LAME –

As an Initial step, used **Nmap** tool to enumerate and scan for open ports and services running on the target machine.

Text

Description automatically generated

With the above results, there is a SSH, FTP and SMB service running on the machine.

Logged in to the FTP session as the service accepts Anonymous logins but as listed the contents in the session, there are no files in it.

Text

Description automatically generated

Then moved forward to enumerate the SMB service and listed out the SMB shares on the machine.

A screenshot of a computer

Description automatically generated with medium confidence

Then logged in to the SMB share session to read the contents and yet no luck in the also.

Text

Description automatically generated

Downloaded the file to the local machine using **mget** tool and read the contents which had not much information.

Background pattern

Description automatically generated with medium confidence

Finally on enumerating on the version of SMB service on the machine and searching exploits on the same, found an excellent exploit which can get us shell on to the machine as shown below.

Graphical user interface

Description automatically generated with medium confidence

Configured all the details for the exploit and ran the same.

Text

Description automatically generated

Command Shell has been achieved on root privileges and hence the flag.

Text

Description automatically generated