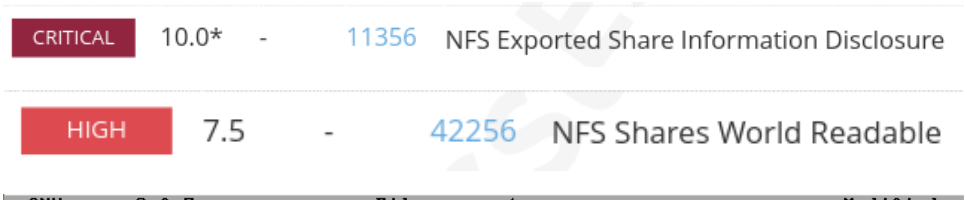
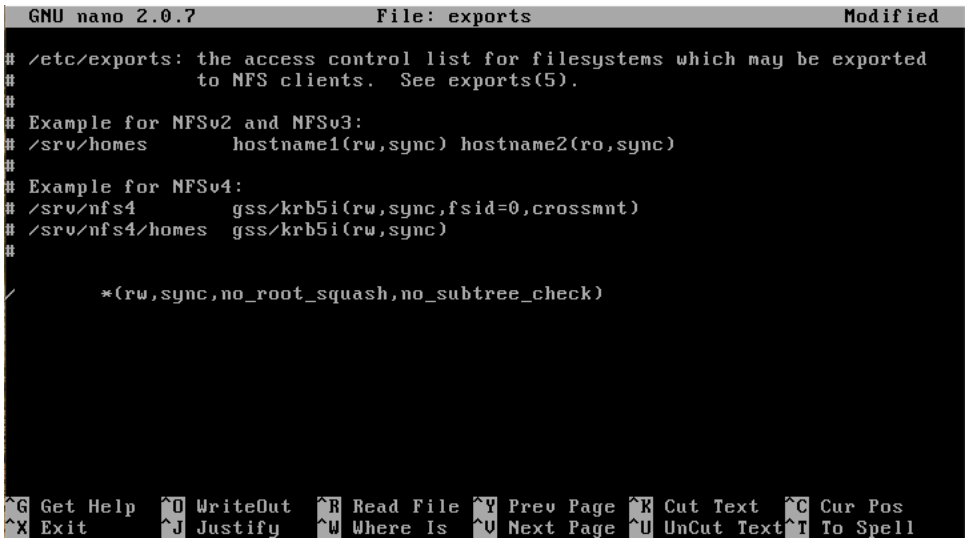
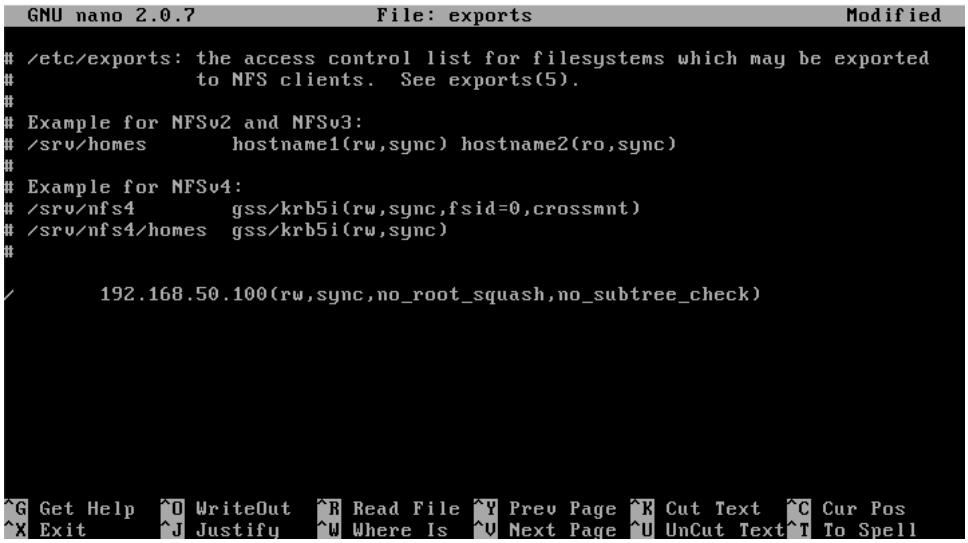


