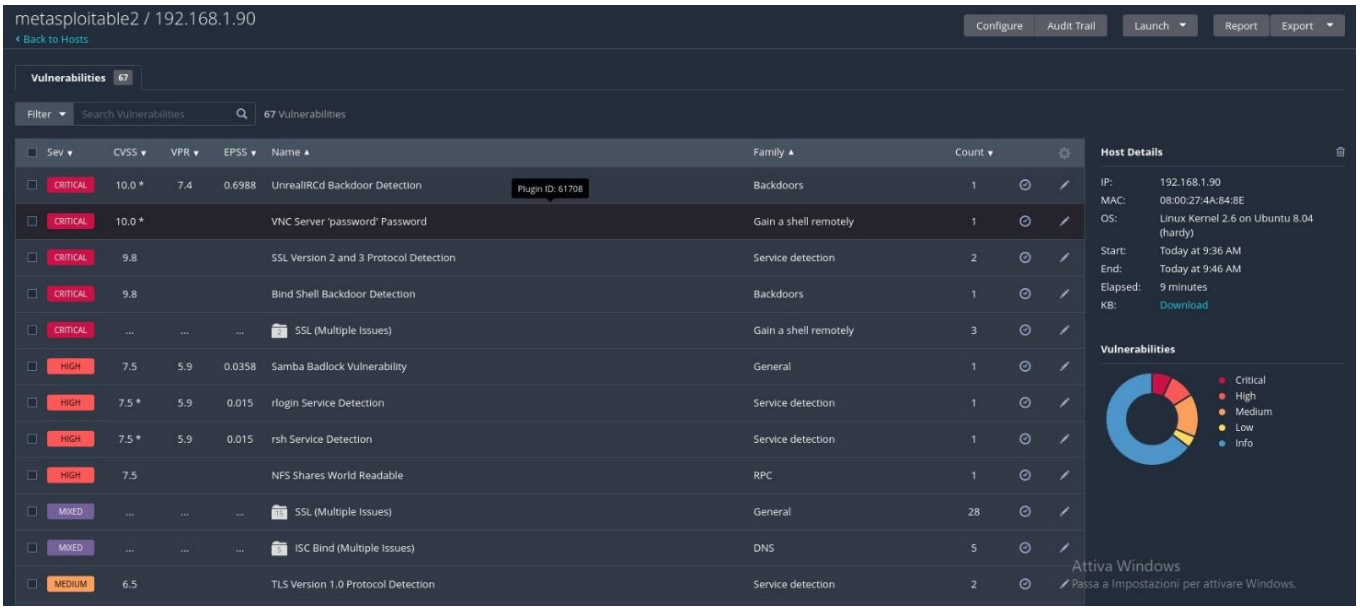
Esercizio S5 L3 del 30/10/24 ***Daniele Paolone***

Vulnerability scanner: Nessus

Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Tramite l' utilizzo del vulnerability scanner Nessus, viene avviata una scansione su applicazioni, dispositivi e reti per individuare vulnerabilità sull' obiettivo prestabilito.

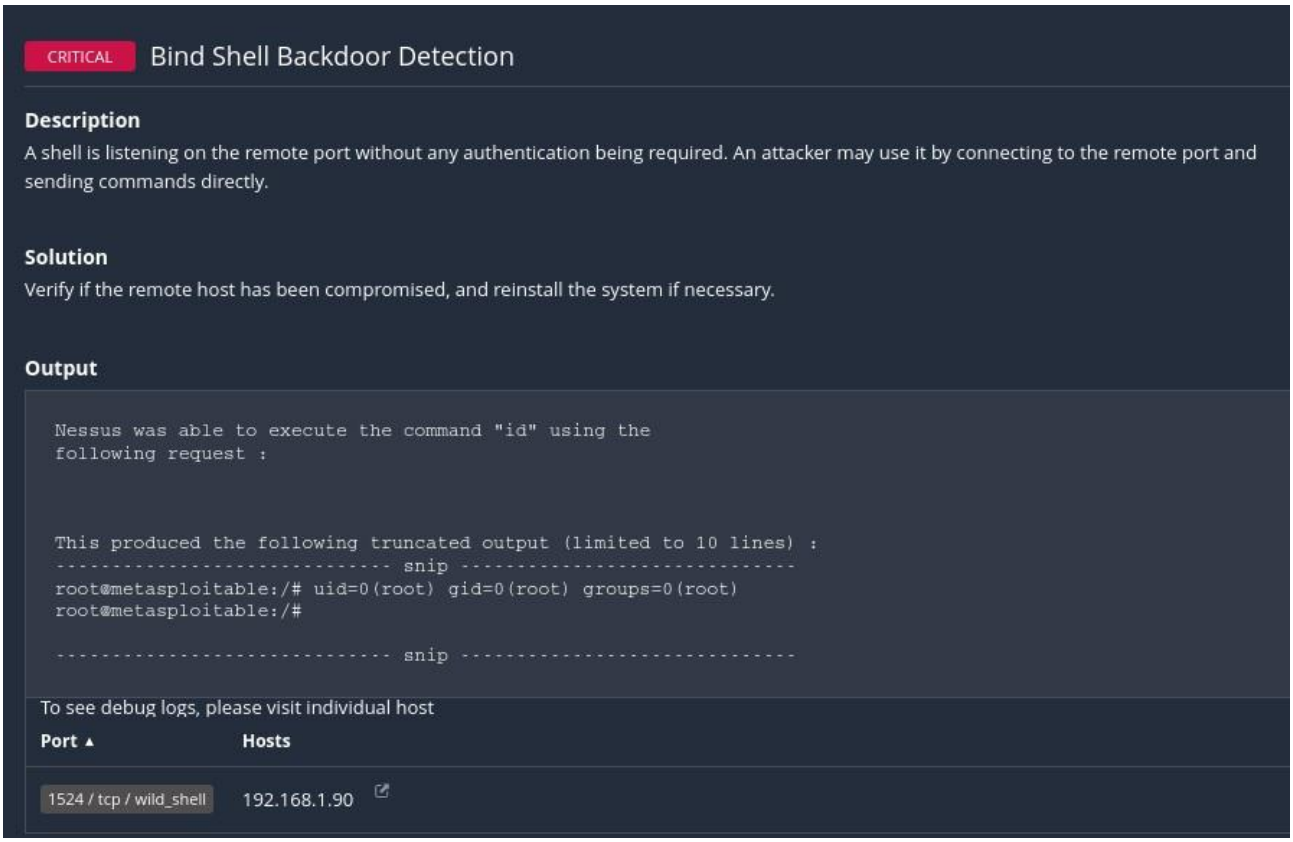
In questo caso, si procederà con l' avvio di una scansione con il plug in "*basic network scan*", fornendo l' indirizzo ip della macchina metasploitable. Al termine della scansione, nell' immagine sottostante sono rappresentate le vulnerabilità rilevate e ordinate in base alla criticità, dalla più alta alla più bassa.



Sulla base di questo elenco, ne verranno analizzate alcune.

