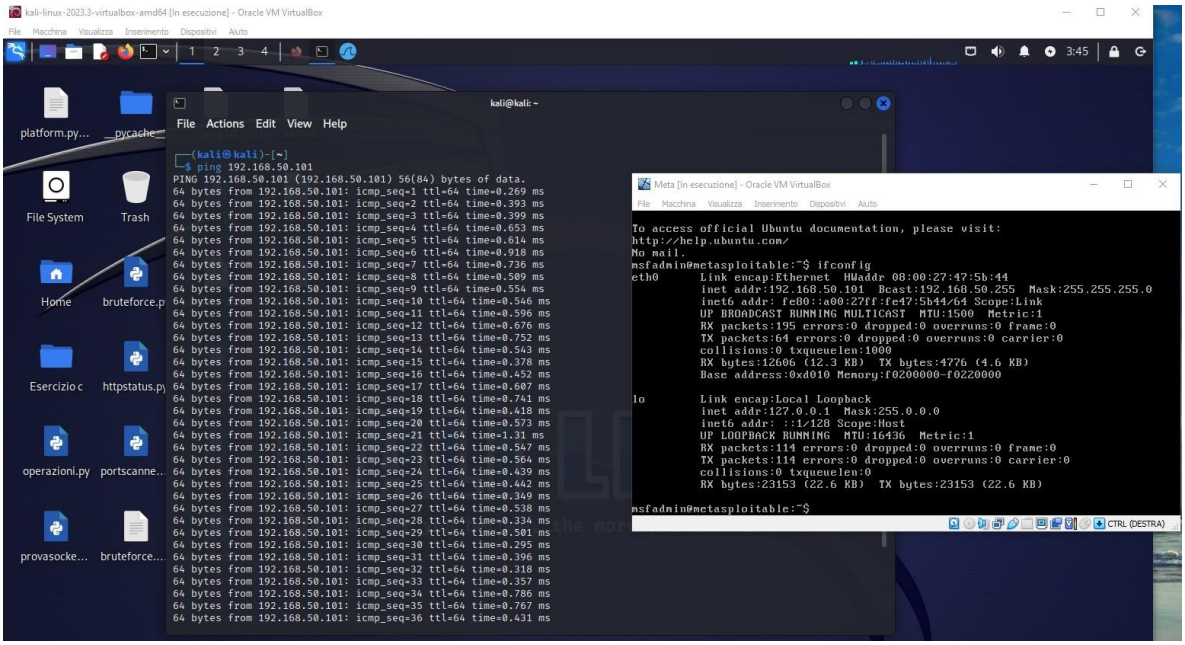
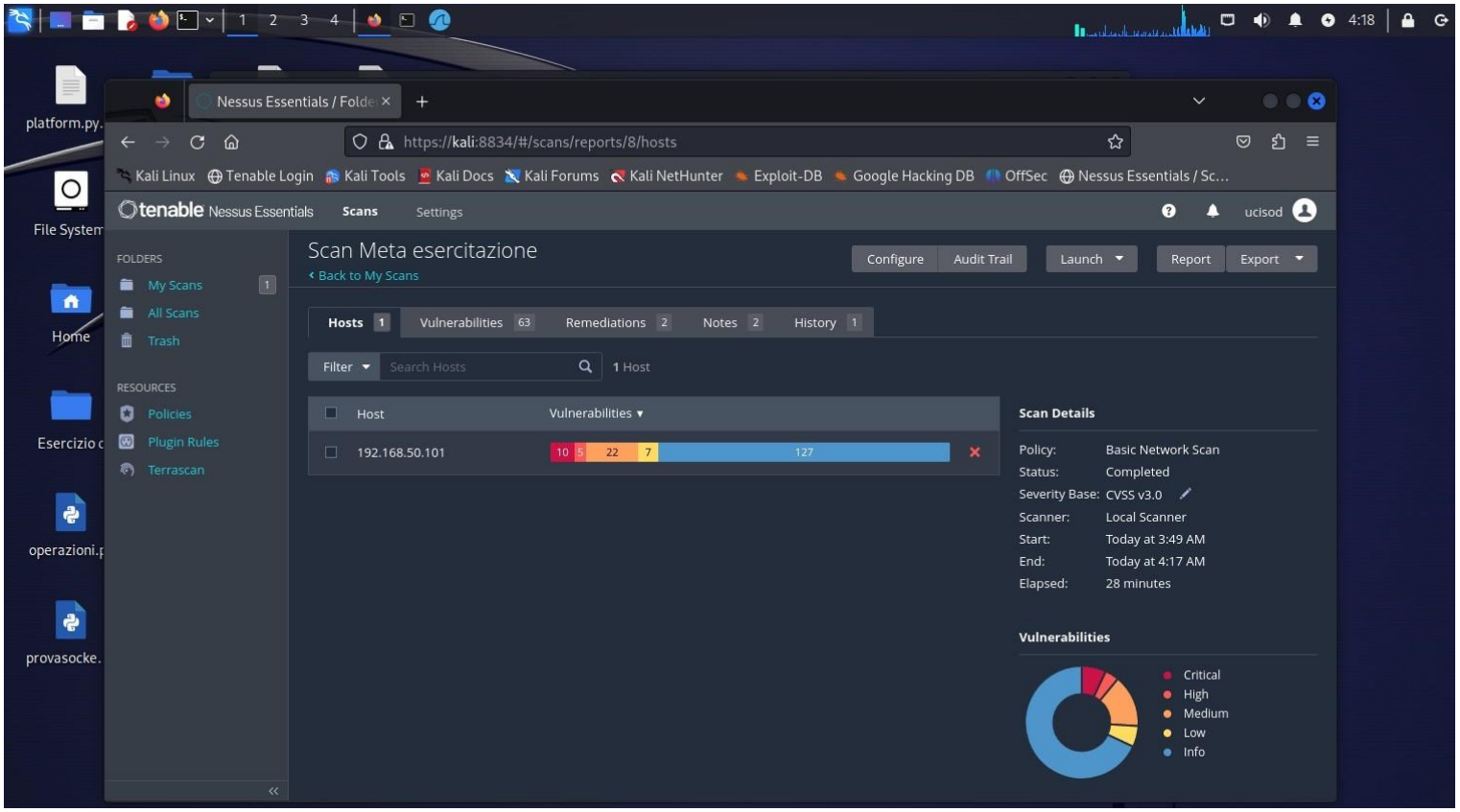
Esercitazione 27/10/2023

