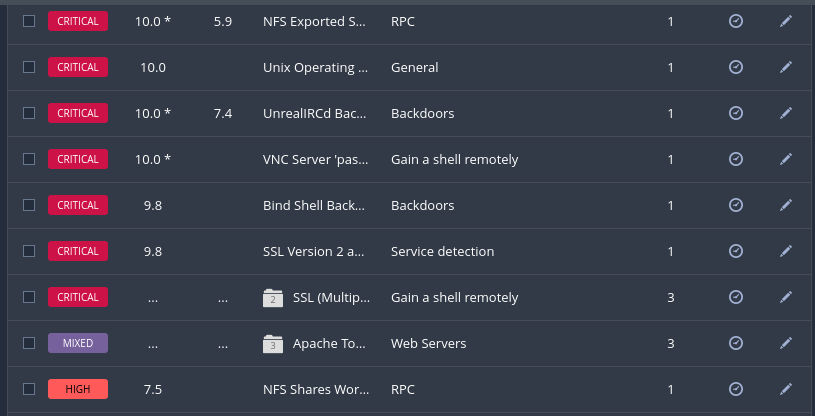
**Traccia:**

Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

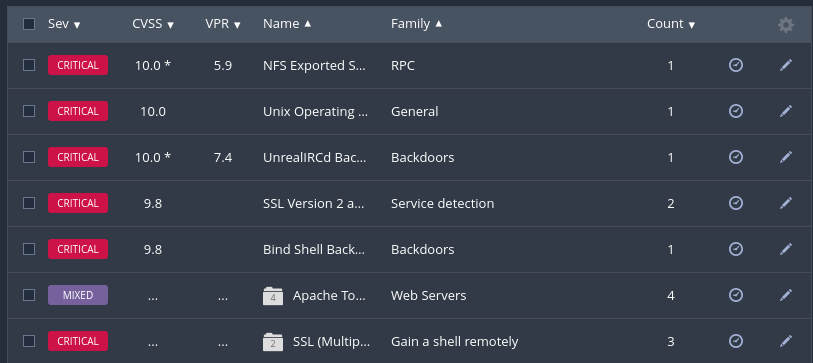
Riprendendo la scansione fatta precedentemente sull’IP di Metaspoitable, scegliamo una criticità e cerchiamo di risolverla. In questo caso ho scelto di risolvere la numero quattro in lista, in cui si avverte che il server VNC ha una password debole:



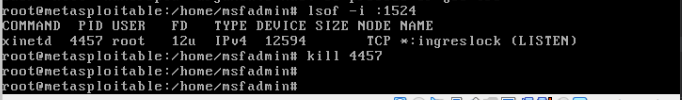
Un modo interessante per aggirare il problema, senza cambiare la password necessariamente, è crittografare la comunicazione tra il client e il server VNC. Per fare ciò abbiamo utilizzato, sul terminale di Metaspoitable, il comando **/etc/vnc/vncserver.conf** per agire sulla configurazione della VNC, e il parametro **SecurityTypes=TLSVnc** (TLS è un protocollo di crittografia che protegge la confidenzialità e l'integrità dei dati durante la trasmissione su una rete), un'opzione di configurazione utilizzata nei server VNC per specificare il tipo di sicurezza che verrà utilizzato durante una connessione VNC. Salvando quest’opzione e riavviando la scansione, possiamo constatare che non risulta più una vulnerabilità di livello critico:



Prendiamone un'altra, sempre tra le criticità, ad esempio la quinta in lista. In questo caso il sistema ci avverte che una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi:



Una soluzione, forse poco ortodossa, ma efficace per contrastare in maniera immediata la cosa, potrebbe essere la chiusura della stessa. Agendo sempre da terminale in root di Metaspoitable, utilizziamo il protocollo **lsof -i :1524** e il comando **kill 4457** per chiudere la backdoor.



Lanciamo un'altra scansione per verificare che la chiusura sia stata effettuata e un'altra criticità eliminata:

