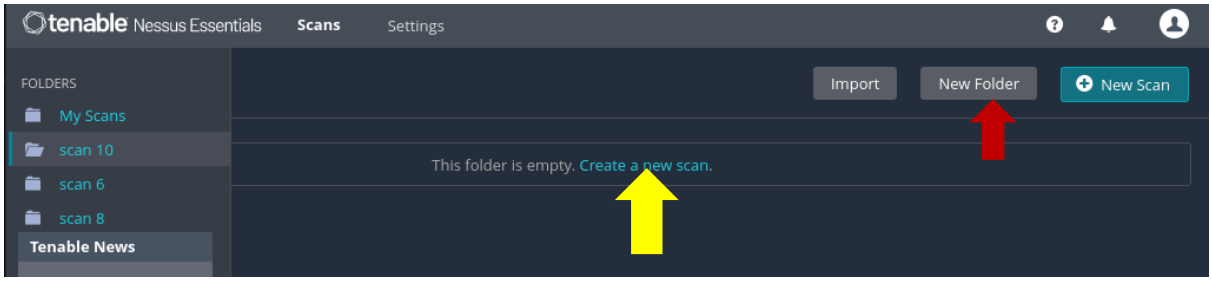
PROGETTO S5/L5

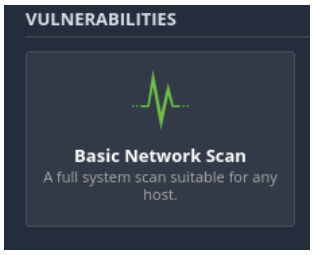
Obiettivo: effettuare la scanzione della macchina Metasploitable usando Nessus(vulnerability scanner),un software che permette di rilevare le vulnerabilità in una rete facendo la sua scanzione.Dopo di che dobbiamo provare ad implementare delle azioni di remedio,da un minimo di 2 fino a un massimo di 4 vulnerabilità critiche/high ottenuto dopo la scazione.

1) Scanzione della Macchina virtuale Metasploitable 2 .

Per la scanzione di Metasploitable2,abbiamo aperto il software Nessus,siamo andati sulla cartella “New Folder” dove abbiamo creato una nuova cartella, come indicato con la freccia rossa qui.



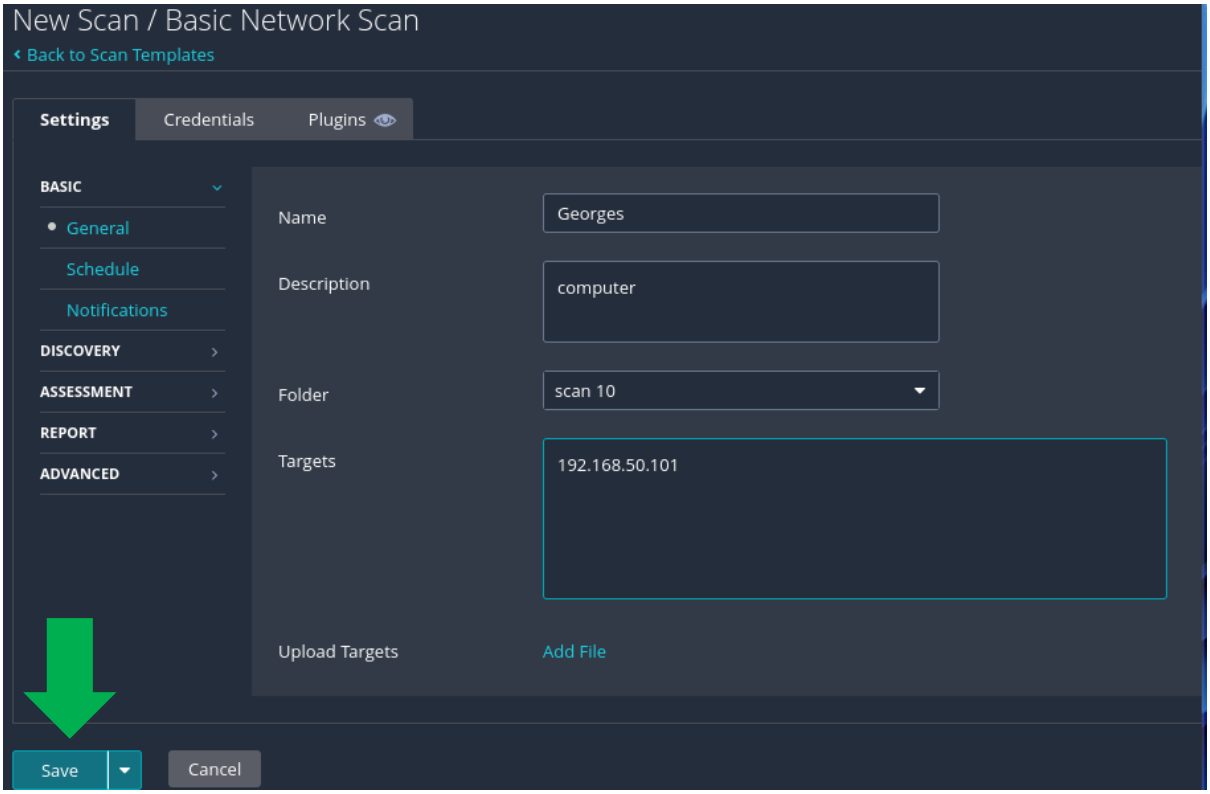
Dopo la creazione della cartella,abbiamo clicato su “create new scan”come indicato sopra con la fraccia gialla. è uscito una nuova schermata e abbiamo clicato su “Basic Network Scan”.



