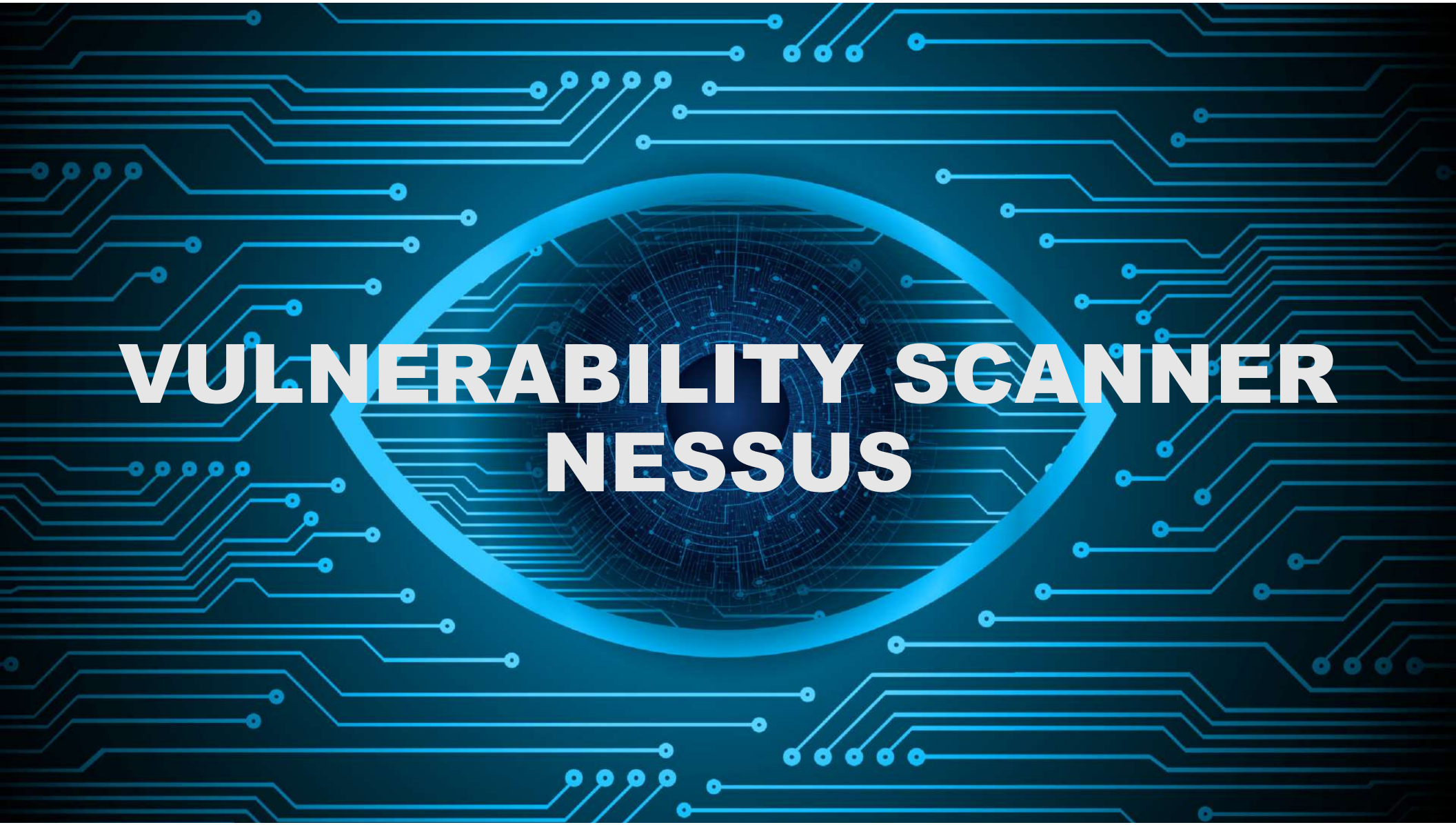
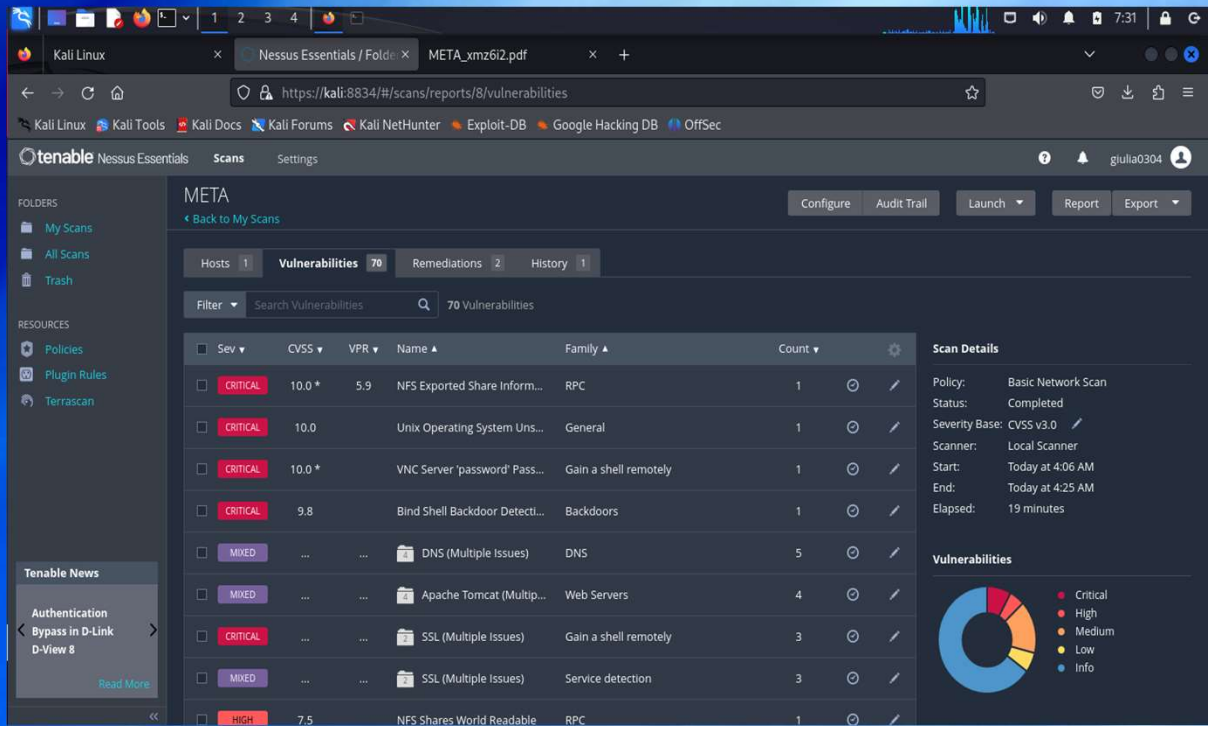

