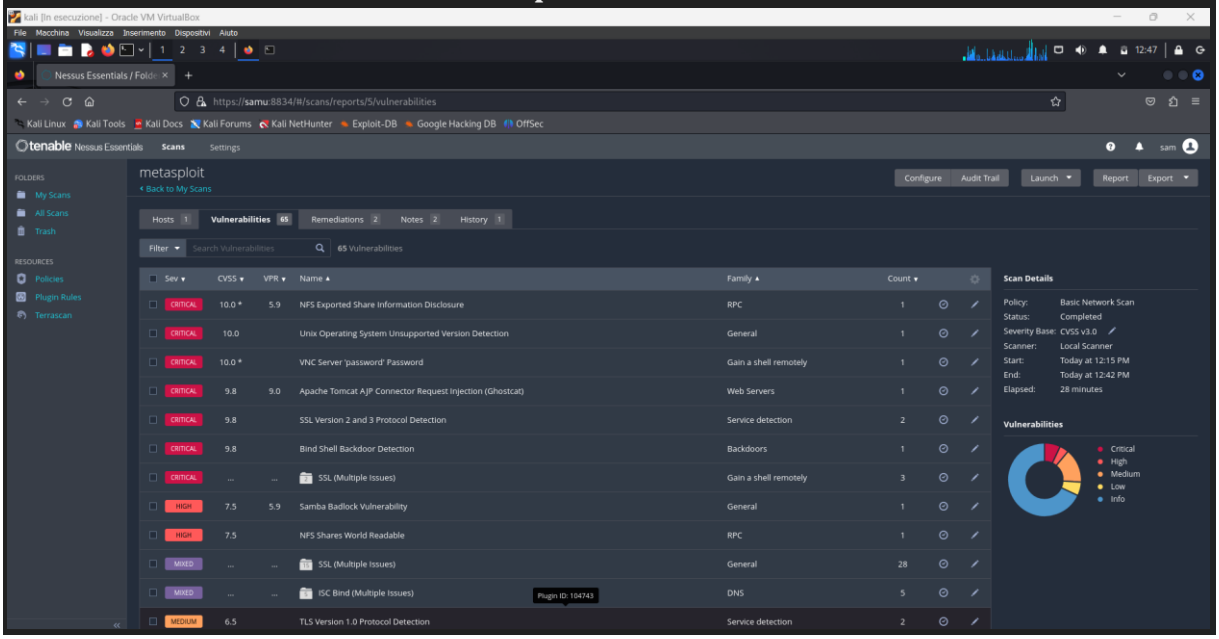
Rapporto Dettagliato di Sicurezza

Introduzione Questo rapporto fornisce un'analisi dettagliata dei risultati ottenuti dalla scansione di sicurezza eseguita su una macchina Metasploitable2 utilizzando il tool Nessus. La scansione ha identificato due vulnerabilità critiche che richiedono attenzione immediata

(tempo ideale per intervenire sulle debolezze critiche rilevate : 1 giorno)

Stato inziale della macchina :"metasploitable2"



1. Rilevazione di Bind Shell Backdoor

- **Gravità**: Critica (9.8)
- **ID Nessus**: 51988
- **Descrizione**: Questo alert indica la presenza di una backdoor tramite bind shell su una delle porte del sistema. Una bind shell crea un punto di ascolto in attesa di connessioni in entrata, che permettono all'attaccante di eseguire comandi sul sistema.
- **Impatto**: La presenza di una bind shell su un sistema è un chiaro indicatore di una compromissione. Essa permette ad un attaccante remoto di prendere il controllo completo del sistema.
- **Soluzione**: È essenziale identificare e rimuovere tutti i componenti legati a questa backdoor. Si consiglia di eseguire una revisione completa del sistema e di ripristinare le operazioni da una copia di backup fidata, se disponibile. Inoltre, è importante investigare come l'attaccante abbia guadagnato l'accesso per evitare future compromissioni.

2. VNC Server 'password' Password:

- **Gravità**: Critica (10.0*)
- **Descrizione**: Il server VNC è configurato con una password debole o predefinita, mettendo a rischio la sicurezza del sistema.
- **Azione Consigliata**: Cambiare immediatamente la password del server VNC con una più sicura.
- **Procedura di Risoluzione**: Utilizzare il comando `vncpasswd` per impostare una nuova password per il server VNC. Assicurarsi che la nuova password sia lunga, complessa e unica.

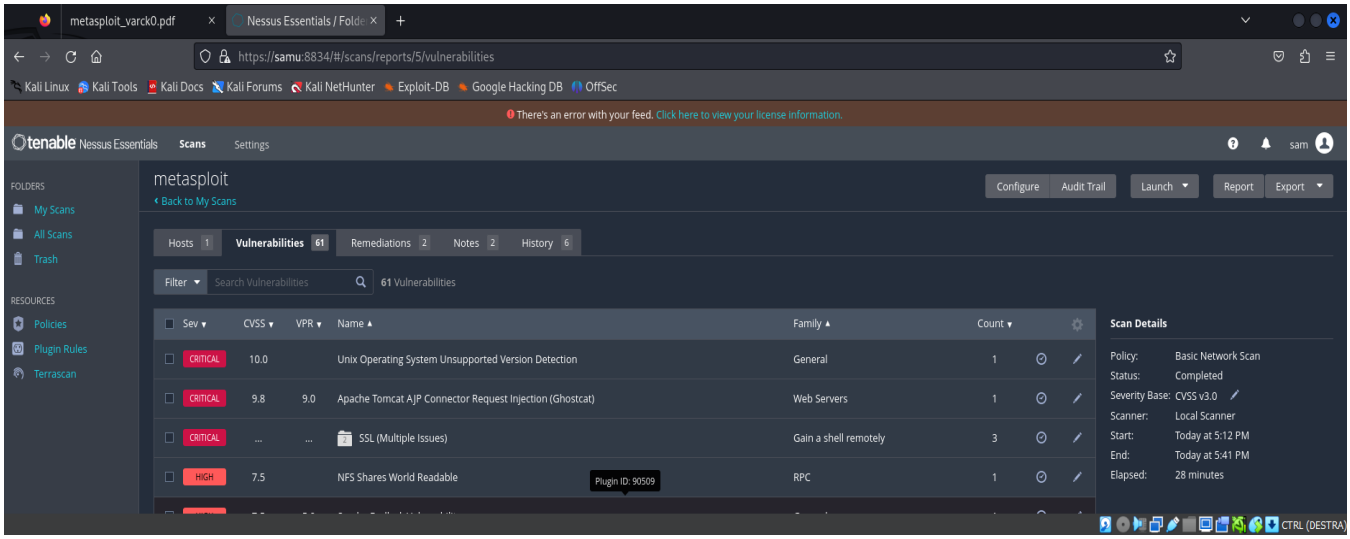
3. NFS Exported Share Information Disclosure:

- **Gravità**: Critica (10.0*)
- **Descrizione**: Le condivisioni NFS sono configurate in modo non sicuro, consentendo la divulgazione non autorizzata di informazioni.
- **Azione Consigliata**: Limitare l'accesso alle condivisioni NFS solo agli utenti autorizzati.
- **Procedura di Risoluzione**: Modificare le autorizzazioni delle condivisioni NFS nel file `/etc/exports` per limitare l'accesso solo agli utenti autorizzati. Aggiungere regole di firewall, se necessario, per limitare l'accesso solo agli IP autorizzati.

4. Rilevamento del Protocollo SSL Versione 2 e 3:

- **Gravità**: Alta
- **Descrizione**: Il protocollo SSL versione 2 e 3 è stato rilevato nel sistema. Questi protocolli sono noti per avere gravi vulnerabilità di sicurezza e non devono essere utilizzati.
- **Azione Consigliata**: Disabilitare completamente il supporto per i protocolli SSL versione 2 e 3.
- **Procedura di Risoluzione**: Modificare la configurazione del server web (ad esempio Apache) per disabilitare il supporto per i protocolli SSL versione 2 e 3. Questo può essere fatto modificando il file di configurazione del server web e impostando esplicitamente i protocolli supportati su TLS.

STATO FINALE DELLA MACCHINA CON 4 CORREZIONI RICHIESTE DALL'ESERCIZIO :


metasploit_varck0.pdf
Nessus Essentials / Folde
https://samu:8834/#/scans/reports/5/vulnerabilities
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
sam
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
metasploit
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 61
Remediations 2
Notes 2
History 6
Filter
Search Vulnerabilities
61 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
CRITICAL 10.0 Unix Operating System Unsupported Version Detection General 1
CRITICAL 9.8 9.0 Apache Tomcat AJP Connector Request Injection (Ghostcat) Web Servers 1
CRITICAL ... ... SSL (Multiple Issues) Gain a shell remotely 3
HIGH 7.5 NFS Shares World Readable RPC 1
Plugin ID: 90509
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:12 PM
End: Today at 5:41 PM
Elapsed: 28 minutes
CTRL (DESTRA)