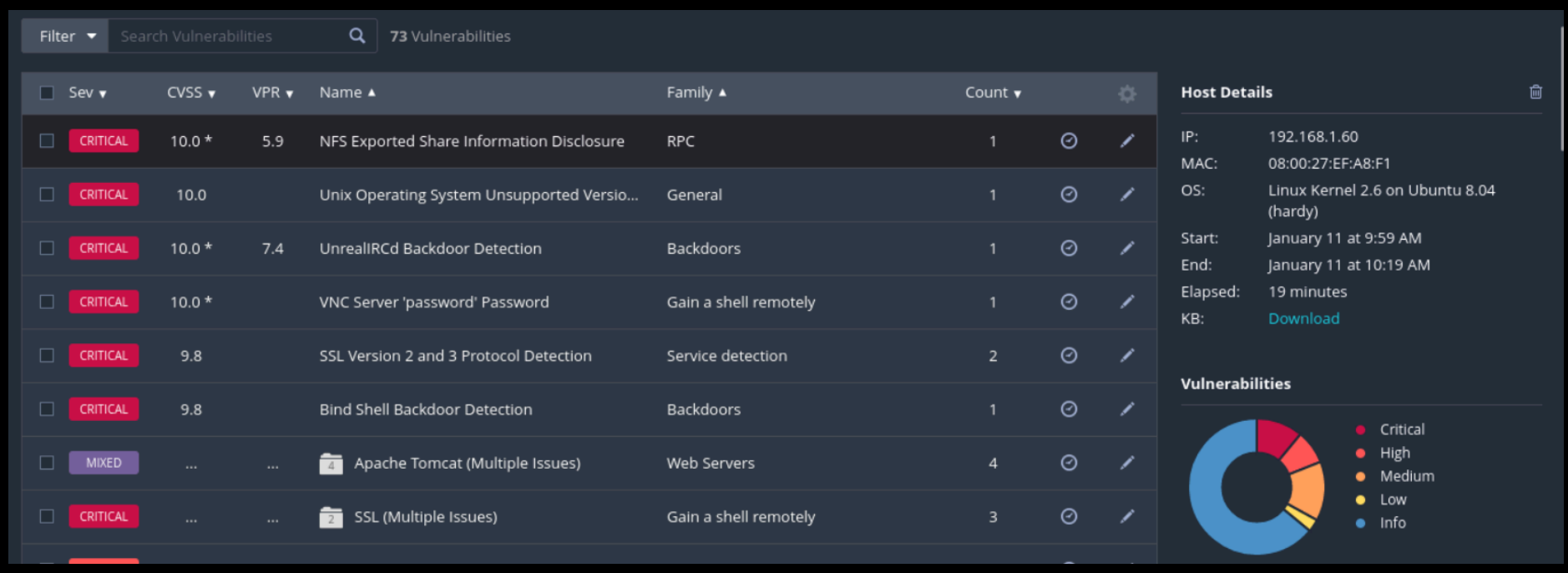
## Metasploitable vulnerability

Richiesta: Scanning vulnerabilità Metasploitable e implemento di azioni di rimedio.
Tool utilizzati: Nessus.

Scanning:

