Per quanto riguarda l'esercizio di oggi abbiamo scaricato ed installato il software Nessus per andare ad eseguire una scansione di Metasploitable alla ricerca delle vulnerabilità.

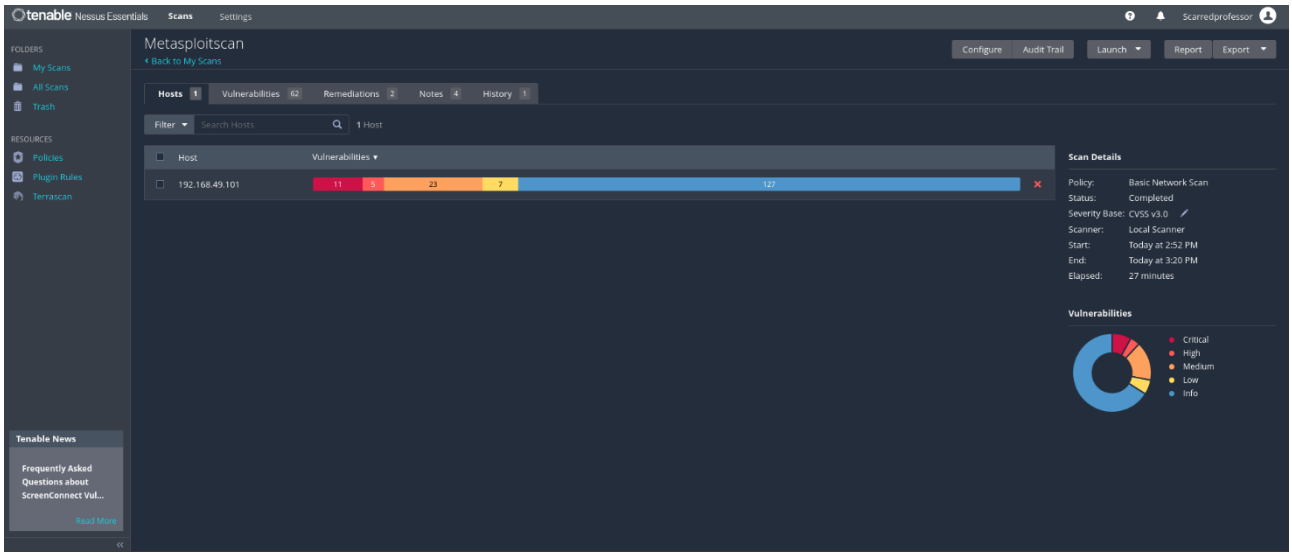
Il software Nessus per questa operazione è stato lanciato in configurazione default ed è ha quindi scansionato la macchina metasploitable, dopo 27 minuti la scansione è terminata evidenziando 11 vulnerabilità critiche, 5 vulnerabilità alte, 23 vulnerabilità basse.

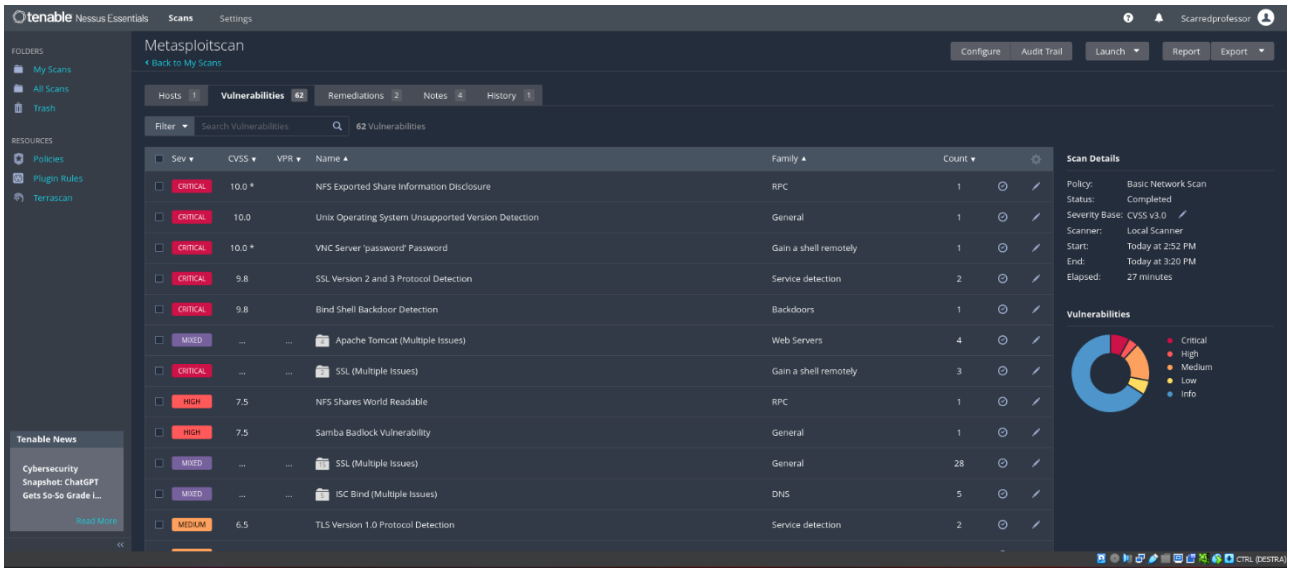
Il programma è in grado di stilare un report (che nello specifico è stato di 229 pagine) dove elenca le varie criticità ed è in grado di fornirci la soluzione oltre ad indicarci il fattore di rischio (se alto, medio, basso) lo score nel sistema CVSS(common vulnerability scoring system) ed informazioni sul plugin di Nessus che ha identificato la vulnerabilità.