VULNERABILITY SCANNER
NESSUS

SCANSIONE INIZIALE

Nella fase iniziale ho eseguito la scansione sulla macchina Metasploitable, sono venute fuori diverse vulnerabilità (come si può vedere in figura), quelle che andrò a risolvere sono le seguenti:

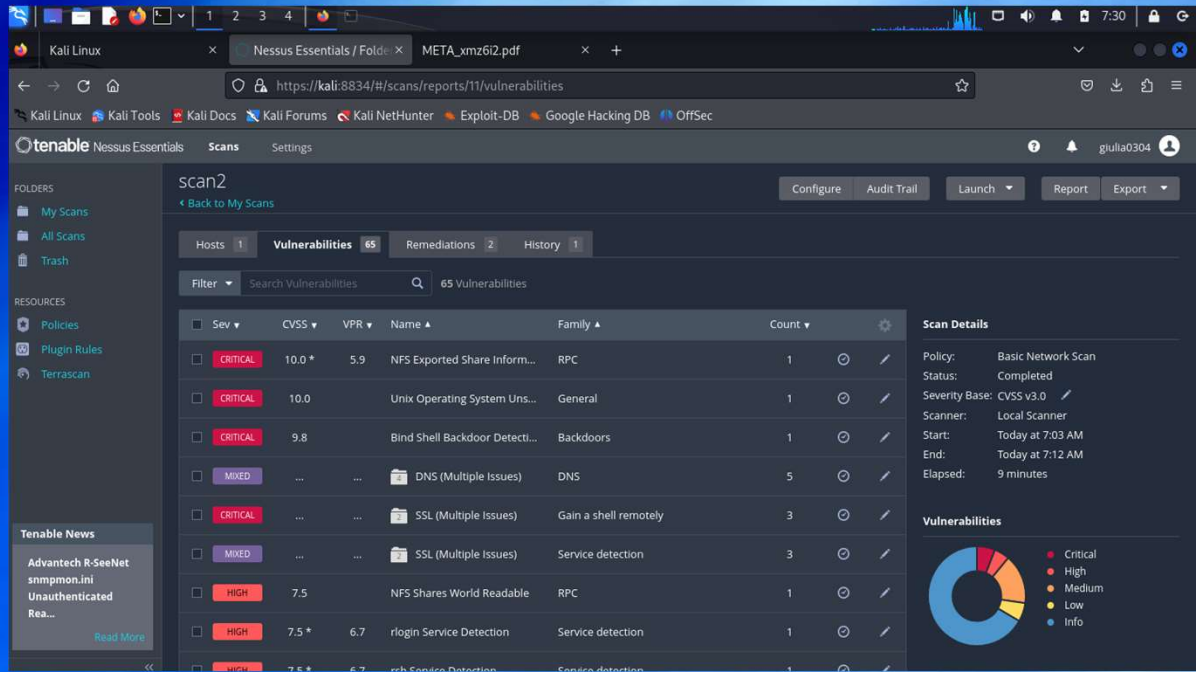
- NFS Exported Share Information Disclosure
- VNC Server 'password' Password
- Bind Shell Backdoor Detection