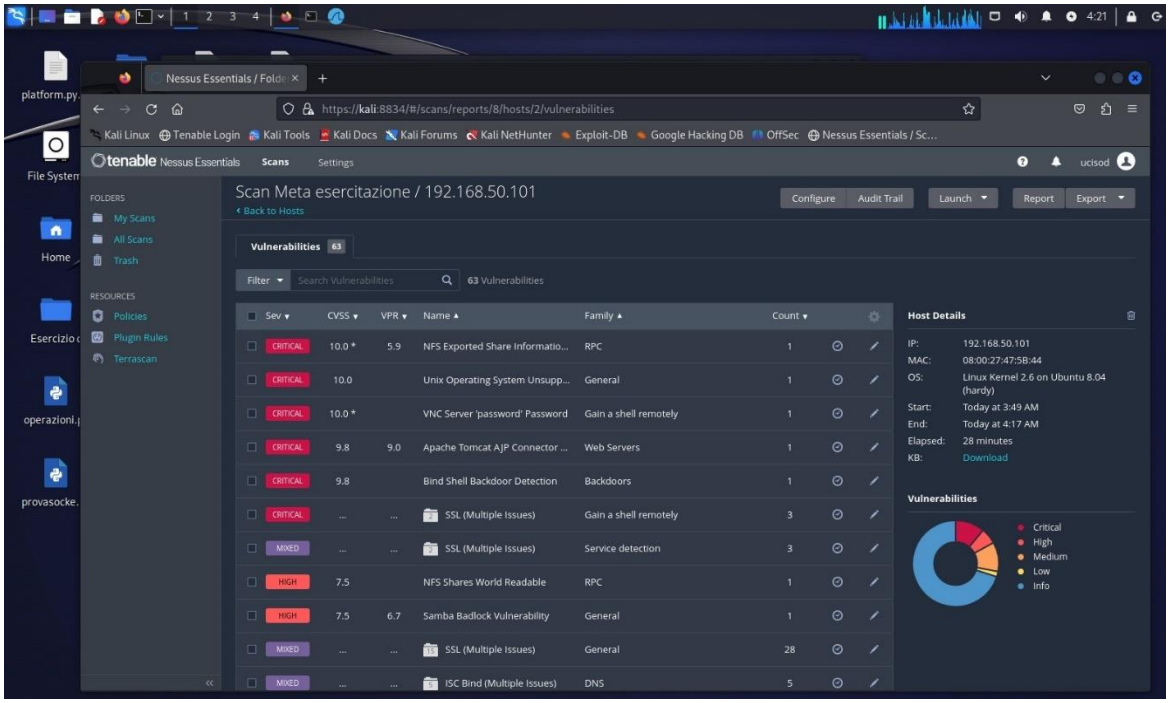
Nell'esercizio odierno ci viene richiesta una scansione delle vulnerabilità del programma Metaspoitable attraverso l'uso di Nessus e di cercare di risolverne da 2 a 4 attraverso azioni.

