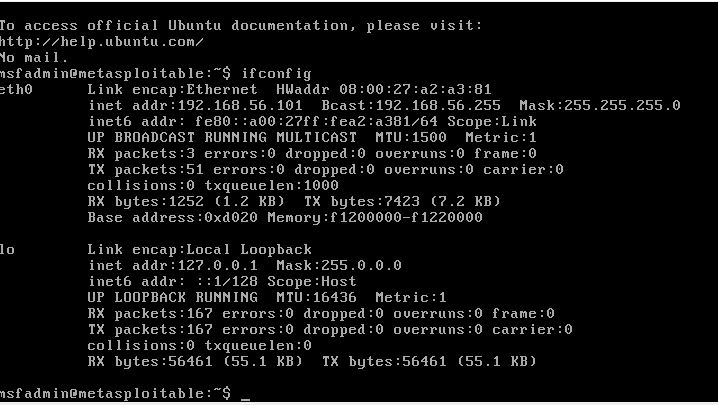
Xuan(James) Zhai

CS3339 Lab

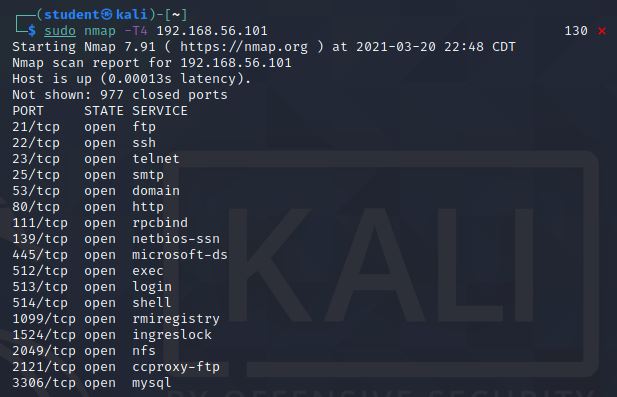
March 26th, 2021

CS 3339 - Lab 5 - Lab Report

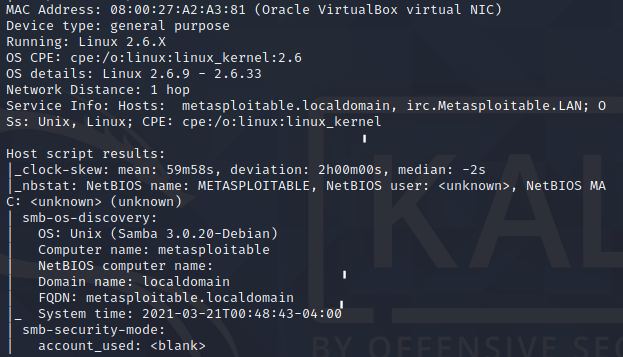
1: Use ifconfig to find the IP interface in Metasploitable2



2: Use nmap to find the target machine on that IP interface.



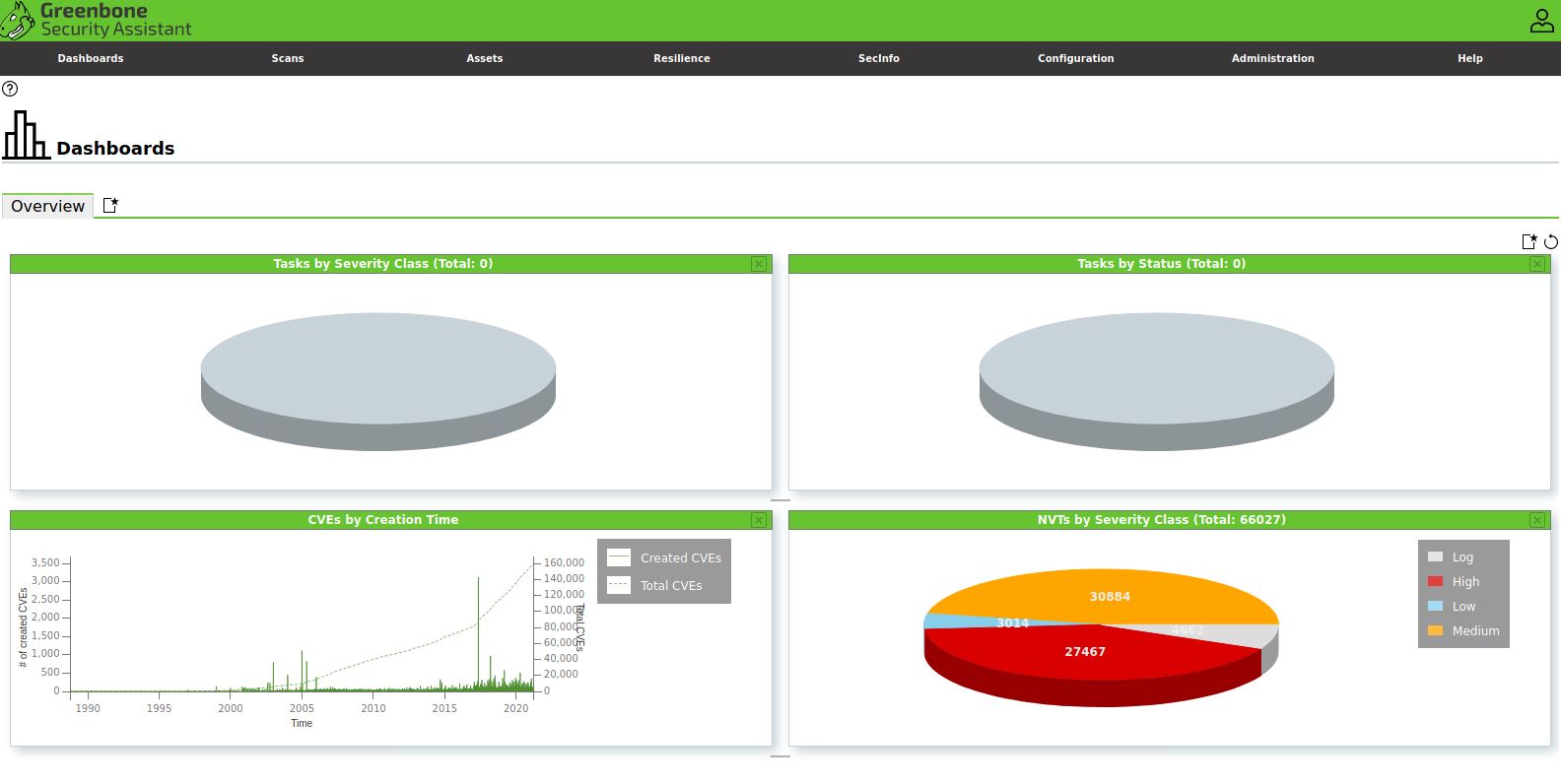
3: OS version detection



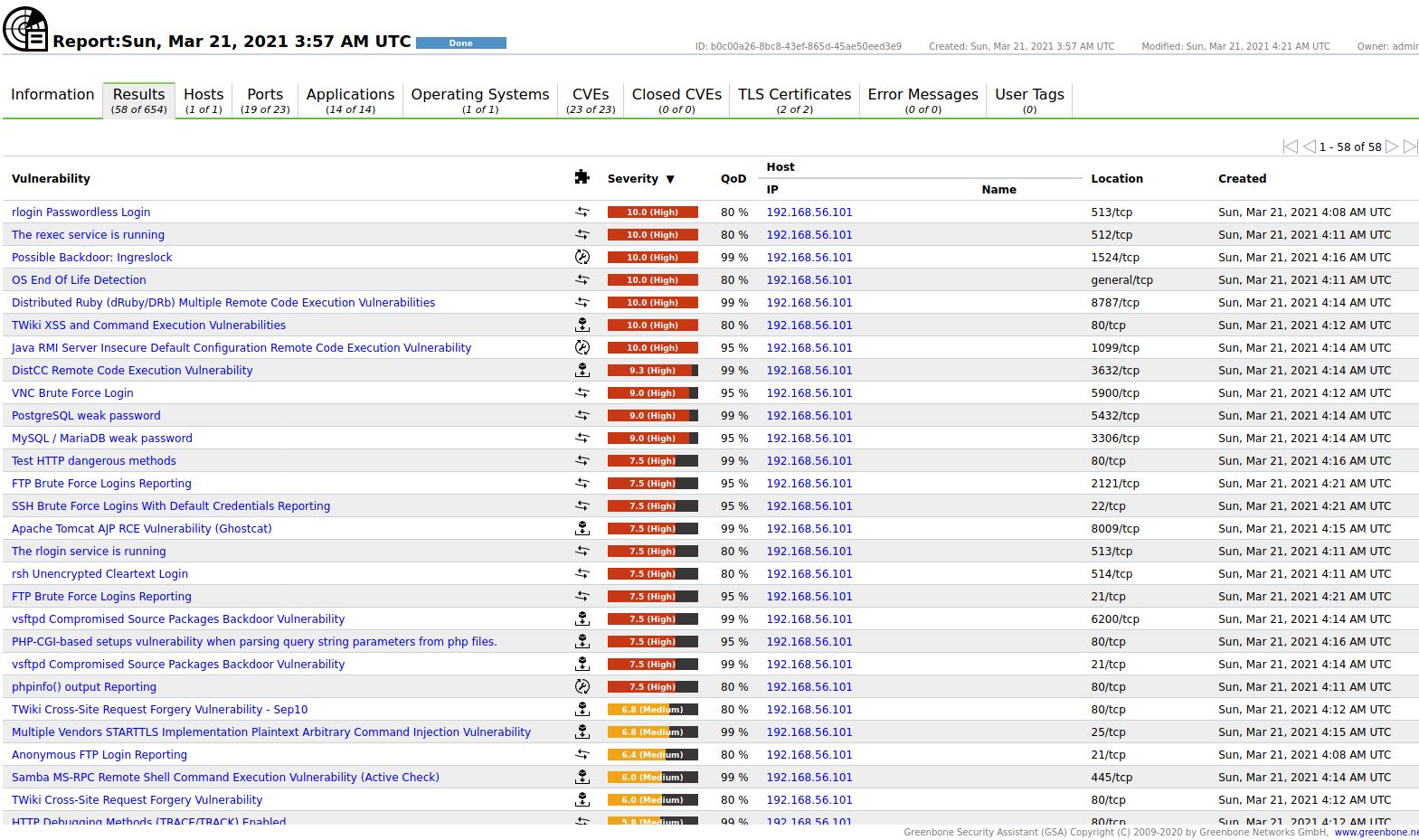
4: Use netstat -antp to check if the OpenVAS manager, and others are listening.



4: Start OpenVAS



5: Scan the vulnerability



6: Analysis

There are many vulnerabilities are identified after scanning; the first one is “rlogin Passwordless Login.” The rlogin, or remote login, program was a tool for remotely using a computer over a network. Without a password, an attacker can easily get a remote access to the machine.

There’s another vulnerability called “Possible Backdoor: Ingreslock.” According to the article from Cyber Security Associates, Ingres database is a SQL database that is commonly used to support very large commercial and government applications. As applications become larger there are additional services are added and in the process of developing the Ingres application, it was decided to have port 1524 open. This port links to a service called ingreslock which is meant to lockdown specific areas of the database application. Inadvertently, ingreslock has a backdoor associated with it that automatically binds when a connection is made with this port. (<https://static1.squarespace.com/static/5ba4e5c87a1fbd36d01467bc/t/5c1cc92588251b338fea2d12/1545390373629/Ingreslock+Vulnerability.pdf> ) In a word, an attacker can access the locked area of the Ingres database using the backdoor and steal information they need.