Scan Metaesploitable

Report generated by Nessus™ Thu, 24 Nov 2022 10:28:28 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.50.103

9	5	24	5	119
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Nov 24 09:49:46 2022
End time: Thu Nov 24 10:28:28 2022

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.50.103
MAC Address: 08:00:27:86:14:54
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

51988 - Bind Shell Backdoor Detection

Description

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

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Plugin Output

tcp/1524/wild_shell

11356 - NFS Exported Share Information Disclosure

Description

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 condivisioni remote.

Risk Factor

Critical

CVSS v2.0 Base Score

Published: 2003/03/12, Modified: 2018/09/17

Plugin Output

udp/2049/rpc-nfs

61708 - VNC Server 'password' Password

Description

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.

Solution

Proteggete il servizio VNC con una password forte.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc