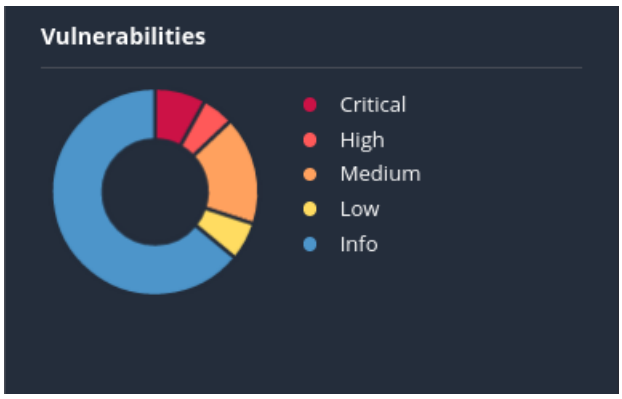
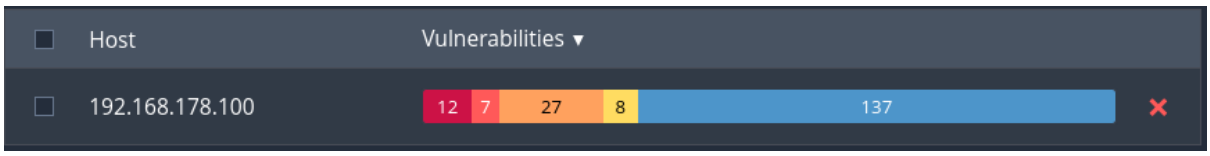
Identificazione e valutazione vulnerabilità: Metasploitable

L'obiettivo di questo report è esporre i risultati di un'analisi delle vulnerabilità effettuata alla macchina Metasploitable tramite l'utilizzo di Nessus. Sono state identificate vulnerabilità di diverse gravità come dimostrato di seguito.

Risultati ottenuti



- Vulnerabilità critiche: 6%
- Vulnerabilità alte: 3,6%
- Vulnerabilità medie: 14,1%
- Vulnerabilità basse: 4,1%
- Vulnerabilità nulle (informazioni sulla macchina): 71,7 %



Lista delle vulnerabilità.

In questa lista sarà contenuta lo score CVSS, ovvero un metodo di valutazione delle vulnerabilità, il quale ne indica la gravità assegnando un voto da 1 a 10, dove 1 indica una gravità nulla mentre il 10 indica una gravità massima.

- **Il Server VNC ha come password la parola "password" - Voto CVSS: 10**
- **Il Server VRC contiene una backdoor – Voto CVSS: 10**
- **Il servizio remoto sulla porta TCP 5432 applica delle cifrature (SSL 2.0 e SSL 3.0) che hanno delle debolezze note – Voto CVSS: 9.8**
- **La versione del sistema operativo *Unix* non è più supportata**
- **Il servizio SMTP sulla porta TCP 25 applica delle cifrature (SSL 2.0 e SSL 3.0) che hanno delle debolezze note – Voto CVSS: 9.8**
- **Backdoor sulla Shell in ascolto sulla TCP 1524 - Voto CVSS: 9.8**