NFS Exported Share Information Disclosure

NFS è un protocollo per la condivisione di file e directory e, se non è configurato in maniera sicura, potrebbe consentire a dei malintenzionati di accedere a risorse non autorizzate. Per aggirare questo problema ho modificato il file /etc/exports e ho modificato l'ultima riga perché in questa c'era il simbolo «/» che sta a significare che si può montare tutto. Mettendolo a commento con il simbolo «#» ho risolto questa vulnerabilità. Infatti nella figura a destra notiamo che questo tipo di vulnerabilità non è presente in «CRITICAL».

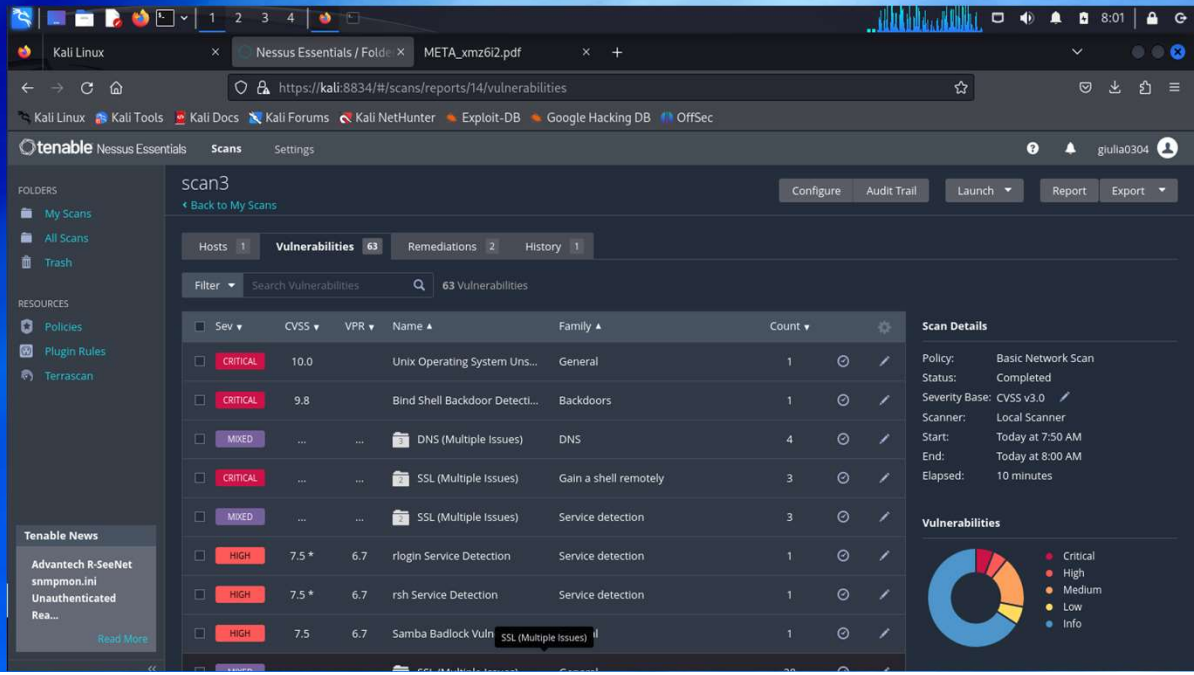
SCAN 3



VNC Server 'password' Password

Questa vulnerabilità riguarda il VNC server in quanto per accedervi la password è «password», questo non va bene perché è molto debole e un possibile attaccante potrebbe accedere senza problemi. Per risolvere ho usato il comando «vncpasswd» sulla macchina Metasploitable e ho inserito una password più forte.
