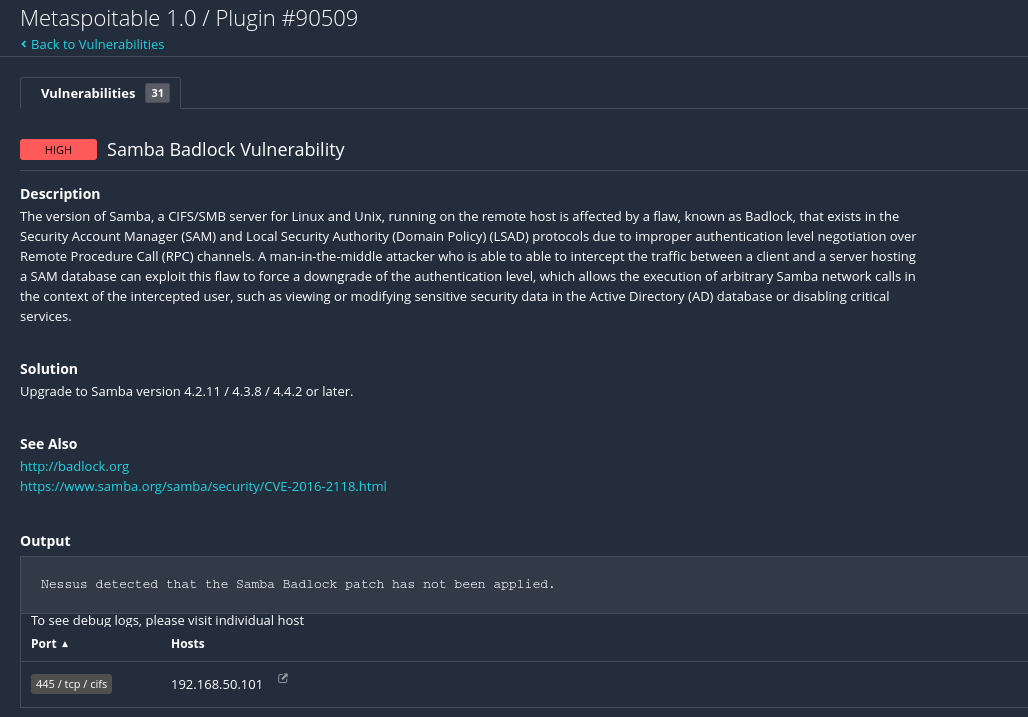
**Piccolo report scansioni Nessus**

Ho eseguito due scansioni differenti, in entrambe scannerizzando tutte le porte richieste, l’unica differenza tra entrambi è che nella prima ho lasciato le impostazioni di Default mentre nella seconda ho effettuato la scansione solo tramite port scanner SYN.

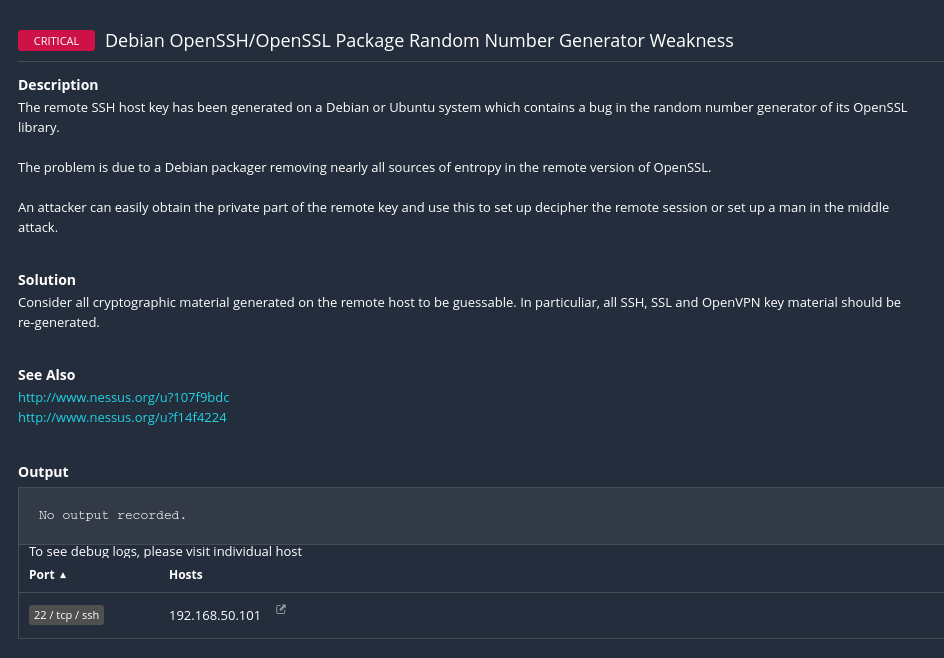
Nella prima ho trovato più criticità della seconda, ma mi sono soffermata ad analizzare e a ricercare principalmente una criticità comune alle due che riguarda il protocollo Samba (nella porta 445).



La **Samba Badlock Vulnerability** è una grave vulnerabilità di sicurezza scoperta nel 2016 nel software **Samba**, che è utilizzato per condividere file e stampanti tra sistemi Linux/Unix e Windows. La vulnerabilità era legata a una gestione errata della comunicazione tra client e server Samba, che poteva permettere a un attaccante remoto di eseguire codice arbitrario, ottenere privilegi elevati o compromettere il sistema. La vulnerabilità è stata denominata "Badlock" e ha avuto un ampio impatto su molte versioni di Samba. È stata risolta con un aggiornamento che ha corretto la gestione delle connessioni e delle autenticazioni.

La semplice soluzione per risolverla sarebbe l’aggiornamento di versione.

Un seconda vulnerabilità che ho analizzato ha la criticità più alta per entrambi ed è il Debian OpenSSH/OpenSSL Package Random Number Generator Weakness(nella porta 22).



La **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness** è una vulnerabilità scoperta nel 2008 in Debian. È stata causata da un difetto nel generatore di numeri casuali utilizzato in **OpenSSL**, una libreria crittografica presente nei pacchetti Debian che comprende anche **OpenSSH**. A causa di un errore nel codice di Debian, il generatore di numeri casuali produceva numeri prevedibili, riducendo la sicurezza delle chiavi crittografiche generate, come quelle usate per le connessioni SSH e la crittografia TLS. Questo avrebbe potuto permettere a un attaccante di decrittare comunicazioni sicure. La vulnerabilità è stata corretta tramite un aggiornamento dei pacchetti vulnerabili.  
La soluzione sarebbe rigenerare il materiale crittografato corrotto per evitare che venga letto facilmente.