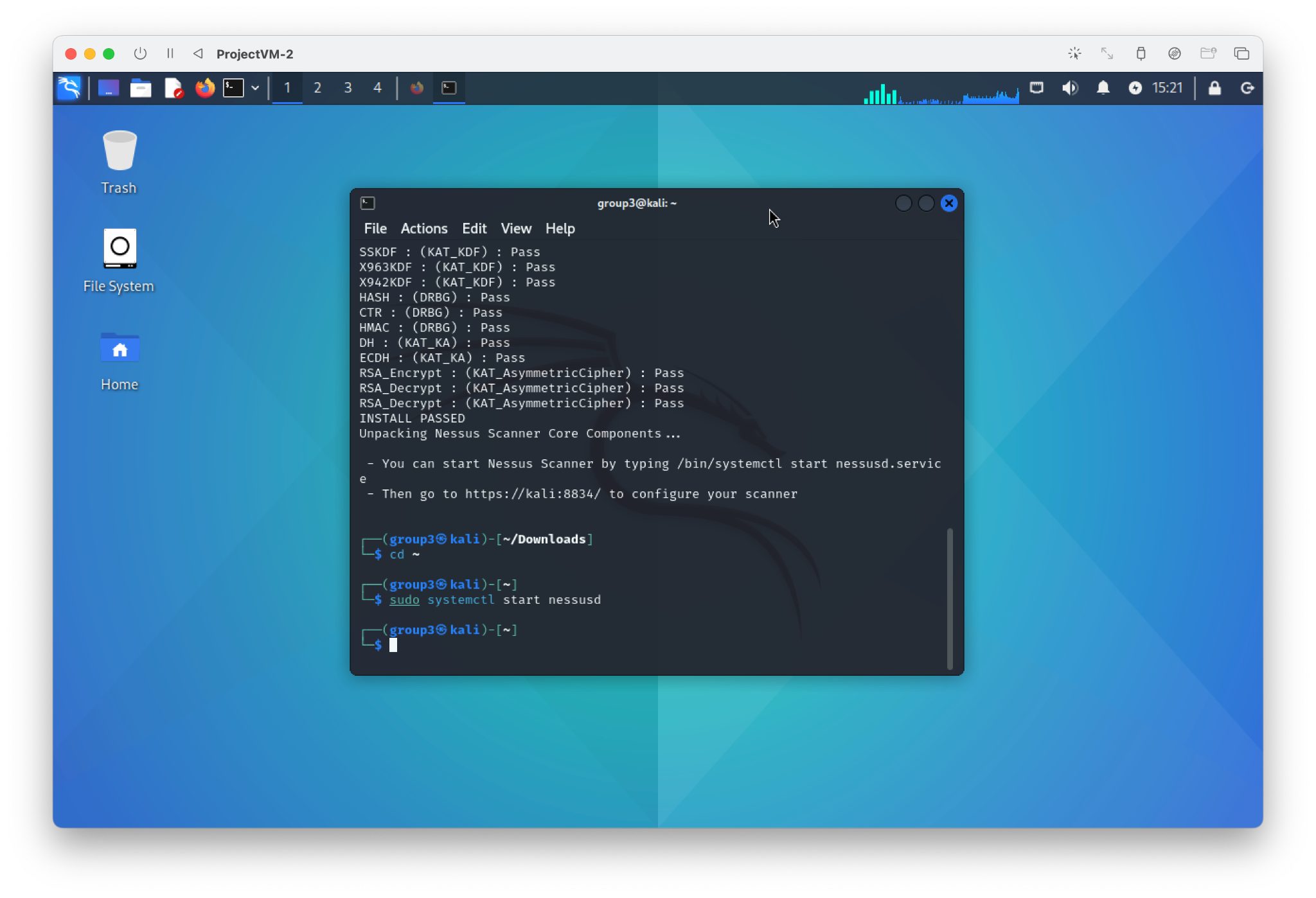
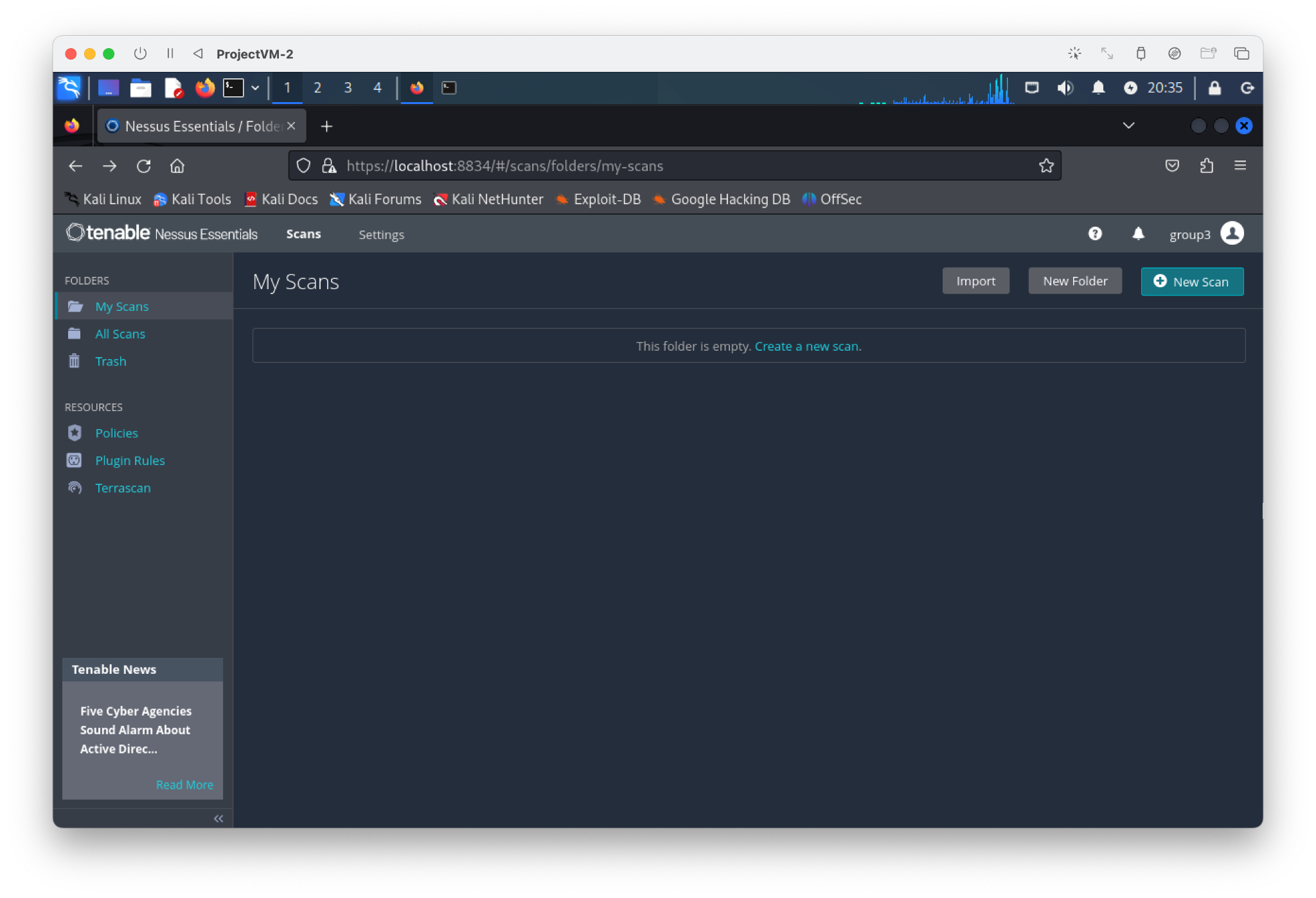
# 1. Scan process (suppose after compiling plugin)

