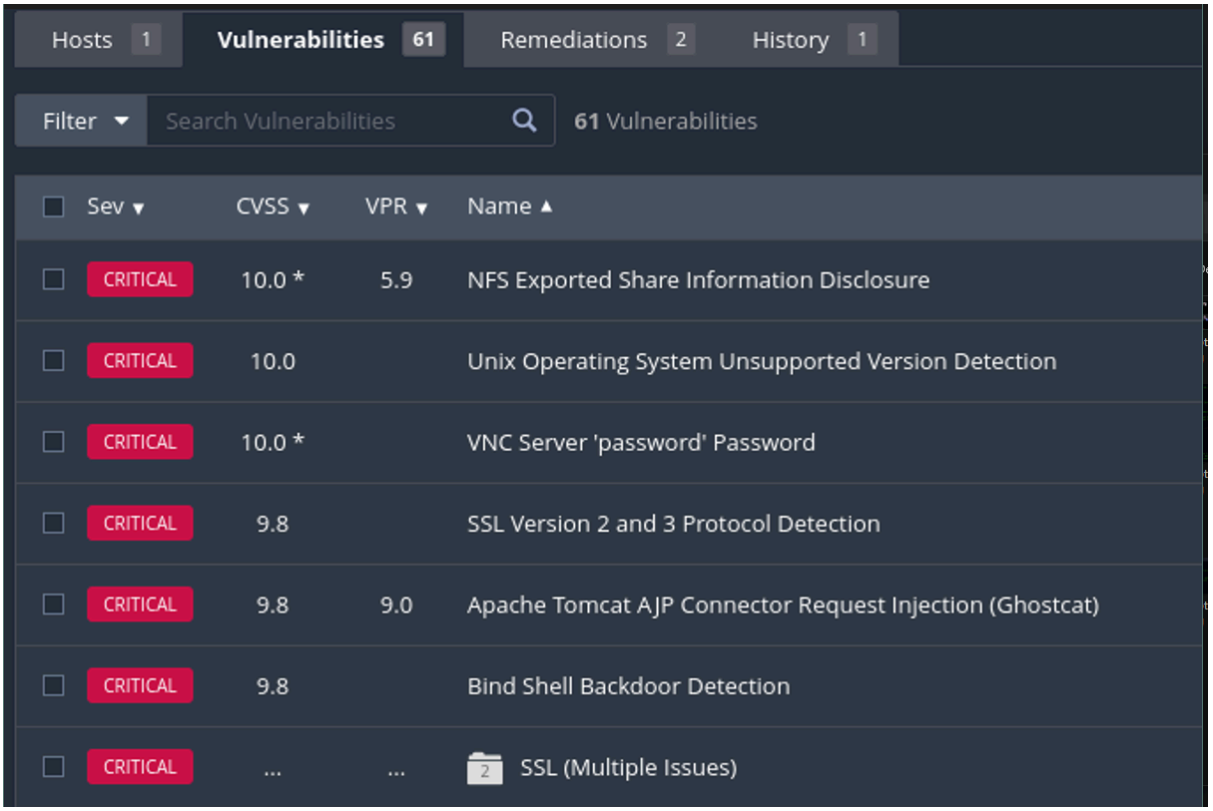
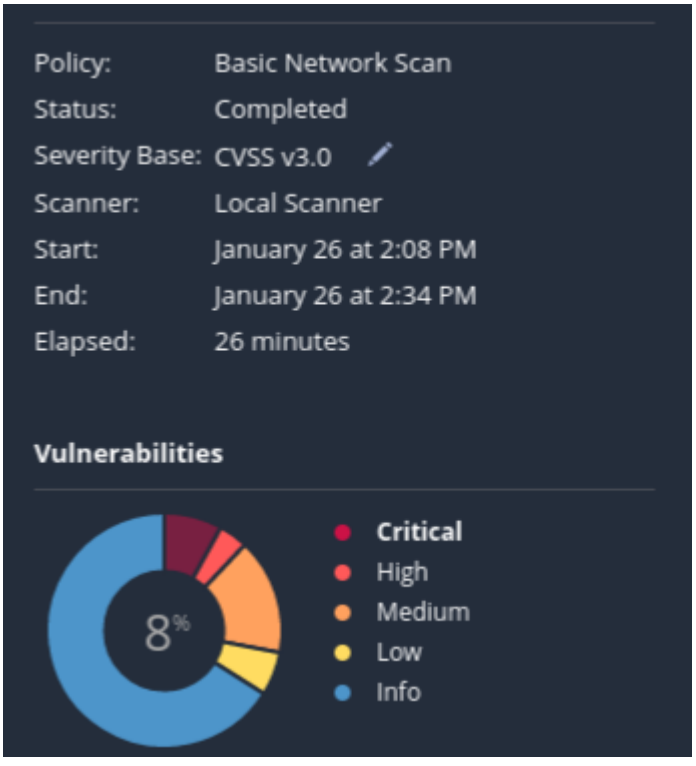
SCANSIONE

Gelosa Matteo

Ho eseguito la scansione con Nessus sulla macchina Metasploitable con ip:(192.168.32.101).
Le vulnerabilità critiche che sono state trovate sono le seguenti:





Ho scelto quattro vulnerabilità critiche da risolvere e correggere.

- **VNC Server 'password' Password**
- **NFS Exported Share Information Disclosure**
- **32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
- **Apache Tomcat AJP Connector Request Injection**

DESCRIZIONE VULNERABILITA'

La prima vulnerabilità che ho scelto "VNC Server 'password' Password" è considerata critica semplicemente perchè la password per accedere al servizio è 'password'.
Un utente malintenzionato potrebbe accedere con molta facilità al server VNC avendo cosi il pieno controllo della macchina.

La seconda vulnerabilità "NFS Exported Share Information Disclosure" è considerata critica in quanto è attivo un server NFS sulla macchina meta a cui è consentito l'accesso a chiunque.
Un utente malintenzionato potrebbe avere accesso a file e directory.

La terza vulnerabilità "32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness" è considerata critica perchè le chiavi generate dall'host SSH sono deboli.
Queste chiavi sono state generate da sistemi contenenti bug e quindi un utente malintenzionato potrebbe facilmente decifrare la connessione.

La quarta vulnerabilità "Apache Tomcat AJP Connector Request Injection" è considerata critica in quanto è presente un connettore AJP vulnerabile in ascolto sull' host remoto.

Un utente malintenzionato potrebbe sfruttare tale vulnerabilità per leggere file dell'applicazione web e più difficilmente potrebbe caricare del codice malevolo.

- **57608 - SMB Signing not required (vulnerabilità a scelta)**

Vulnerabilità considerata critica in quanto la firma al servizio smb non è richiesta.
Questo comporta che un attaccante malintenzionato possa compiere azioni malevole.