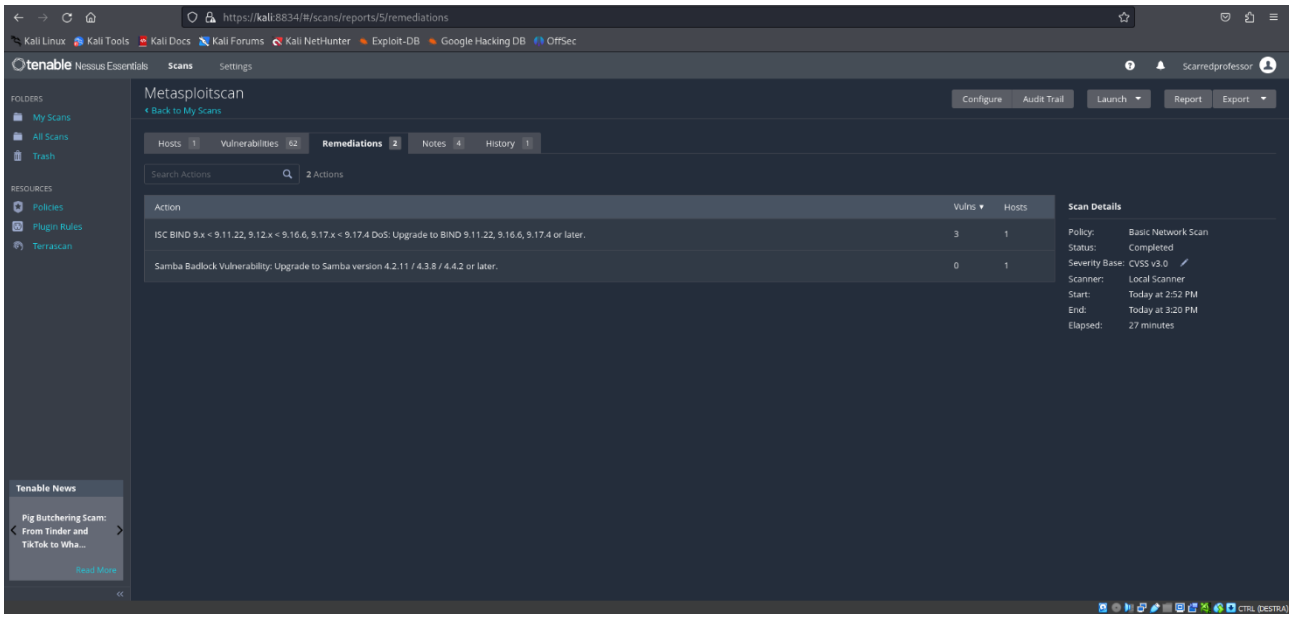
Il CVSS attribuisce un punteggio alle vulnerabilità basandosi su vari aspetti, divisi in tre gruppi principali:

