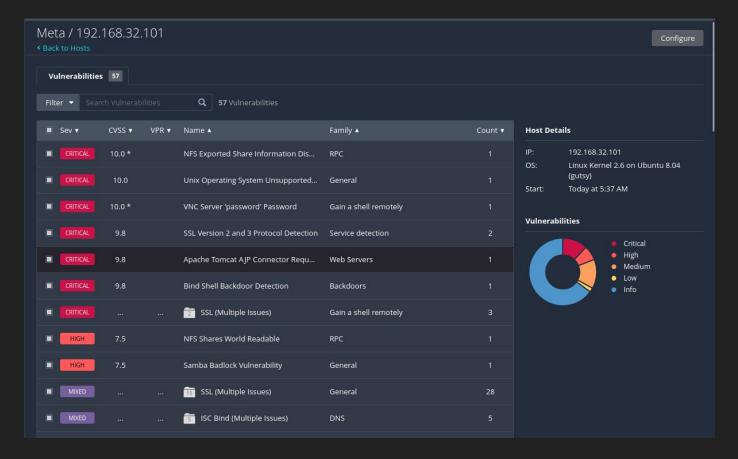
Oggi abbiamo
usato il tool
Nessus per fare
una scansione
vulnerabilità
sulla nostra
macchina
Metasploitable,
IP 192.168.32.101

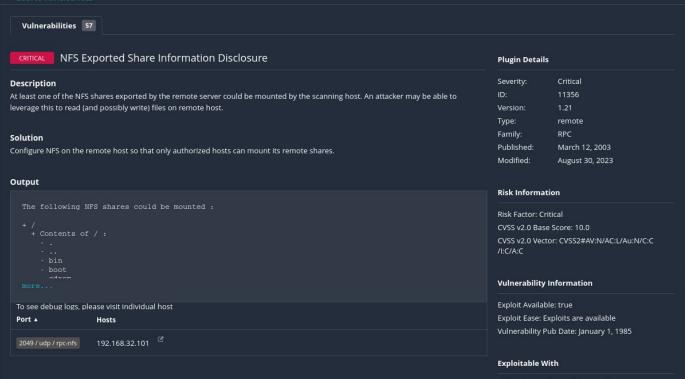
Ha trovato tanti vulnerabilità, di cui andremo a rimediare cuatro.



La prima vulnerabilità trovata è un sistema di Network File Sharing (NFS) pubblica, che può essere accesa per utenti **non** autorizzati che poi avranno il potere di fare molte cose.come vedere informazioni sensibili, modificare i file. fare *privilege* escalation, e anche inserire malware.

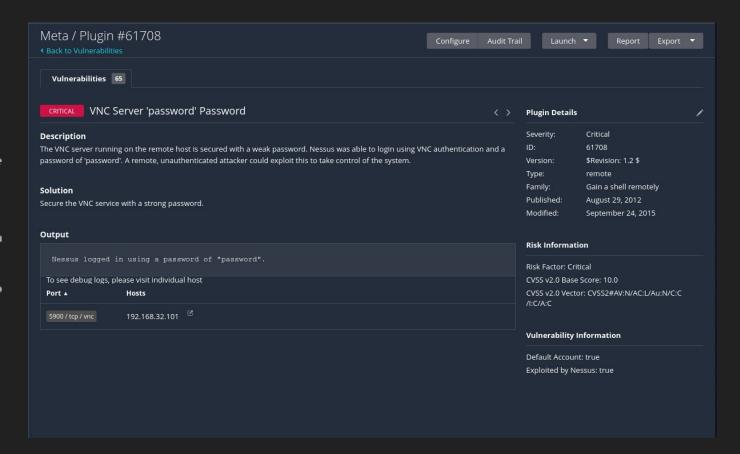
Meta / Plugin #11356

Back to Vulnerabilitie



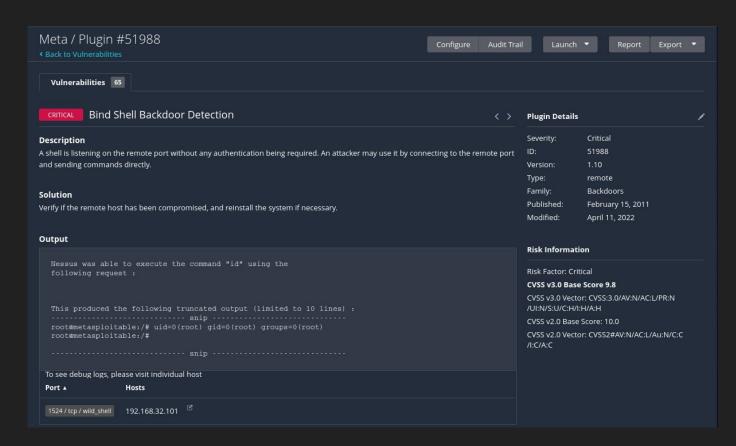
Metasploit (NES Mount Scanner)

Un'altra vulnerabilità critica trovata e la nostra password molto debole al server VNC.Nessus é riuscito ad indovinare questa password. Possiamo risolvere questo rischio cambiando ad una password più forte e sicura.



Una backdoor di bind shell è un tipo di software dannoso che apre una porta su nostra macchina meta, in attesa di una connessione in entrata da un utente malintenzionato. Crea una shell collegata a una porta specifica, consentendo all'aggressore di ottenere accesso e controllo non autorizzati sul sistema compromesso.

Ovviamente queste e uno dei rischi piu critici che possiamo avere dentro nostra macchina



Samba é un tipo di server hosted per la nostra macchina linux che consente una comunicazione tra una database SAM e un cliente. Metasploitable ha una versione vecchia di cui si ha trovato un rischio di sicurezza che consente l'intercettazione di traffico per parte di un attaccante fungendo di man-in-the-middle

