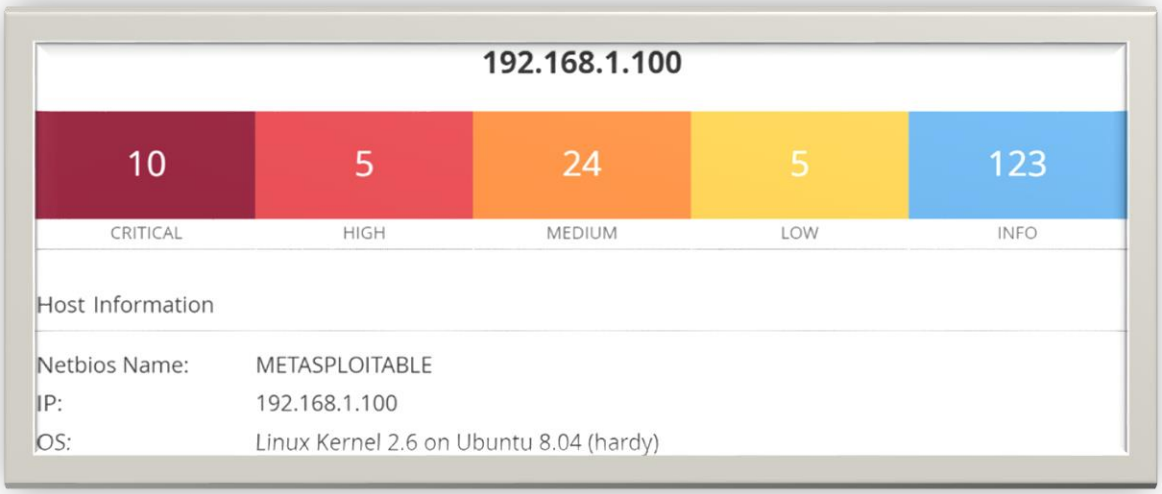
Analisi delle vulenrabilità



Queste sono le vulnerabilità critiche che andrebbero sistemate:

1) Apache Tomcat AJP connector (Ghostcat): è presente sul Web server Apache Tomcat un file in ascolto su un host remoto che ha accesso in scrittura e in lettura. Rappresenta una grave minaccia in quanto potrebbe permettere l'aggiunta di backdoor e la manipolazione dei file.

Rimendi: aggiornare le configurazioni di AJP in modo tale che richiedano l'autorizzazione per essere usato, e aggiornare il server Tomcat all'ultima versione disponibile.

2) Bind Shell Backdoor Detection: una shell è in ascolto su una porta remota senza che ci sia bisogno di un autorizzazione. Un attaccante può sfruttare la porta remota per inviare comandi direttamente.

Rimedi: verificare se l'host remoto è stato già compromesso, e reinstallare il sistema se necessario.

3) Debian OpenSSh/OpenSSL Weakness: la chiave del host remoto SSH che è stata generata da Debia o Ubuntu ha un bug nella generazione randomica dei numeri usati per la crittografia. Un attaccante può facilmente manipolare e decifrare la seguenza numerica e cambiarla a proprio piacimento per impostare un attacco.

Rimedi: considerando che tutte le chiavi siano facilemente decifrabili, reimpostare e configurare nuovamente le chiavi del SSh, SSL e della OpenVPN.

4) NFS information disclosure: è possibile accedere ai file condivisi sul Network File System su un host remoto. Un attaccante può fare leva su questi file e sovrasciverli per usarli a proprio vantaggio.

Rimedi: configurare il NFS sul host remoto in modo tale che solo gli host autorizzati possano inserire file remoti sul server.

5) Unix Operating System Unsupported Version Detection: il sistema operativo del host remoto non è più supportata. Con la mancanza di supporto vengono meno le patches di sicurezza per la protezione del sistema.

Rimedi: fare l'upgrade del sistema operativo Unix per sopperire a queste mancanze.