Prima di tutto controllo che le macchine riescano a pingare tra loro



Poi sono andata a controllare le criticità





1 vulnerabilità livello critico:

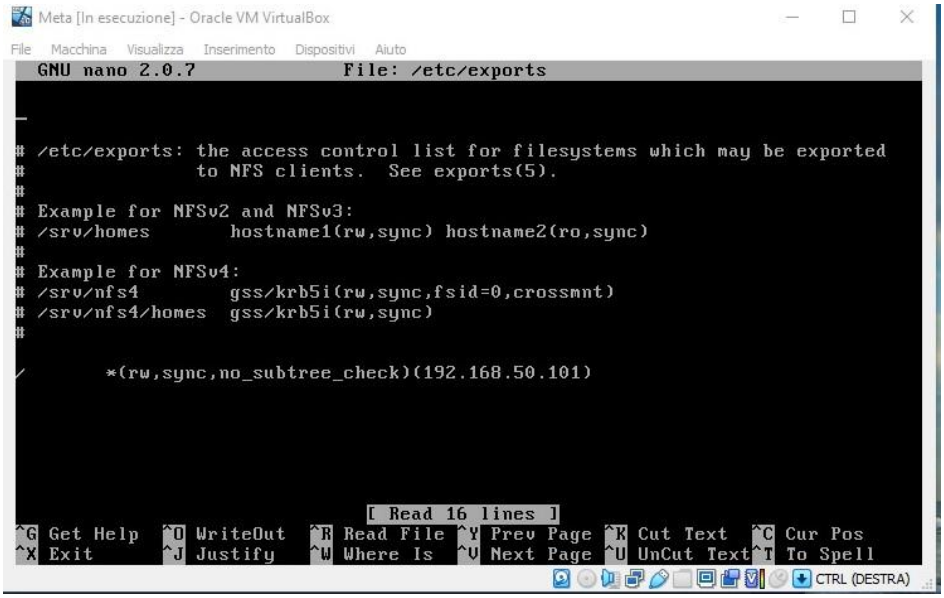
Nome: **NFS Exported Share Information Disclosure**

Descrizione: la descrizione ci riporta che almeno un file NFS (Network File System), cioè un file o directory che sono presenti su un server NFS che li rende accessibili ai soli client che hanno i permessi per accedervi, non è sufficientemente protetto, pertanto un utente malintenzionato potrebbe avere accesso a questa condivisione e sfruttarla per accedere al file sull'host remoto, leggendolo o modificandolo.

Soluzione: Come possibile soluzione ci riporta quella di configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni

Procedimenti svolti:

Per prima cosa sono andata su Meta come amministratore e attraverso il comando "sudo nano /etc/exports" ho modificato l'editor di testo inserendo l'ip di Meta stesso
Quindi ho prima ricaricato la configurazione su Meta e poi verificato l'effettiva avvenuta modifica in cui ho autorizzato solo Meta ad accedere alla condivisione NFS



2 vulnerabilità livello critico:

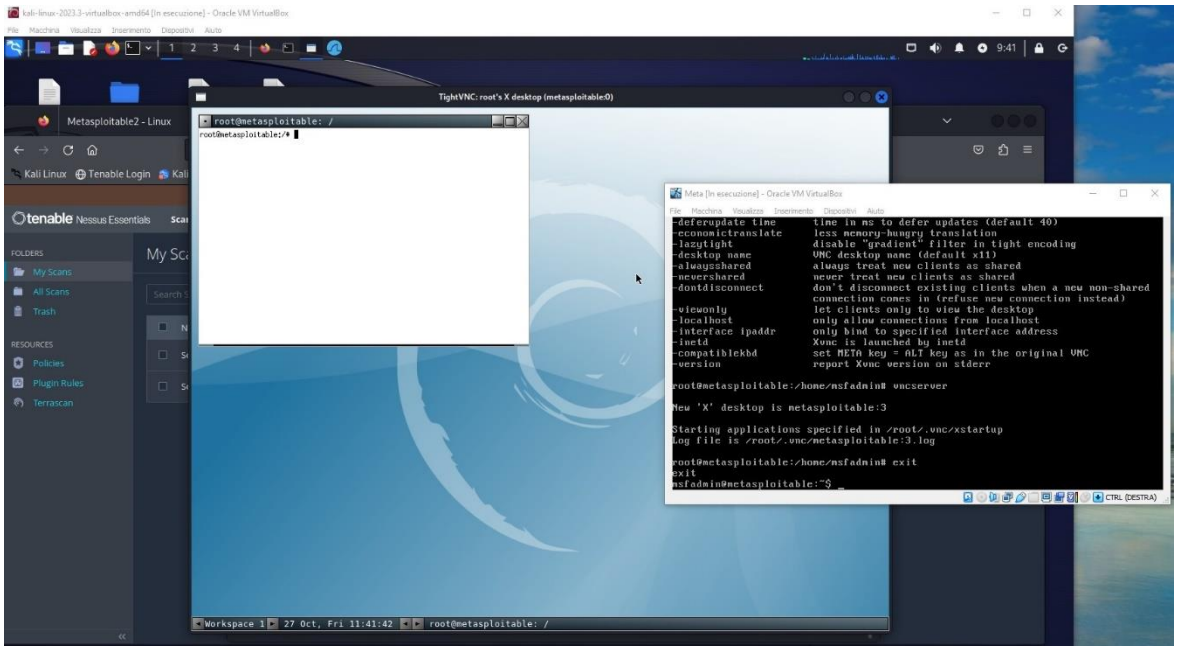
Nome: **VNC Server 'password' Password**

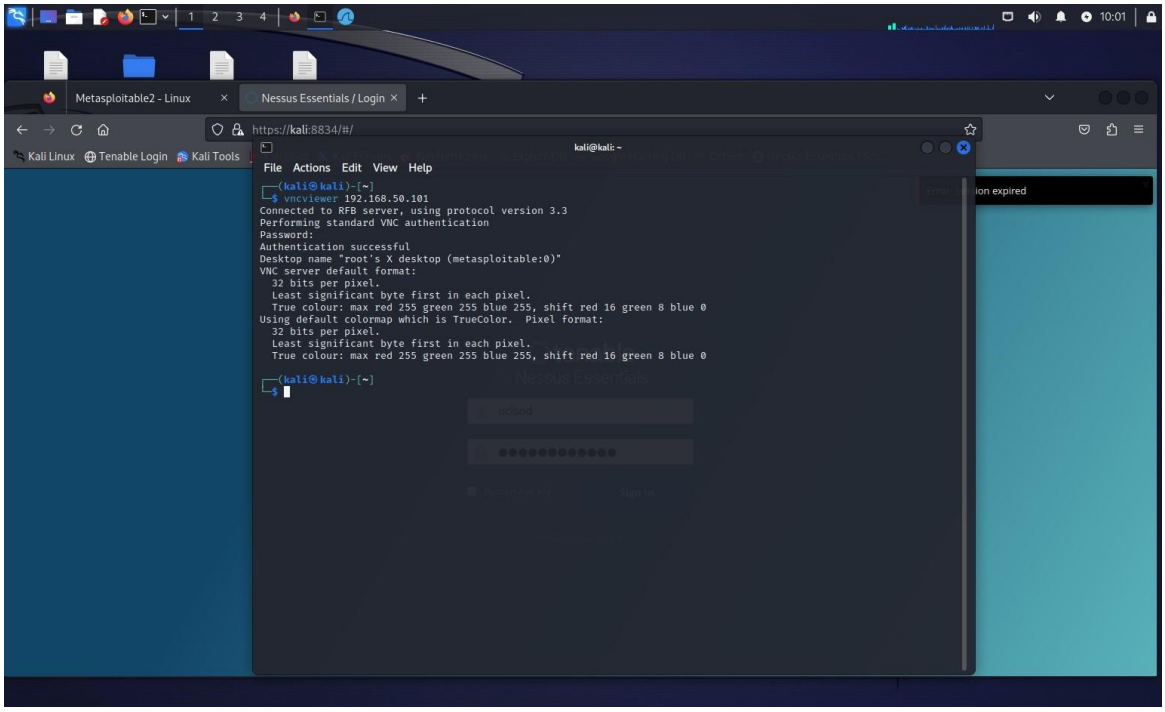
Descrizione: La terza criticità si riferisce al fatto che il server VNC (Virtual Network Computing) in esecuzione sull'host remoto non è sufficientemente protetto poiché ha una password debole e ci avvisa del fatto che Nessus è riuscito ad accedervi utilizzando una password standard "password". Un utente malintenzionato non autenticato, dunque, potrebbe sfruttare questa situazione per assumere il controllo del sistema

Soluzione: Nessus ci consiglia di proteggere il servizio VNC con una password complessa

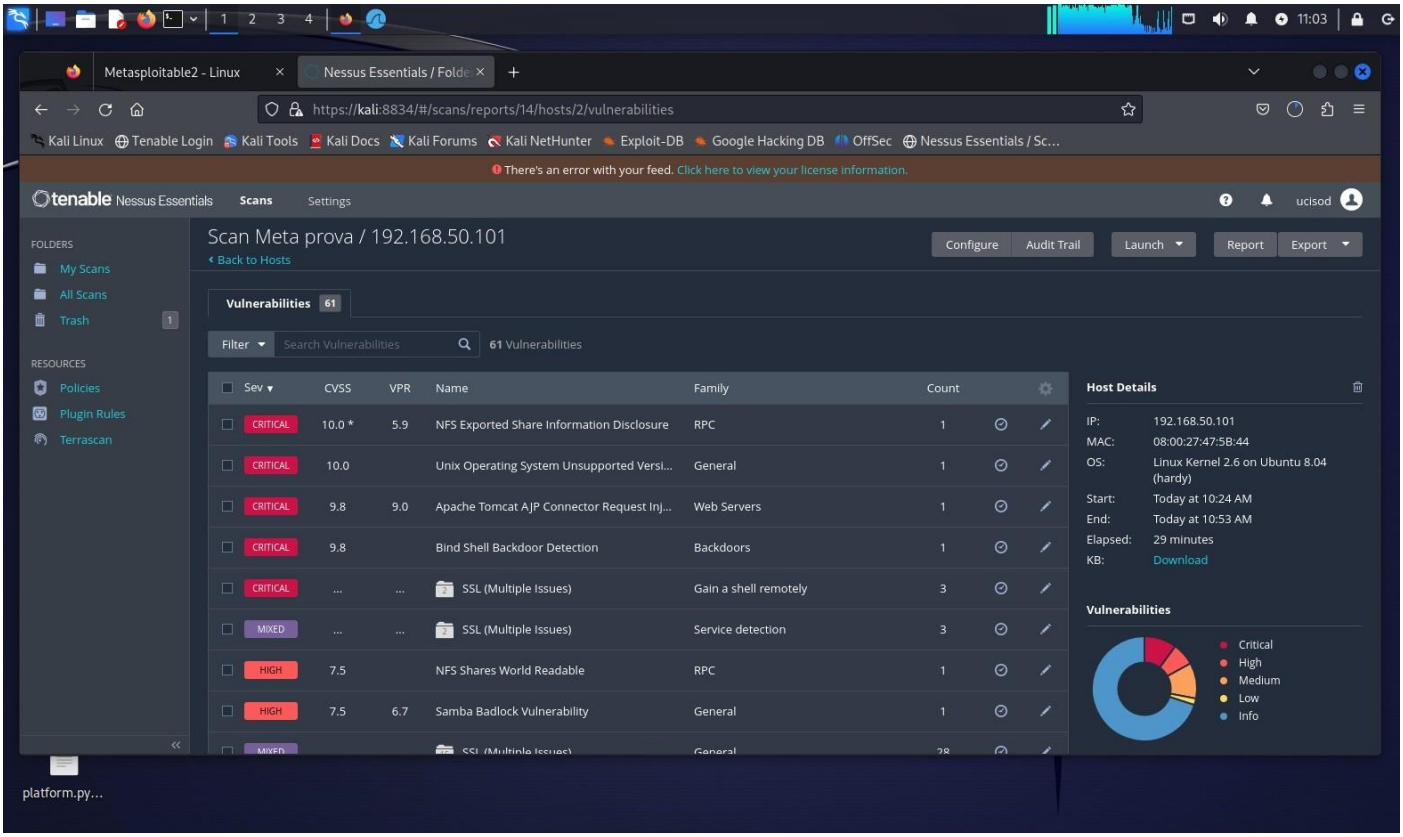
Procedimenti svolti:

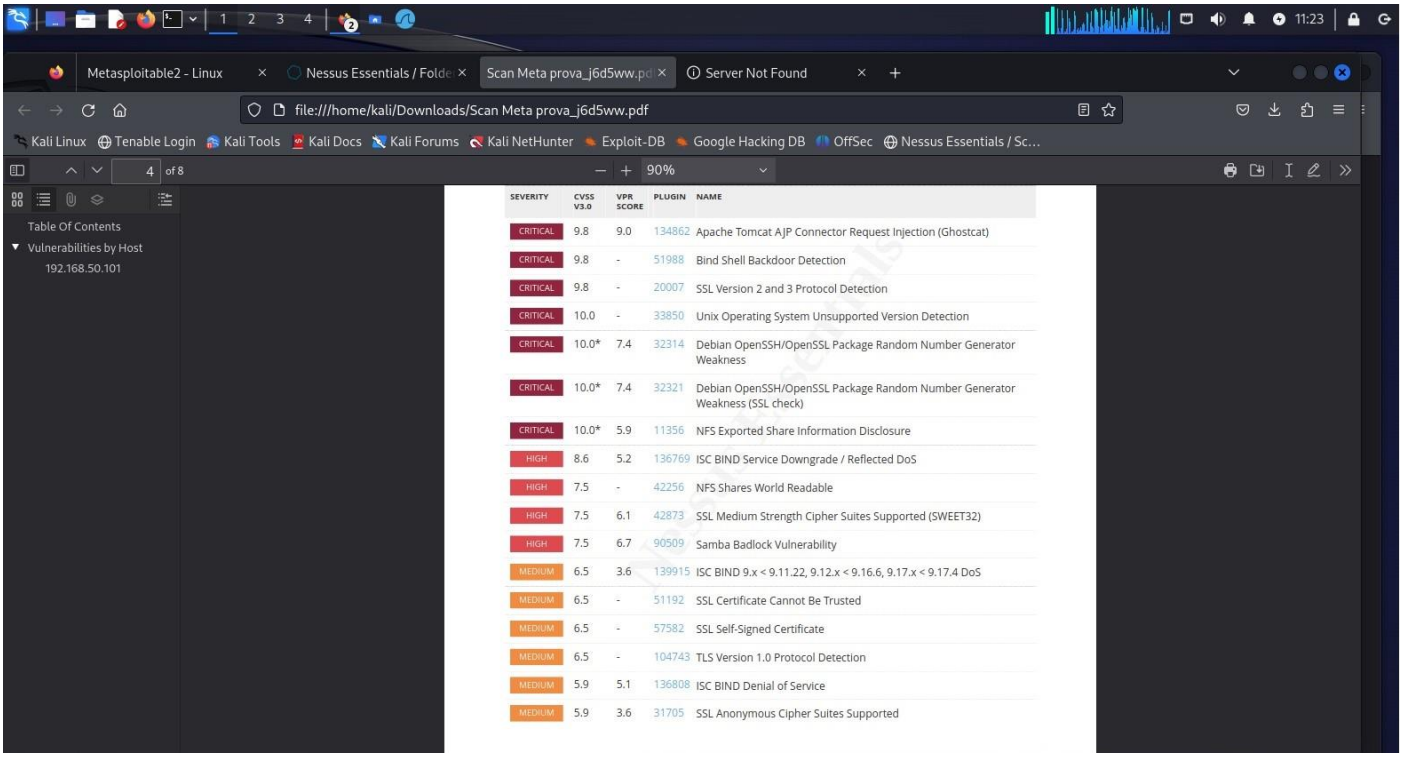
Sono entrata in Meta come amministratore e poi ho digitato il comando "vncpassw" e ho cambiato la password inserendone una nuova un po' più complessa. Poi ho killato (terminato) il processo e restartato il vnc con il comando "vncserver" e infine sono andata su kali e ho digitato vncviewer con l'indirizzo ip di Meta per verificare che la nuova password fosse stata correttamente inserita