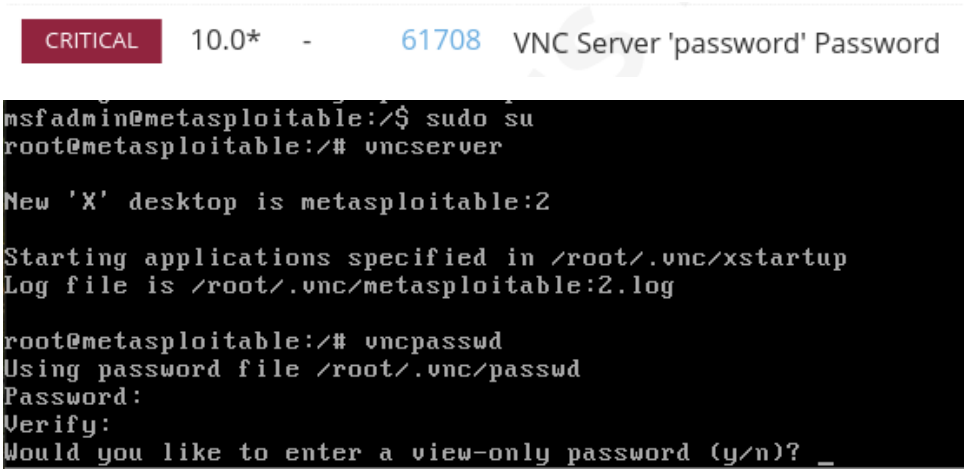




**Descrizione:** È stato individuato un errore di divulgazione delle informazioni riguardante le condivisioni NFS esportate sul sistema. Inizialmente, le condivisioni NFS erano configurate per consentire l'accesso a tutti gli host tramite il carattere jolly '*'. Questa configurazione esponeva le condivisioni NFS a potenziali rischi di sicurezza, consentendo a qualsiasi host di accedere alle risorse esportate.

**Soluzione:** Per risolvere questo problema, ho apportato le seguenti modifiche alla configurazione delle condivisioni NFS:

- Ho individuato e aperto il file di configurazione delle esportazioni NFS, generalmente denominato 'exports'.
- All'interno di questo file, ho localizzato la definizione della condivisione NFS interessata.

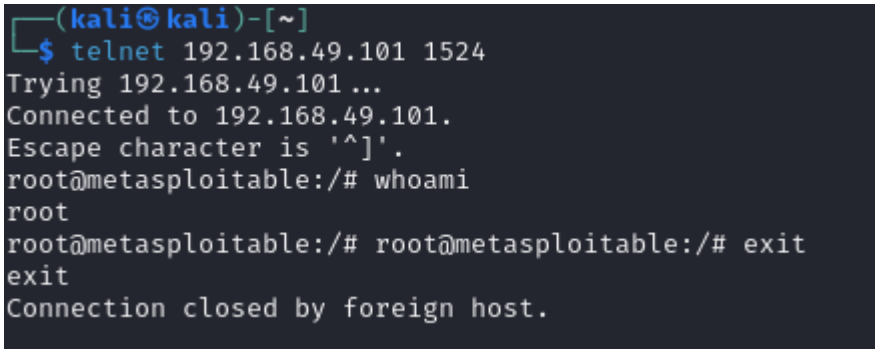
- Ho modificato i permessi della condivisione, sostituendo il carattere jolly '*' *con l'indirizzo IP specifico consentito. In questo caso, ho cambiato da* '*' a '192.168.50.100' per limitare l'accesso solo a questo indirizzo IP.
- Dopo aver apportato questa modifica, ho salvato il file di configurazione e ho riavviato il servizio NFS affinché le modifiche avessero effetto.

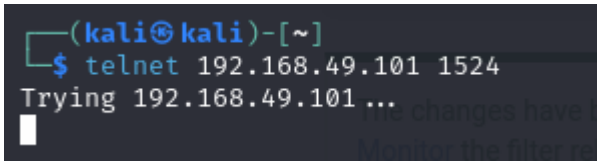


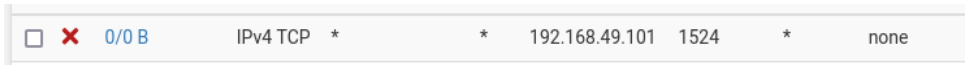

**Descrizione:** È stato riscontrato un problema relativo alla password del server VNC, dove la password predefinita era impostata su 'password'. Questa configurazione predefinita rappresentava un rischio per la sicurezza in quanto rendeva facile indovinare o scoprire la password per accedere al server VNC.