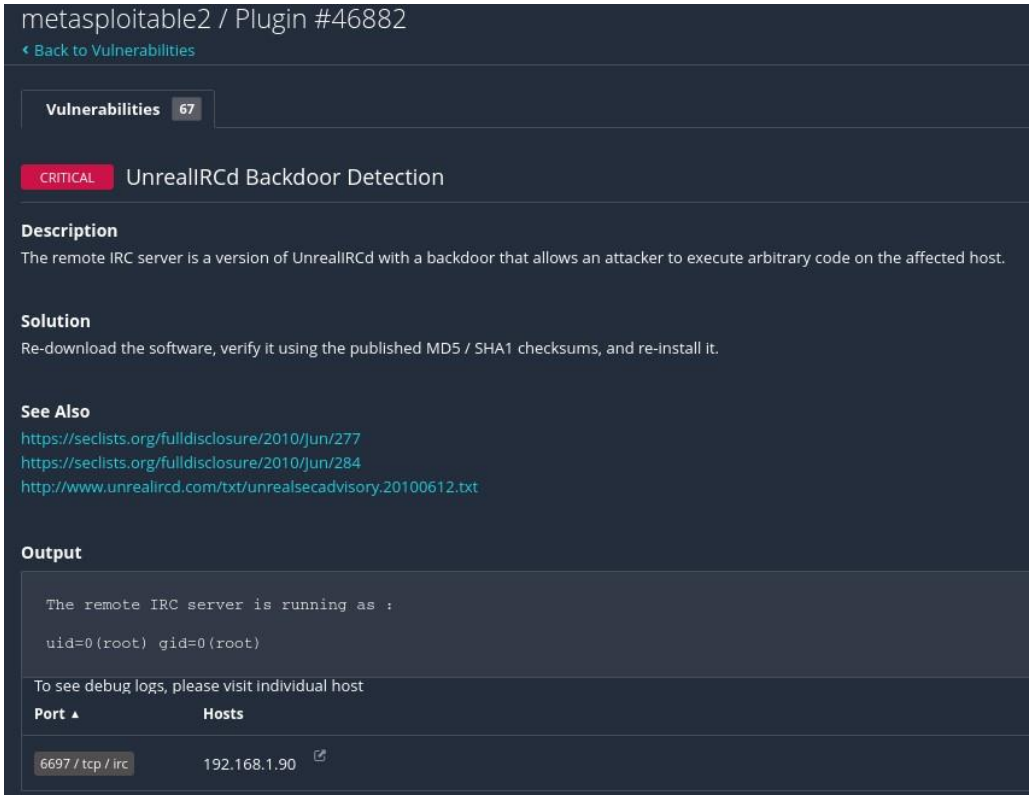
1° Vulnerabilità

La prima da analizzare è una backdoor. Essa consente un accesso non autorizzato all' attaccante su un dispositivo, all' insaputa dell' utente. Questo permette il controllo del dipositivo da remoto. E' stata trovata sulla porta 1524.
La soluzione proposta da Nessus, è di reinstallare il sistema.



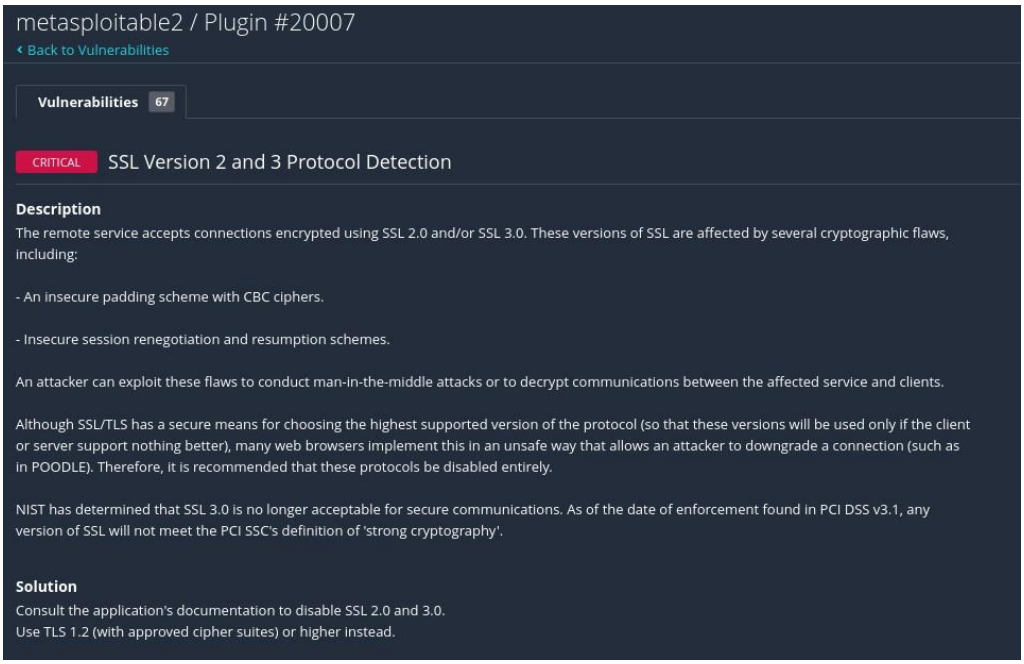
2° Vulnerabilità

La seconda è sempre una backdoor ed è stata trovata sulla porta 6697. Questa backdoor permette all' attacante di eseguire del codice sulla macchina host.
La soluzione proposta da Nessus, è di scaricare di nuovo il software e, prima di installarlo, fare un controllo dell' integrità del software attraverso algoritmi di hashing (MD5/SHA1).



