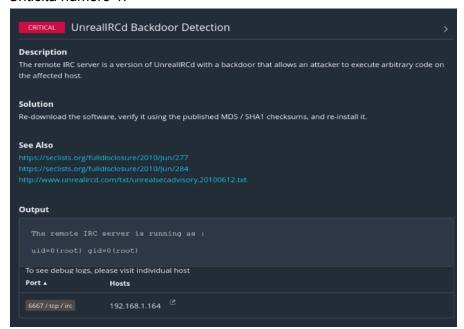
Nessus_Essentials

entrando su Nessus Essentials, ho avviato una nuova scansione e utilizzando la scansione Base ho inserito i dati dell'indirizzo ip di metasploitable che dopo essere stato analizzato mi ha rivelato 9 criticità di cui 5 mostrate qui sotto:

Criticità numero 1:



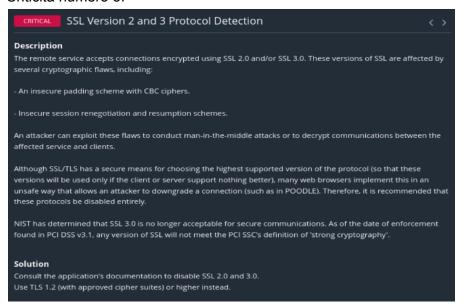
Come soluzione consiglia di disinstallare e reinstallare il software "UnrealIRCd Backdoor Detection" usando la versione pubblicata. (qui è stata lasciata anche una backdoor)

Criticità numero 2:



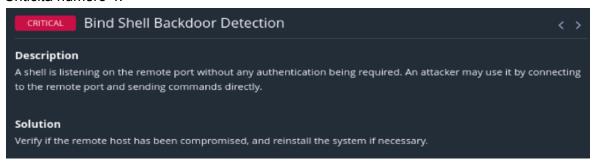
Come soluzione consiglia di Modificare la Password di "VNC Server 'password' Password" usandone una più forte.

Criticità numero 3:



Come soluzione consiglia di Disabilitare SSL 2.0 e 3.0 e di usare TLS 1.2.

Criticità numero 4:



Come soluzione consiglia di verificare se l'host remoto è stato compromesso e in caso di manomissione di reinstallare direttamente tutto il sistema, qui è stata lasciata anche una Backdoor.

Criticità numero 5:

Description The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack. Solution Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Come soluzione consiglia di Crittografare il materiale e rigenerare le chiavi SSH, SSL, OpenVPN,

attenzione perchè si è deboli agli attacchi man in the middle.

Diego Petronaci