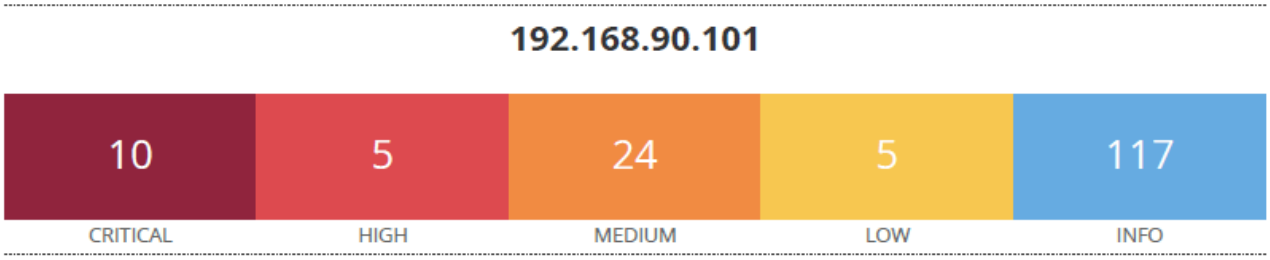
Scan_Metasploitable

Report generated by Nessus™ Thu, 24 Nov 2022 15:23:25 CET

Floriana Feminò

25/11/2022



VULNERABILITY ASSESSMENT – REPORT TECNICO

Informazioni sulla scansione

Inizio: 24/11/ 2022 14:53:49

Termine: 24/11/2022 15:23:25

Informazioni sull'host

Netbios Name: METASPLOITABLE

IP: 192.168.90.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

VULNERABILITA' DA CORREGGERE

61708 - VNC Server 'password' Password

Descrizione:

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password di tipo "password". Un attaccante remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

Soluzione:

Proteggere il servizio VNC con una password forte.

Fattore di Rischio: Critico

Plugin Output: tcp/5900/vnc

51988 - Bind Shell Backdoor Detection

Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione:

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

Fattore di rischio: Critico

Plugin Output: tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure

Descrizione:

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

Soluzione:

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

Fattore di Rischio: Critico

Plugin Output: udp/2049/rpc-nfs