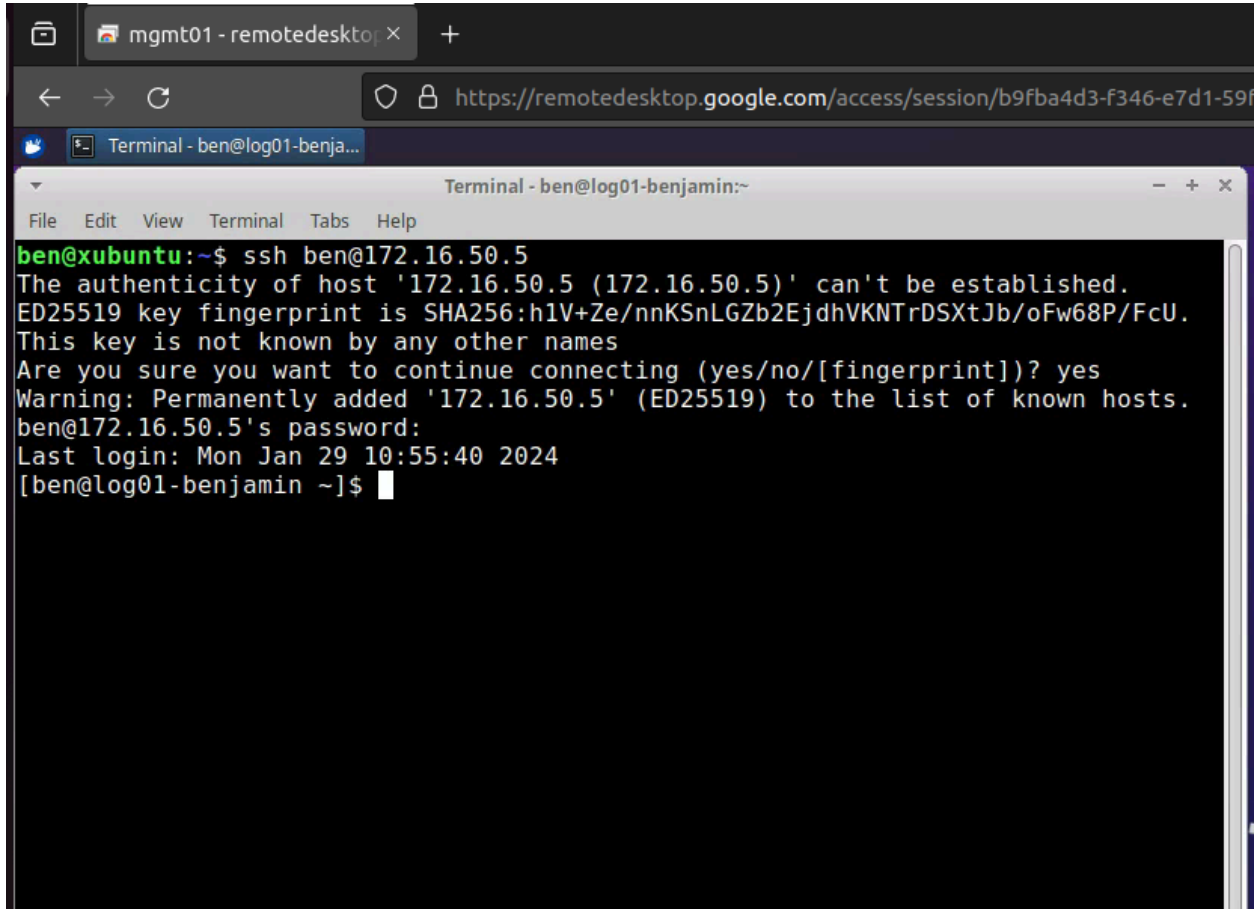


Lab2-2_SyslogOrganizationOnLog01
SEC-350
Ben W
SP24

Deliverables:

