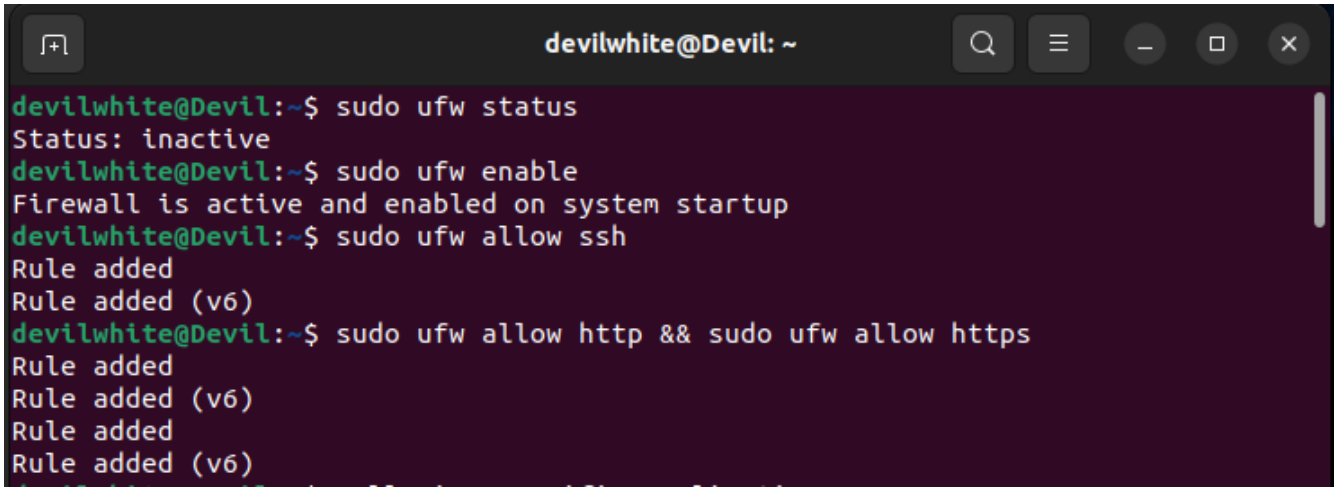
Cyber Security Basic Tasks

Task 1: Set Up Basic Firewall Rules

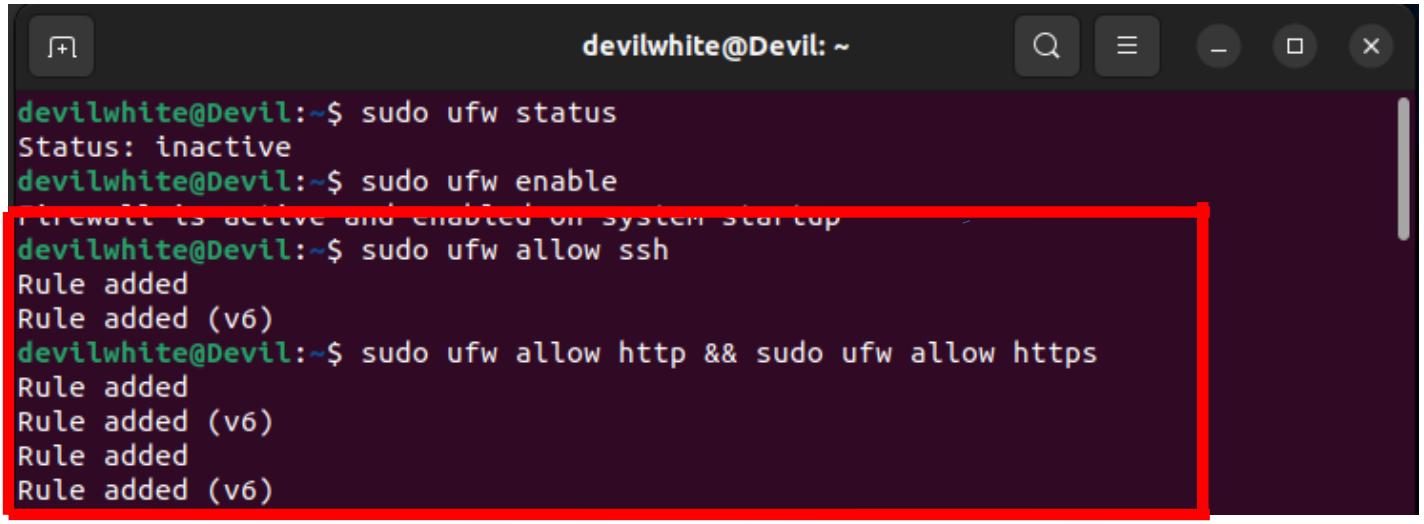
- **Ubuntu Firewall (UFW) Configuration (Enable UFW)**

To enable Firewall in Ubuntu run the command: sudo ufw enable



- **Allow Specific Applications or Ports:**

  To Allow port 22 which is used for ssh: sudo ufw allow ssh



To allow Application: sudo ufw allow app_name

```
devilwhite@Devil:~$ sudo ufw allow apache
Rule added
Rule added (v6)
devilwhite@Devil:~$
```