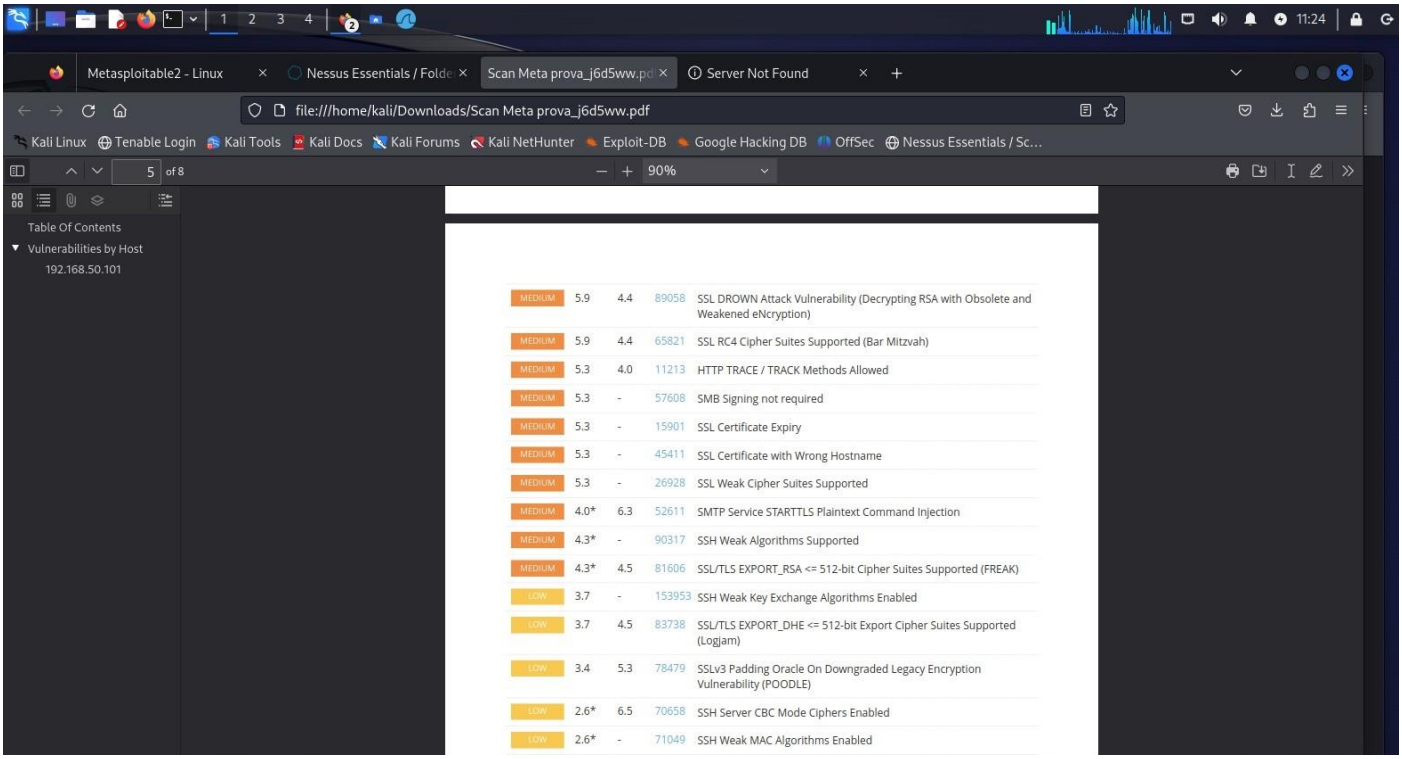




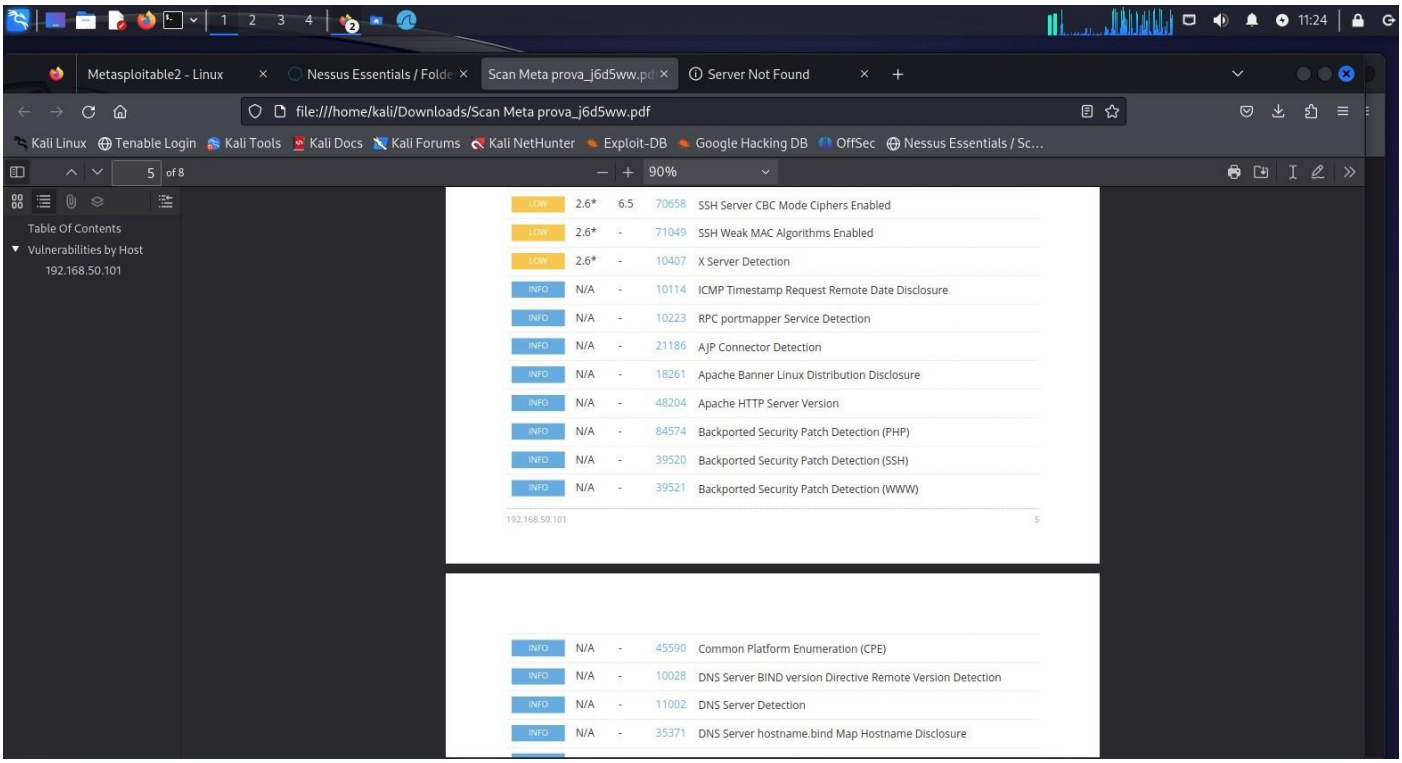
Nel report finale (che non riesco a condividere perché salta la connessione, ho provato fino ad ora sia tramite connessione che tramite chiavetta USB), purtroppo appare ancora come critica la prima vulnerabilità ma non compare più la seconda.







MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	6.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled



LOW	2.6*	6.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)

INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure