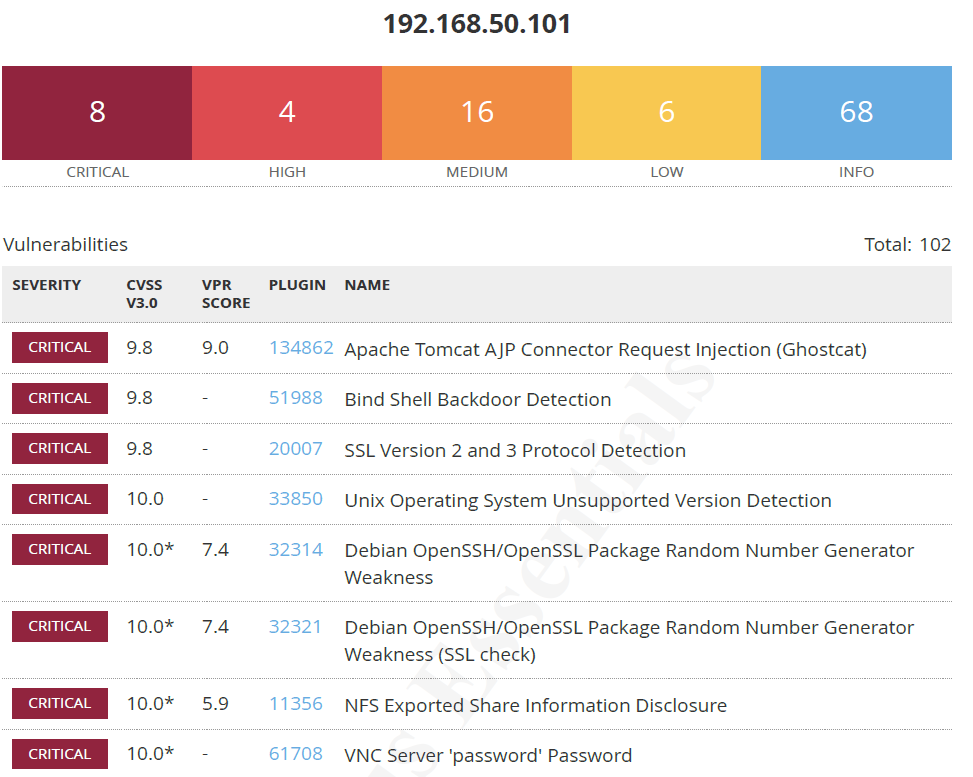
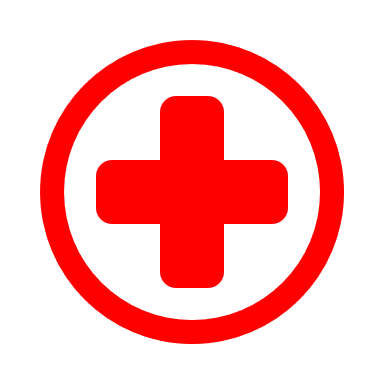
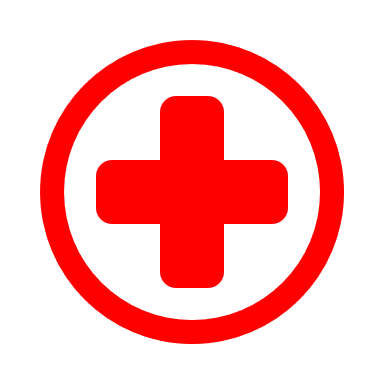
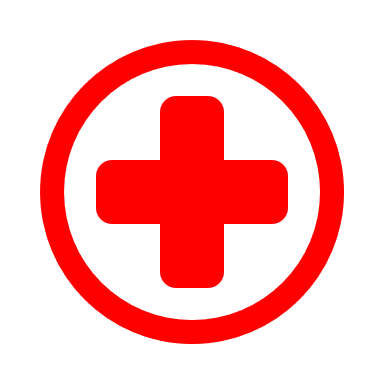
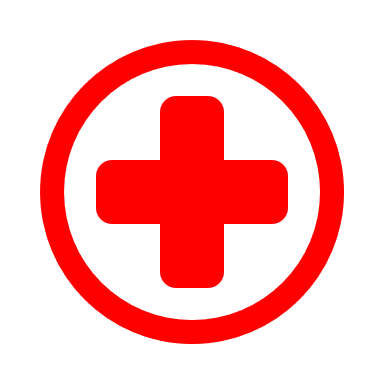
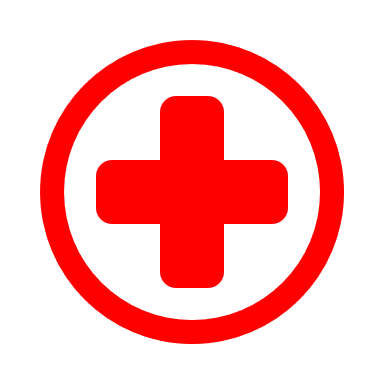
**Scansione vulnerabilità Metasploitable e risoluzione criticità**

Per questo esercizio, siamo andati ad effettuare un vulnerability scanner con Nessus sulla nostra macchina Metasploitable.

