Lab Task 4

1. *Port 2049*: This port is associated with the Network File System (NFS) service. NFS is a distributed file system protocol that allows you to share files between networked computers. The NFS service on Metasploitable is misconfigured to allow 'no_root_squash' and 'no_all_squash' options, which provide root access to the NFS share. This misconfiguration can be exploited by an attacker who has gained access to the NFS share, as it allows them to perform actions that are normally restricted to the root user.
2. *Port 3632*: This port is associated with the Distcc service. Distcc is a distributed C/C++ compiler that allows you to speed up compilation by distributing it across multiple machines. The Distcc service on Metasploitable is misconfigured to allow access from any IP address without authentication. This misconfiguration can be exploited by an attacker who has gained access to the network, as it allows them to execute arbitrary code on the machine running the Distcc service.
3. *Port 5900*: This port is associated with the Virtual Network Computing (VNC) service. VNC is a graphical desktop sharing system that allows you to remotely control another computer. The VNC service on Metasploitable is misconfigured to use weak or no authentication, which allows an attacker to easily bypass the authentication and gain full control over the VNC session.
4. *Port 6000*: This port is associated with the X Window System, which provides a graphical user interface (GUI) for Unix-based operating systems. The X Window System on Metasploitable is misconfigured to allow connections from any IP address without authentication. This misconfiguration can be exploited by an attacker who has gained access to the network, as it allows them to capture the X11 server's authentication cookie and gain unauthorized access to the X11 server.