## 1. Start Nessus

* sudo systemctl start nessusd

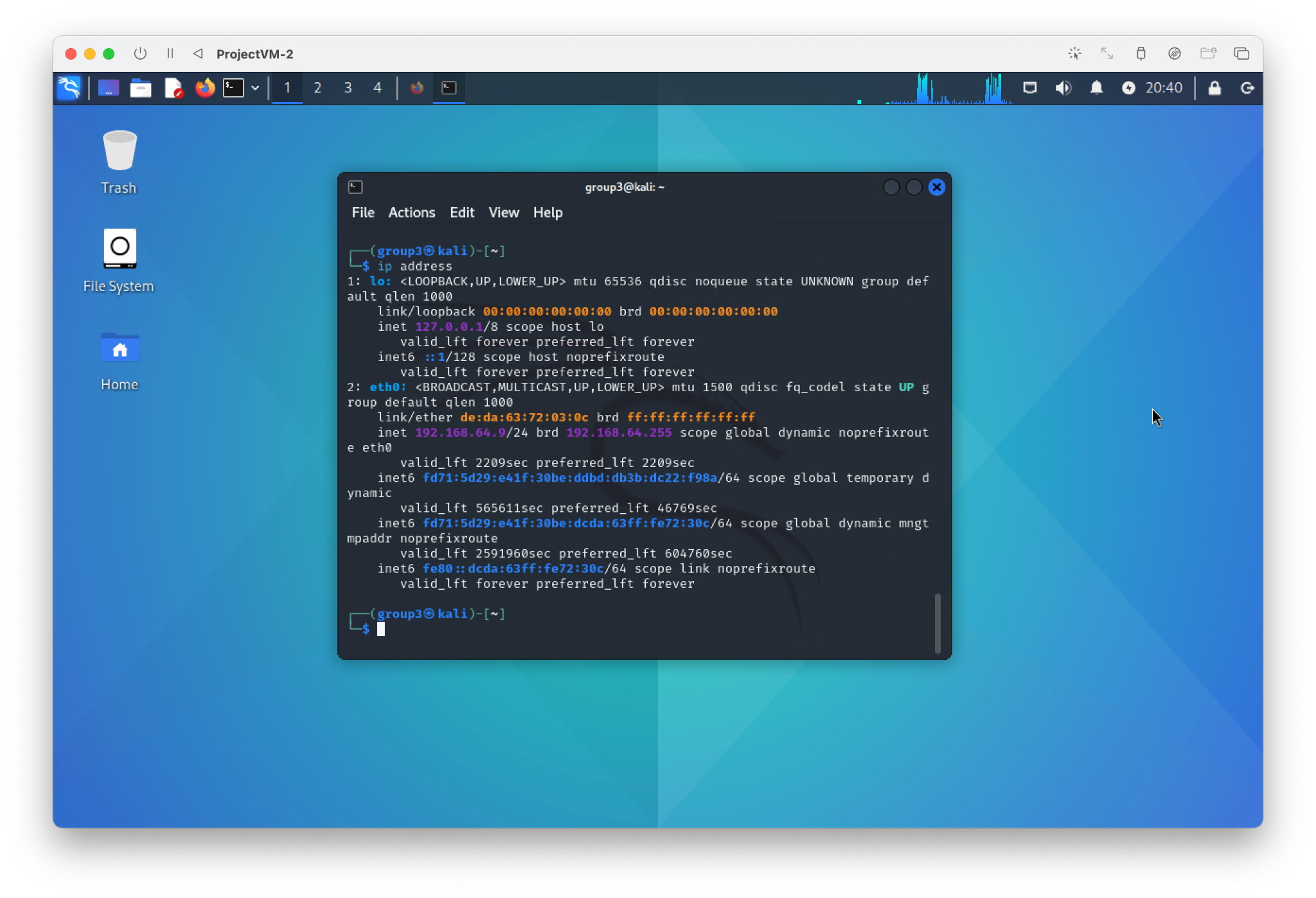


## 2. Go to the “<https://localhost:8834>” website



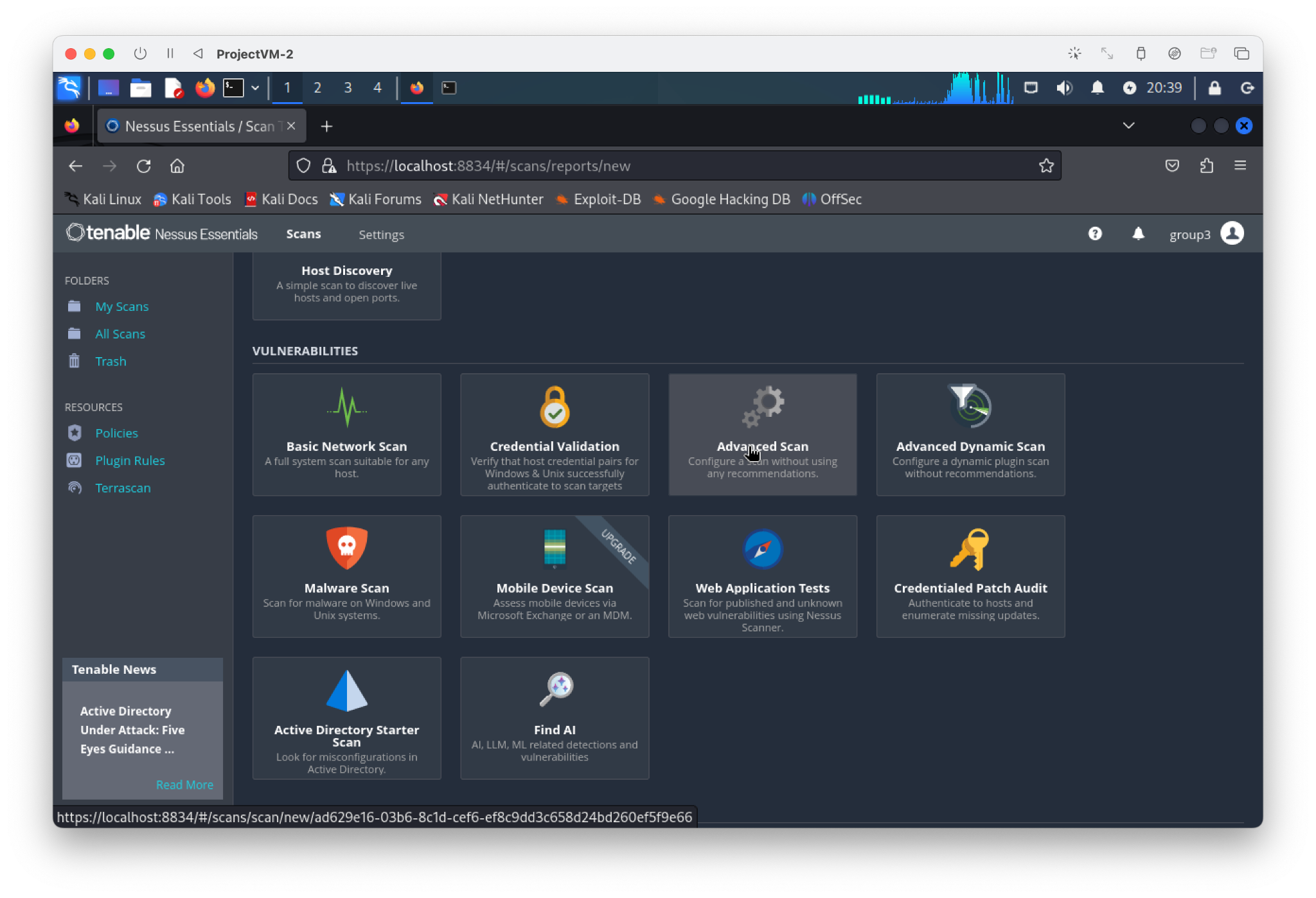
## 3. Check IP address

* ip address