Una volta ottenuti i risultati, prenderemo alcune delle vulnerabilità critiche ed andremo ad effettuare le remediation action per risolvere tali criticità.



Date queste vulnerabilità critiche, andremo a eseguire azioni su quelle evidenziate.

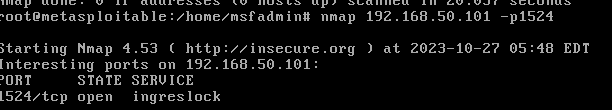
**Vulnerabilità 1: Blind Shell Backdoor Detection**

La prima vulnerabilità ci dice che è presente una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un soggetto ostile potrebbe utilizzare tale vulnerabilità per collegarsi alla porta e inviare direttamente comandi. In tal caso, il sistema potrebbe essere compromesso.



Dal dettaglio della vulnerabilità, possiamo notare che questa è la porta compromessa, andremo pertanto a lavorare direttamente su questa porta cercando di risolvere i problemi ad essa legata.

Andremo quindi ad effettuare una scansione con nmap della suddetta porta, per capire quale servizio sia attivo su di essa.



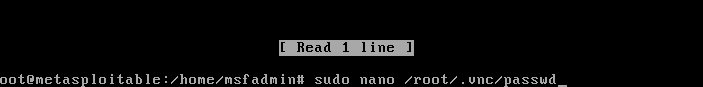
Dalla scansione, possiamo notare che sulla porta 1524 è in ascolto il servizio ingreslock. Per risolvere la vulnerabilità, andremo quindi commentare il servizio in ascolto per disattivarlo e porre rimedio al problema.



Servizio commentato (ingreslock)

**Vulnerabilità 2: VNC server “password” password**

Dal risultato della scansione, risulta che il server VNC ha una passowrd debole e che Nessus è riuscito ad eseguire il login con la password “password”. Un attaccante potrebbe sfruttare tale vulnerabilità per prendere il controllo del sistema. Per porre rimedio a ciò, andremo ad impostare una password più forte per il servizio sopra citato.



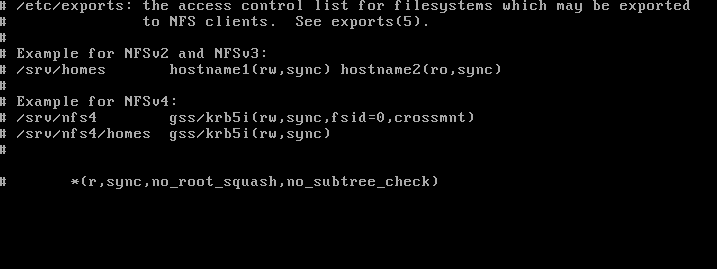
Una volta entrati nel file, modificheremo la password per renderla più sicura.

**Vulnerabilità 3: NFS Exported Share Information Disclosure**

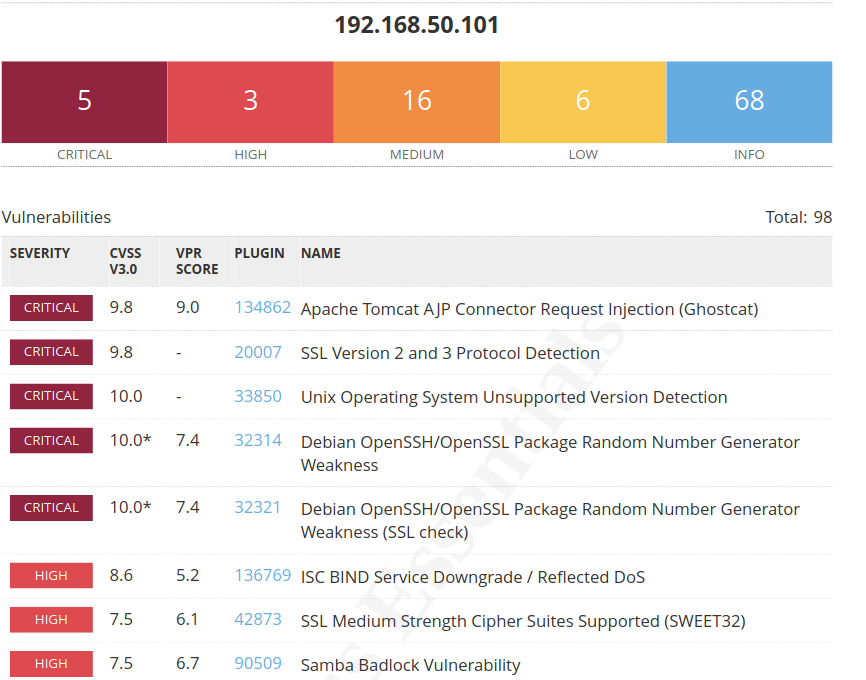
Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

NFS è un protocollo che consente ad un client di accedere a cartelle condivise da server remoti come se fossero in locale.

Andremo quindi a lavorare sul file relativo a questi permessi.



Abbiamo commentato l’ultima riga, eliminando di fatto tutti i permessi al suo interno che permettevano a chiunque di modificare i file sull’host remoto.



Come possiamo vedere, le nostre vulnerabilità non sono più presenti nel risultato della nuova scansione in quanto risultano risolte.