S5L5

Gli obiettivi dell'esercizio di oggi riguarda nello specifico la risoluzione di alcune criticità scoperte tramite Nessus della macchina virtuale Metasploitable.

Nello specifico ho deciso di risolvere due criticità riscontrate sulla mia macchina virtuale:

- VNC server password password

- NFS Exported share information disclosure

Prima criticità:

Il problema della prima criticità riguarda la debolezza delle password del DNC da cui si può accedere alla shell di Metasploitable come mostrato nelle seguenti immagini.

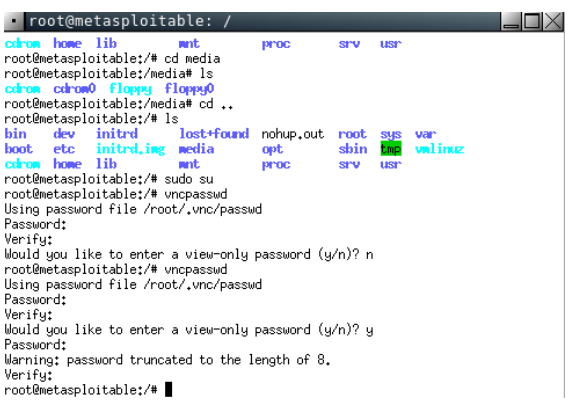
La risoluzione di questa criticità consiste nel cambiare le password della macchina di Metasploitable da remoto secondo i seguenti parametri

-Password di almeno otto caratteri

-Presenza di almeno un numero

-Presenza di almeno un carattere inusuale

-Presenza di almeno una lettera maiuscola



Seconda criticità:

La seconda criticità riguarda invece l'accesso o la modifica da remoto ad informazioni riguardo il Network File System, che riguardano anche le password associate ad un nome utente, oppure può consentire ad un attaccante di accedere alla shell di un sistema. Questo si può confermare tramite i seguenti passaggi:

1) Inizio con il creare una sottodirectory che chiamerò "metasploitable_share" all'interno della directory già esistente "/mnt"

2) Utilizzo il comando mount per accedere da remoto al NFS

3) Per avere conferma di ciò ho provato a copiare un file di testo nella cartella ".ssh".

4) Poi genero una chiave SSH sulla macchina usata per il test.

5) Dopo ho creato un file "authorized_keys" nella macchina attaccante e ho eliminato il contenuto del file "id_rsa.pub".

6) Infine, subito dopo aver copiato il file nella directory ".ssh", mi sono connesso alla macchina di Metasploitable con la chiave SSh creata in precedenza nel punto 4)

Per risolvere questa criticità basta:

- Restringere gli indirizzi IP che possono accedere alle directory NFS.
- Imporre solo il permesso di lettura dei file.