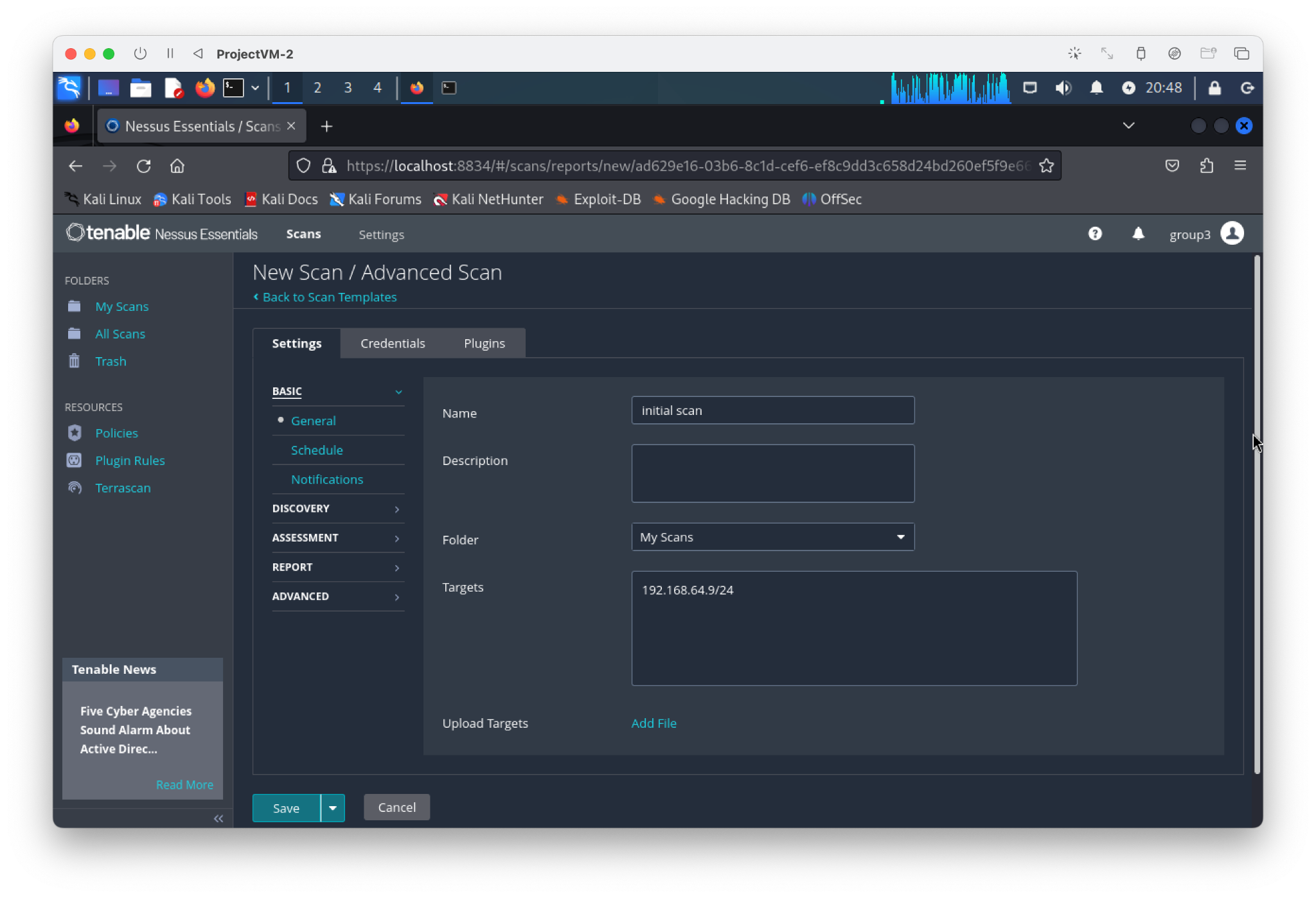


## 4. Create new scan

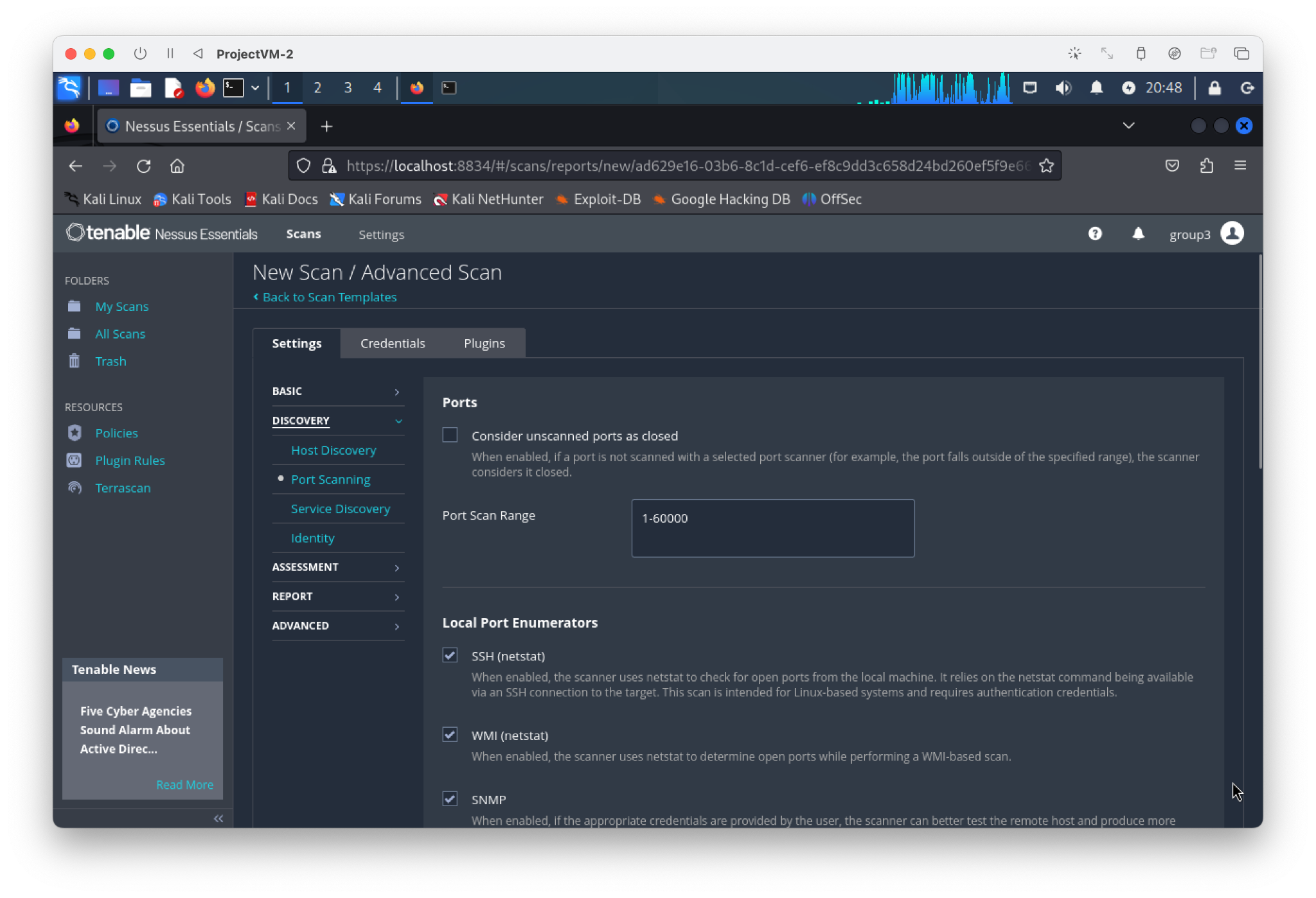
* Select scan type



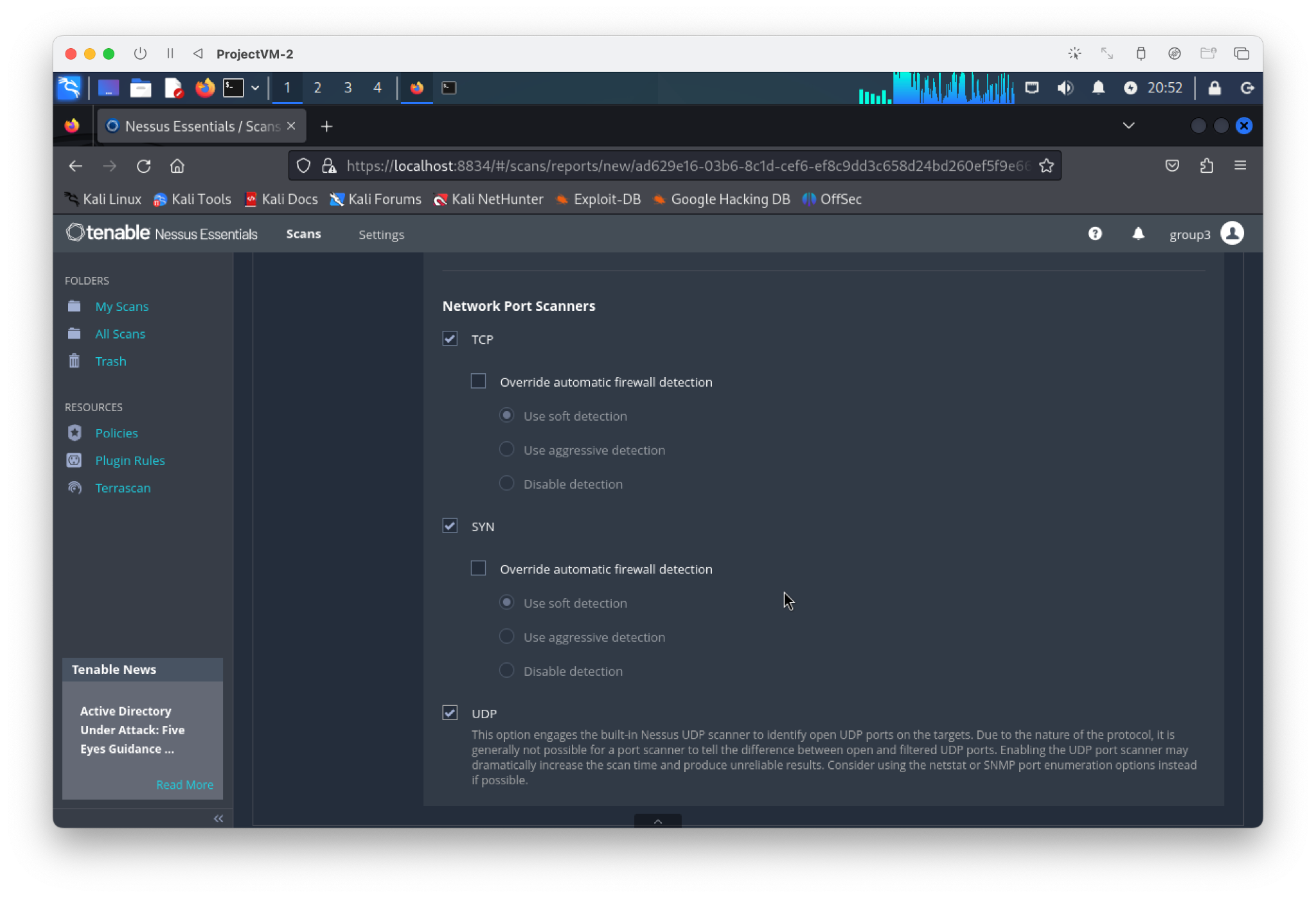
* set target



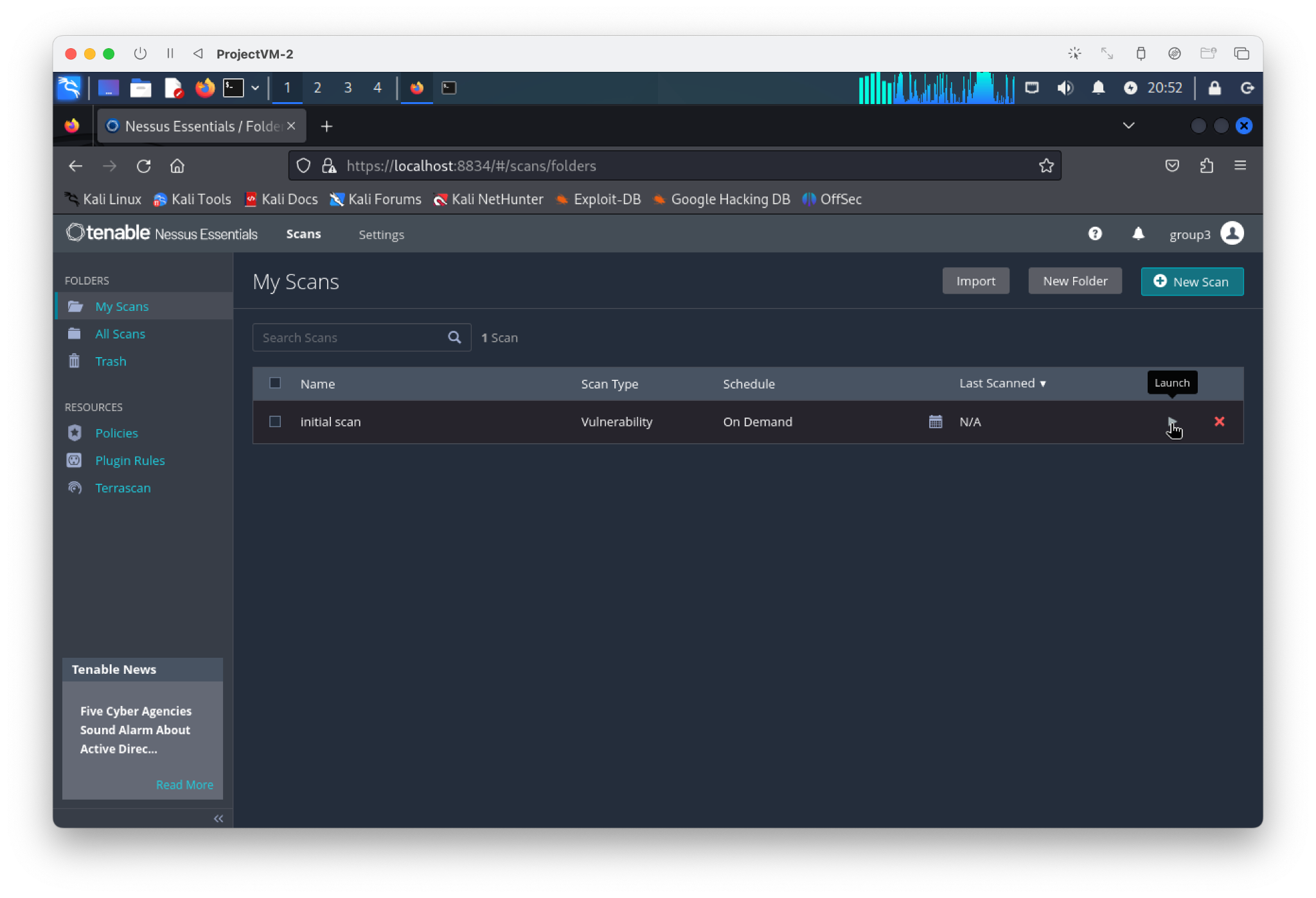
* set port



* check TCP & UDP (for

