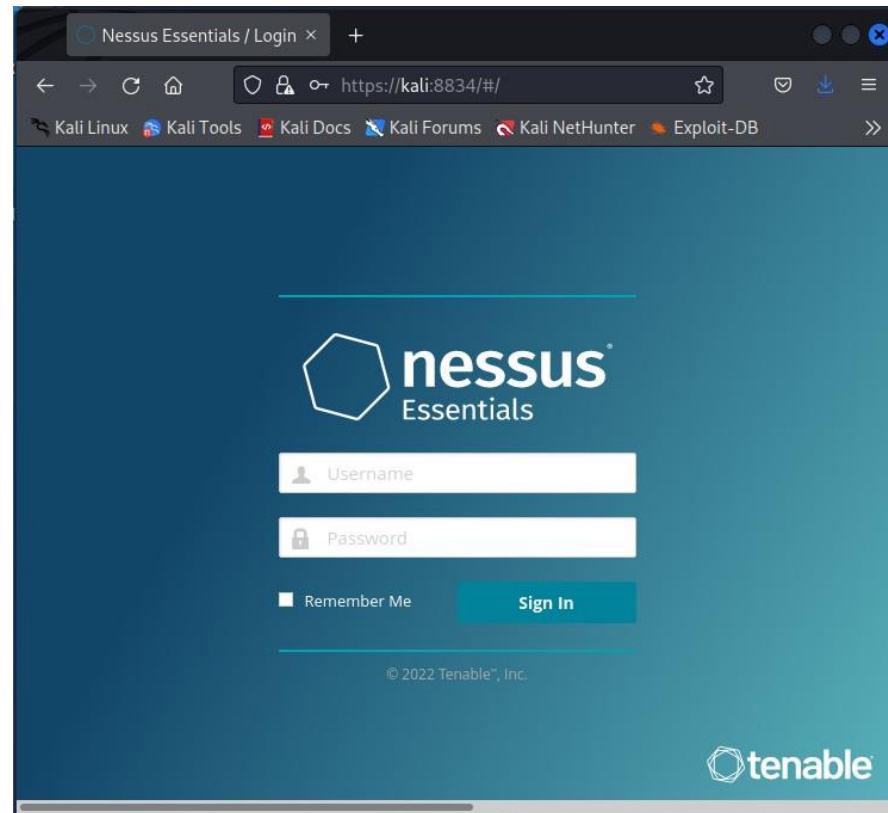


Vulnerability Assessment con Nessus da VM Kali su VM Metasploitable



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ /bin/systemctl start nessusd.service  
  
(kali@kali)-[~]  
$
```



Vulnerability Assessment con Nessus

Da VM Kali, attraverso il vulnerability scanner Nessus, si analizzano le vulnerabilità della VM Metasploable, avviando, prima il demone da terminale con il comando: `/bin/systemctl start nessusd.service`, come mostrato nell'immagine in alto e, successivamente, come mostrato nell'immagine in basso, tramite il browser si accede alla sua Web GUI attraverso l'indirizzo: `https://kali:8834/#/`, con le proprie credenziali.

Scan Templates

[← Back to Scans](#)

Scanner

Search Library



DISCOVERY

**Host Discovery**

A simple scan to discover live hosts and open ports.

VULNERABILITIES

**Basic Network Scan**

A full system scan suitable for any host.

**Advanced Scan**

Configure a scan without using any recommendations.

**Advanced Dynamic Scan**

Configure a dynamic plugin scan without recommendations.

**Malware Scan**

Scan for malware on Windows and Unix systems.

**Mobile Device Scan**

Assess mobile devices via Microsoft Exchange or an MDM.

**Web Application Tests**

Scan for published and unknown web vulnerabilities using Nessus Scanner.

**Credentialed Patch Audit**

Authenticate to hosts and enumerate missing updates.

**Intel AMT Security Bypass**

Remote and local checks for CVE-2017-5689.

Vulnerability Assessment con Nessus

All'interno della Web GUI, cliccando sul pulsante *New Scan*, si avrà accesso ai modelli di scansione da effettuare.

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: VulnerabilityAssessment

Description: Vulnerability test VM Metasploitable

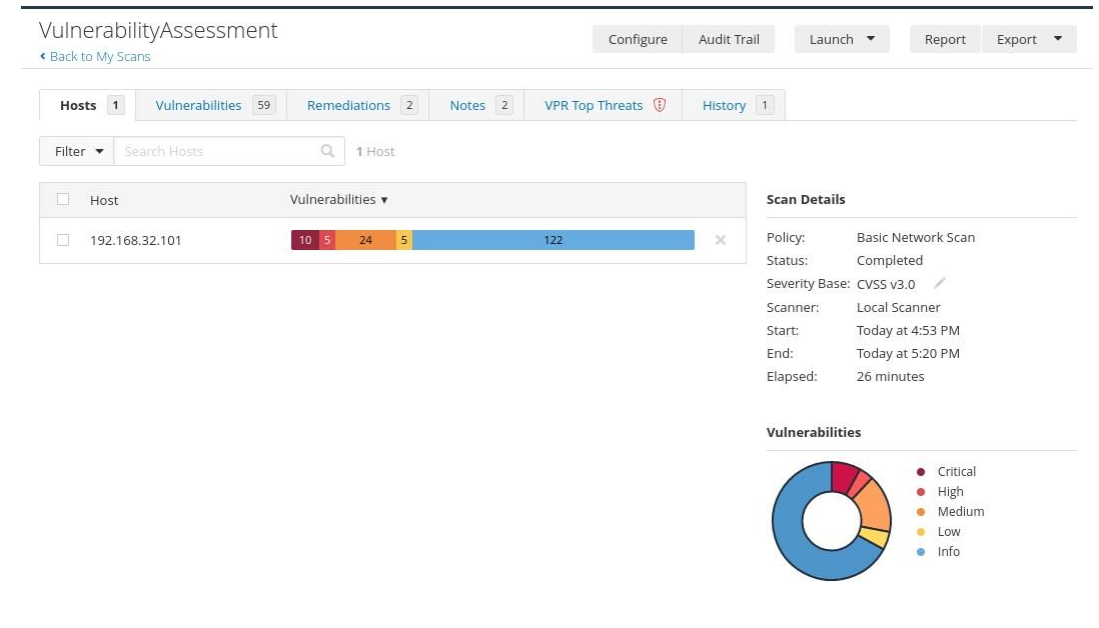
Folder: My Scans

Targets: 192.168.32.101

Upload Targets [Add File](#)

Save

Cancel



Vulnerability Assessment con Nessus

Per una semplice scansione di base, basta inserire solo poche, fondamentali, informazioni, come mostrate nell'immagine a sinistra e, a scansione terminata, si avrà un resoconto di essa, come mostrato nell'immagine a destra, da poter scaricare in modo dettagliato.

Vulnerability Assessment con Nessus

Link report dirigente: <https://github.com/torlxx/WEEK5/blob/main/Report%20dirigente.pdf>

Link report tecnico: <https://github.com/torlxx/WEEK5/blob/main/Report%20tecnico.pdf>

Link report tre vulnerabilità di alto livello: <https://github.com/torlxx/WEEK5/blob/main/Report%20tre%20vulnerabilit%C3%A0%20di%20alto%20livello.pdf>