EXPERIMENT NUMBER 9

Name of Student: Sangeet Agrawal	PRN: 21070122140	Section: CS-B3

Title: Report on SIEM SPLUNK and NESSUS based on workshop conducted on 13-14 September 2024.

Objective: To make students understand SIEM SPLUNK and NESSUS tools.

Theory:

1. SIEM SPLUNK:

Splunk is a tool for Security Information and Event Management (SIEM). It collects, monitors, and analyzes data from various sources, like logs and servers, to help detect security threats in real time.

- Data Collection: Gathers data from different sources like servers and apps.
- Real-Time Monitoring: Monitors security events as they happen, enabling quick detection.
- Alerts and Dashboards: Custom dashboards and alerts help visualize data and notify you of issues.
- Incident Response: Helps investigate security incidents by allowing fast searches through logs.

2. NESSUS:

Nessus is a vulnerability scanner used to detect security weaknesses in systems.

- Vulnerability Scanning: Identifies known vulnerabilities like outdated software or misconfigurations.
- Compliance Checks: Ensures systems meet security standards like PCI-DSS.
- Reports: Provides detailed reports on vulnerabilities and fixes.
- Plugins: Regular updates help detect new vulnerabilities.

Installation:

1. **Installing SPLUNK on macOS Apple Silicon:**

   SPLUNK wasn't working on either the Windows or Linux OS of the college desktops, nor on my laptop.

2. **Installing NESSUS on macOS Apple Silicon:**

Nessus has a native macOS installer, and it works well with Apple Silicon. Follow these steps to install and set it up.

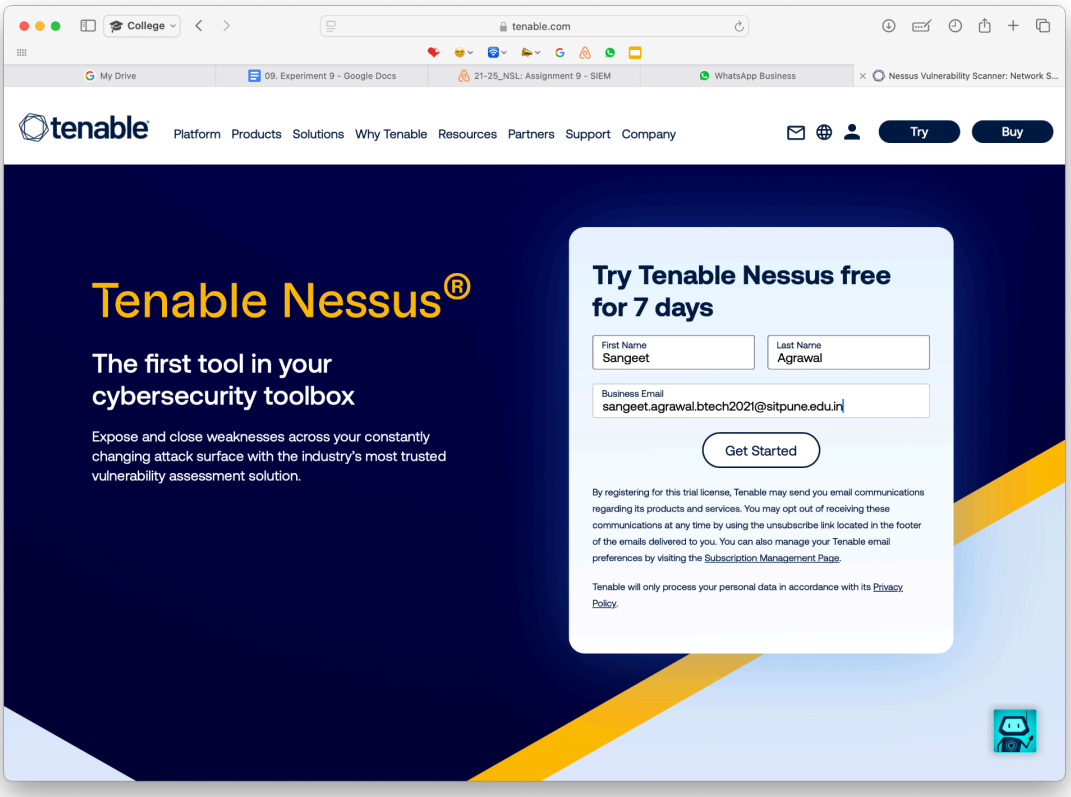
Steps:

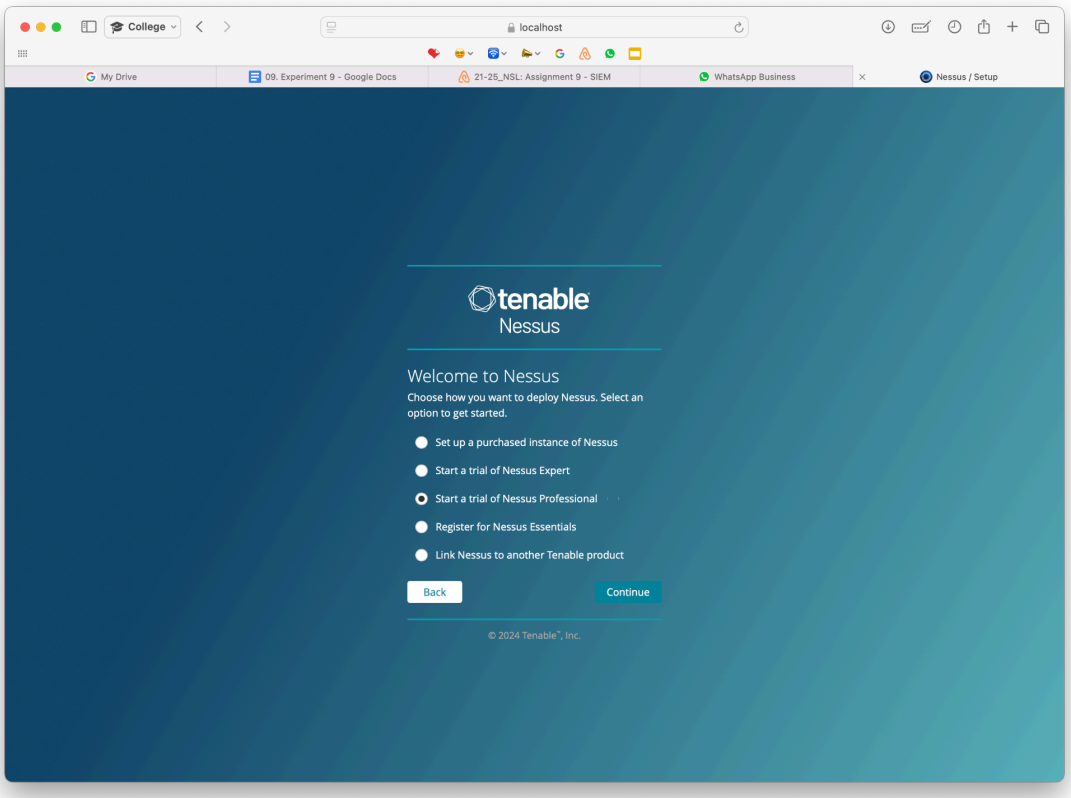
1. Download Nessus for macOS:
   a. Go to the official Nessus download page: Nessus Downloads.
   b. Choose the macOS version and download the installer package (.pkg file).
2. Install Nessus:
   a. Open the .pkg file and follow the installation prompts.
3. Start Nessus:
   a. Once installed, open Terminal and start the Nessus service:

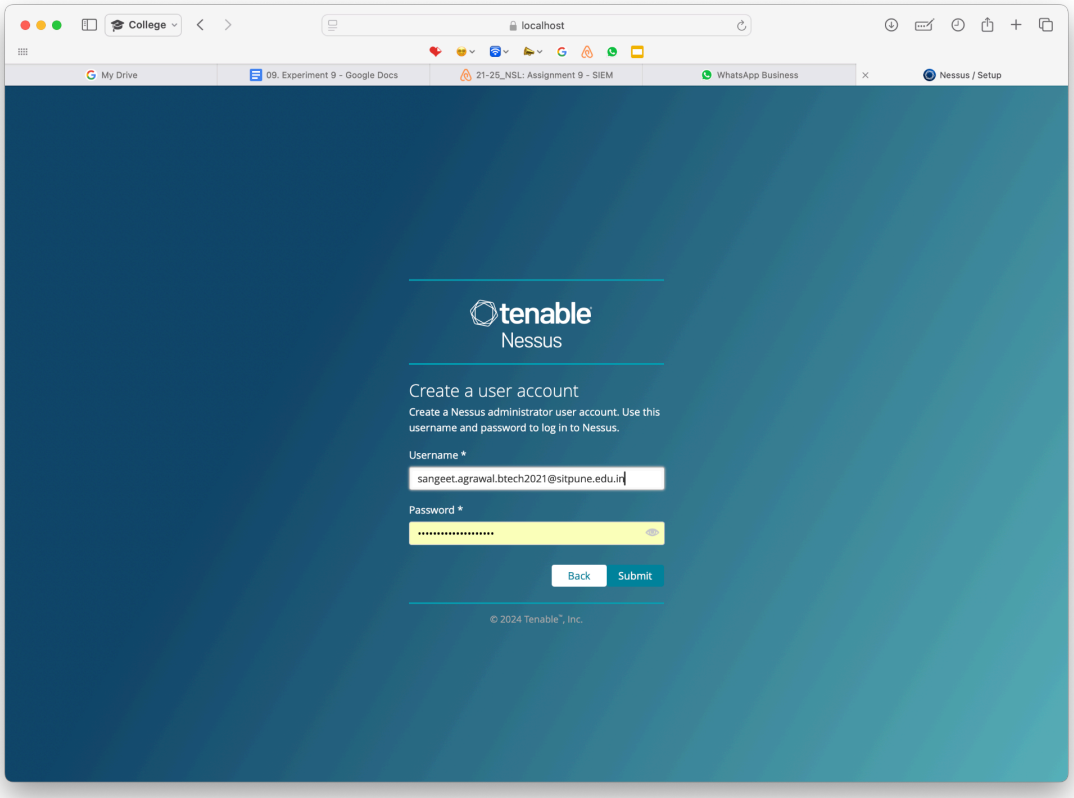
```
sudo /Library/Nessus/run/sbin/nessusd
```

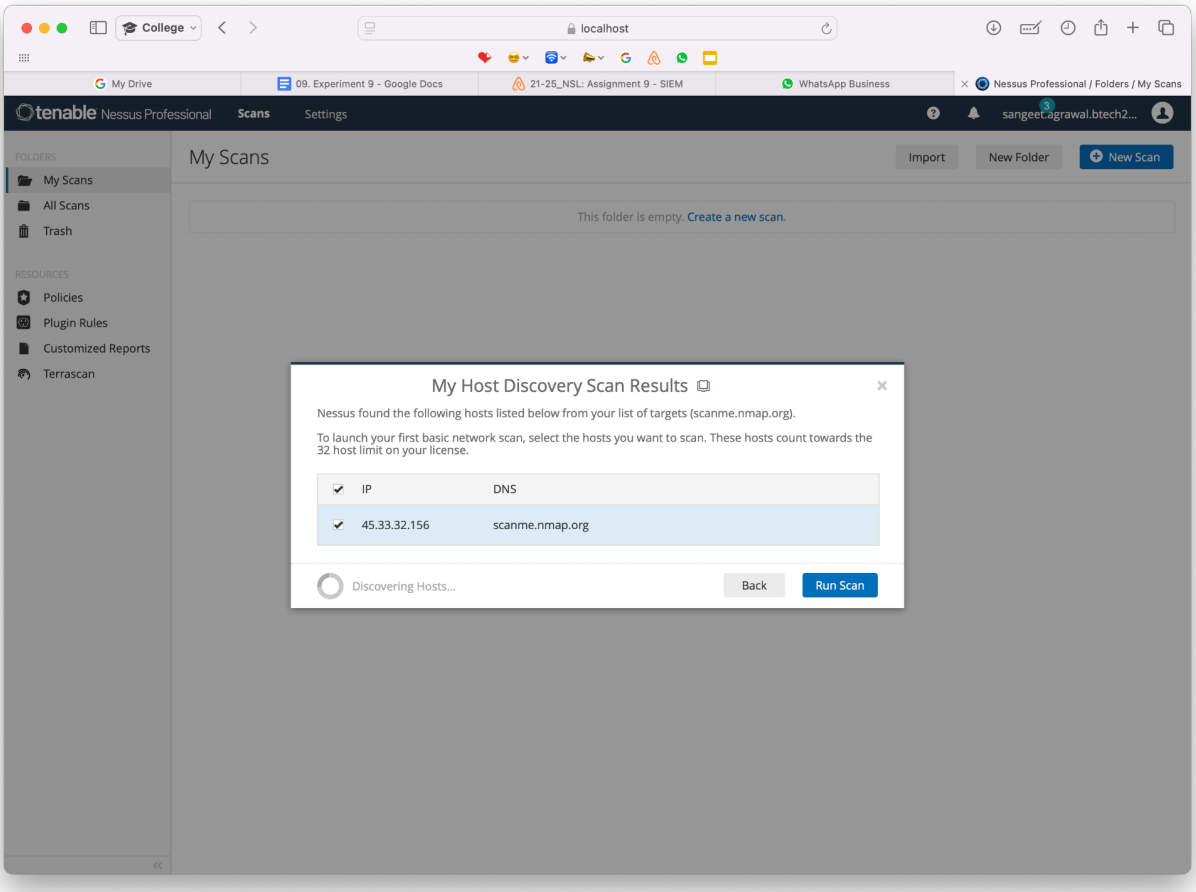
4. Access Nessus:
   Open your browser and go to https://localhost:8834. Follow the setup steps to configure your account and run your first scan.

