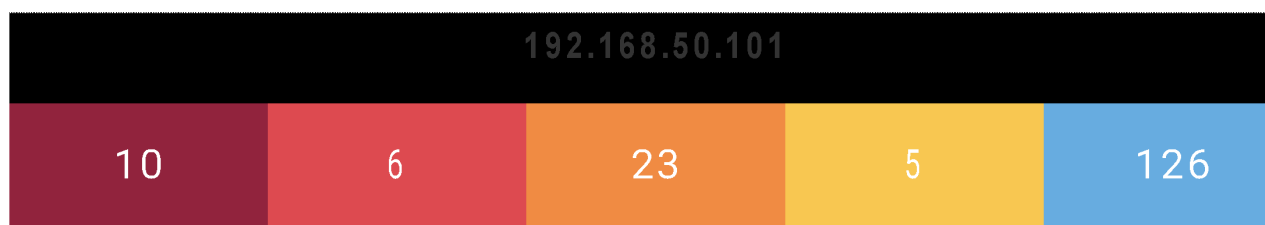


# Report Nessus

MACCHINA TARGET: Metasploitable  
Software Nessus versione 10.3.0 debian9 amd 64  
Ip target:192.168.1.36

Ho fatto alcune scansioni con il software Nessus. Ho optato per una scansione base con le porte più comuni utilizzate dai sistemi ed ho riscontrato alcune criticità da risolvere in maniera urgente.

## 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

11356 - NFS Exported Share Information Disclosure

## Riassunto

È possibile accedere alle condivisioni NFS sull'host remoto.

## Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato può essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) i file su host remoto.

## Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le condivisioni remote.

**Fattore di rischio:** Critico

## 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**