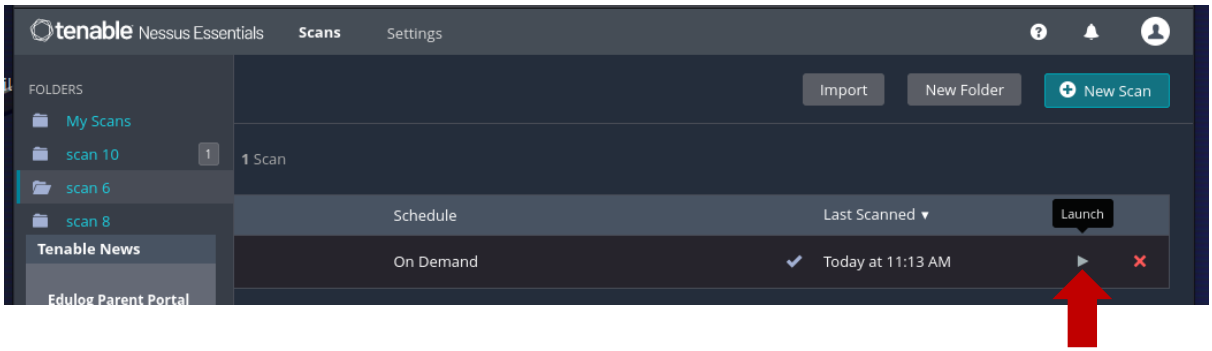
Clicando su Basic Network Scan abbiamo ottenuto la schermata qua sotto,e abbiamo inserito le informazioni richiesti come si può vedere su l’imagine sotto. Dopo di che abbiamo salvato tutto clicando su save(

Indicato con una freccia verde).

