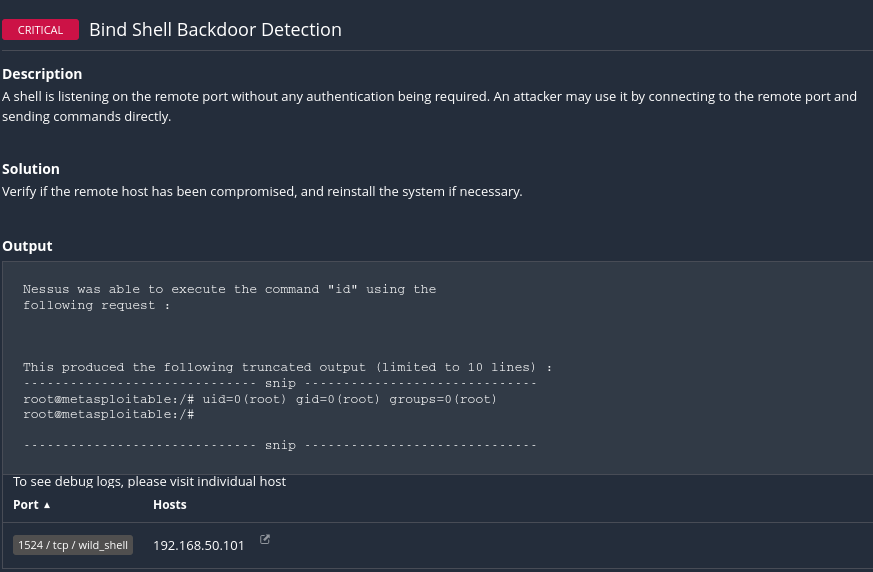
**ANALISI REPORT VULNERABILITÀ**

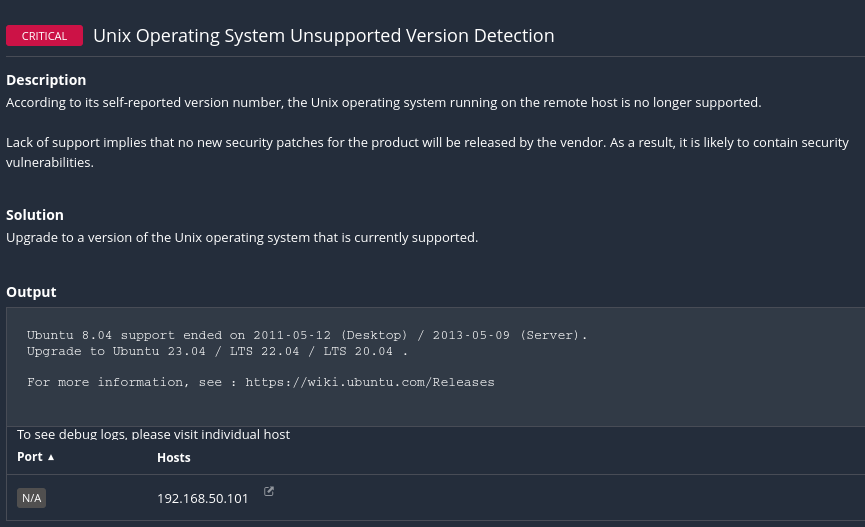
1) **Bind Shell Backdoor Detection**  
  
Si riferisce a una Shell che è associata alla porta 1524 (Ingreslock, utilizzata solitamente come backdoor). Eseguirà tutto ciò che viene inviato a quella porta su Bash e risponderà con l'output.  
Metasploitable include un servizio Shell aperto sulla porta 1524.  
Può essere utilizzata come strumento in fase di test per diagnosticare e risolvere problemi, ma può essere utilizzata da un black hat per connettersi a questa porta ed eseguire comandi in remoto.  
  
Shell: è un'interfaccia utente che fornisce l'accesso ai servizi di un sistema operativo e consente agli utenti di eseguire comandi.  
Bash: un tipo di Shell, applicazione che processa comandi.



