Arnav Surve
Devin Bendell
CNIT 270
01/11/2023

Lab 1

```
arnavsurve@pal-nat186-13-214.itap.purdue.edu ~
➜  ssh cyberstudent@10.48.16.40
The authenticity of host '10.48.16.40 (10.48.16.40)' can't be established.
ED25519 key fingerprint is SHA256:88W63l4d8lfPw0qQCoRT55ZmxIsHLC6rLs8rSecmy8o.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Figure 1: SSH Key Fingerprint Security Alert

```
cyberstudent@16F22:~$ ssh-keygen -l -f /etc/ssh/ssh_host_ed25519_key.pub
256 SHA256:88W63l4d8lfPw0qQCoRT55ZmxIsHLC6rLs8rSecmy8o root@270 (ED25519)
cyberstudent@16F22:~$
```

Figure 2: Output of SSH Keygen Command

If the SSH keys displayed in the client program and on the server do not match, a possible non-malicious reason could be that the SSH key generated on the server is using a different algorithm than the client (for example, ECDSA vs ed25519).