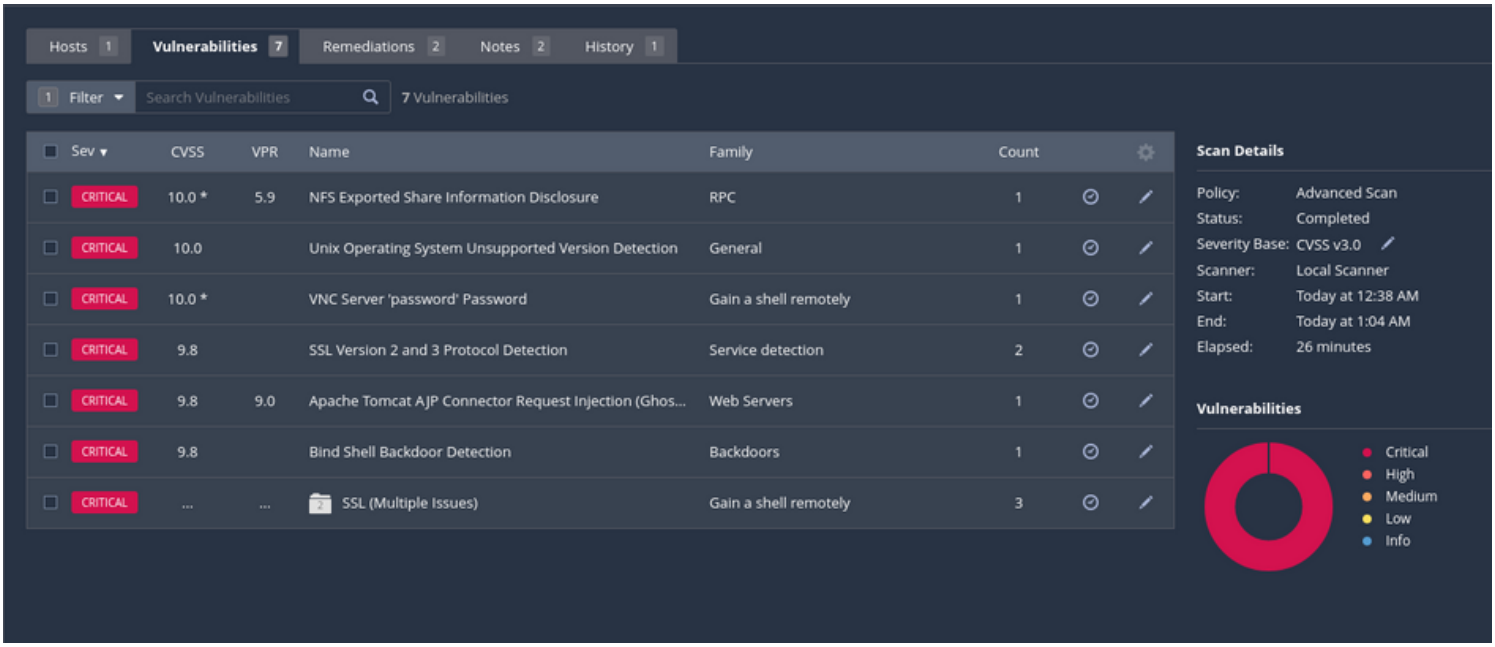
Report della scansione con Nessus

Traccia: Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo)
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.
Gli obiettivi dell'esercizio sono:
Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni
Familiarizzare con alcune delle vulnerabilità note che troverete spesso.

Target:

Metasploitable (IP 192.168.50.101)

Approfondimento sulle vulnerabilità critiche riscontrate:



- **NFS Exported Share Information Disclosure (CVSS 10.0)**
  - **Descrizione**: questa vulnerabilità indica che le informazioni sensibili possono essere divulgate attraverso condivisioni NFS esportate in modo improprio.
  - Un attaccante potrebbe sfruttare questa vulnerabilità per accedere a dati riservati.
  - Si consiglia di rivedere le condivisioni NFS e applicare le migliori pratiche di sicurezza per limitare l'accesso solo agli utenti autorizzati.

- **Unix Operating System Unsupported Version Detection (CVSS 10.0)**
  - **Descrizione**: la versione del sistema operativo Unix in uso non è più supportata e potrebbe contenere vulnerabilità non corrette.
  - La mancanza di supporto significa che non ci sono più aggiornamenti di sicurezza per le vulnerabilità conosciute, aumentando il rischio di compromissione del sistema.
  - Aggiornare a una versione supportata del sistema operativo che riceve regolarmente patch di sicurezza.
- **VNC Server 'password' Password (CVSS 10.0)**
  - **Descrizione**: è stata trovata una configurazione debole nel server VNC, dove la password è impostata sul valore predefinito o su una parola facilmente indovinabile.
  - Gli attaccanti possono facilmente accedere al server VNC e assumere il controllo del sistema.
  - Cambiare immediatamente la password con una forte e unica e considerare l'uso di autenticazione a più fattori.
- **SSL Version 2 and 3 Protocol Detection (CVSS 9.8)**
  - **Descrizione**: sono state rilevate versioni obsolete e insicure del protocollo SSL, che sono vulnerabili a vari attacchi crittografici.
  - Gli attaccanti possono intercettare o manipolare dati sensibili durante la trasmissione.
  - Disabilitare SSLv2 e SSLv3 a favore di TLS 1.2 o superiore.
- **Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVSS 9.8)**
  - **Descrizione**: la vulnerabilità 'Ghostcat' permette agli attaccanti di leggere o includere file sul server Tomcat attraverso il connettore AJP.
  - Compromissione dell'integrità dei dati e possibile esecuzione di codice remoto.
  - Aggiornare Apache Tomcat all'ultima versione e disabilitare il connettore AJP se non necessario.
- **Bind Shell Backdoor Detection (CVSS 9.8)**
  - **Descrizione**: è stata rilevata una backdoor sul sistema, che permette un accesso remoto non autorizzato.
  - Gli attaccanti possono ottenere un accesso completo al sistema compromesso.
  - Rimuovere la backdoor e condurre un'indagine forense per determinare l'entità della compromissione.
- **SSL (Multiple Issues) (CVSS 9.8)**
  - **Descrizione**: ci sono molteplici problemi relativi a SSL, che possono includere configurazioni deboli, cifrature obsolete o certificati scaduti.
  - Potenziali attacchi man-in-the-middle o decriptazione dei dati trasferiti.
  - Revisionare la configurazione SSL/TLS, disabilitare cifrature deboli e rinnovare i certificati scaduti.