

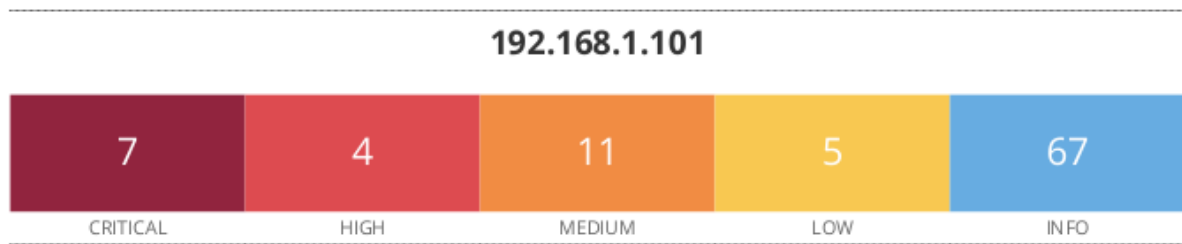
REPORT NESSUS

Macchina Target: Metasploit

Tool utilizzato: Nessus 10.3.0 debian9 amd64

IP Target: 192.168.1.101

VULNERABILITA' DELL'HOST



Informazioni sull'host

Nome Netbios: Metasploitable

IP Target: 192.168.1.101

VULNERABILITA'

CRITICAL Bind Shell Backdoor Detection

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Riassunto

L'host remoto potrebbe essere compromesso.

Descrizione

Una shell sta ascoltando una 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 remoto è stato compromesso e reinstalla il Sistema se necessario.

Fattore di rischio: CRITICO

CRITICAL

NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Riassunto

E' 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

CRITICAL

VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

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.

Soluzione

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

Fattore di rischio: CRITICO