Come si può vedere nell'immagine a destra, rifacendo un'altra scansione, questa vulnerabilità non compare più come «CRITICAL».

SCAN 2

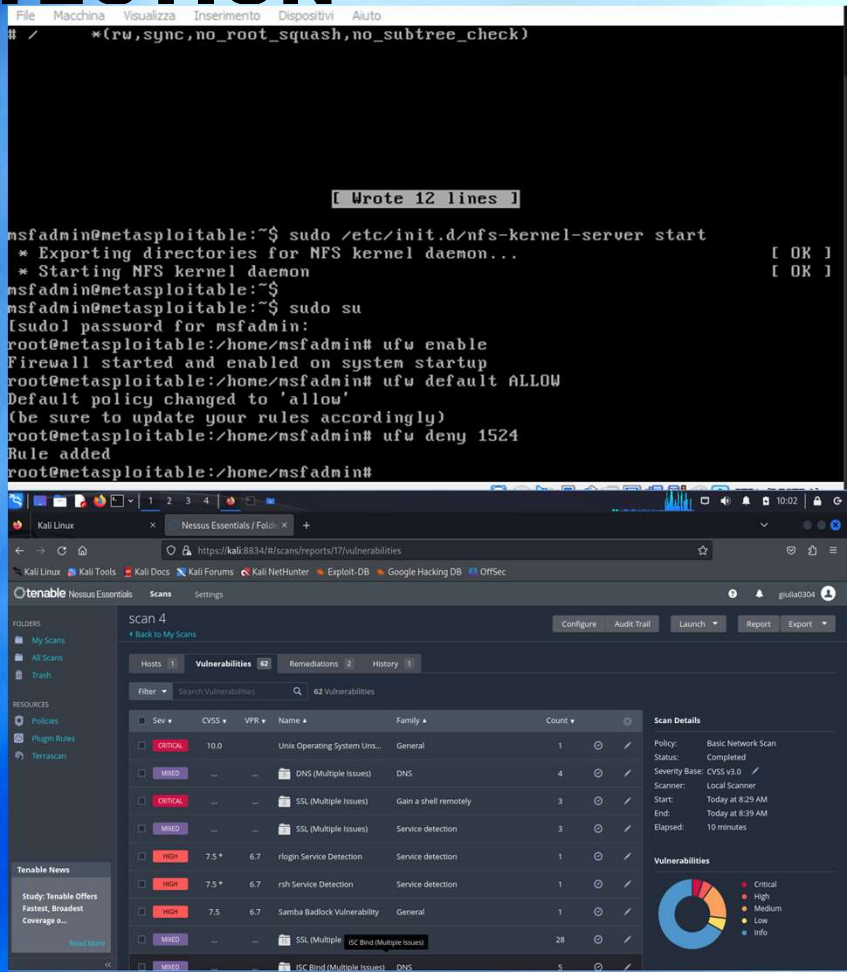


BIND SHELL BACKDOOR DETECTION

Questo tipo di vulnerabilità ci dice che una shell è in ascolto su una porta remota senza autenticazione. Un malintenzionato potrebbe sfruttare questa cosa connettendosi alla porta e prendere il controllo.
Per risolvere questa vulnerabilità ho usato dei comandi:

- «ufw enable» per attivare il firewall
- «ufw default ALLOW» che permette tutte le connessioni di base.
- «ufw deny 1524» per chiudere la seguente porta che è responsabile della backdoor.

Così facendo non risulterà più come vulnerabilità critica.



REPORT NESSUS

I PDF DEI REPORT SONO INVIATI SEPARATAMENTE

- SCANSIONEINIZIALE.PDF
- SCANSIONEFINALE.PDF