REPORT WEEKLY PROJECT - NESSUS

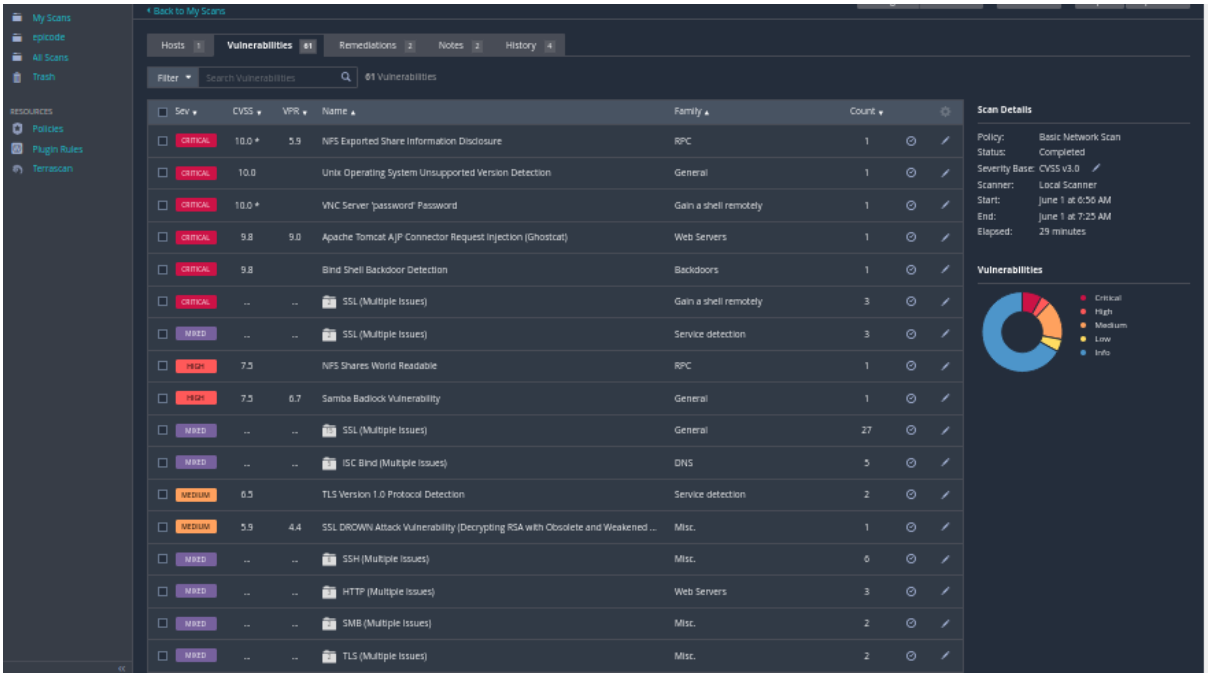
Il progetto di questa settimana riguarda l'utilizzo dello strumento **Nessus** per effettuare delle scansioni. Nessus è un **Vulnerability Scanner** utilizzato durante un Penetration Test per **individuare potenziali vulnerabilità presenti su un determinato obiettivo**, al fine di sfruttarle successivamente nella fase di exploitation.

Nello specifico ci viene richiesto di **effettuare una prima scansione**, seguita dall'**implementazione delle remediation action** per le vulnerabilità identificate, e infine un **secondo scan per verificare l'esito** delle modifiche apportate. Tutte e tre le fasi devono essere **accompagnate da report esplicativi**. In particolare, i report per la scansione iniziale e per il rescan, dopo l'applicazione delle azioni correttive, sono generati automaticamente da Nessus. Il seguente testo è stato elaborato per fornire una spiegazione più dettagliata delle azioni intraprese.

Procediamo quindi con l'installazione dello strumento sulla macchina Kali e successivamente avviamo la scansione. Il target selezionato è Metasploitable, con indirizzo IP 192.168.50.101.

