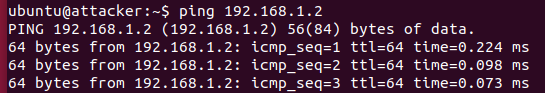
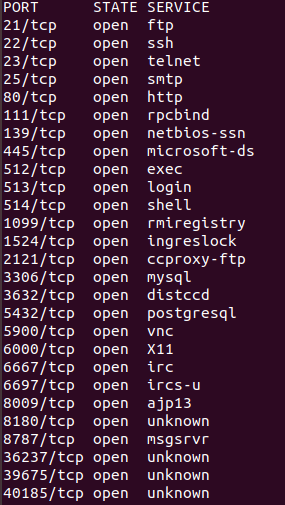
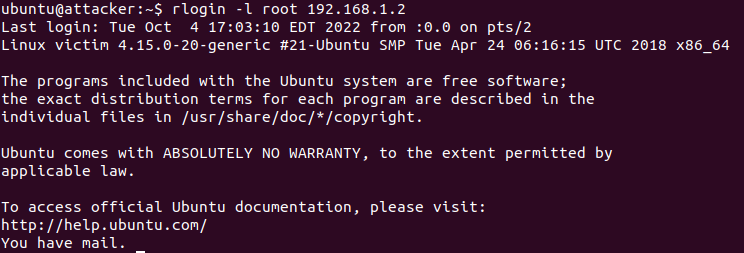
**Metasploit Lab Exercise**



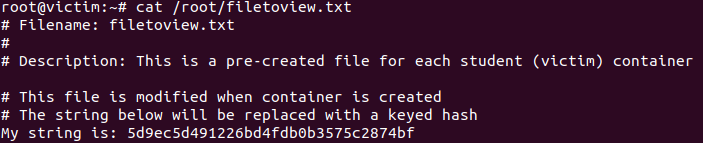
Attacker pings victim’s system to verify connectivity.



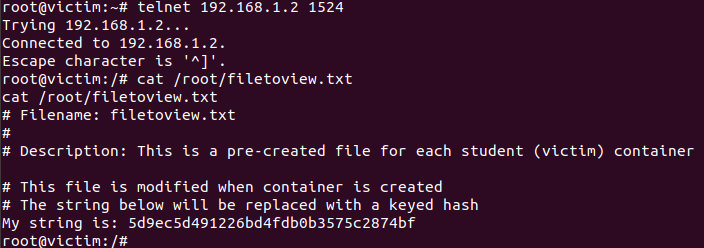
Ran ‘nmap’ scan to see the services run on all ports



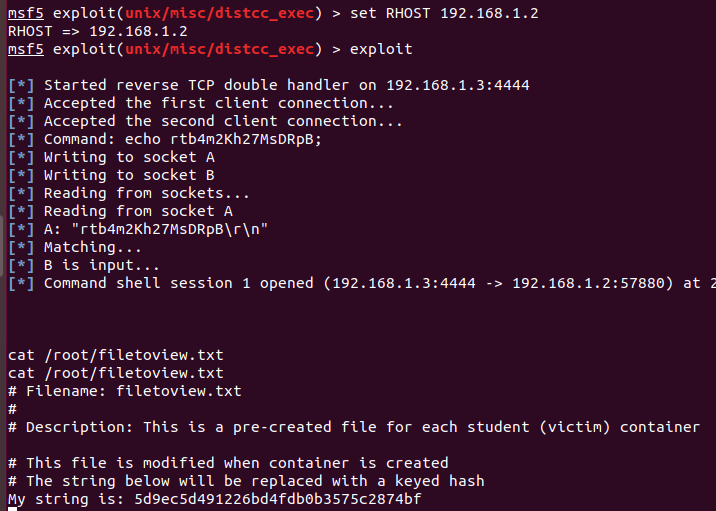
Remotely logged into victim’s system with root privileges



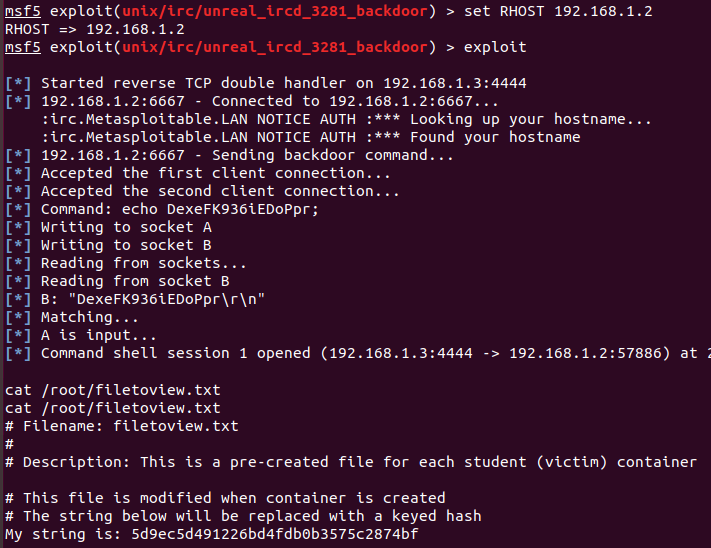
Viewed a .txt file on victim’s system



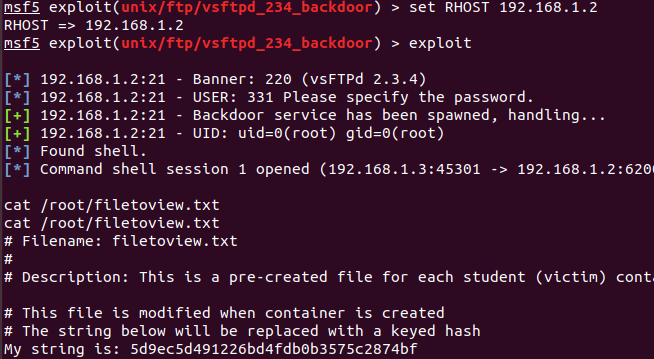
Ran telnet to access the ingreslock service on port 1524. Viewed same file on victim’s system.



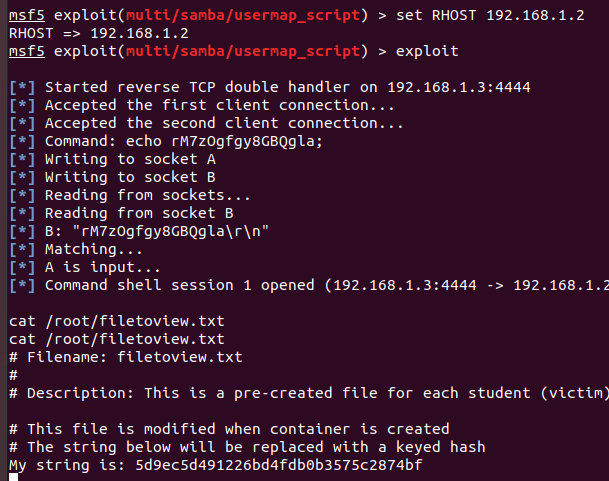
Used an exploit on distccd service to enter victim’s system and display same file. I searched for distccd exploit in the Metasploit console, used the exploit, set the remote host to my victim’s IP address 192.168.1.2, and then ran the exploit to give me root access to my victim’s system.



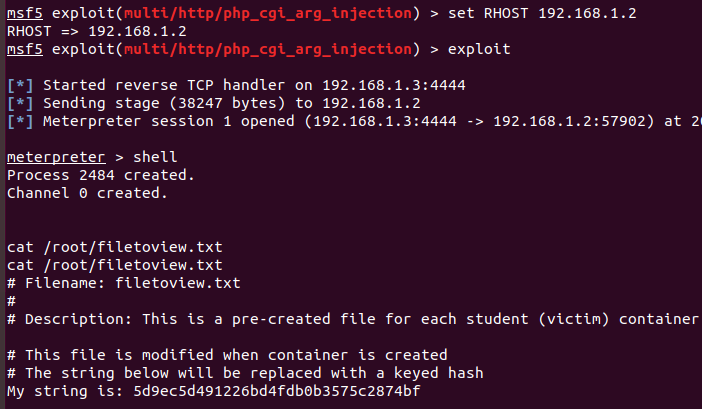
Used exploit on IRC daemon to enter victim’s system and display same file.



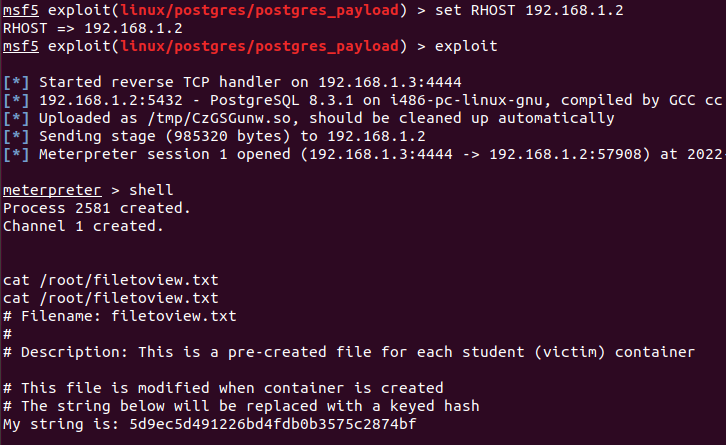
Used exploit on VSFtpd service to enter victim’s system and display same file.



Used exploit on Samba service to enter victim’s system and display same file.



Used exploit on HTTP php service to enter victim’s system and display same file.



Used exploit on Postgres service to enter victim’s file system and display same file.