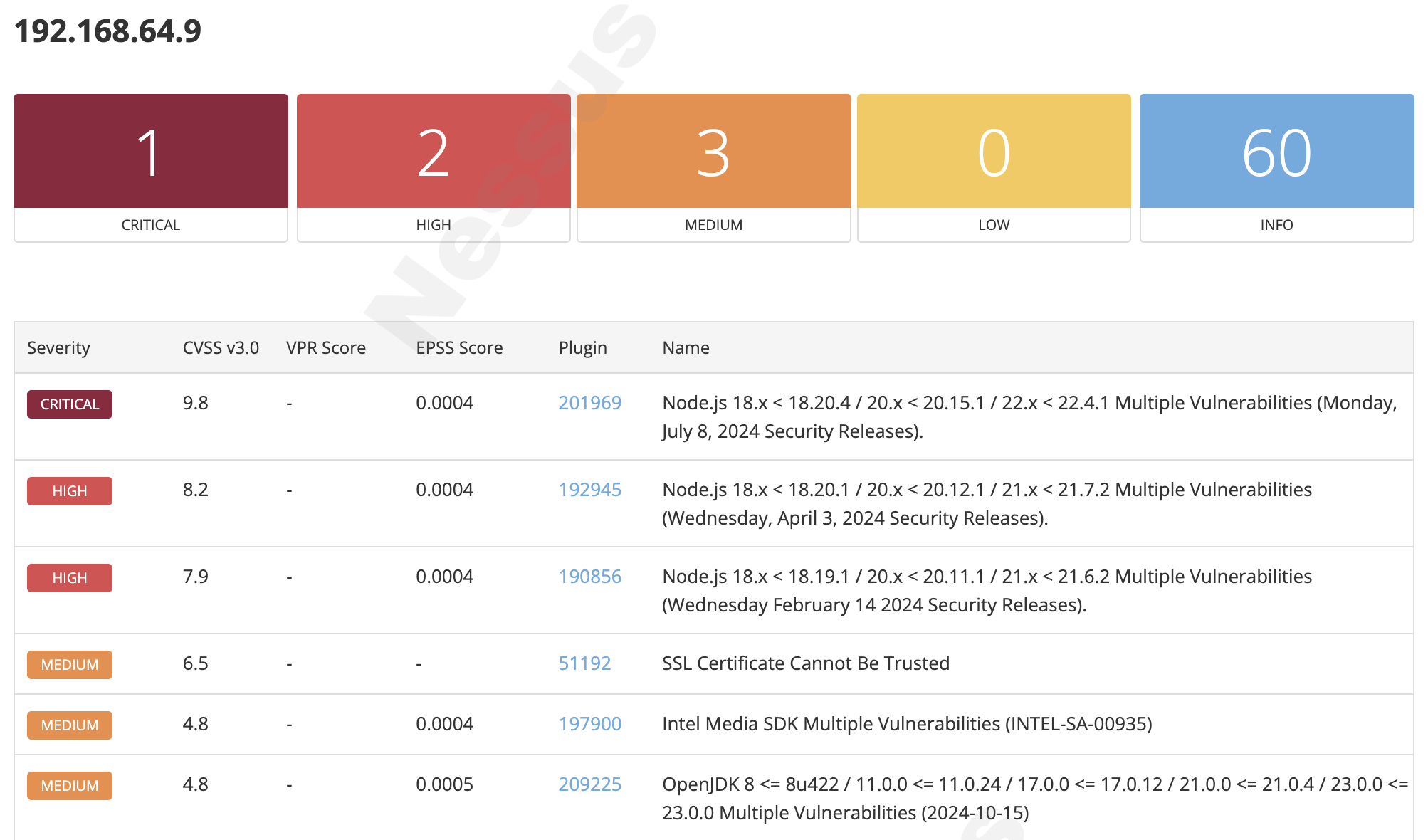


## 5. Launch the scan



# 2. Analyzation of the initial scan

## 1. Scan Result



## 2. Vulnerabilities

### Node.js

A vulnerability was detected in the Node.js version included by default in Kali Linux. It may be an outdated version or a specific version maintained for OS stability, which can result in vulnerabilities being present.

### SSL

A vulnerability was detected in the SSL certificate present in Kali Linux, indicating it is not trusted. If the certificate is issued by the server itself, Nessus may classify it as untrusted.

### Intel Media SDK

A vulnerability was detected in the video processing library included by default in Kali Linux. It may be an outdated version that has not been updated to the latest release.

### OpenJDK 8

A vulnerability was detected in the OpenJDK included in the default Java runtime environment of Kali Linux. This can occur if it has not been updated to the latest version.