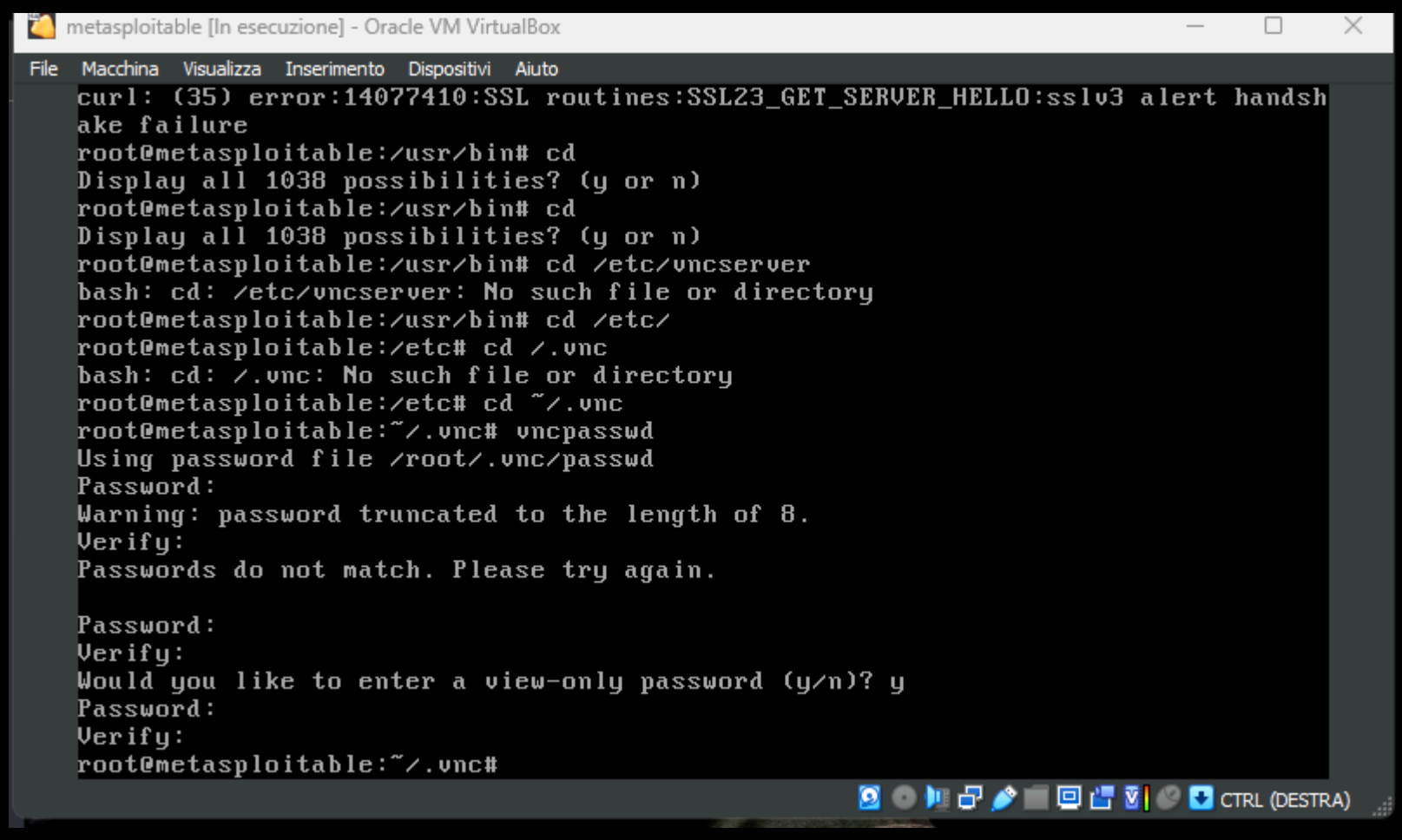



Notiamo un’elevata criticità delle vulnerabilità rilevate.

Obiettivo: Ridurre il livello di criticità di almeno 2 vulnerabilità critiche.

Vulnerabilità 1:
VNC Server “password” Password

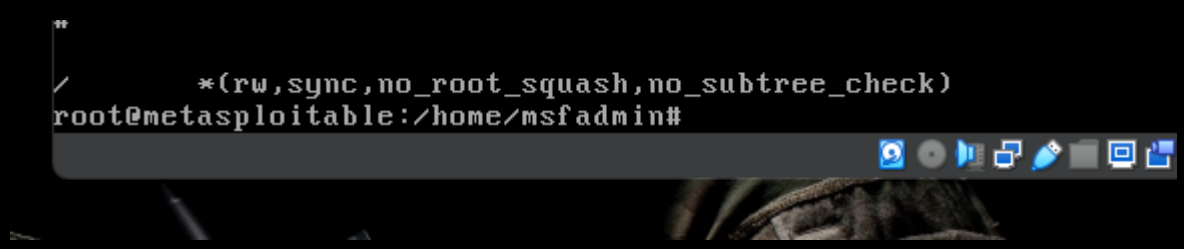
**Risoluzione:**



Cambio della password “password” con una password più sicura “GHlje25%”.

