Vulnerability Assessment Metaspoitable

Report generated by Nessus™ Thu, 24 Nov 2022 08:54:46 EST

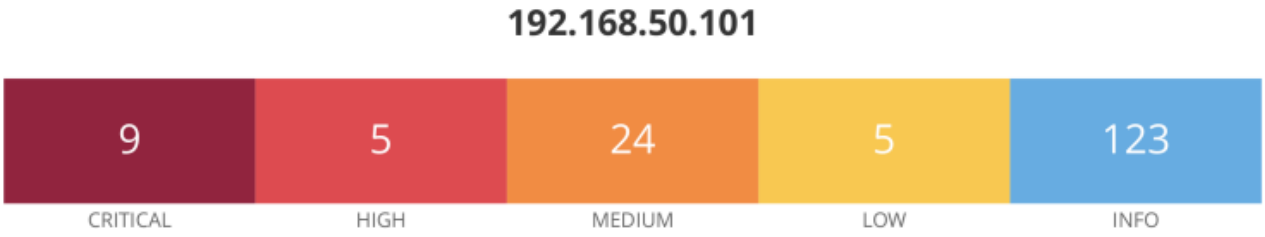
REPORT TECNICO 25/11/2022

FACCILONGO DOMENICO

NESSUS: VULNERABILITY ASSESSMENT METASPOITABLE

METASPOITABLE IP: 192.168.50.101

VULNERABILITIES TROVATE:



SCAN INFORMATION:

Start Time: 24/11/2022 h.14:50

End Time: 24/11/2022 h.15:17

HOST INFORMATION:

Netbios Name: METASPOITABLE

IP: 192.168.50.101

MAC Address: 08:00:27:7B:21:1D

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

VULNERABILITIES CRITICAL

51988 - Bind Shell Backdoor Detection (Risk Factor: CRITICAL)

Plugin output: tcp/1524/wild_shell

Description:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato potrebbe utilizzarlo collegandosi alla porta e inviando comandi diretti.

Soluzione:

Verifica se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

11356 - NFS Exported Share Information Disclosure (Risk Factor: CRITICAL)

Plugin Output: udp/2049/rpc-nfs

Description:

Almeno una delle condivisoni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

Soluzione:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisone remote.

61708 - VNC Server 'password' Password (Risk Factor: CRITICAL)

Plugin Output: tcp/5900/vnc

Description:

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

Soluzione:

Proteggi il servizio VNC con una password sicura.