Day 8 – Vulnerability Scanning with Nessus Essentials

# What is Vulnerability Scanning?

Vulnerability scanning is an automated process used to proactively identify security weaknesses in systems, networks, or applications. It involves scanning devices, applications, and services to detect known vulnerabilities such as outdated software, missing patches, or misconfigurations.  
  
These scans are a key component of vulnerability management and cybersecurity hygiene, helping organizations mitigate risks before they can be exploited by attackers.

# Types of Vulnerability Scans

|  |  |  |  |
| --- | --- | --- | --- |
| Scan Type | Description | Access Level | Purpose |
| External Scans | Target externally-facing IP addresses to identify vulnerabilities in perimeter and cloud systems. | Public-facing | Assess security posture from an external perspective. |
| Internal Scans | Conducted within the organization's network to find vulnerabilities in internal systems. | Internal network access | Identify risks that could be exploited after a breach. |
| Unauthenticated Scans | Performed without valid credentials, relying on publicly accessible information. | No credentials required | Detect basic weaknesses visible to external attackers. |
| Authenticated Scans | Use valid credentials to access deeper layers of the system. | Valid user credentials | Uncover hidden vulnerabilities and compliance issues. |

# Tool Used: Nessus Essentials

Nessus Essentials is a free vulnerability scanner by Tenable, ideal for students and professionals to perform deep vulnerability assessments on up to 16 IPs.

# Installation of Nessus Essentials on Kali Linux

1. Download Nessus:  
 - Visit https://www.tenable.com/products/nessus/nessus-essentials  
 - Choose the Debian/Kali .deb package.

2. Navigate to the Download Directory:  
 cd Downloads  
 ls

3. Install Nessus:  
 sudo dpkg -i Nessus-10.x.x-debian6\_amd64.deb

4. Start the Nessus Service:  
 sudo systemctl start nessusd.service

5. Access Nessus in Browser:  
 - Visit: https://localhost:8834  
 - Click Advanced → Proceed to localhost

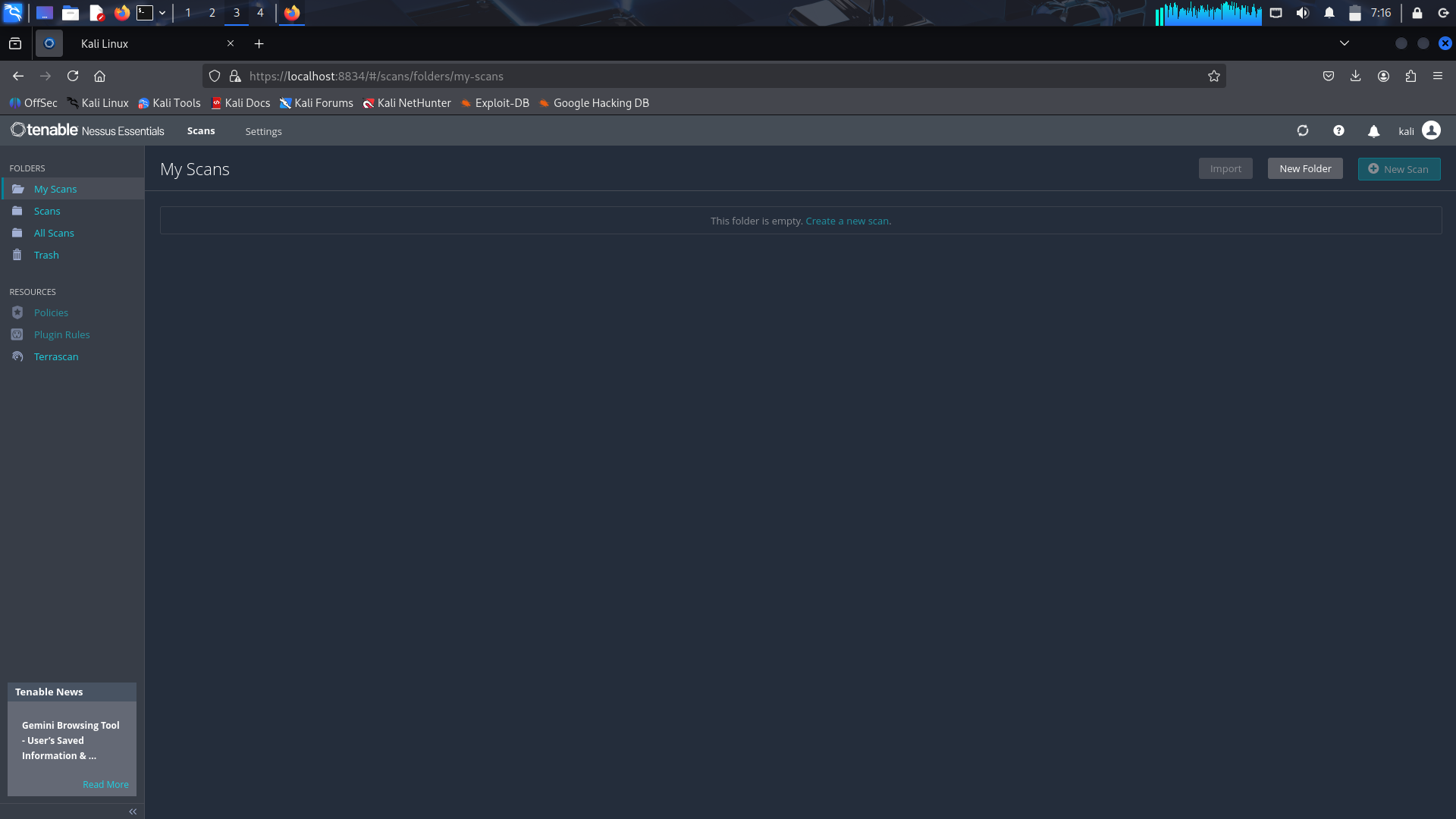
6. Register Nessus Essentials:  
 - Select Nessus Essentials  
 - Enter name and email, receive activation code  
 - Create a local Nessus account

7. Explore the Nessus Dashboard:  
 - Log in and explore scan templates, vulnerabilities, and results

# Practical Use Case of Nessus:

- Created a Basic Network Scan  
- Added a target IP address  
- Started a scan and reviewed results  
- Nessus showed categorized vulnerabilities with CVEs, severity ratings, descriptions, and remediation steps

# Dashboard:



# Outcome of Day 8

- Understood the concept and types of vulnerability scanning.  
- Installed and configured Nessus Essentials on Kali Linux.  
- Performed a vulnerability scan against a target.  
- Interpreted scan results to understand system weaknesses.