Esercizio S5L4

Vincenzo Colletta

Utilizzo dello strumento Nessus

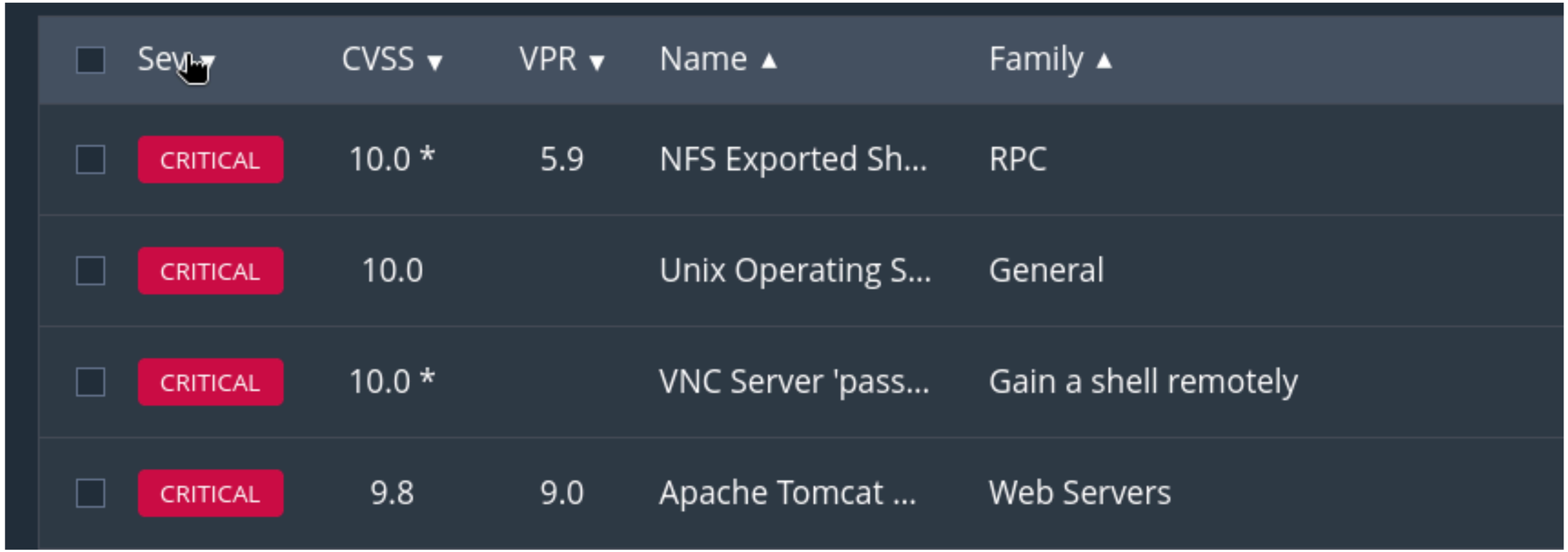
Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni.

Nessus è un noto software di scansione di vulnerabilità utilizzato per identificare potenziali punti deboli all'interno di reti e sistemi informatici. Questo strumento è ampiamente utilizzato da professionisti della sicurezza informatica, amministratori di rete e pen tester per valutare la sicurezza di un sistema o di una rete.
Ecco alcune delle principali caratteristiche di Nessus:

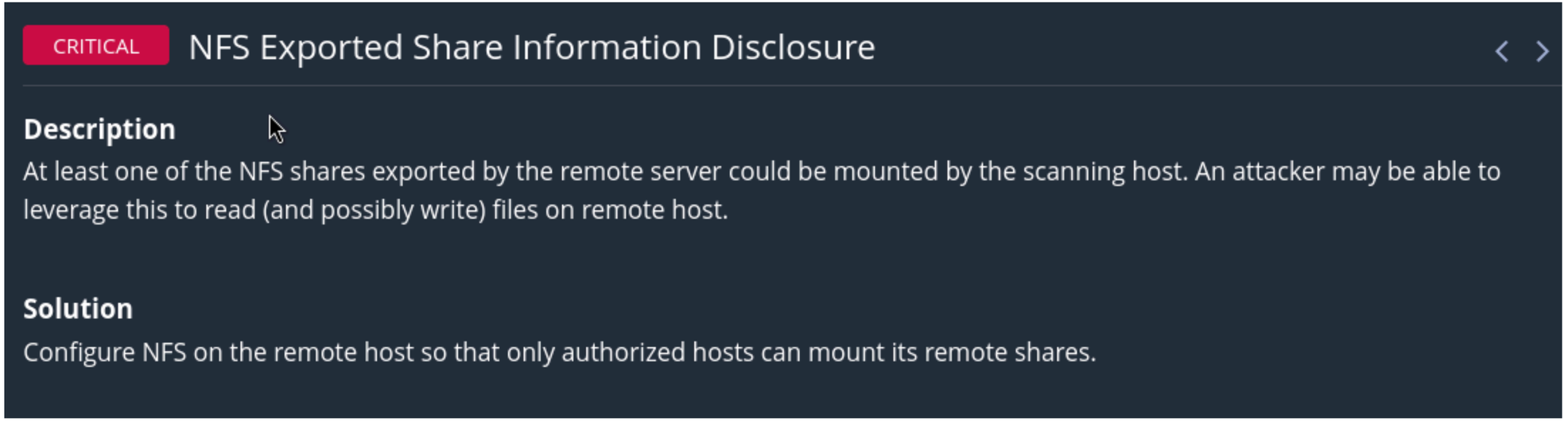
- **Scansione di vulnerabilità**: Nessus esegue scansioni complete o mirate su reti o sistemi per identificare vulnerabilità conosciute. Utilizza un database di vulnerabilità costantemente aggiornato per confrontare i risultati delle scansioni con le vulnerabilità note.
- **Classificazione delle vulnerabilità**: Dopo la scansione, Nessus classifica le vulnerabilità in base alla loro gravità e al loro potenziale impatto sulla sicurezza del sistema. Questo aiuta gli amministratori di sistema a concentrarsi sulle minacce più critiche.
- **Report dettagliati**: Nessus genera report dettagliati che forniscono informazioni sulle vulnerabilità rilevate, inclusi dettagli tecnici e suggerimenti su come mitigare o risolvere tali problemi.
- **Scansione regolare**: Gli utenti possono programmare scansioni periodiche per monitorare costantemente la sicurezza dei loro sistemi e reti.
- **Compliance e conformità**: Nessus può aiutare le organizzazioni a conformarsi a standard di sicurezza specifici fornendo report personalizzati che mostrano il grado di aderenza ai requisiti di sicurezza.
- **Supporto per reti eterogenee**: Nessus è in grado di scansionare una vasta gamma di dispositivi e sistemi operativi, rendendolo adatto per reti eterogenee.

Elenco di alcune vulnerabilità

Andremo ad analizzare le prime 4 vulnerabilità critiche

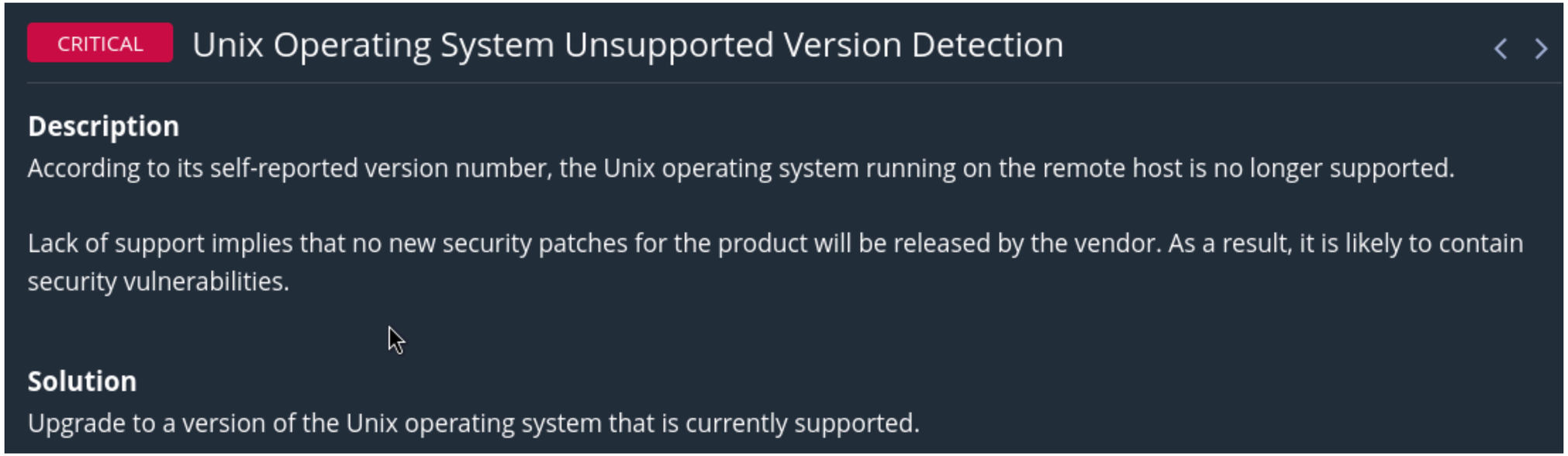


Sev	CVSS	VPR	Name	Family
CRITICAL	10.0 *	5.9	NFS Exported Sh...	RPC
CRITICAL	10.0		Unix Operating S...	General
CRITICAL	10.0 *		VNC Server 'pass...	Gain a shell remotely
CRITICAL	9.8	9.0	Apache Tomcat ...	Web Servers



La prima criticità rileva la possibile esposizione non autorizzata di informazioni o condivisioni NFS(Network File System).