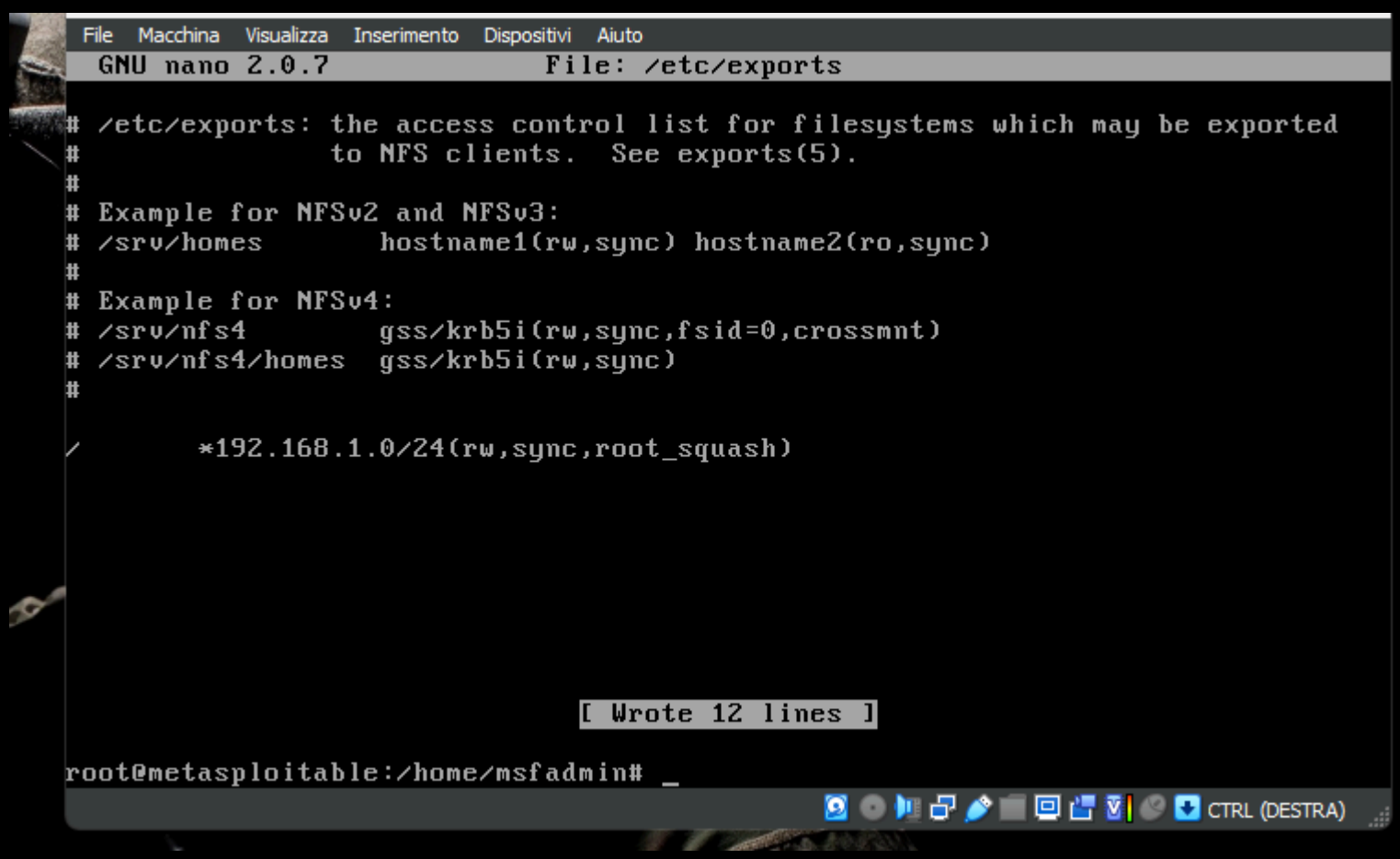
Vulnerabilità 2:
NFS Exported Share Information Disclosure

**Problema:**




Riguarda le configurazioni non sicure del Network File System (NFS) che possono permettere la divulgazione non autorizzata di informazioni. NFS è utilizzato per condividere file tra sistemi in una rete. Se non configurato correttamente, può esporre file sensibili o permettere a un attaccante di montare il filesystem in modo non autorizzato.

**Soluzione:**




**Spiegazione:**

- 192.168.1.0/24: Questo indica che solo i dispositivi nella subnet 192.168.1.0 con una maschera di sottorete di 255.255.255.0 (che è cosa significa /24) possono montare questa condivisione NFS.
- rw: Permette sia lettura che scrittura sulla condivisione NFS.
- sync: Richiede che le modifiche al filesystem siano confermate sul disco prima che le operazioni di scrittura siano considerate complete.

- root_squash: Mappa le richieste da UID/GID 0 (root) a un UID/GID anonimo, di solito rendendo root equivalente all'utente "nobody", per una maggiore sicurezza.