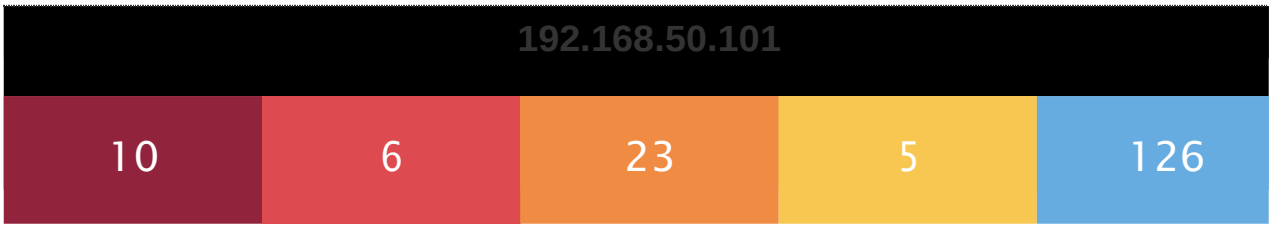
Report Vulnerabilità

Scansione sulla macchina target con indirizzo 192.168.50.101 con nessus versione 10.3.0 Debian 9 amd 64

VULNERABILITÀ DELL'HOST



Informazioni sull'host

Nome Netbios: METASPLOITABLE

IP target:192.168.50.101

MAC Address: 08:00:27:52:71:A7

Sistema operativo: Linux Kernel 2.6 on Ubuntu 8.04

Vulnerabilità

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.

Solution

Metti in sicurezza il servizio VNC con una password più efficace e complessa.

Fattore di rischio: Critico