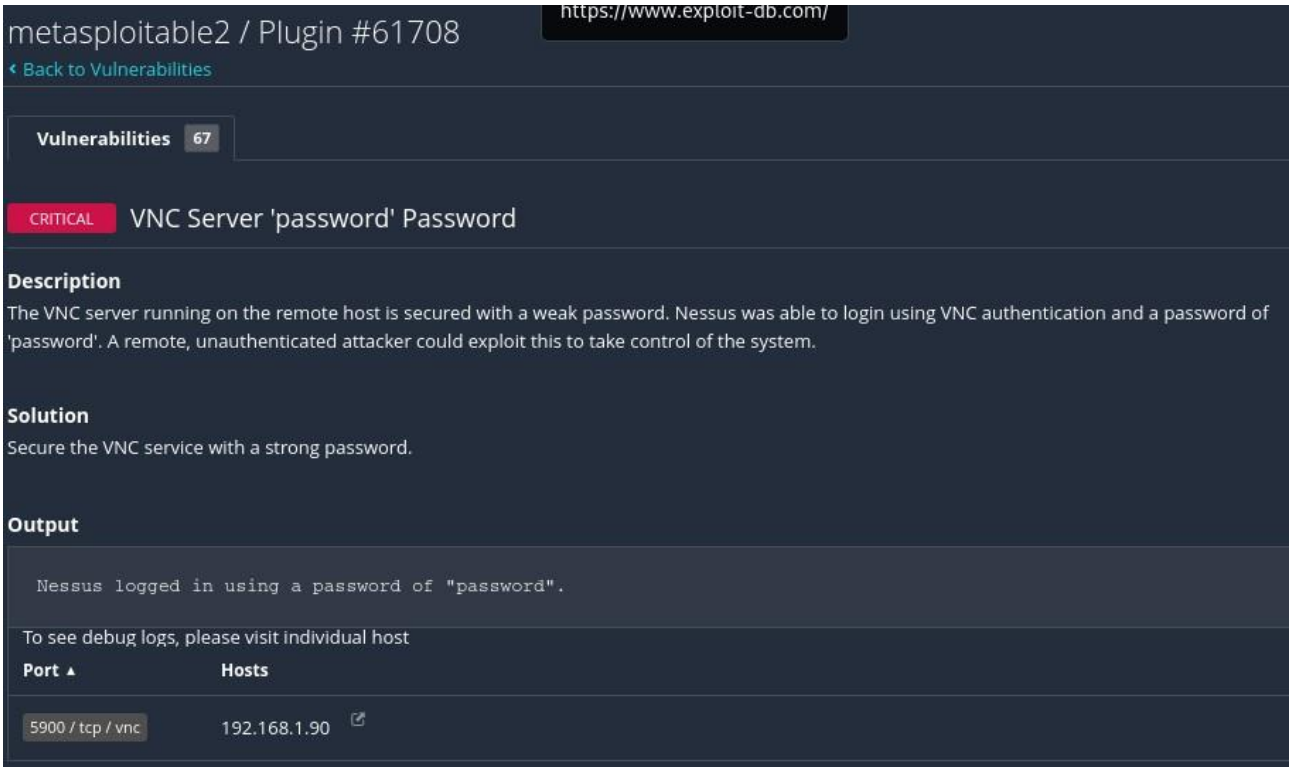
3° Vulnerabilità

La terza vulnerabilità riguarda una vecchia versione (2.0/3.0) del protocollo di cifratura SSL. La versione utilizzata dalla macchina è affetta da importanti difetti di crittografia che consente di eseguire un attacco *man-in-the-middle*. E' stata trovata sulla porta 25.
La soluzione proposta da Nessus, è di disabilitare queste versioni di SSL e di passare all' utilizzo del protocollo di cifratura TLS.



4° Vulnerabilità

La quarta vulnerabilità riguarda l' uso di una password troppo debole da parte dell' utente. Un attaccante può accedere al dispositivo, in modo anche autenticato, attraverso il server VNC, exploitando la debolezza della password. E' stata trovata sulla porta 5900. La soluzione proposta da Nessus, è l' uso di una password forte.



5° Vulnerabilità

La quinta vulnerabilità riguarda una versione obsoleta del protocollo SAMBA. Questa versione è affetta da un errore che permette all' attaccante, attravero il *MITM*, di passare ad un livello di autenticazione più debole, in modo da poter ottenere permessi per vedere o modificare dati sensibili. E' stata trovata sulla porta 445.
La soluzione proposta da Nessus, è l' utilizzo di versioni più recenti del protocollo SAMBA.