S5L5
PROGETTO

ALESSANDRO MARASCA

EPICODE - CS0124

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.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti. Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

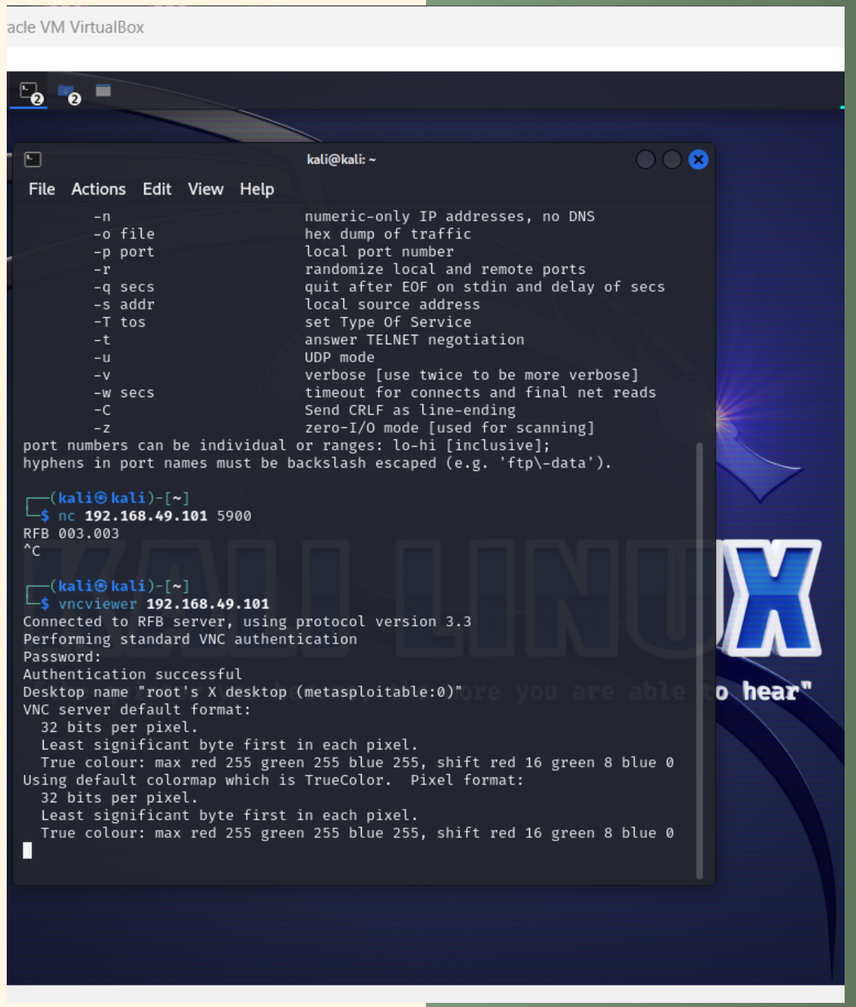
VNC SERVER ‘password’ PASSWORD

PROBLEMA

COME SUGGERITO DALLO SCREEN E DALLA TRACCIA, OSSERVIAMO COME SIA POSSIBILE ACCEDERE AL VNC DA KALI LINUX, QUINDI DOBBIAMO ANDARE A MODIFICARE LA PASSWORD

SOLUZIONE

MODIFICHIAMO LA PSW PER RISOLVERE LA CRITICITÀ DIRETTAMENTE DALLA SHELL DI METASPLOITABLE 2



ESITO

STABILITA UNA CONNESSIONE CON METASPLOITABLE 2 (NC IP + PORTA 5900) E INSERITA LA PASSWORD “PASSWORD” ACCEDIAMO ALLA SHELL DI METASPLOITABLE 2.

A QUESTO PUNTO ACCEDIAMO COME **ROOT** SU META, ENTRIAMO IN VNCPASSWD E MODIFICHIAMO LA PASSWORD (È CONSIGLIATA UNA PWD DI ALMENO 8 CARATTERI COMPOSTI DA ALMENO UNA LETTERA MAIUSCOLA, UN NUMERO E UN CARATTERE SPECIALE.

COME POSSIAMO OSSERVARE NON È PIÙ POSSIBILE ACCEDERE.

CRITICITÀ RISOLTA

NFS EXPORTED SHARED INFORMATION DISCLOSURE

NFS configurato erroneamente può fornire a un attaccante accesso non autorizzato a dati sensibili o ottenere la shell sul proprio sistema

Come risolvere?

MITIGATION

01 Imposta le restrizioni appropriate su tutte le condivisioni NFS, ad esempio limitando gli indirizzi IP che possono montare le condivisioni esposte

02 Imposta le restrizioni appropriate su tutte le condivisioni NFS, ad esempio limitando gli indirizzi IP che possono montare le condivisioni esposte.

03 Non esportare l’ home directory .

04 **Utilizza l'opzione "root_squash" nelle impostazioni NFS per impedire agli utenti root remoti di accedere alla condivisione con privilegi elevati.**

GRAZIE

PROGETTO
S5L5

ALESSANDRO MARASCA
EPICODE - CS0124