

Ex. No. 4	Vulnerability Scanning using Nessus
Date of Exercise	29/08/23

Aim:

To scan a target IP and raise an alert if it discovers any vulnerabilities using Nessus, a security vulnerability scanning tool.

Description:

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it. It works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

Algorithm:

- Download Nessus and execute the following commands
 1. `sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb`
 2. `sudo systemctl start nessusd.service`
 3. `sudo systemctl status nessusd.service`
- Open link in Firefox

- Create Nessus Essentials account and download
- Click Basic Network Scan
- Create new scan and click Basic Network scan
- Configure Settings and save
- Launch Scan
- Viewing the Results

Output:

Welcome to Nessus Essentials ✕

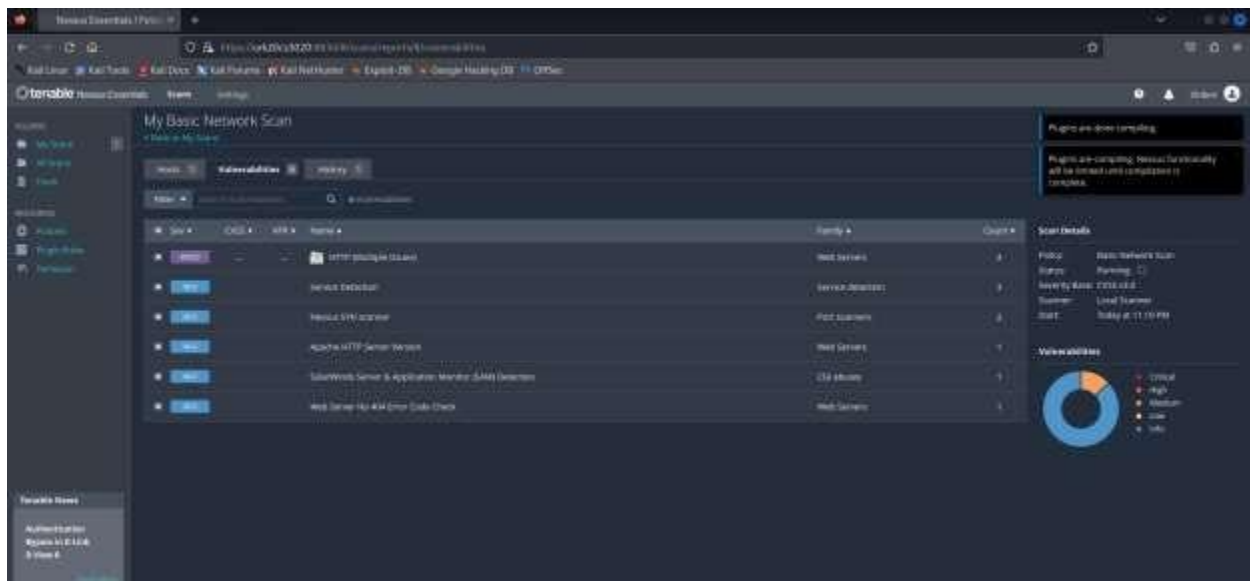
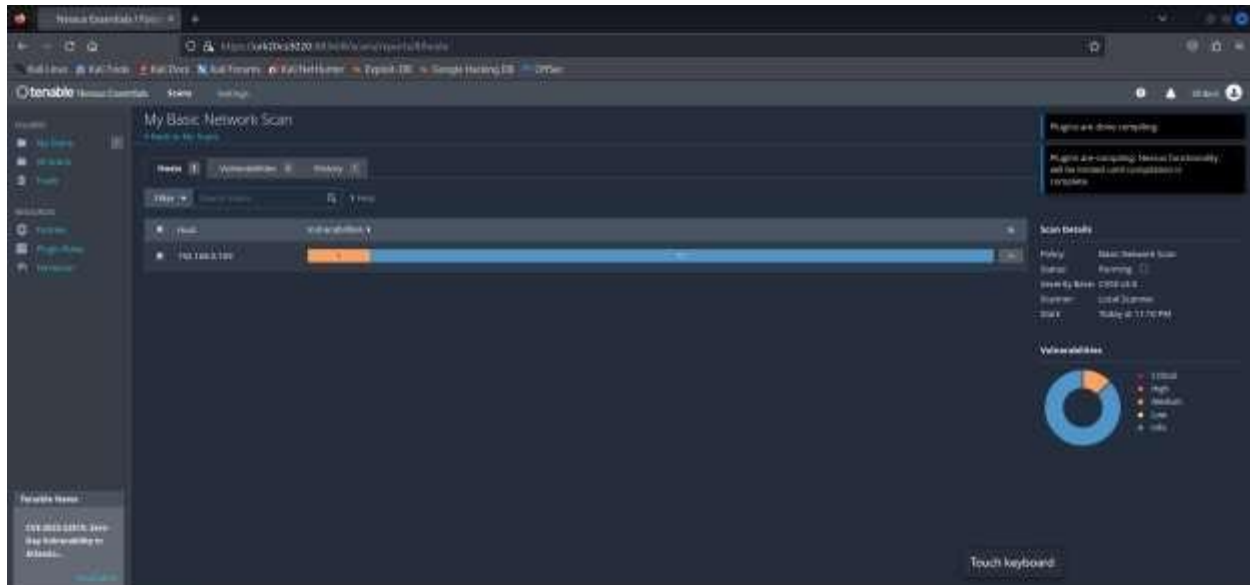
To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

