



VulnerabilityAssessment2

Report generated by Nessus™

Fri, 25 Nov 2022 16:40:10 CET

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.32.101.....	4
-----------------------	---

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, dopo le soluzioni adottate, sono state rilevate: 39 minacce suddivise in:

Critica

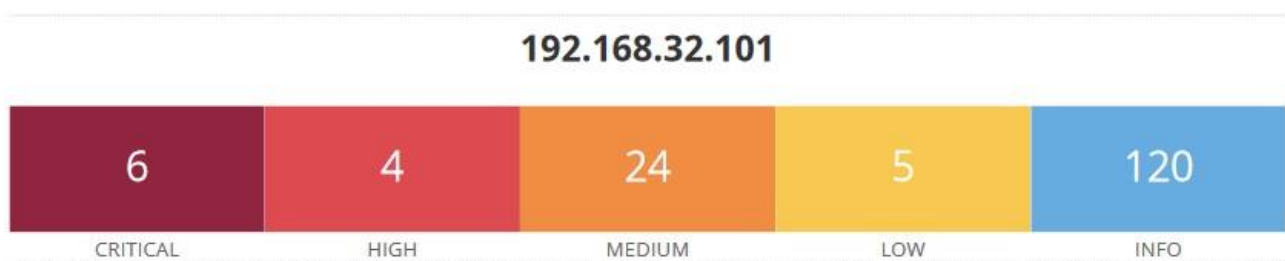
Alta

Media

Bassa

e 120 Informazioni su applicazioni e servizi.

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



51988 - Bind Shell Backdoor Detection

La seguente vulnerabilità è stata risolta tramite la soluzione di Nessus e una guida del seguente link:

<https://rawhex.com/blog/2016/03/22/a-guide-to-recognising-backdoors-using-metasploitable-2/>

11356 - NFS Exported Share Information Disclosure

La seguente vulnerabilità è stata risolta tramite la soluzione di Nessus e una guida del seguente link:

<https://linuxconfig.org/how-to-change-vnc-password-on-linux>

61708 - VNC Server 'password' Password

La seguente vulnerabilità è stata risolta tramite la soluzione di Nessus e una guida del seguente link:

<https://access.redhat.com/documentation/en>

[us/red_hat_enterprise_linux/8/html/managing_file_systems/exporting-nfs-shares_managing-file-systems](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/managing_file_systems/exporting-nfs-shares_managing-file-systems)

Orlando Tangari