**Soluzione:** Per risolvere questo problema, sono stati eseguiti i seguenti passaggi:

- Accedendo al sistema con i privilegi di root, si è avviato il server VNC.
- Successivamente, è stato modificato immediatamente la password predefinita 'password' utilizzata dal server VNC.
- È stato utilizzato il comando o lo strumento appropriato per cambiare la password del server VNC. Ad esempio, è stato utilizzato il comando **`vncpasswd`** seguito dal prompt per inserire e confermare la nuova password desiderata.
- Dopo aver cambiato con successo la password, è stato confermato che il server VNC stesse utilizzando correttamente la nuova password per l'autenticazione.



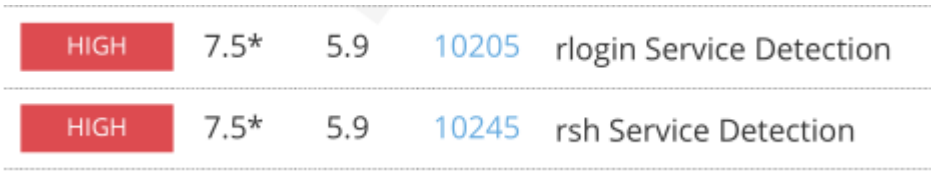



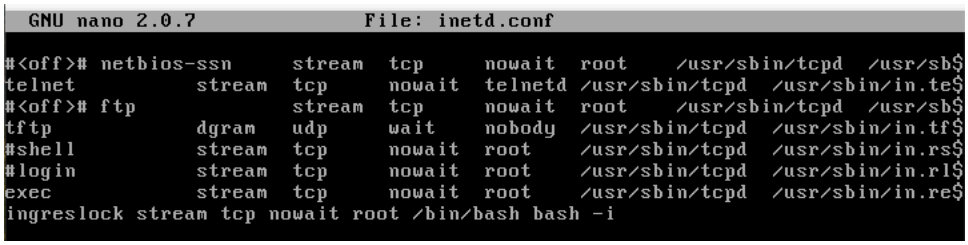




È stata individuata la presenza di una backdoor a bind shell sul sistema, con la quale era possibile connettersi al porto remoto senza autenticazione e inviare comandi direttamente. Questa vulnerabilità rappresentava un rischio significativo per la sicurezza del sistema.

**Soluzione:** Per risolvere questo problema, sono stati eseguiti i seguenti passaggi:

- Ho effettuato una prova di connessione alla backdoor utilizzando il comando Telnet per verificare la sua accessibilità e funzionalità.
- Dopo aver confermato che la backdoor era operativa, ho immediatamente agito per mitigare il rischio.
- Ho creato una regola nel firewall per bloccare il traffico verso la porta utilizzata dalla backdoor. Questa regola è stata configurata per impedire qualsiasi connessione in entrata o in uscita sulla porta specifica associata alla backdoor.
- Dopo aver implementato la regola del firewall, ho ripetuto il test utilizzando Telnet per tentare di accedere alla backdoor. Questa volta, il tentativo di connessione è stato respinto, confermando l'efficacia della regola del firewall nell'impedire l'accesso non autorizzato alla backdoor.






Sul sistema è stato individuato il servizio rlogin e rsh attivi, rappresentando potenziali vulnerabilità di sicurezza. Entrambi i servizi consentono l'accesso remoto al sistema senza crittografia dei dati, mettendo a rischio le credenziali degli utenti per possibili attacchi di intercettazione.

**Soluzione:** Per mitigare questi rischi di sicurezza, ho eseguito i seguenti passaggi:

- Accedendo al sistema come utente con privilegi di amministratore.
- Navigando nella directory /etc/ per individuare il file di configurazione del servizio inetd, denominato inetd.conf.
- All'interno del file inetd.conf, ho individuato le righe relative ai servizi rlogin e rsh.
- Ho disabilitato le righe relative ai servizi rlogin e rsh aggiungendo il carattere di commento "#" all'inizio di ciascuna riga. Questo ha impedito al servizio inetd di avviare i servizi rlogin e rsh durante l'avvio del sistema.
- Dopo aver apportato queste modifiche, ho salvato il file di configurazione e ho riavviato il servizio inetd affinché le modifiche avessero effetto.

Vulnerabilities Total: 109

| 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* | 5.1 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 5.1 | 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 |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 6.7 | 90509 | Samba Badlock Vulnerability |
| HIGH | 7.5* | 5.9 | 10205 | rlogin Service Detection |
| HIGH | 7.5* | 5.9 | 10245 | rsh Service Detection |
| MEDIUM | 6.5 | 3.6 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |

Come possiamo osservare nei screenshot, è evidente che le criticità di sicurezza individuate precedentemente sono state efficacemente risolte. Le azioni correttive intraprese hanno portato a una significativa mitigazione dei rischi presenti nel sistema.