Oggi effettueremo un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni scegliendo una scansione di tipo <<basic network scan>>
Come previsto oltre al report completo con 118 vulnerabilità di cui :

- 9 critical
- 6 high
- 18 medium
- 7 low
- 78 Info

Ci soffermeremo sulle prime 4 vulnerabilità critiche :

- **1.NFS Exported Share Information Disclosure**
  Divulgazione delle informazioni sulle condivisioni esportate da NFS

- **2.Unix Operating System Unsupported Version Detection**
  Rilevamento della versione non supportata del sistema operativo Unix

- **3.VNC Server 'password' Password**
  Password "password" del server VNC

- **4.Bind Shell Backdoor Detection**
  Rilevamento backdoor di shell vincolata

1.NFS sta per "Network File System" ed è un protocollo di condivisione di file e una tecnologia di rete che consente a computer in una rete di accedere e condividere file e directory tra loro
Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.
Soluzione
Aggiornare Nfs con la versione successiva Nfsv4
Limitare attraverso Firewall o nfs stesso per far accedere determinati indirizzi ip.
Anche tramite l'Acl (lista controllo degli accessi)

2.Ci avverte che abbiamo un sistema obsoleto e non usciranno più patch di sicurezza relativi a questo tipo di sistema

Soluzione
Aggiornare il sistema operativo con una versione più recente

3.Ci avverte che all’interno della macchina ha trovato un server Vnc con una password troppo debole .Infatti Nessus è riuscito a trovare la password

Soluzione
Aggiorna la password ,utilizzando parole non comuni

4.Ci avvisa che c'è un problema di sicurezza in cui una shell (un'interfaccia da linea di comando) è in esecuzione su una porta remota del sistema, e questa shell non richiede alcuna autenticazione o password per accedervi. Questo scenario è estremamente rischioso, poiché un potenziale attaccante può connettersi a questa porta e ottenere accesso diretto al sistema, consentendogli di eseguire comandi o operazioni non autorizzate.

Soluzione
Isolare il sistema.
Controllare se il sistema è corrotto
La reinstallazione del sistema è spesso l'opzione più sicura per garantire che il sistema sia di nuovo sotto controllo e non soggetto a ulteriori compromissioni