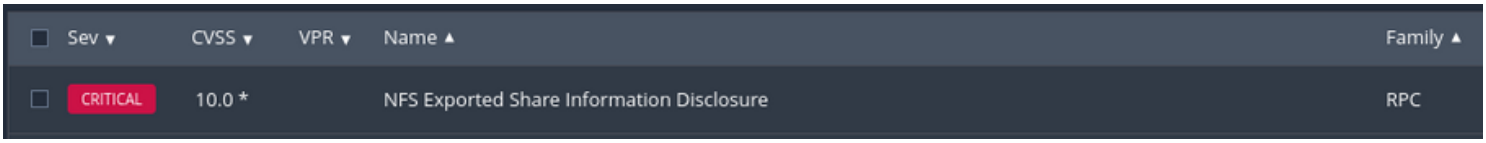
Report Nessus S5L4

Analizziamo le prime quattro vulnerabilità critiche individuate da Nessus della macchina Metasploitable 2

1)



Descrizione:
Si sta facendo riferimento a condivisioni NFS (Network File System) esportate da un server remoto, il che significa che il server remoto consente ad altri host di accedere ai suoi file tramite il protocollo NFS. La preoccupazione qui è che almeno una di queste condivisioni NFS può essere montata (ovvero, accessibile) dall'host di scansione, che potrebbe essere un potenziale attaccante. Questo suggerisce che c'è una vulnerabilità nella configurazione di accesso alle condivisioni NFS.

Soluzione:
Si consiglia di configurare il server NFS sul sistema remoto in modo che solo gli host autorizzati siano in grado di montare (accedere) alle sue condivisioni remote. Questa è una misura di sicurezza importante per impedire a persone non autorizzate di accedere ai file sul server tramite NFS. In altre parole, si dovrebbe impostare una configurazione che limiti chi può accedere alle risorse condivise tramite NFS per evitare possibili attacchi informatici.

2)

Descrizione:
In base al numero di versione autodichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato (Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server)).
L'assenza di supporto implica che il produttore non rilascerà nuovi aggiornamenti di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione:
Effettuare l'aggiornamento a una versione del sistema operativo Unix attualmente supportata.

Per maggiori info: https://wiki.ubuntu.com/Releases

3)

Descrizione:
Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare l'accesso utilizzando l'autenticazione VNC e una password: 'password'. Un attaccante remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

Soluzione:
Proteggere il servizio VNC con una password robusta.

4)

Descrizione:
Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un aggressore potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.
Nessus è stato in grado di eseguire il comando "id" utilizzando la seguente richiesta:
Ciò ha prodotto l'output troncato seguente (limitato a 10 righe):
ruby
---------- snip ----------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
---------- snip ----------

Nessus ha eseguito il comando "id" con successo sul sistema remoto e ha restituito le informazioni sull'utente corrente, mostrando che l'utente corrente è "root" con un ID utente (UID) di 0, un gruppo principale (GID) di 0 e facente parte dei gruppi con GID 0. Questo indica che Nessus è riuscito a eseguire comandi con privilegi di amministratore (root) sul sistema remoto.

Soluzione:
Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.