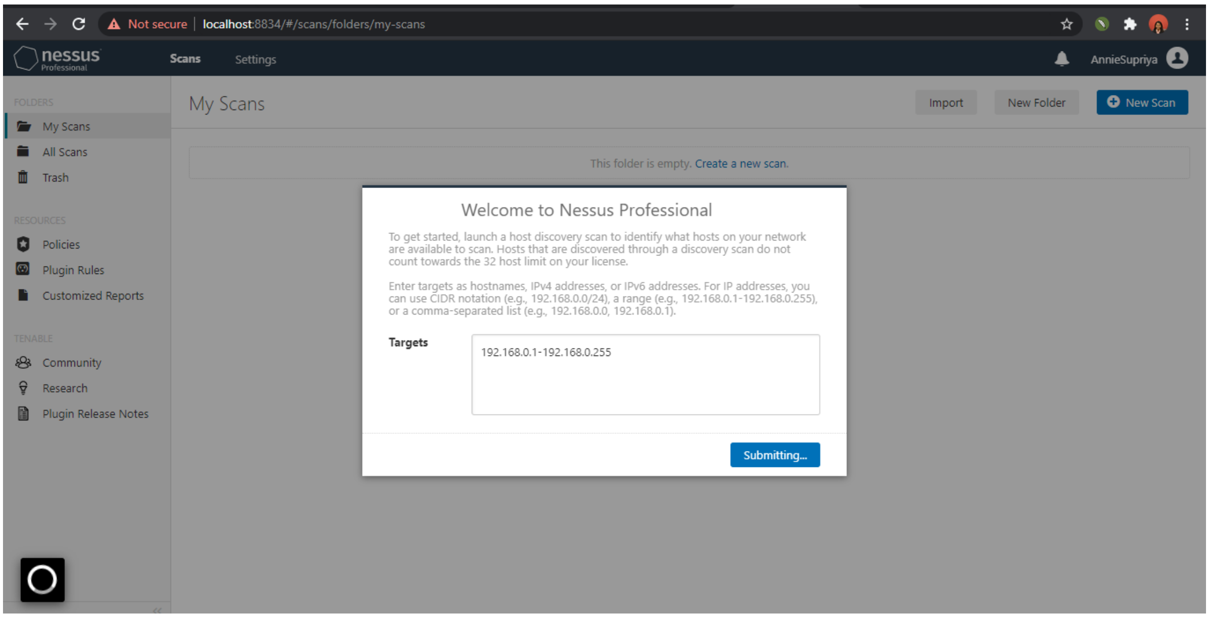
# OUTSTANDING-3

Using Nessus Professional tool to scan the entire OS and identifying the open ports.

**Step-1:** Downloading the Nessus Professional tool from “Tenable” and login.



My Scans

This folder is empty. Create a new scan.

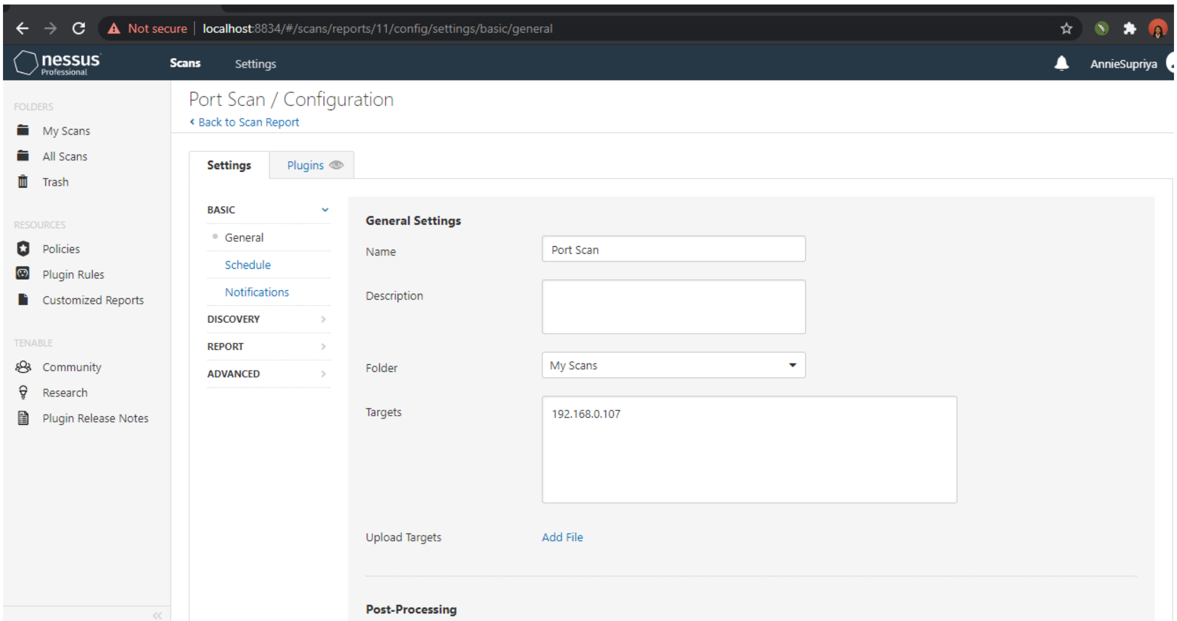
Welcome to Nessus Professional

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 32 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: 192.168.0.1-192.168.0.255

**Step-2:** Configuring a port scan in-order to find the open ports.



Port Scan / Configuration

General Settings

Name: Port Scan

Description:

Folder: My Scans

Targets: 192.168.0.107

Upload Targets: Add File

Post-Processing

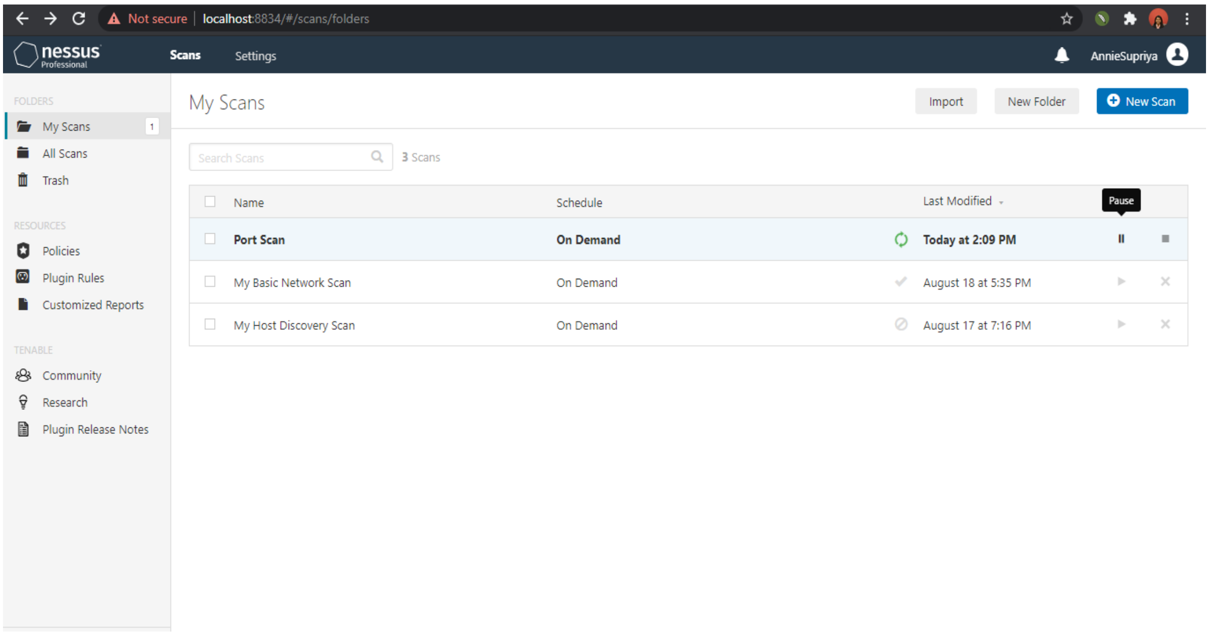
Opening a new scan and selecting the host discovery option.

Providing a name for the scan. Giving out the range of targets which are required for the analysis of the scan. The range of IP addresses are from 192.168.0.1 to 192.168.0.255.

Then in the scanning section we are choosing the open ports scanning for all the ports.

Saving the port scan for later use.

**Step-3:** Launching the port scan from the host computer for that IP range in the configured scan.

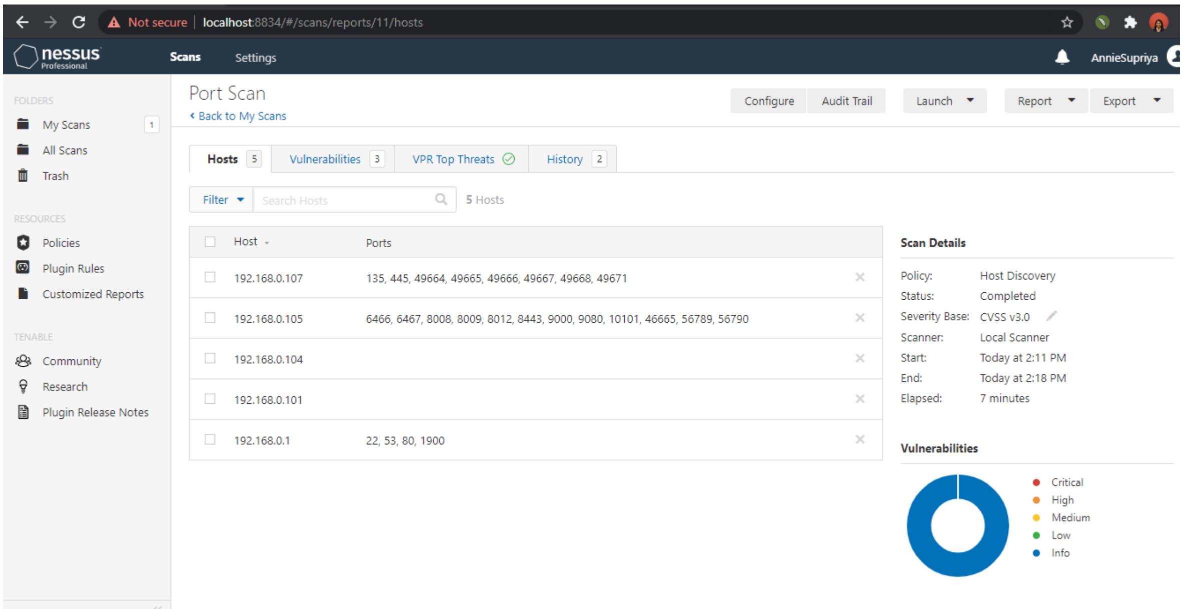


My Scans

3 Scans

| | Name | Schedule | Last Modified |
|---|---|---|---|
| □ | **Port Scan** | **On Demand** | **Today at 2:09 PM** |
| □ | My Basic Network Scan | On Demand | August 18 at 5:35 PM |
| □ | My Host Discovery Scan | On Demand | August 17 at 7:16 PM |

**Step-4:** The Scan is completed with the ports mentioned for the hosts.



Port Scan

5 Hosts

| | Host | Ports |
|---|---|---|
| □ | 192.168.0.107 | 135, 445, 49664, 49665, 49666, 49667, 49668, 49671 |
| □ | 192.168.0.105 | 6466, 6467, 8008, 8009, 8012, 8443, 9000, 9080, 10101, 46665, 56789, 56790 |
| □ | 192.168.0.104 | |
| □ | 192.168.0.101 | |
| □ | 192.168.0.1 | 22, 53, 80, 1900 |

**Scan Details**

| | |
|---|---|
| Policy: | Host Discovery |
| Status: | Completed |
| Severity Base: | CVSS v3.0 |
| Scanner: | Local Scanner |
| Start: | Today at 2:11 PM |
| End: | Today at 2:18 PM |
| Elapsed: | 7 minutes |

**Vulnerabilities**

There are 5 host IP addresses in the provided range. The ports are mentioned for each of the host address. Each of the ports are specifically used for certain applications for a desired output.

**The List of applications and its corresponding ports which are used by those applications also mentioning the Network protocol it uses.**

1. Port 53
   Port 53 is used by the protocol of TCP and UDP for Domain Name System(DNS). Applications using Cisco Webex Team and Kerio Personal Firewall(KPF) 2.1.4. KPF has a default rule to accept incoming packets from DNS, which allows remote attackers to bypass the firewall filters via packets with a source port of 53.
2. Port 80
   This port is generally used for Hypertext Transfer Protocol using the protocol of TCP and UDP. The applications which are used under this port are :
   ATT Remote Monitor, BT Homesafe, Dungeons and Dragons, Eyeon, Gadspot IP, Halo, Lord of the Rings, Lorex IP Surveillance, Rise of Legends, etc.
3. Port 10070
   The applications that use this port is Socom, Socom 2 and Sony Playstation 3. It uses both UDP and TCP separately for certain application according to its usage.
4. Port 1990
   Cisco STUN Priority 1 is the application using this particular port. Guaranteed communication over TCP port 1990 is the main difference between TCP and UDP.
5. Port 8443
   Port 8443 for the network protocol of TCP. The applications used are Tanium Server, Client and Appliance & https port for controller GUI/API. A remote attacker could exploit this vulnerability using an HTTP POST request over port 8443 (TCP) to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable system with SYSTEM privileges.
6. Port 445
   Port 445 is used by Microsoft Directory Services for Active Directory (AD) and for the Server Message Block (SMB) protocol over TCP/IP.
   Port 445 is used for Server Message Blocks (SMB). They all serve Windows File and Printer Sharing.
   Protocol Name: Microsoft-ds
7. Port 8008
   Port 8008 is using TCP network protocol for the application PPLive. PPTV, developed by PPLive, is a leading online TV service offering both live streaming and video-on-demand of TV programs/shows, movies, drama, sports, news and entertainment video contents.
8. Port 8009
   The application Apache JServ Protocol v13 uses this port with the network protocol of TCP. The Apache JServ Protocol (AJP) is a binary protocol that can proxy inbound requests from a web server through to an application server that sits behind the web server.
9. Port 22
   Port 22 is used by the application SSH. Secure Shell - most common use is command line access, secure replacement of Telnet. Could also be used as an encrypted tunnel for secure communication of virtually any service.
   The network protocol used here are TCP and SCTP.

10. Port 135
    in computing - Distributed Computing Environment (DCE), a framework and toolkit for developing client/server applications
    in Internet - Remote procedure call (RPC), a communication process that allows for executing a subroutine or procedure in another address space
    Protocol Name: loc-srv,epmap