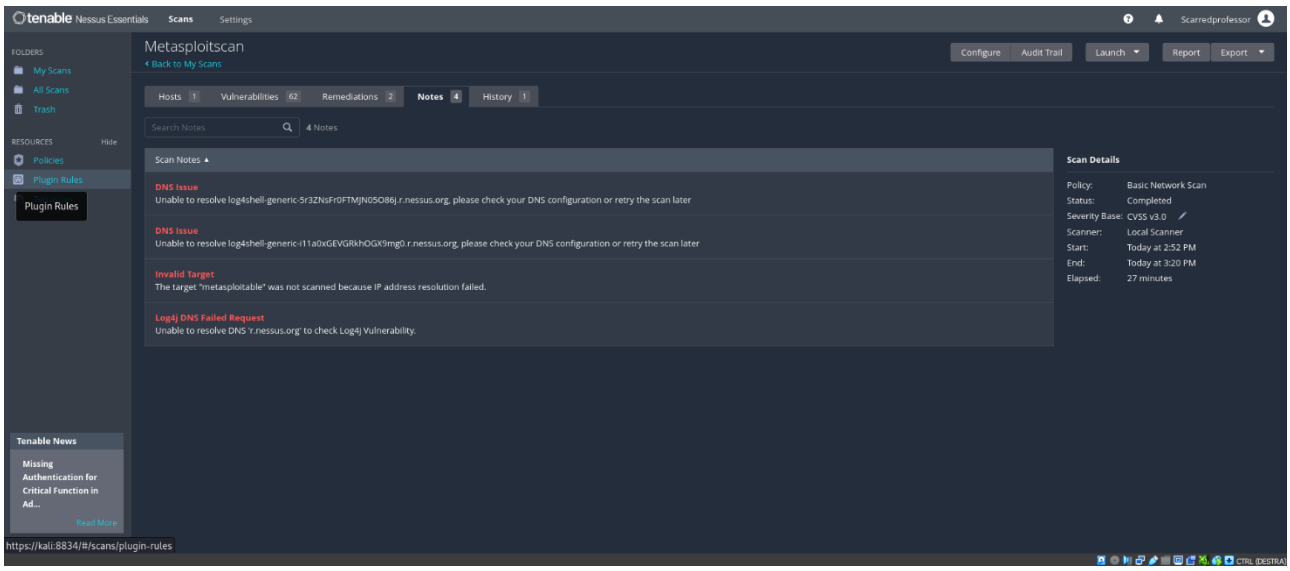
1. **Base Score (Punteggio Base):** Questo rappresenta la gravità intrinseca della vulnerabilità e è calcolato prendendo in considerazione svariati aspetti, tra cui la complessità dell'attacco richiesto, l'impatto sull'integrità, la disponibilità e la riservatezza dei dati. Questi aspetti sono ponderati in modo da ottenere un punteggio compreso tra 0 e 10, dove 10 rappresenta la gravità massima.
2. **Temporal Score (Punteggio Temporale):** Questa componente riflette la variabilità della vulnerabilità nel tempo. Ad esempio, può tener conto del livello di diffusione di patch o di soluzioni temporanee che possono ridurre il rischio.
3. **Environmental Score (Punteggio Ambientale):** Questo valuta l'impatto specifico della vulnerabilità nell'ambiente in cui si trova il sistema vulnerabile. Fattori come la criticità dei dati, il valore del sistema e la presenza di contromisure di sicurezza vengono presi in considerazione per calcolare questa componente.

I tre punteggi (Base, Temporale e Ambientale) sono combinati per ottenere un punteggio complessivo. Questo punteggio numerico aiuta gli esperti di sicurezza informatica, gli amministratori di sistema e altri professionisti a comprendere rapidamente la gravità di una vulnerabilità e a prendere decisioni informate sulla gestione del rischio.




tenable Nessus Essentials
Scans
Settings
Scarredprofessor
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Metasploitscan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
Notes 4
History 1
Filter
Search Vulnerabilities
62 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
CRITICAL 10.0 * NFS Exported Share Information Disclosure RPC 1
CRITICAL 10.0 Unix Operating System Unsupported Version Detection General 1
CRITICAL 10.0 * VNC Server 'password' Password Gain a shell remotely 1
CRITICAL 9.8 SSL Version 2 and 3 Protocol Detection Service detection 2
CRITICAL 9.8 Bind Shell Backdoor Detection Backdoors 1
MIXED Apache Tomcat (Multiple Issues) Web Servers 4
CRITICAL SSL (Multiple Issues) Gain a shell remotely 3
HIGH 7.5 NFS Shares World Readable RPC 1
HIGH 7.5 Samba Badlock Vulnerability General 1
MIXED SSL (Multiple Issues) General 28
MIXED ISC Bind (Multiple Issues) DNS 5
MEDIUM 6.5 TLS Version 1.0 Protocol Detection Service detection 2
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:52 PM
End: Today at 3:20 PM
Elapsed: 27 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Cybersecurity Snapshot: ChatGPT Gets So-So Grade i...
Read More


https://kali:8834/#/scans/reports/5/remediations
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
tenable Nessus Essentials
Scans
Settings
Scarredprofessor
Metasploitscan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
Notes 4
History 1
Search Actions
2 Actions
Action
Vulns
Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later. 3 1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later. 0 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:52 PM
End: Today at 3:20 PM
Elapsed: 27 minutes
Tenable News
Pig Butchering Scam: From Tinder and TikTok to Wha...
Read More


tenable Nessus Essentials
Scans
Settings
Scarredprofessor
Metasploitscan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
Notes 4
History 1
Search Notes
4 Notes
Scan Notes
DNS Issue
Unable to resolve log4shell-generic-5r3ZNsFr0FTMJN05O86j.r.nessus.org, please check your DNS configuration or retry the scan later
DNS Issue
Unable to resolve log4shell-generic-i11a0xGEVGRkhOGX9mg0.r.nessus.org, please check your DNS configuration or retry the scan later
Invalid Target
The target "metasploitable" was not scanned because IP address resolution failed.
Log4j DNS Failed Request
Unable to resolve DNS 'r.nessus.org' to check Log4j Vulnerability.
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:52 PM
End: Today at 3:20 PM
Elapsed: 27 minutes
Plugin Rules
Tenable News
Missing Authentication for Critical Function in Ad...
Read More
https://kali:8834/#/scans/plugin-rules