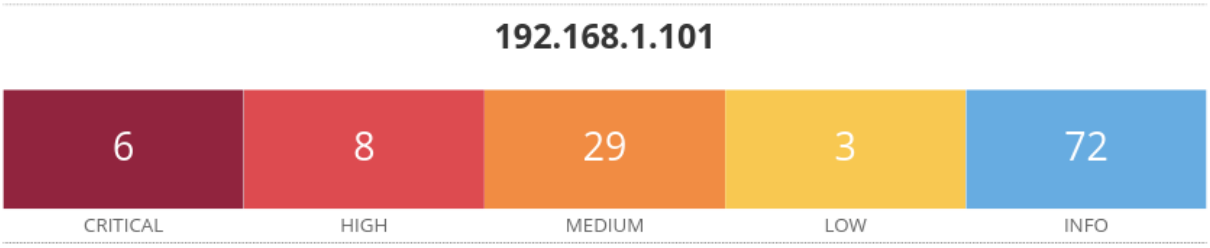
SCANSIONE FINE

In questo report, riporto il risultato finale della nuova scansione dopo aver risolto le 3 vulnerabilità che ho preso in esame.

Questo è il risultato finale



Informazioni sull'host

IP: 192.168.1.101

MAC: 08:00:27:E5:4A:BF

OS: Kernel Linux 2.6 su Ubuntu 8.04 (hardy)

Inizio: 05 Marzo alle 1:52 PM

Fine: 05 Marzo alle 3:33 PM

Tempo scansione: 2 ore

Andrò ad inserire solo una lista delle vulnerabilità **CRITICAL**

Descrivo nuovamente le 4 colonne della tabella:

- **CSVV v3.0:** Il CVSS (Common Vulnerability Scoring System) è uno standard industriale per valutare e assegnare un punteggio numerico alle vulnerabilità delle informazioni. La versione 3.0 fornisce un modello migliorato e più accurato per valutare il rischio associato alle vulnerabilità.
- **VPR SCORE:** indica la probabilità di sfruttamento di una vulnerabilità.
- **PLUGIN:** componenti software specializzati che ampliano le funzionalità di uno strumento di sicurezza, consentendo di identificare e valutare le potenziali minacce alla sicurezza all'interno di un sistema.
- **NAME:** nome della vulnerabilità

CVSS V3.0	VPR SCORE	PLUGIN	NAME
9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
10.0	-	33850	Unix Operating System Unsupported Version Detection
10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Come si può notare dalla nuova scansione effettuata, i metodi di risoluzione hanno funzionato e le vulnerabilità VNC Server 'password' Password, NFS Exported Share Information Disclosure e Bind shell backdoor detection sono scomparse dalla scansione di Nessus.