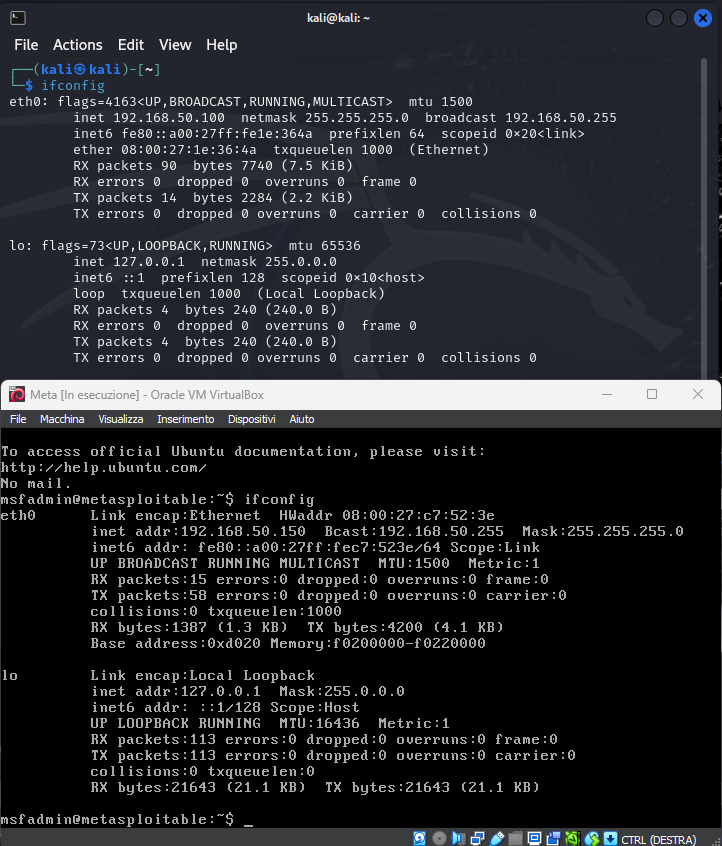
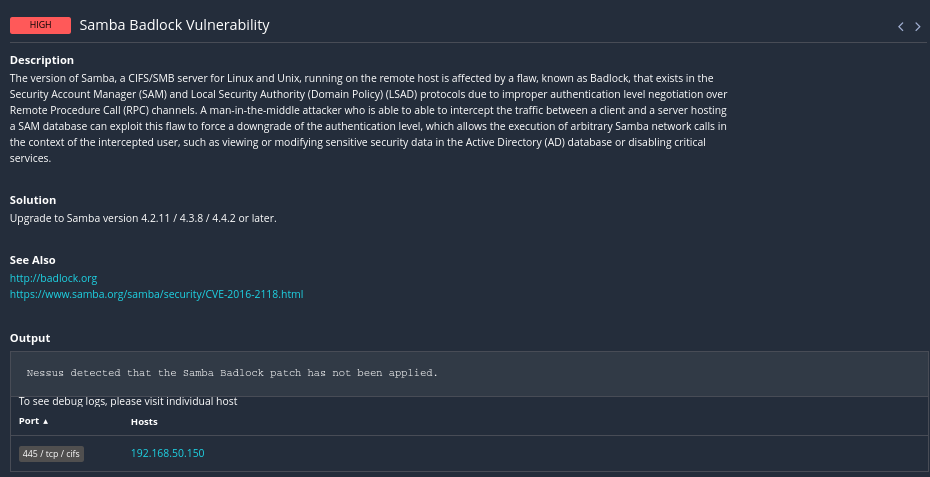
Build Week 2 Traccia giorno 4

Innanzitutto impostare le nostre macchine virtuali nel seguente modo:

* IP Kali Linux: 192.168.50.100 IP
* Metasploitable: 192.168.50.150



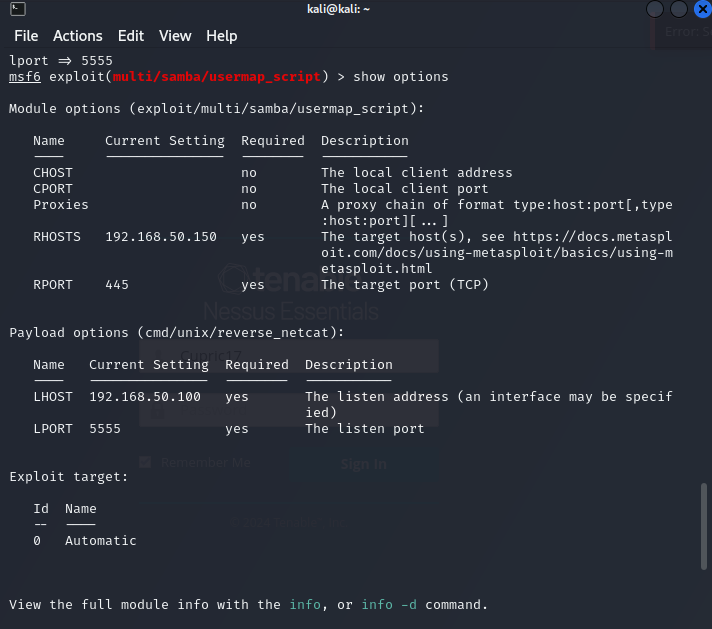
Successivamente tramite una scansione con Nessus troviamo la vulnerabilità di nostro interesse

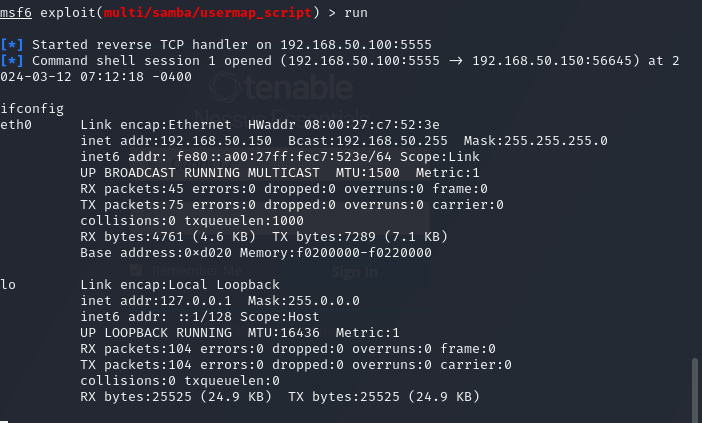
Come possiamo vedere Il difetto noto come Badlock è una vulnerabilità presente nella versione di Samba, un server CIFS/SMB per sistemi Linux e Unix. Questo difetto è localizzato nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD), che sono componenti critici per la gestione dell'autenticazione e della sicurezza in un ambiente Windows, come Active Directory (AD).

l problema deriva da una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call), che consente a un utente malintenzionato che si trova in mezzo alla comunicazione tra un client e il server Samba di eseguire un attacco di "man-in-the-middle".

Sfruttando questa falla, un attaccante può forzare un downgrade del livello di autenticazione durante la comunicazione tra il client e il server. Ciò significa che l'attaccante può manipolare il flusso di traffico per far sì che il server accetti un livello di autenticazione meno sicuro di quello richiesto, aprendo la porta a varie forme di attacco.

Con MSFConsole utilizzando l’exploit al path exploit/multi/samba/usermap\_script con le seguenti configurazioni:



Riusciamo a sfruttare la vulnerabilità, ed eseguendo il comando *ifconfig* verifichiamo l’indirizzo di rete della macchina vittima.