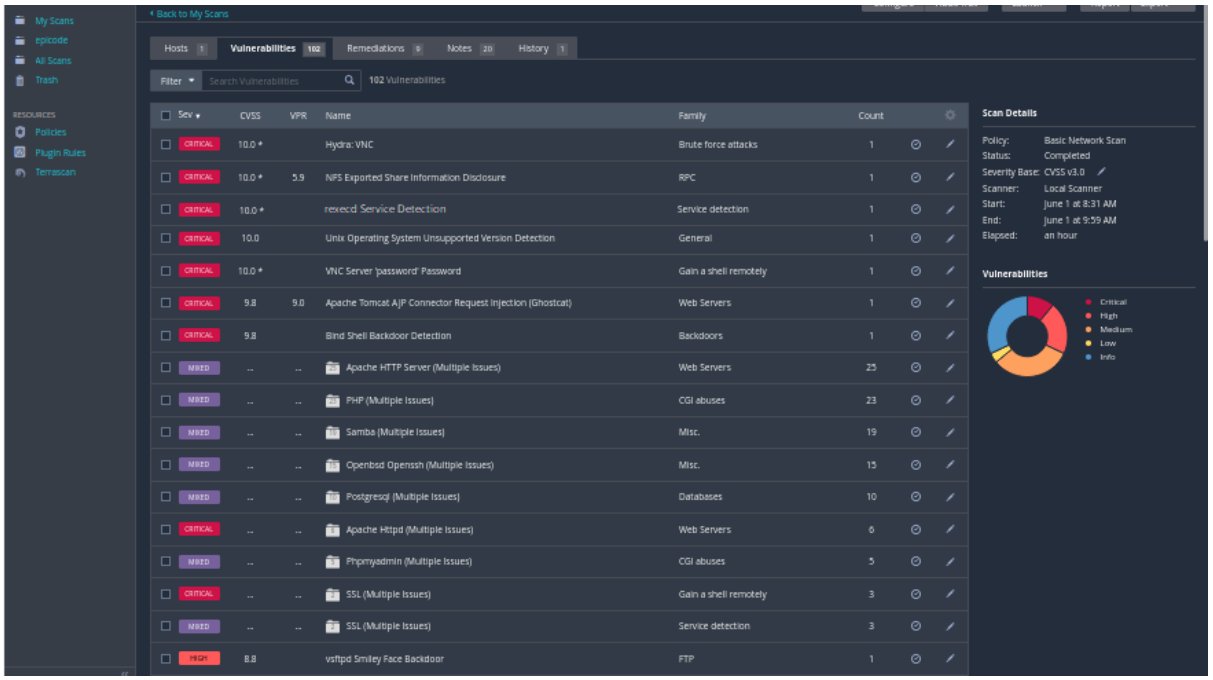
La prima scansione che eseguiamo è una **"Basic Network Scan",** una sorta di scansione preliminare che ci consente di esplorare l'ambiente e ottenere una panoramica delle potenziali vulnerabilità presenti.

Alla conclusione della scansione, otteniamo i seguenti risultati:
- 10 vulnerabilità di livello "CRITICO"
- 5 vulnerabilità di livello "HIGH"
- 24 vulnerabilità di livello "MEDIO"
- 5 vulnerabilità di livello "BASSO"
- 132 vulnerabilità di livello "INFO"



Successivamente, procediamo con una seconda scansione sempre di tipo "Basic Network Scan", ma questa volta selezionando **parametri personalizzati**. Nelle sezioni "Discovery" e "Assessment" scegliamo l'opzione "**custom**" come "tipo di scansione", che ci consente di includere numerosi parametri **aggiuntivi.** È fondamentale condurre una fase di Valutazione delle Vulnerabilità (VA) **approfondita per ottimizzare al meglio la successiva fase di exploitation.**

Alla fine di questa seconda scansione più approfondita, otteniamo i seguenti risultati:
- **32 vulnerabilità di livello "CRITICO"**
- **61 vulnerabilità di livello "HIGH"**
- 99 vulnerabilità di livello "MEDIO"
- 12 vulnerabilità di livello "BASSO"
- 144 vulnerabilità di livello "INFO"



Come è evidente, i risultati sono **significativamente peggiorati dopo aver ampliato i parametri** di scansione.

Procediamo quindi **all'applicazione delle remediation action**, ovvero le misure di sicurezza atte a **ridurre il rischio** associato a ciascuna vulnerabilità critica individuata.

Prendendo in considerazione **lo scoring system** del report redatto da Nessus, il quale ci fornisce le linee guida **sulla priorità delle varie implementazioni**, andiamo a risolvere le seguenti vulnerabilità:

- **Divulgazione di informazioni sulle condivisioni NFS**
- **Password predefinita del server VNC**
- **Rilevazione di una backdoor bind shell**
- **Rilevazione del servizio "rexecd"**

APPLICAZIONE REMEDIATION ACTION

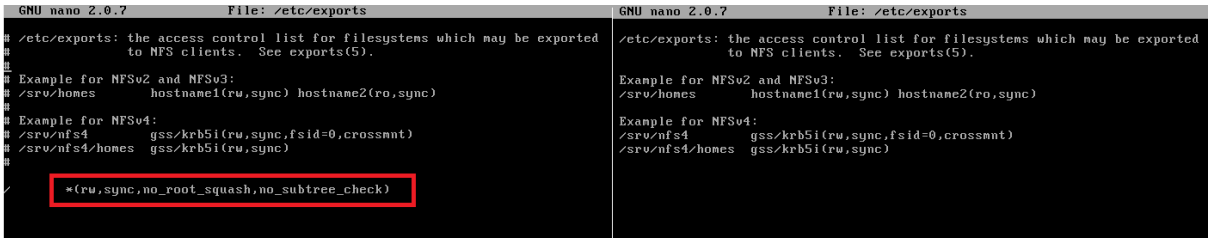
Vulnerabilità critica 1 - Divulgazione di informazioni sulle condivisioni NFS

Questa vulnerabilità riguarda l'utilizzo di NFS (Network File System), che consente la condivisione di file e directory tra sistemi in una rete. Tuttavia, se la condivisione NFS non è configurata correttamente, potrebbero verificarsi divulgazioni non autorizzate di dati sensibili, consentendo a utenti esterni di accedere, leggere e potenzialmente modificare i dati.
In particolare il servizio è attivo sulla porta 2049/tcp.

Remediation action consigliata da Nessus:
Configurare NFS in modo che solo gli host autorizzati possano accedere alle condivisioni.

Remediation action applicata per questa vulnerabilità:
modifica dei permessi di accesso ai file tramite la rimozione di una stringa all'interno del file /etc/exports.

Segue screen



Vulnerabilità critica 2 - Password predefinita del server VNC

Questa vulnerabilità riguarda il server VNC (Virtual Network Computing) e indica che la password per l'accesso al server non è stata cambiata o è stata impostata come "password". Ciò rappresenta un grave rischio per la sicurezza, in quanto consente a chiunque che indovini la password di accedere al computer e controllarlo da remoto.

Remediation action consigliata da Nessus:
Aumentare la sicurezza di VNC utilizzando una password più forte.

Remediation action applicata per questa vulnerabilità:
modifica della password tramite il comando ~/.vnc/passwd dove troviamo una stringa di caratteri da sostituire con la nostra nuova password.

Segue screen dell'operazione effettuata.

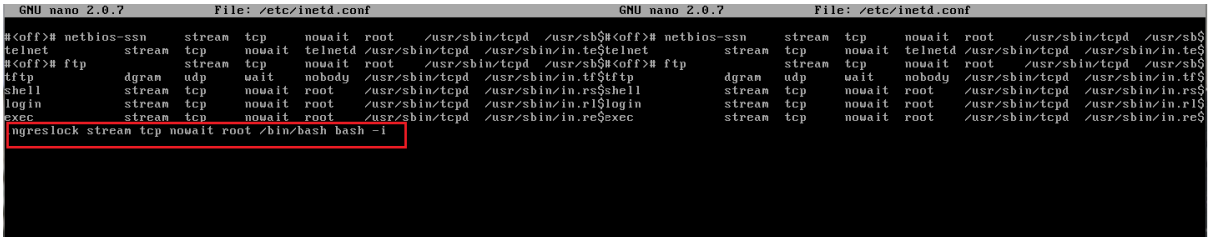
Vulnerabilità critica 3 - Rilevazione di una backdoor bind shell

Questa vulnerabilità riguarda il rilevamento di una backdoor attiva sul sistema target. In particolare, indica che il servizio wild_shell è in esecuzione sulla porta 1524/tcp. Questo servizio rappresenta un tipo di shell remota che ascolta su una porta specifica senza richiedere alcuna autorizzazione. Quando un client si connette a questa porta, viene stabilita una connessione remota tra il client e il sistema, consentendo all'attaccante di ottenere un controllo completo sul sistema remoto.

Remediation action consigliata da Nessus:
Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Remediation action applicata per questa vulnerabilità:
rimozione della backdoor tramite modifica del file /etc/inetd.conf dove cancelliamo la stringa.

Segue screen dell'operazione effettuata.



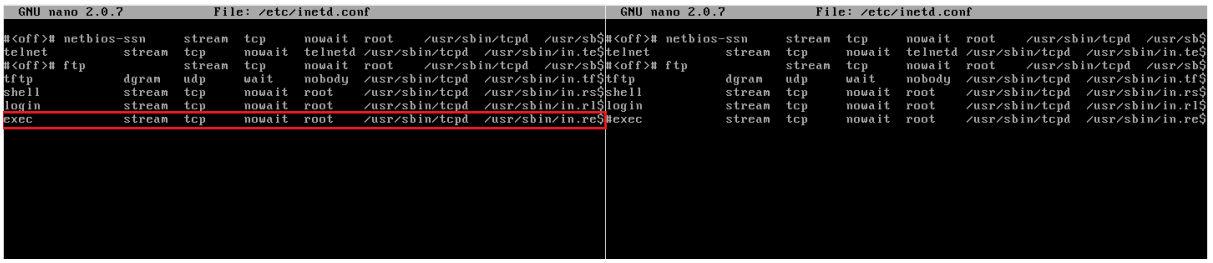
Vulnerabilità critica 4 - Rilevazione del servizio "rexecd"

Questa vulnerabilità riguarda la rilevazione del servizio "rexecd" attivo sul sistema target. Il servizio "rexecd" è un demone di rete che consente l'esecuzione di comandi remoti su un sistema Linux, ma è considerato obsoleto e presenta notevoli rischi per la sicurezza. Pertanto, è consigliabile disabilitarlo o rimuoverlo completamente.

Remediation action consigliata da Nessus:
Commentare la riga 'exec' nel file /etc/inetd.conf e riavviare il processo inetd.

Remediation action applicata per questa vulnerabilità:
rimozione del servizio rexecd tramite la modifica del file /etc/inetd.conf con il commento della riga "exec".

Segue screen dell'operazione effettuata



RESCAN FINALE

Per avere **conferma** che tutte le **remediation action applicate siano andate a buon fine** andiamo ad effettuare un'ultima scansione.
Ne risulta che **tutte le azioni messe in atto** sono state utili a risolvere i problemi di sicurezza critici che l'host presentava **prima del nostro intervento**.

Segue screen dell'operazione.