*Report Vulnerabilità*

**VULNERABILITÀ DELL’HOST**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **192.168.50.101** | |  |  |
| 10 | 6 | 23 | 5 | 126 |



**51988 - Bind Shell Backdoor Detection**

**Riassunto**

L’host remoto potrebbe essere compromesso.

## Descrizione

Una shell sta ascoltando sulla porta remota senza alcuna autenticazione richiesta. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

## Soluzione

Verifica se l’host remote è stato compromesso e reinstalla il Sistema se necessario.

**Fattore di rischio**: **Critico**

**61708 - VNC Server 'password' Password**

# Riassunto

Il server VNC, che viene eseguito sull’host remoto, non è sicuro in quanto ha una password debole.

# Descrizione

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password 'password'.

Un attaccante remoto e non autenticato potrebbe sfruttarlo per prendere il controllo del sistema.

**Fattore di rischio: Critico**