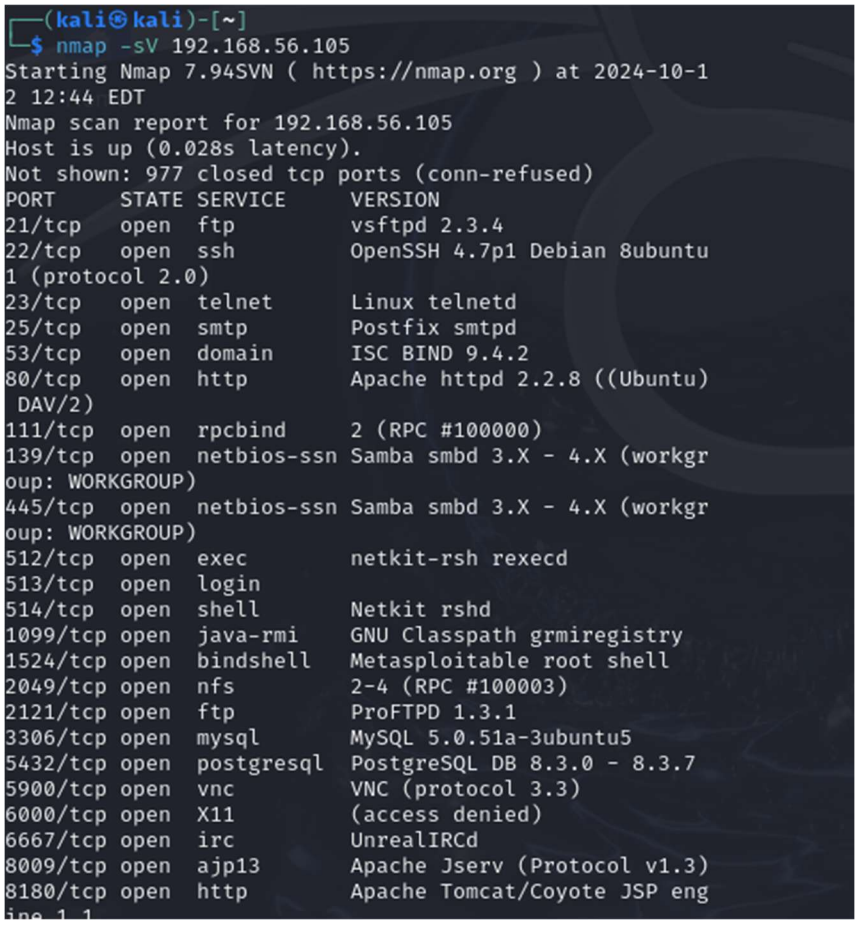
# Metasploitable Analysis Report

**Services Running:** After running a Nmap scan of the machine we can see what services the machine is running. The screenshot below shows cases that scan and the result of the services.




**Architecture:** With the list of services, we can determine how the machines are laid out. First, the web services that are being used are Apache and Tomcat. The databases in use are MySQL and PostgreSQL. The file system services in place are Samba, FTP, and NFS. Lastly, the network services are SSH, HTTP, HTTPS, and Netcat.

**External Connections:** Upon reviewing the website, the only connections being made are the local storage database. From here the website obtains information for users and resources needed. With that being said there doesn't appear to be any external connections being made it outside services.

**Password Storage:** The passwords are stored on the local database, i.e., MySQL. The majority of passwords are encrypted with hash algorithms. The metasploitable databases use MySQL and PostgreSQL to store information about the user's information, including

their passwords. For the most part the passwords stored are done in plain text, however there are a few that are stored using hashing algorithms.

**Recommendations:** While searching for passwords I was able to find passwords that were not protected. To remedy this situation an overview of the passwords used needs to be done and upon finding unprotected passwords, either remove them from text files or use hashing and salting techniques to make them unreadable. Regular audits of passwords are also a good practice to ensure the security of the system and protect against unauthorized access to passwords.