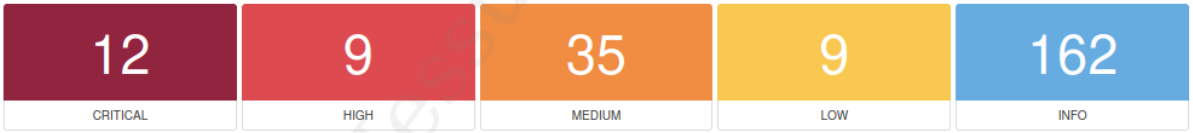
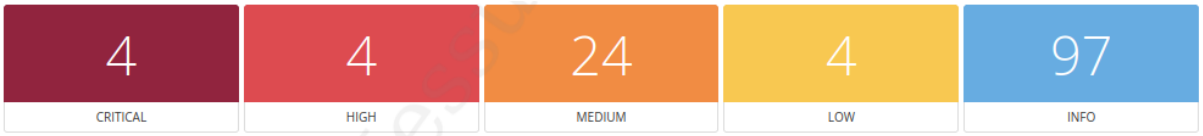
Gentile dirigente,

Desidero informarla riguardo alle criticità di sicurezza che ho identificato durante la scansione della sua macchina Metasploitable utilizzando il software Nessus. Queste criticità rappresentano delle vulnerabilità che potrebbero essere sfruttate da potenziali attacchi informatici. Mi sono preso la libertà di risolvere queste problematiche per garantire la sicurezza delle sue informazioni.

Prima scansione delle vulnerabilità:



Scansione finale delle vulnerabilità:



Ecco un elenco delle criticità di livello critico che ho riscontrato e risolto:

1. NFS Exported Share Information Disclosure: Questa vulnerabilità permetteva la divulgazione non autorizzata delle informazioni contenute nelle condivisioni NFS. Ho adottato misure per impedire l'accesso non autorizzato a queste informazioni riservate.

2. Bind Shell Backdoor Detection: Sono stati rilevati indizi di un possibile backdoor denominato "Bind Shell". Questo tipo di backdoor può consentire l'accesso non autorizzato al sistema. Ho eliminato questa minaccia per evitare intrusioni indesiderate.

3. VNC Server "password" Password: La scansione ha rivelato una password debole utilizzata per il server VNC. Questo avrebbe potuto facilitare un attacco di forza bruta o l'accesso non autorizzato. Ho rimosso l’accesso al Server VNC eliminando il file di configurazione della password.

4. rexecd Service Detection: Il servizio rexecd è stato individuato durante la scansione. Questo servizio è noto per le sue vulnerabilità e potrebbe essere sfruttato per ottenere accesso non autorizzato al sistema. Ho disabilitato il servizio per prevenire potenziali attacchi.

5. Unix Operating System Unsupported Version Detection: È stata individuata una versione non supportata del sistema operativo Unix. Le versioni non supportate potrebbero non ricevere gli aggiornamenti di sicurezza necessari per proteggere il sistema. Ho eseguito l'aggiornamento del sistema operativo per garantire che sia protetto da eventuali vulnerabilità.

6. Apache Tomcat Web Server SEoL (<= 5.5.x): Durante la scansione, ho individuato una versione obsoleta del server web Apache Tomcat. Le versioni obsolete possono presentare falle di sicurezza note. Ho disabilitato il servizio di Tomcat per mitigare tali rischi.

7. Apache Tomcat AJP Connector Request Injection (Ghostcat): Ho rilevato una vulnerabilità nota come "Ghostcat", che consente a un attaccante remoto di eseguire codice malevolo sul server Tomcat. Ho applicato le correzioni necessarie per impedire eventuali attacchi attraverso questa vulnerabilità.

8. Debian OpenSSH Package Random Number Generator Weakness: Durante la scansione, ho identificato una debolezza nella generazione dei numeri casuali all'interno del pacchetto OpenSSH di Debian. Questa debolezza avrebbe potuto compromettere la sicurezza delle comunicazioni crittografate. Ho corretto questa debolezza per garantire la sicurezza delle connessioni SSH.

Mi preme sottolineare che queste azioni sono state intraprese per garantire la sicurezza delle sue informazioni e prevenire potenziali violazioni dei dati

Cordiali saluti,
da Anatoliy Prysyazhnyuk,
04.06.2023