# PRINCIPALI VULNERABILITA TROVATE

La scansione ha rilevato le seguenti vulnerabilità di sicurezza:

* Sistema Unix non aggiornato: il sistema Unix presente non è più supportato dalla casa madre, quindi non possono essere immessi aggiornamenti. Questo è molto pericoloso perché il sistema, essendo antiquato, potrebbe essere facilmente aggirato. Si consiglia di installare una nuova versione di Unix, possibilmente l'ultima versione disponibile, se questa non entra in conflitto con la struttura di rete.
* NFS non configurato correttamente: il servizio NFS è in esecuzione, ma non ci sono limitazioni alle condivisioni NFS. Ciò significa che un utente malintenzionato potrebbe accedere a qualsiasi file sul sistema leggerlo i scriverci un file malevolo. Si consiglia di riconfigurare il servizio NFS per limitare l'accesso alle condivisioni solo agli IP autorizzati.
* Server VNC con password debole: la password del server VNC è stata rilevata con un semplice attacco brute-force. Si consiglia di cambiare la password con una password forte, composta da almeno 10 caratteri e che includa caratteri speciali, alfanumerici, maiuscoli e minuscoli, e utilizzare riferimenti all azienda o nomi o numeri di telefono comunemente usati da noi
* Backdoor abilitata: è stata rilevata una shell che è in ascolto su una porta remota senza che sia richiesta alcuna autenticazione. Ciò significa che chiunque può accedere al sistema operativo. Si consiglia di configurarla per richiedere autenticazione.
* Bug nel generatore di numeri casuali di OpenSSL: è stato rilevato un bug nel generatore di numeri casuali di OpenSSL che potrebbe consentire a un utente malintenzionato di ottenere la chiave privata del server. Si consiglia di rigenerare tutto il materiale crittografico generato sull'host
* Servizio rlogin abilitato: il servizio rlogin è un protocollo obsoleto che trasmette tutti i dati in chiaro, inclusi nomi utente e password. Si consiglia di disabilitare il servizio rlogin. È anche vulnerabile ad attacchi di tipo ARP che potrbberro bloccare tutta la rete

Raccomandazioni per la risoluzione delle vulnerabilità

* Aggiornare il sistema Unix alla versione più recente.
* Configurare il servizio NFS per limitare l'accesso alle condivisioni solo agli IP autorizzati.
* Cambiare la password del server VNC con una password forte.
* Disabilitare la backdoor o configurarla per richiedere autenticazione.
* Rigenerare tutto il materiale crittografico generato sull'host remoto.
* Disabilitare il servizio rlog