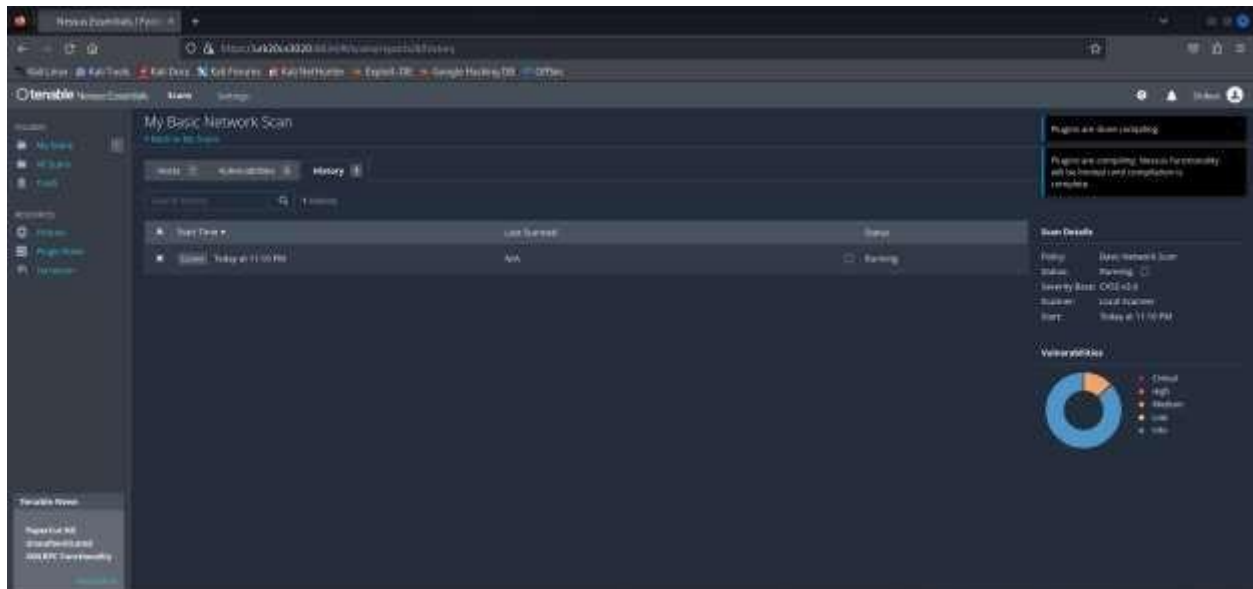
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

karunya.edu

Close Submit



**Result:**

The given experiment has been carried out and the output has been verified successfully.