Traccia:

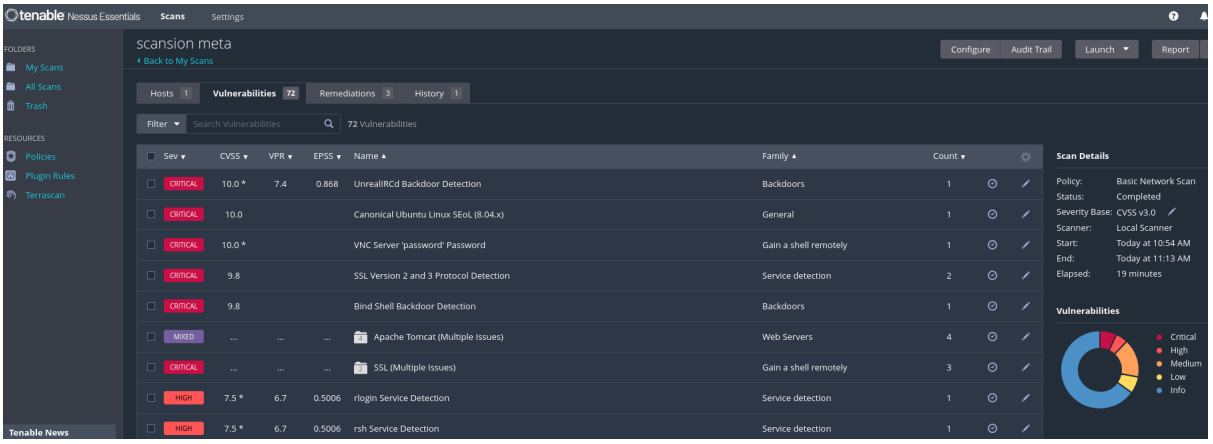
Effettuare un Vulnerability Assessment con Nessus sulla macchina **Metasploitable** indicando come target **solo** le **porte comuni** (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo)

A valle del completamento della scansione, **analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web**.

Gli obiettivi dell'esercizio sono:

- **Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni**
- **Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester**

SVOLGIMENTO:



ho selezionato il tipo di scansione (basic network scan) ho selezionato poi common ports inserito il target della macchina meta ho salvato le modifiche e ho fatto partire la scansione come si vede dallo screenshot.

REPORT VULNERABILITY ASSESSMENT CON NESSUS

OBIETTIVO: documentare la scansione eseguita con nessus su metasploitable sulle porte comuni.
TITOLO: vulnerability assessment-metaploitable
AUTORE: Emanuela Parisi
DATA SCANSIONE: 27/09/2025
TOOL: Nessus
TARGET: IP 192.168.50.101

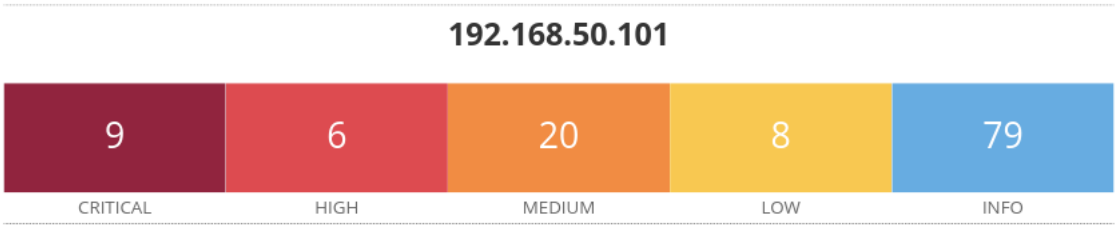
SOMMARIO ESECUTIVO

Questa attività di laboratorio aveva come obiettivo introdurre l'utilizzo di Nessus per eseguire un primo Vulnerability Assessment su una macchina volutamente vulnerabile (*Metasploitable*). È stata configurata e avviata una scansione di tipo *Basic Network Scan*, limitata alle porte comuni.
La scansione è durata 19 minuti e sono state trovate 122 vulnerabilità di cui diverse classificate come critical high.

INTRODUZIONE:
lo scopo dell'attività era familiarizzazione con la logica dei report di nessus e sulla comprensione dell'interfaccia di nessus
AMBITO: solo le porte comuni

METODOLOGIA DI SCANSIONE:
TIPO DI SCAN UTILIZZATO: Basic network scan
TARGET IP: 192.168.50.101

RISULTATI GENERALI
TOTALE VULNERABILITÀ: 122
CLASSIFICAZIONE PER SEVERITÀ:



ANALISI DELLE VULNERABILITÀ PIÙ RILEVANTI

UnrealIRCd Backdoor Detection

- CVE: CVE-2010-2075
- Descrizione: Versioni compromesse di UnrealIRCd contengono una backdoor che consente l'esecuzione di comandi remoti.
- Host/Porta: TCP/6667
- Impatto: Compromissione completa del sistema.
- Mitigazione: Reinstallazione da sorgente sicura, aggiornamento a versione supportata.

VNC Server 'password' Password

- Descrizione: Il servizio VNC consente l'accesso remoto utilizzando la password debole "password".
- Host/Porta**:** TCP/5900
- Impatto**:** Accesso remoto non autorizzato.
- Mitigazione**:** Disabilitare VNC non necessario, impostare password robuste.

SSL Version 2 and 3 Protocol Detection

- Descrizione: Il server supporta protocolli SSLv2/SSLv3, obsoleti e insicuri.
- Host/Porta: TCP/443
- Impatto: Attacchi Man-in-the-Middle, decrittazione del traffico.
- Mitigazione: Disabilitare SSLv2/v3, configurare TLS 1.2 o superiore.