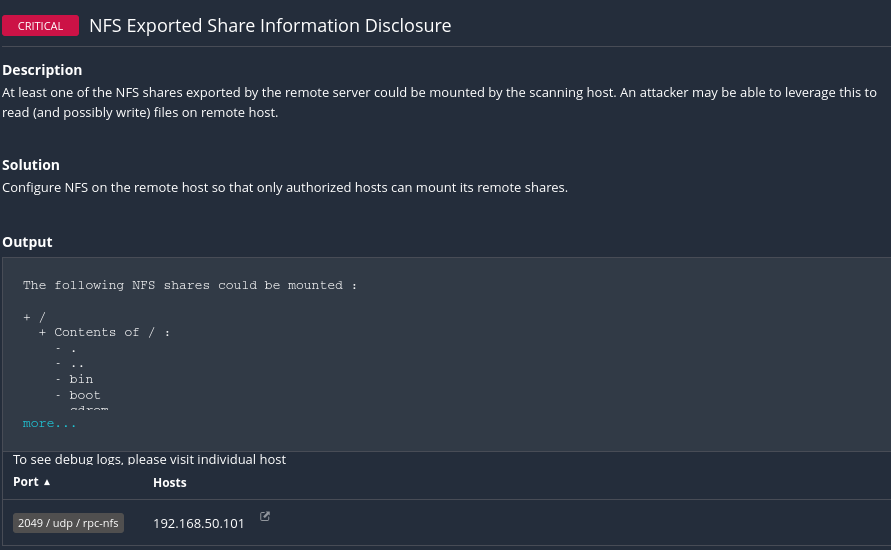


**Soluzione** (https://www.tenable.com/plugins/nessus/51988):   
Controllare se l’host è stato compromesso e successivamente di reinstallare il sistema operativo.

2) **Unix Operating System Unsupported Version Detection**  
  
Si riferisce alla versione del sistema operativo presente sulla macchina:   
Ubuntu 8.04 (supporto terminato nel 12 maggio 2011).  
Data la versione, il sistema operativo non è più supportato.  
La mancanza di supporto implica che il fornitore del S.O. non rilascerà alcuna nuova patch di sicurezza. Di conseguenza, è molto probabile che contenga vulnerabilità.

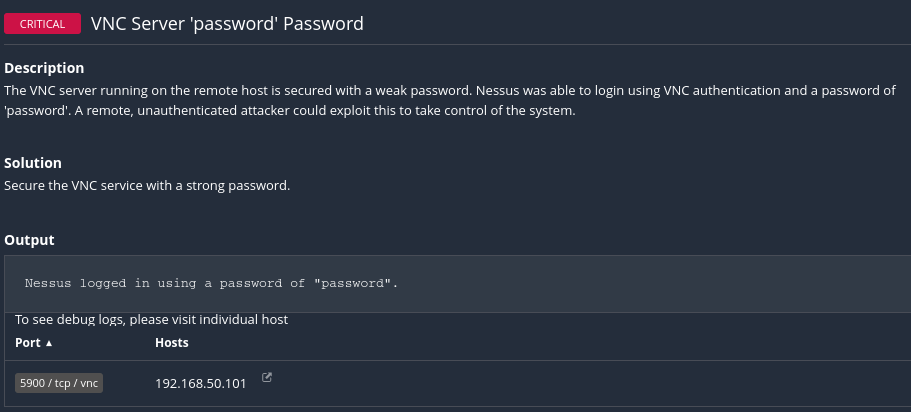


**Soluzione** (https://www.tenable.com/plugins/nessus/33850):   
Aggiornare il sistema operativo alla versione Ubuntu 23.04 e non alla più recente (23.10) in quanto quest’ultima potrebbe non essere testata sufficientemente.

3) **NFS Exported Share Information Disclosure**  
  
Si riferisce al protocollo NFS (Network File System) che agisce sulla porta 2049.  
NFS consente ad un utente di accedere (quindi visualizzare, archiviare e aggiornare) in remoto ai file (tra i più importanti file di boot, librerie, root) su una rete di computer come se fossero archiviati localmente.



**Soluzione** (https://www.tenable.com/plugins/nessus/11356):   
Configurare l’NFS sull’host in modo che solo gli host autorizzati possano usufruire dei suoi file in remoto.

4) **VNC Server 'password' Password**Si riferisce al VNC (Virtual Network Control) che opera attraverso la porta 5900.  
È un sistema di condivisione dello schermo creato per controllare in remoto un altro computer. Ciò significa che lo schermo, la tastiera e il mouse di un computer possono essere utilizzati in remoto da un altro dispositivo come se si fosse seduti proprio di fronte ad esso.  
In questo caso Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password".  
Un black hat potrebbe accedere grazie ad un semplice attacco a dizionario.



**Soluzione** (https://www.tenable.com/plugins/nessus/61708):  
Proteggere il servizio VNC con una password più complessa, formata da caratteri alfanumerici maiuscoli, minuscoli e caratteri speciali.