REPORT DI VULNERABILITA’

Descrizione:

In questa fase, abbiamo eseguito una scansione iniziale della nostra infrastruttura per identificare eventuali vulnerabilità. Il grafico allegato mostra l'elenco delle vulnerabilità riscontrate, suddiviso per gravità (critico, alto, medio, basso).

Risultati della Scansione:

- Critiche: 9
- Alte: 5
- Medie: 18
- Basse: 7

Grafico Vulnerabilità:

File Allegato in cartella > ScanzioneIniziale.pdf

Vulnerabilità da Risolvere:

VNC Server ‘password’ Password

Descrizione: Il server VNC è protetto con una password debole.Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Criticità: 10

Rimedio: Mettere in sicurezza il servizio VNC con una password sicura

NFS Exported Share Information Disclosure

Descrizione: Questa condivisione NFS esportate dal server remoto potrebbe essere montata all’host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull’host remoto.

Criticità: 10

Rimedio: Configurare NFS sull’host remoto che solo gli host autorizzati possano montare le sue condivisioni remote.

Bind Shell Backdoor Detection

Descrizione: Una shell è in ascolto su una porta remota senza che sia richiesta nessuna autorizzazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviare direttamente i comandi.

Criticità: 9.8

Rimedio: Verifica la la porta remota dell' host è stata compromessa, in caso reinstallare il sistema se necessario.

SSL v 2.0 e v 3.0 Protocol Detection

Descrizione: Il servizio remoto accetta connessioni crittografate SSL v 2.0 e v 3.0, ma queste versioni sono affette da alcuni difetti. Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o decrittografare le comunicazioni tra il servizio interessato e il client.

Criticità: 9.8

Rimedio: Disabilitare SSL 2.0 e 3.0.