1. Remote Desktop connection of mgmt01 ssh to log01



The screenshot shows a remote desktop session titled 'mgmt01 - remotedesktop'. The browser address bar displays 'https://remotedesktop.google.com/access/session/b9fba4d3-f346-e7d1-59f...'. A terminal window titled 'Terminal - ben@log01-benja...' is open, showing the following text:

```
ben@xubuntu:~$ ssh ben@172.16.50.5
The authenticity of host '172.16.50.5 (172.16.50.5)' can't be established.
ED25519 key fingerprint is SHA256:h1V+Ze/nnKSnLGZb2EjdhVKNTrDSXtJb/oFw68P/FcU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.50.5' (ED25519) to the list of known hosts.
ben@172.16.50.5's password:
Last login: Mon Jan 29 10:55:40 2024
[ben@log01-benjamin ~]$
```

2. Log message from web01

```
[root@log01-benjamin ben]# ls -lR --color /var/log/remote-syslog/web01-benjamin/
/var/log/remote-syslog/web01-benjamin/:
total 4
-rw-----. 1 root root 97 Feb  6 16:22 2024.02.06.SEC350.log
[root@log01-benjamin ben]# cat /var/log/remote-syslog/web01-benjamin/2024.02.06.SEC350.log
2024-02-06T16:22:10-05:00 web01-benjamin SEC350[2580]: Testing web01 - log01 custom rsyslog conf
[root@log01-benjamin ben]#
```

3. Log messages of failed ssh to web01

```
ben@xubuntu:~$ ssh ben@172.16.50.5
ben@172.16.50.5's password:
Last login: Tue Feb  6 16:28:43 2024 from 172.16.150.10
[ben@log01-benjamin ~]$ sudo -i
[sudo] password for ben:
[root@log01-benjamin ~]# cat /var/log/
local/ lock/ log/
[root@log01-benjamin ~]# cat /var/log/remote-syslog/web01-benjamin/2024.02.06.
2024.02.06.SEC350.log 2024.02.06.sshd.log 2024.02.06.sudo.log
[root@log01-benjamin ~]# cat /var/log/remote-syslog/web01-benjamin/2024.02.06.sshd.log
2024-02-06T16:30:28-05:00 web01-benjamin sshd[2716]: Failed password for ben from 172.16.150.10 port 50522 ssh2
2024-02-06T16:30:30-05:00 web01-benjamin sshd[2716]: Accepted password for ben from 172.16.150.10 port 50522 ssh2
2024-02-06T16:30:30-05:00 web01-benjamin sshd[2716]: pam_unix(sshd:session): session opened for user ben by (uid=0)
2024-02-06T16:30:32-05:00 web01-benjamin sshd[2720]: Received disconnect from 172.16.150.10 port 50522:11: disconnected by user
2024-02-06T16:30:32-05:00 web01-benjamin sshd[2720]: Disconnected from user ben 172.16.150.10 port 50522
2024-02-06T16:30:32-05:00 web01-benjamin sshd[2716]: pam_unix(sshd:session): session closed for user ben
[root@log01-benjamin ~]#
```

4. Auth messages from fw01 on log01

```
file edit view terminal tabs help
[root@log01-benjamin ben]# cd /var/log/remote-syslog/
[root@log01-benjamin remote-syslog]# tree .
.
├── fw01-benjamin
│   ├── 2024.02.06.agetty.log
│   ├── 2024.02.06.sshd.log
│   └── 2024.02.06.systemd.log
└── web01-benjamin
    ├── 2024.02.06.SEC350.log
    ├── 2024.02.06.sshd.log
    └── 2024.02.06.sudo.log

2 directories, 6 files
[root@log01-benjamin remote-syslog]# cat /var/log/remote-syslog/fw01-benjamin/2024.02.06.sshd.log
2024-02-06T21:42:43-05:00 fw01-benjamin sshd[404724]: pam_unix(sshd:session): session closed for user ben
2024-02-06T21:42:48-05:00 fw01-benjamin sshd[405139]: pam_unix(sshd:session): session opened for user ben(uid=1003) by (uid=0)
2024-02-06T21:42:57-05:00 fw01-benjamin sshd[405139]: pam_unix(sshd:session): session closed for user ben
[root@log01-benjamin remote-syslog]#
```

5. Tech Journal:

https://github.com/benjamin-weatherill/SEC-350/wiki/Lab2%E2%80%902_SyslogOrganizationOnLog01