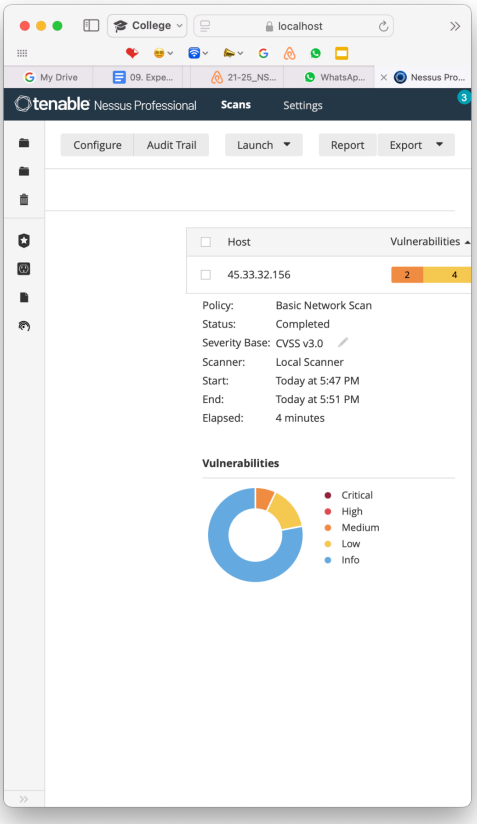
Screenshots for Nessus:

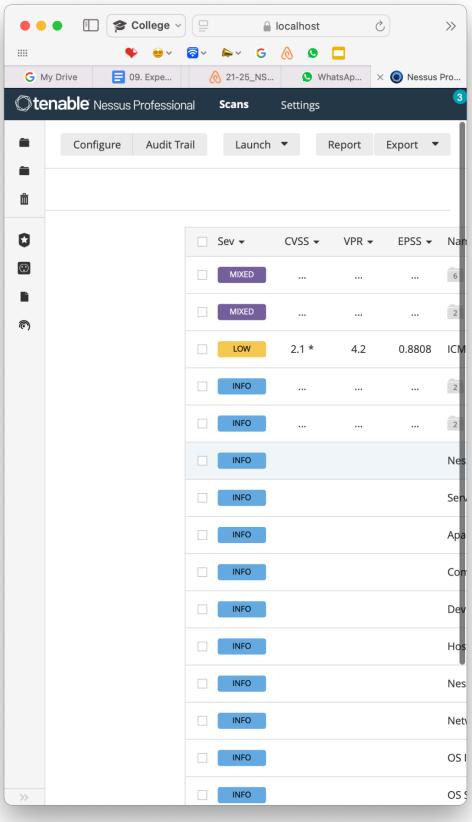





College
localhost
My Drive
09. Experiment 9 - Google Docs
21-25_NSL: Assignment 9 - SIEM
WhatsApp Business
Nessus / Setup
tenable
Nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
sangeet.agrawal.btech2021@sitpune.edu.in
Password *
Back
Submit
© 2024 Tenable™, Inc.


College
localhost
My Drive
09. Experiment 9 - Google Docs
21-25_NSL: Assignment 9 - SIEM
WhatsApp Business
Nessus Professional / Folders / My Scans
tenable Nessus Professional
Scans
Settings
sangeet.agrawal.btech2...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Terrascan
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
My Host Discovery Scan Results
Nessus found the following hosts listed below from your list of targets (scanme.nmap.org).
To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 32 host limit on your license.
IP
DNS
45.33.32.156
scanme.nmap.org
Discovering Hosts...
Back
Run Scan





Conclusion:

The workshop on SIEM SPLUNK and NESSUS provided valuable hands-on experience with two key tools in the cybersecurity domain. Splunk's log monitoring and real-time analysis capabilities, coupled with Nessus's vulnerability scanning, offer comprehensive solutions for enhancing system security.

Note: Students are suggested to use Linux OS-based tools or free Windows OS-based tools.