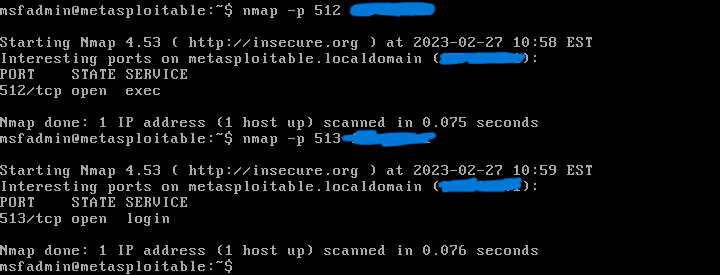
This project will aim to find vulnerabilities by attacking a Metasploitable 2 VM. While gaining root access to the machine is important, this project will ultimately seek to secure the discovered exploits within Metasploitable 2.

First, we need to get IP address, which will then allow us to do an *nmap* command

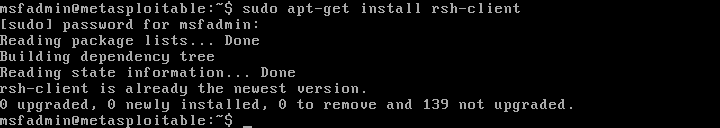


Note: The VM’s IP address will be censored for this demonstration.

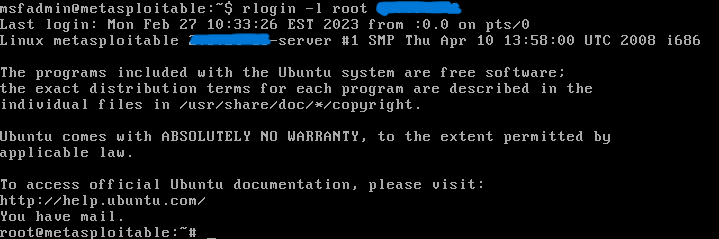
With the IP address received, I want to observe if port 513 is open, as it allows users to login to the host remotely



Port 513 has not been secured. I’ll attempt to install RSH-client (a remote login utility that it allows users to connect to remote machines)



The RSH-client was successfully installed. Now I’ll try to gain remote access using the command *rlogin -l root ipaddress.*



Success. I’ll check *.rhosts* in order to see the permissions of remote logins.



The ++ means that all computers should be treated as friendlies and will be allowed to remotely connect. Thus Metasploitable 2 has an RSH-server running and allowing remote connectivity through port 513.

To fix this vulnerability, I’ll remove the ++ from *.rhosts*, so remote connections will require a password.



The contents of .rhosts is now null, so reconnection should now require a password.



From the figure above, the RSH-server is now more secure.

Future work on this project will focus on vulnerabilities relating to an IRC server running on port 6667.