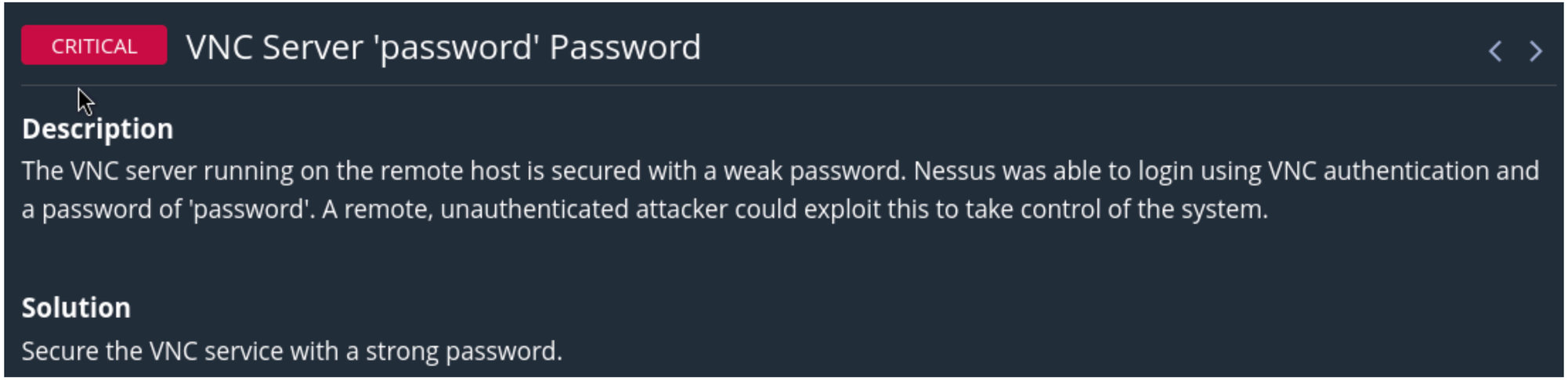
Il programma ci suggerisce anche la soluzione, ovvero, configurare un NFS su un host remoto in modo che solo gli host utilizzati, possano accedere.



Questo errore rileva una versione non supportata del sistema operativo Unix.

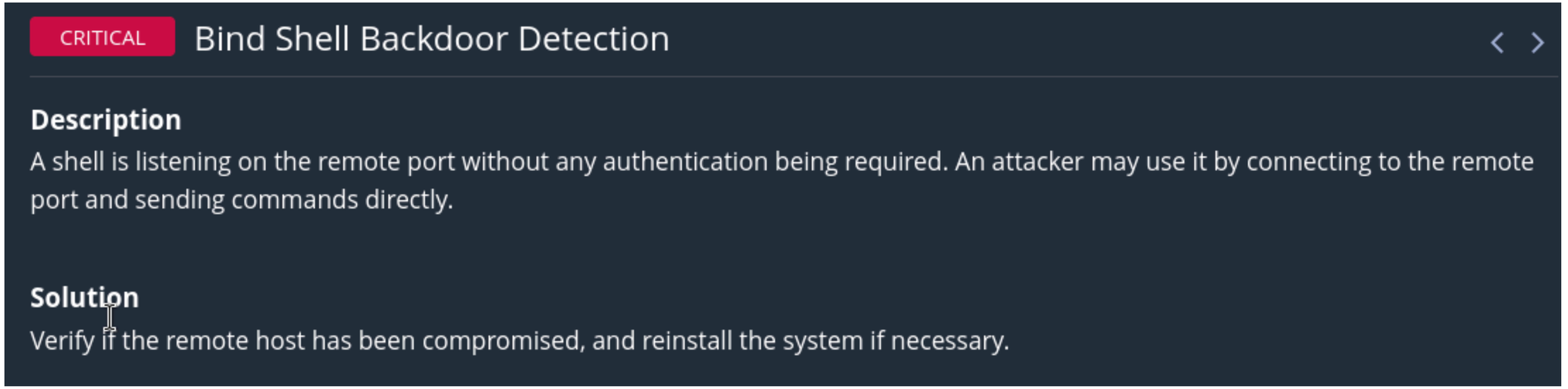
La soluzione è appunto l'aggiornamento.

È importante lavorare con sistemi che siano supportati dalle case produttrici.



Questo errore ci indica che la password del VNC server, è debole e che Nessus ha trovato una corrispondenza con la password.

La soluzione è appunto utilizzare una password più robusta.



In questa situazione specifica, Nessus sta rilevando che una Shell, è in ascolto su una porta remota senza richiedere nessuna autenticazione. Questo è un grave problema di sicurezza perchè un attaccante potrebbe sfruttare questa opportunità per connettersi a quella porta remota e inviare comandi direttamente senza doversi autenticare.
La soluzione è verificare se l'host è stato compromesso e se necessario reinstallare il sistema.