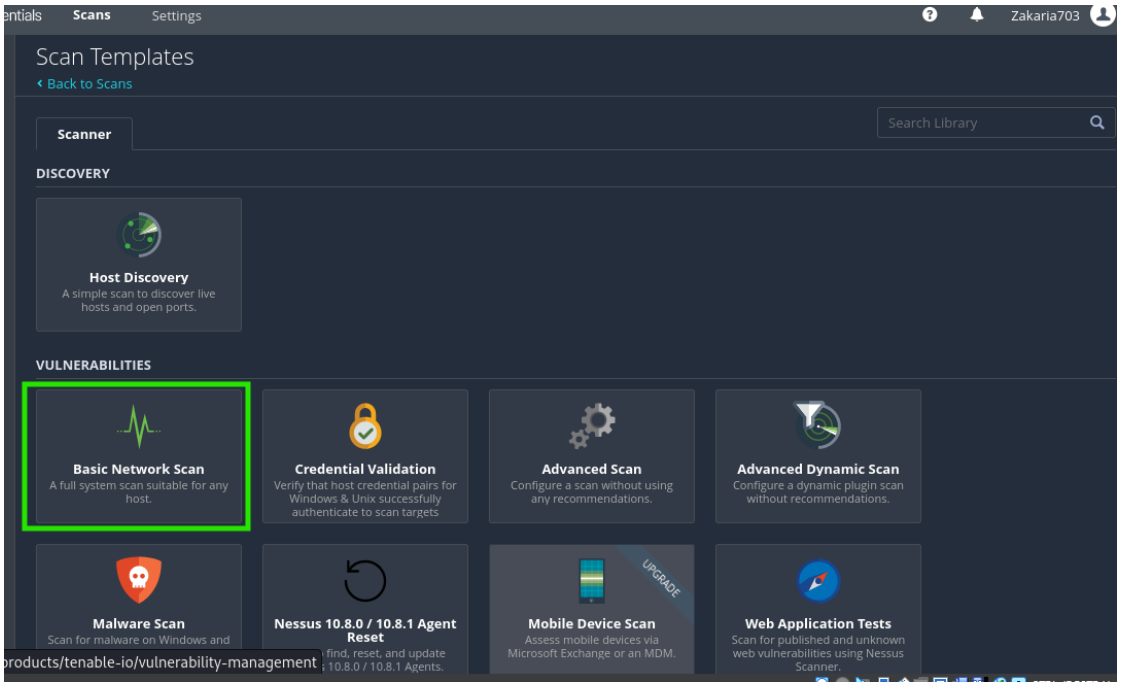
S5/L3

L’esercizio di oggi consiste nell’effettuare un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Prima cosa attiviamo il service di Nessus tramite il commando:

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd.service
[sudo] password for kali:
```

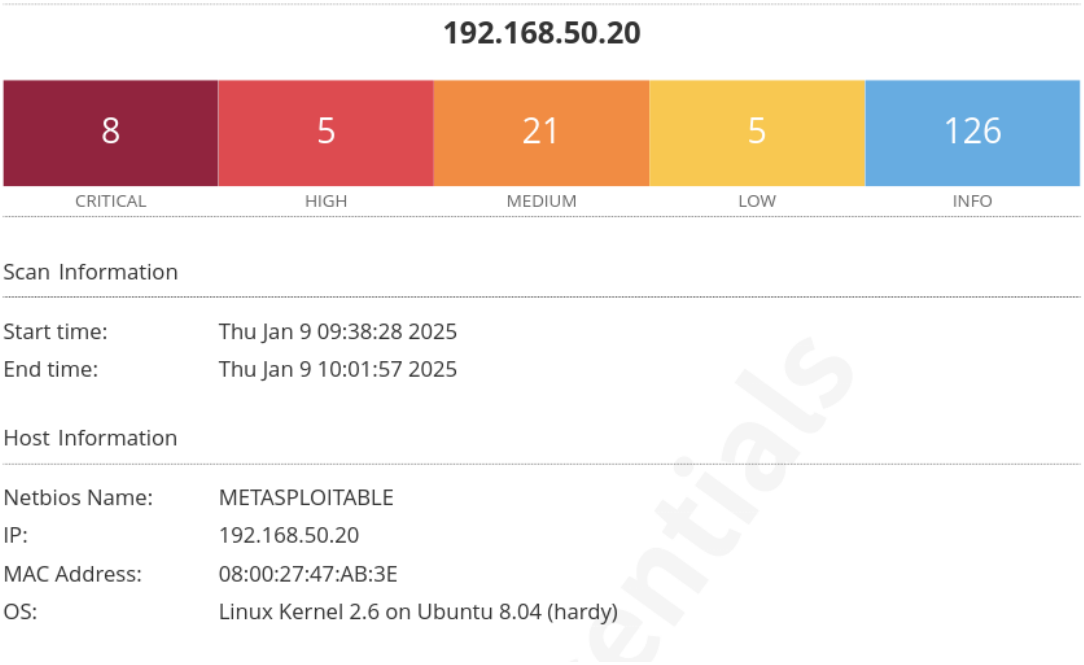
Dopo di che possiamo aprire Firefox ed andare sul sito https://Kali/8834, e andiamo a creare una nuova scansione e selezioniamo Basic Network Scan



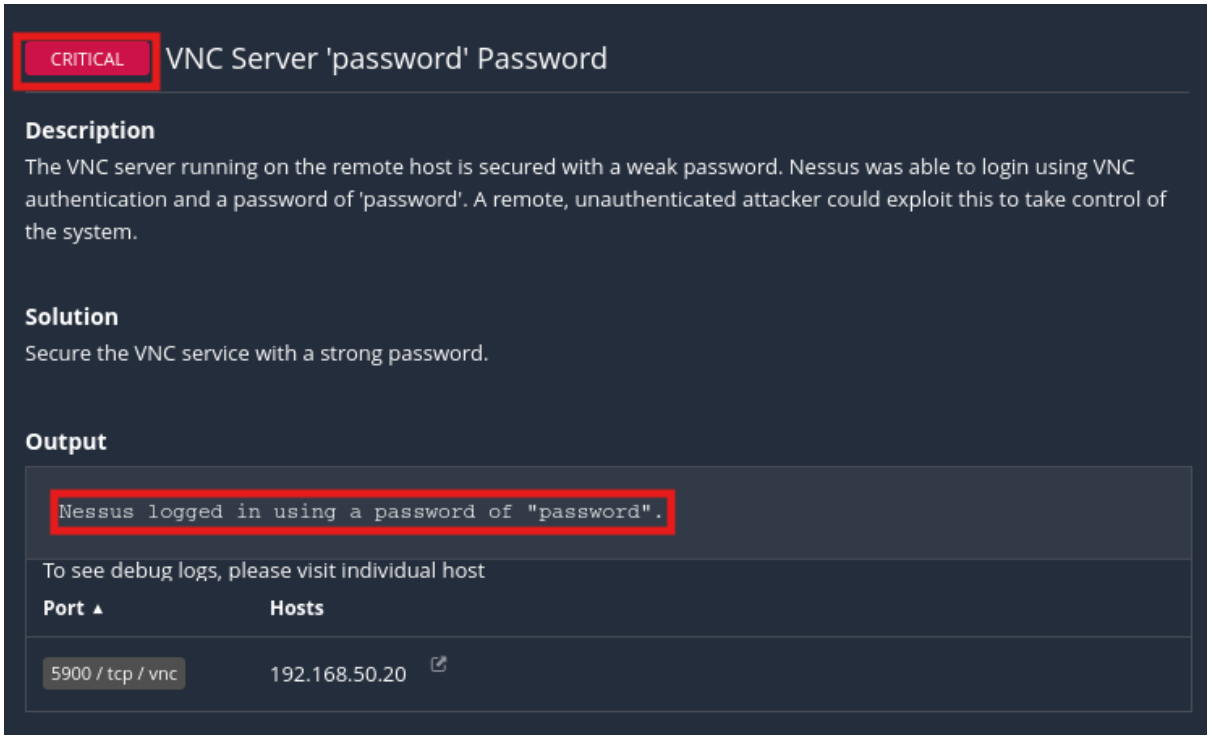
Poi bisogna inserire i parametri importanti come l’indirizzo del target e le porte da analizzare mentre per il resto se non ci sono specifiche si possono lasciare di default.

Poi avviamo la scansione è si attende che venga completata.

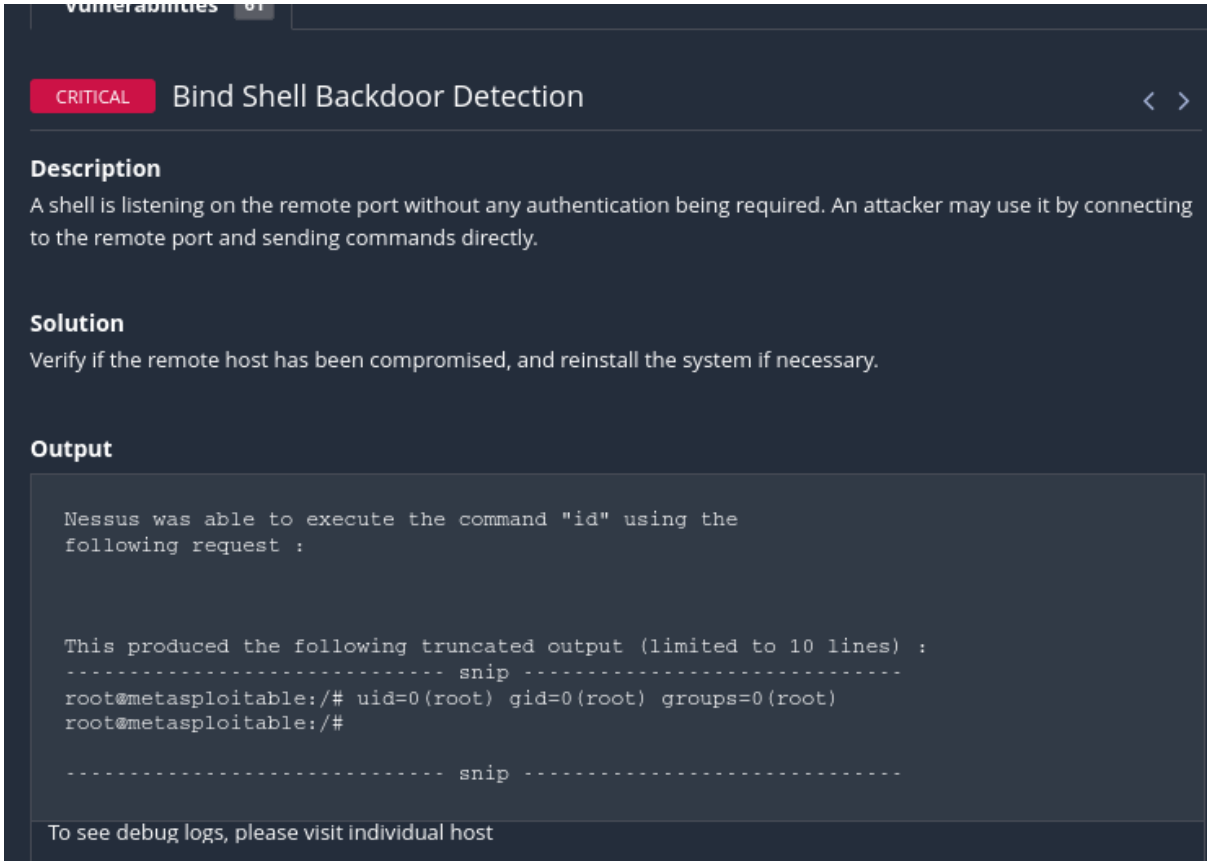
Una volta completata la scansione come prima cosa controlliamo se tutte le porte interessate sono state analizzate.



Questa è la prima pagina del report dove troviamo tutte le vulnerabilità e informazioni come l'orario della scansione, ip del target ecc.

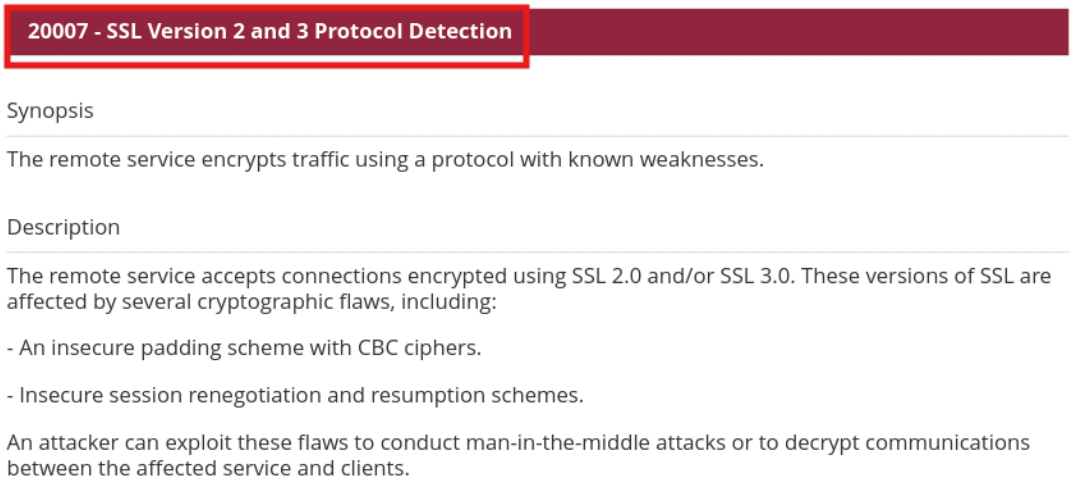


Come possiamo notare qua una delle vulnerabilità critiche è dovuta dalla password del server VNC che è troppo semplice, come possiamo vedere in basso dove c'è l'output Nessus è entrato scrivendo semplicemente" password".



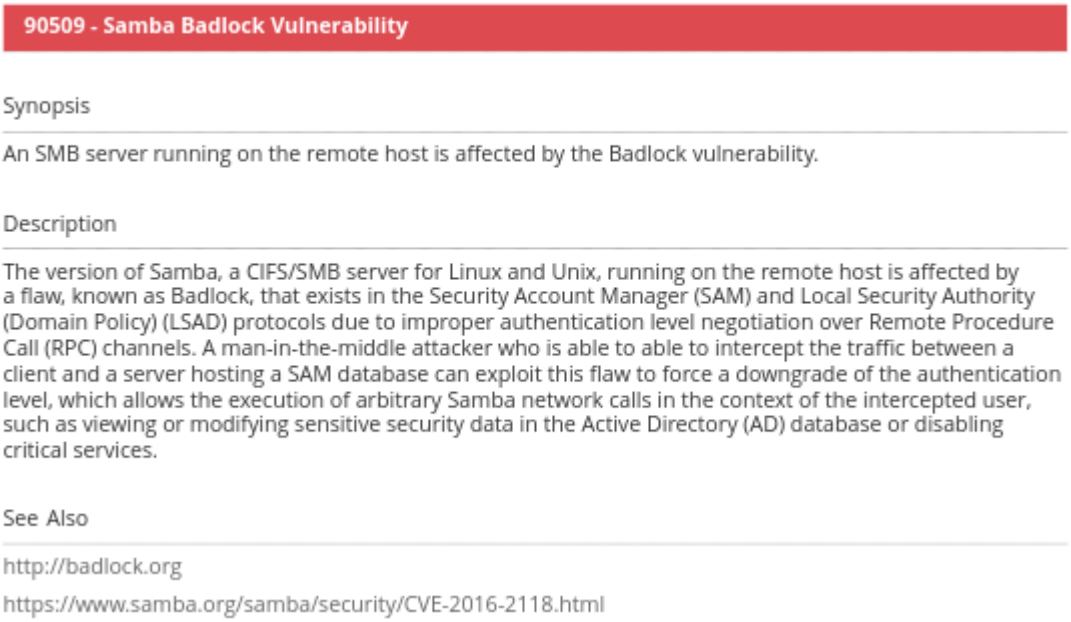
Qua invece ci dice che c'è un programma in ascolto senza nessuna autenticazione è che quindi potrebbe essere pericoloso per un attaccante dato che potrebbe connettersi e" ascoltare" tutto.

La soluzione che ci consiglia è verificare se è stato compromesso è in caso reinstallare il sistema.



In questo caso invece ci viene segnalato che usiamo delle versioni obsolete che hanno delle vulnerabilità, un attaccante potrebbe usare queste crepe per fare un attacco di man-in-the-middle.

La soluzione che ci fornisce è di disattivare queste 2 versioni ed invece utilizzare versioni migliori come ad esempio TLS 1.2 che è un protocollo molto più sicuro.



90509 - Samba Badlock Vulnerability

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

Qui invece ci viene segnalato che il server SMB è affetto da una vulnerabilità quindi questa dovrebbe essere una vulnerabilità che deve essere risolta al più presto.

Per risolverla dobbiamo aggiornare il server ad una versione più nuova.

Spesso quando si risolvono le vulnerabilità, non ne risolviamo solo una ma anche altre magari di livello più basso dato che ad esempio aggiornando il sistema, i creatori risolvono anche altri problemi.