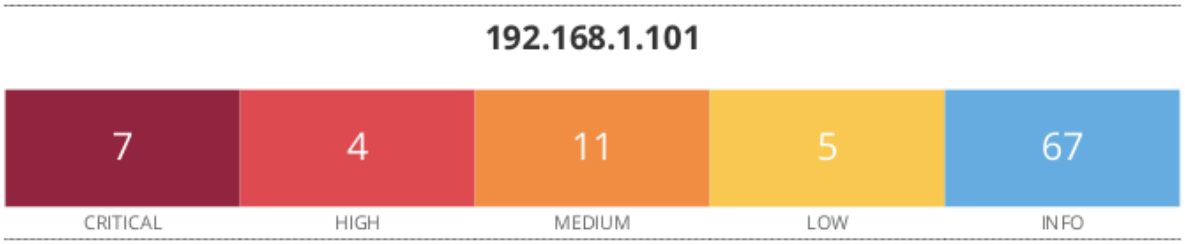
REPORT NESSUS

Macchina Target: Metasploit
Tool utilizzato: Nessus 10.3.0 debian9 amd64
IP Target: 192.168.1.101

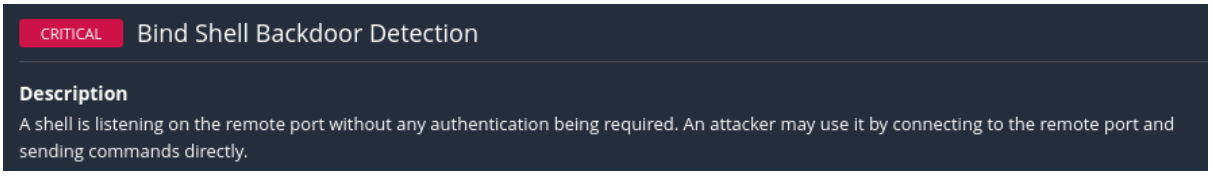
VULNERABILITA' DELL'HOST



Informazioni sull'host

Nome Netbios: Metasploitable
IP Target: 192.168.1.101

VULNERABILITA'



Riassunto

L'host remoto potrebbe essere compromesso.

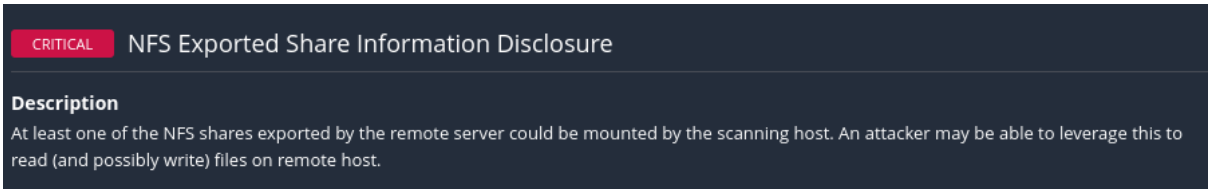
Descrizione

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

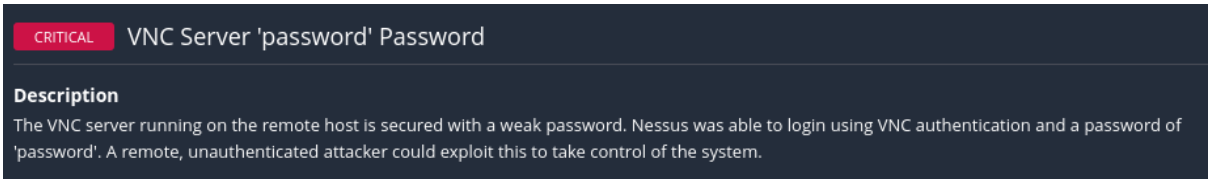


Riassunto
E’ possibile accedere alle condivisioni NFS sull’host remoto.

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



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