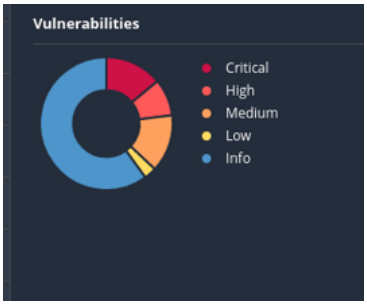
PROGETTO S5/L5



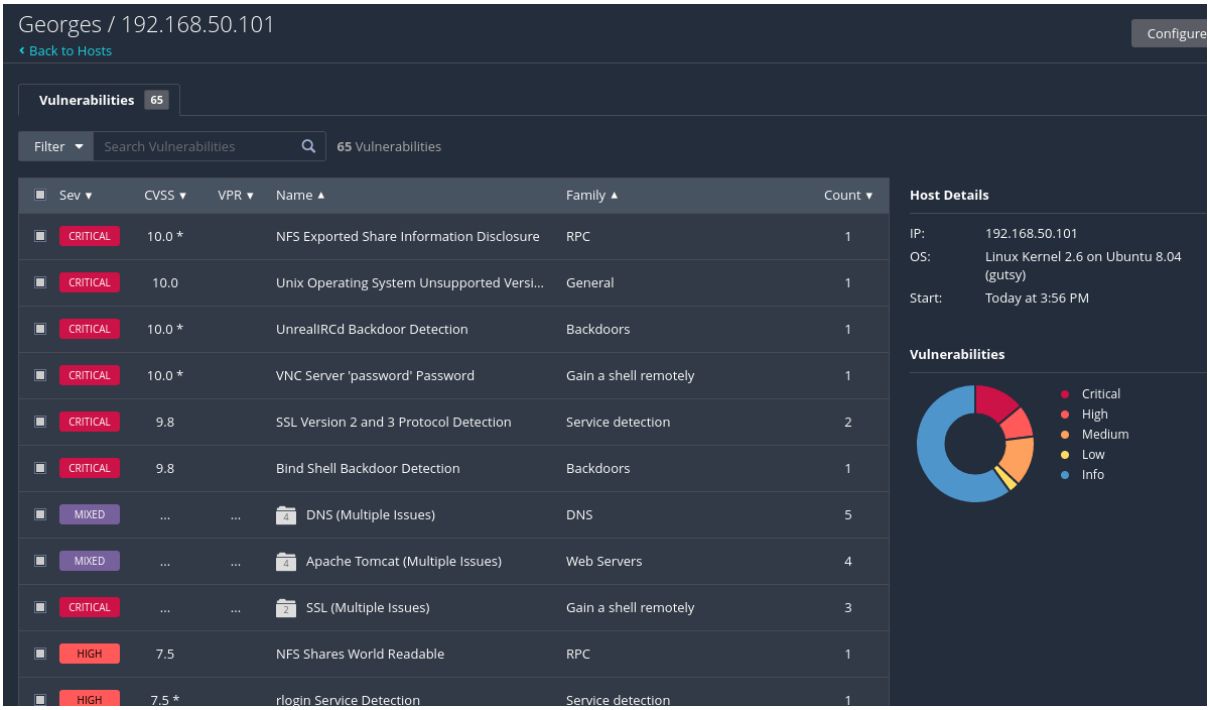
Dopo di che abbiamo iniziato la scanzione clicando su Launch,come indica la freccia rossa su l'imagine che segue.



Dopo la scazione abbiamo ottenuto un report con i diversi livelli di vulnerabilità andando dal più critico al più basso.come possiamo vedere sulle imagini seguenti.

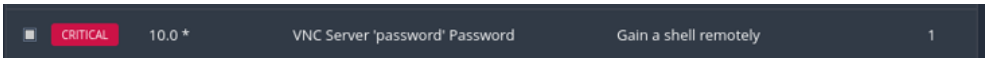


PROGETTO S5/L5



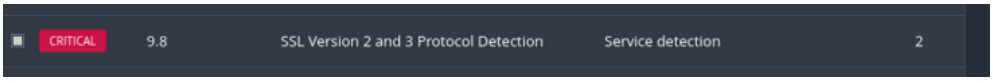
2)Implementazione delle azione di remedio

A) La prima azione di remedio che abbiamo scelto è quella di VNC Server.



VNC(Virtual Network Computing) Server: è un software che consente la condivisione del desktop di un computer o server attraverso una rete. In questo caso Nessus ci fa capire che la password del sistema è molto debole, quindi come approccio di risoluzione di questa vulnerabilità abbiamo cambiato la password usando la comanda "passwd" inserendo vecchia password e due volte new password.e dopo verificzione era ben cambiato la password.

B) la seconda vulnerabilità che vogliamo risolvere è la seguente:



PROGETTO S5/L5

SSL version 2 and 3 protocol Detection: è una funzione o un test di sicurezza che verifica la presenza o l'abilitazione dei protocolli SSL version 2 e version 3 su un server.

Per risolvere questo problema abbiamo disabilitato questa funzione.L'approccio della disabilitazione è dovuto al fatto che: SSL è stato uno dei primi protocolli utilizzati per garantire la sicurezza delle comunicazioni su internet,ma a causa di vulnerabilità e debolezze di sicurezza scoperte nel tempo, sia nella versione 2 che nella versione 3, sono stati considerati obsoleti e insicuri.

Quindi per la disabilitazione, abbiamo aperto il file di configurazione di Appache con la comanda: "sudo nano /etc/apache2/apache2.conf " e abbiamo aggiunto le seguente linee alla fine del file: "SSLProtocol All -SSLv2 -SSLv3" e per finire abbiamo risettato tutto con la comanda: sudo apache2 restart.

C)Configurazione del firewal

Come ultimo approccio abbiamo configurato il firewall per filtrare il traffico di rete, provando di risolvere in questo caso e in un colpo più di una vulnerabilità. Per fare questo abbiamo usato la comanda:

Sudo iptables -P INPUT DROP per bloccare tutto il traffico in ingresso.

Poi abbiamo fatto l'update con la comanda: sudo apt-get update.

E in seguito upgrade con la comanda: sudo apt-get upgrade .

E per finire abbiamo configurato l'auditing del sistema installando auditd con la comanda: sudo apt-get install auditd Dopo aver fatto tutto questo abbiamo scanzionato di nuovo la rete e abbiamo ottenuto

PROGETTO S5/L5

questo risultato: