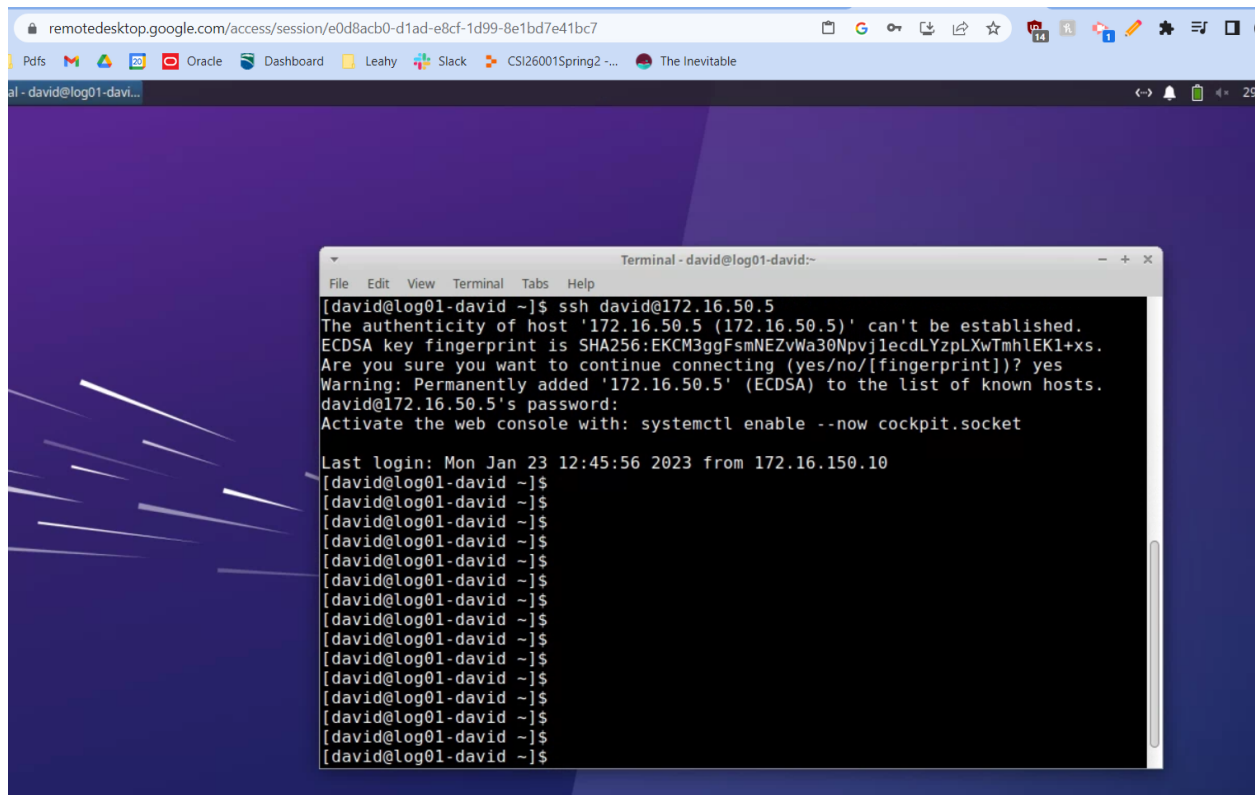
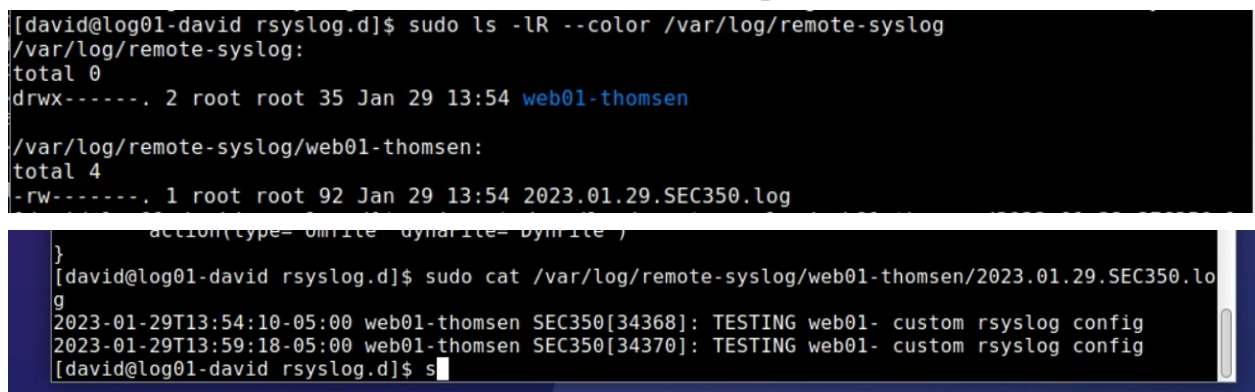


David Thomsen

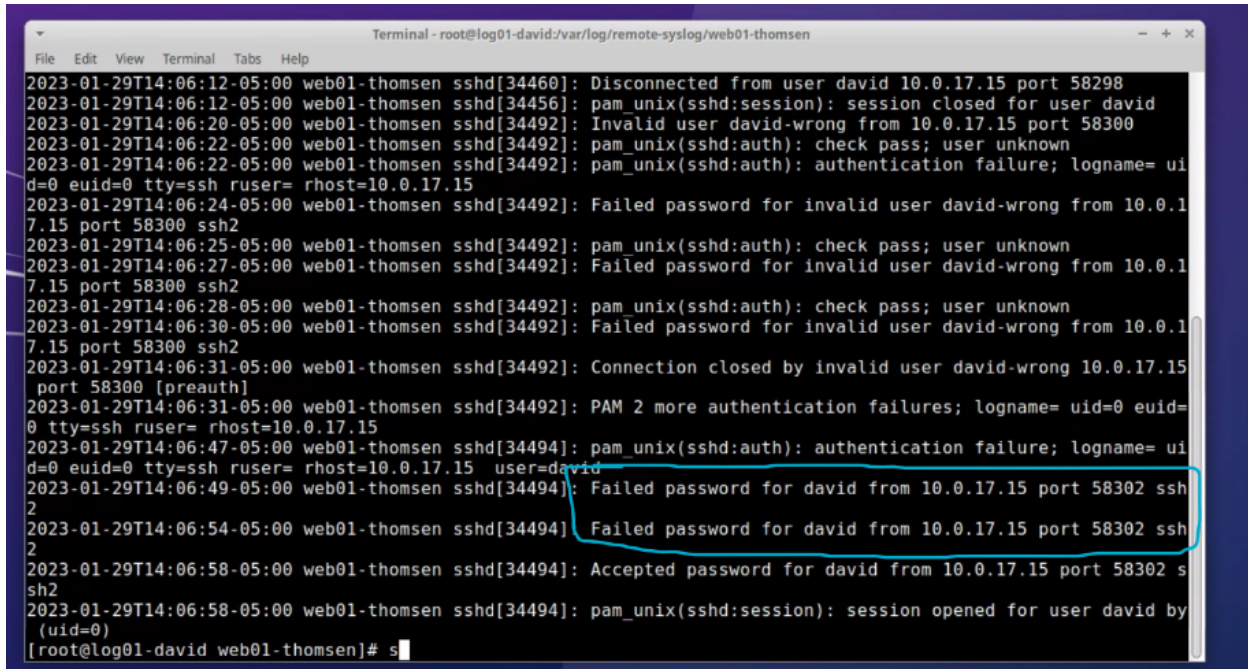
Deliverable 1. Using a chrome remote desktop session on mgmt01, ssh into your log01's named user account similar to the screenshot below. (Note, the session below uses ssh key authentication which you are welcome to configure). Provide a screenshot that shows your CRD session as well as your SSH login.



Deliverable 2. Provide a screenshot that shows steps 3 and 4 from above.

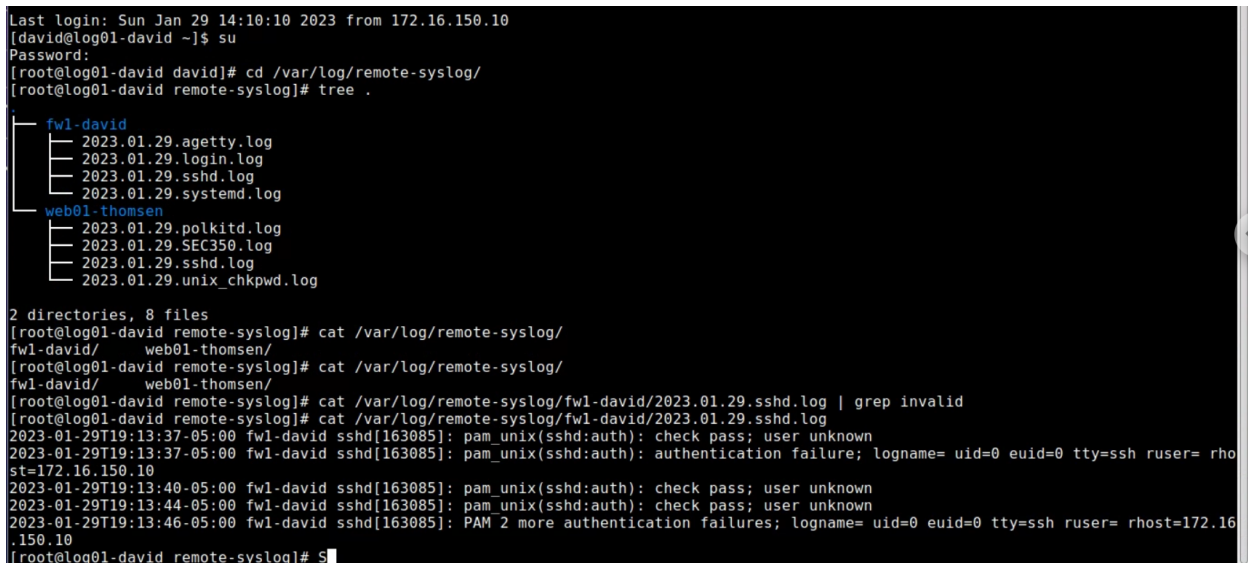


Deliverable 3. Login to log01 via mgmt01, Take a screenshot showing the failed login from your mgmt01 linux system.



```
Terminal - root@log01-david:/var/log/remote-syslog/web01-thomsen
File Edit View Terminal Tabs Help
2023-01-29T14:06:12-05:00 web01-thomsen sshd[34460]: Disconnected from user david 10.0.17.15 port 58298
2023-01-29T14:06:12-05:00 web01-thomsen sshd[34456]: pam_unix(sshd:session): session closed for user david
2023-01-29T14:06:20-05:00 web01-thomsen sshd[34492]: Invalid user david-wrong from 10.0.17.15 port 58300
2023-01-29T14:06:22-05:00 web01-thomsen sshd[34492]: pam_unix(sshd:auth): check pass; user unknown
2023-01-29T14:06:22-05:00 web01-thomsen sshd[34492]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.17.15
2023-01-29T14:06:24-05:00 web01-thomsen sshd[34492]: Failed password for invalid user david-wrong from 10.0.17.15 port 58300 ssh2
2023-01-29T14:06:25-05:00 web01-thomsen sshd[34492]: pam_unix(sshd:auth): check pass; user unknown
2023-01-29T14:06:27-05:00 web01-thomsen sshd[34492]: Failed password for invalid user david-wrong from 10.0.17.15 port 58300 ssh2
2023-01-29T14:06:28-05:00 web01-thomsen sshd[34492]: pam_unix(sshd:auth): check pass; user unknown
2023-01-29T14:06:30-05:00 web01-thomsen sshd[34492]: Failed password for invalid user david-wrong from 10.0.17.15 port 58300 ssh2
2023-01-29T14:06:31-05:00 web01-thomsen sshd[34492]: Connection closed by invalid user david-wrong 10.0.17.15 port 58300 [preauth]
2023-01-29T14:06:31-05:00 web01-thomsen sshd[34492]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.17.15
2023-01-29T14:06:47-05:00 web01-thomsen sshd[34494]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.17.15 user=david
2023-01-29T14:06:49-05:00 web01-thomsen sshd[34494]: Failed password for david from 10.0.17.15 port 58302 ssh2
2023-01-29T14:06:54-05:00 web01-thomsen sshd[34494]: Failed password for david from 10.0.17.15 port 58302 ssh2
2023-01-29T14:06:58-05:00 web01-thomsen sshd[34494]: Accepted password for david from 10.0.17.15 port 58302 ssh2
2023-01-29T14:06:58-05:00 web01-thomsen sshd[34494]: pam_unix(sshd:session): session opened for user david by (uid=0)
[root@log01-david web01-thomsen]# s
```

Deliverable 4. Submit a screenshot showing the tree structure of log01 /var/log/remote-syslog directory as well as the contents of a failed login message from fw01. It should look like the following screenshot. If tree is missing, install it.



```
Last login: Sun Jan 29 14:10:10 2023 from 172.16.150.10
[david@log01-david ~]$ su
Password:
[root@log01-david david]# cd /var/log/remote-syslog/
[root@log01-david remote-syslog]# tree .
.
├── fw1-david
│   ├── 2023.01.29.agetty.log
│   ├── 2023.01.29.login.log
│   ├── 2023.01.29.sshd.log
│   └── 2023.01.29.systemd.log
├── web01-thomsen
│   ├── 2023.01.29.polkitd.log
│   ├── 2023.01.29.SEC350.log
│   ├── 2023.01.29.sshd.log
│   └── 2023.01.29.unix_chkpwd.log
└── 2 directories, 8 files
[root@log01-david remote-syslog]# cat /var/log/remote-syslog/fw1-david/web01-thomsen/2023.01.29.sshd.log | grep invalid
2023-01-29T19:13:37-05:00 fw1-david sshd[163085]: pam_unix(sshd:auth): check pass; user unknown
2023-01-29T19:13:37-05:00 fw1-david sshd[163085]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.150.10
2023-01-29T19:13:40-05:00 fw1-david sshd[163085]: pam_unix(sshd:auth): check pass; user unknown
2023-01-29T19:13:44-05:00 fw1-david sshd[163085]: pam_unix(sshd:auth): check pass; user unknown
2023-01-29T19:13:46-05:00 fw1-david sshd[163085]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.150.10
[root@log01-david remote-syslog]# s
```

<https://github.com/dthomsen116/SEC-350/wiki/Lab-2.2---Syslog-Organization-on-log01>