VulnerabilityAssessment

Report generated by Nessus™ Thu, 24 Nov 2022 17:20:20 CET

TABLE OF CONTENTS

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.32.101
MAC Address:	08:00:27:F4:08:97
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

A seguito della scansione effettuata tramite software Nessus sull'host in questione, sono state rilevate: 44 minacce suddivise in:

Critica

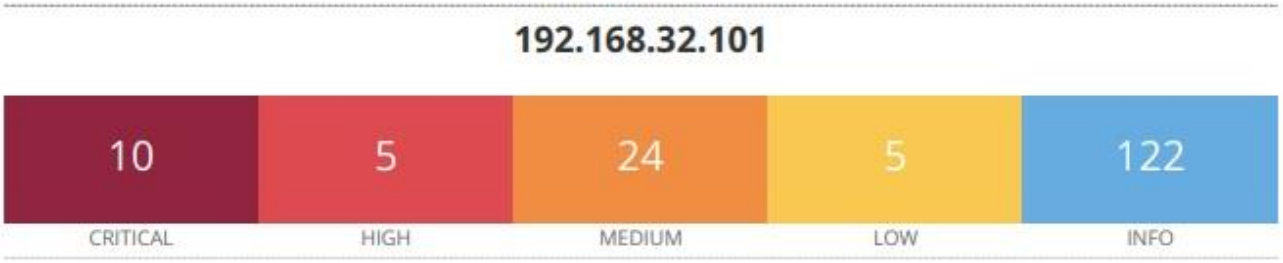
Alta

Media

Bassa

e 122 Informazioni su applicazioni e servizi.

(In questa analisi verranno evidenziate tre vulnerabilità di livello critico)



51988 - Bind Shell Backdoor Detection

Sinossi: L'host remoto potrebbe essere stato compromesso.

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

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

11356 - NFS Exported Share Information Disclosure

Sinossi: 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 (e possibilmente scrivere) file su host remoto.

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

61708 - VNC Server 'password' Password

Sinossi: Il server VNC in esecuzione sull'host remoto è protetto con una password debole.

Descrizione: Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un aggressore remoto e non autenticato potrebbe sfruttare

Soluzione: Proteggi il servizio VNC con una password complessa.