- Block Specific Ports or Applications: sudo ufw deny port_number && sudo ufw deny app_name

```
devilwhite@Devil:~$ sudo ufw deny 8080
Rule added
Rule added (v6)
devilwhite@Devil:~$ sudo ufw deny 8080
Skipping adding existing rule
Skipping adding existing rule (v6)
devilwhite@Devil:~$ sudo ufw deny apache
Rule updated
Rule updated (v6)
devilwhite@Devil:~$
```

- **Advanced Rules:**

  Allow traffic from a specific IP: sudo ufw allow from IP_Address

```
devilwhite@Devil:~$ sudo ufw allow from 192.168.1.100
Rule added
devilwhite@Devil:~$
```

Deny all incoming connections except those explicitly allowed: suo ufw default deny incoming && sudo ufw default allow outdoing

```
devilwhite@Devil:~$ sudo ufw default deny incoming && sudo ufw default allow out
going
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
devilwhite@Devil:~$
```

- Check and Apply Changes: sudo ufw verbose

```
devilwhite@Devil:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
80/tcp (Apache)            DENY IN     Anywhere
8080                       DENY IN     Anywhere
Anywhere                   ALLOW IN    192.168.1.100
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
80/tcp (Apache (v6))       DENY IN     Anywhere (v6)
8080 (v6)                  DENY IN     Anywhere (v6)

devilwhite@Devil:~$
```

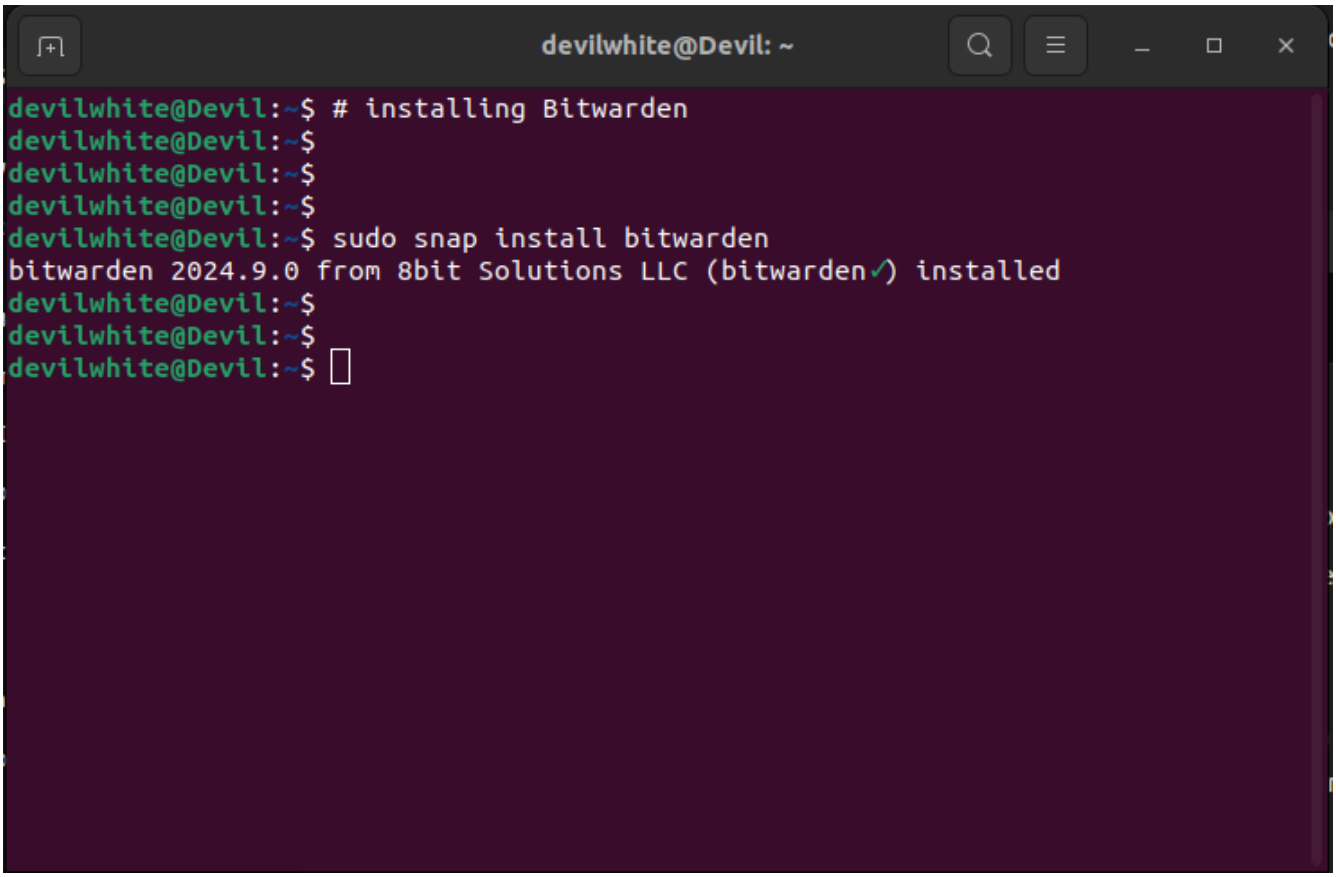
- Disable UFW (if necessary): sudo ufw disable

```
devilwhite@Devil:~$ sudo ufw disable
Firewall stopped and disabled on system startup
devilwhite@Devil:~$
```

Task 2: Use a Password Manager

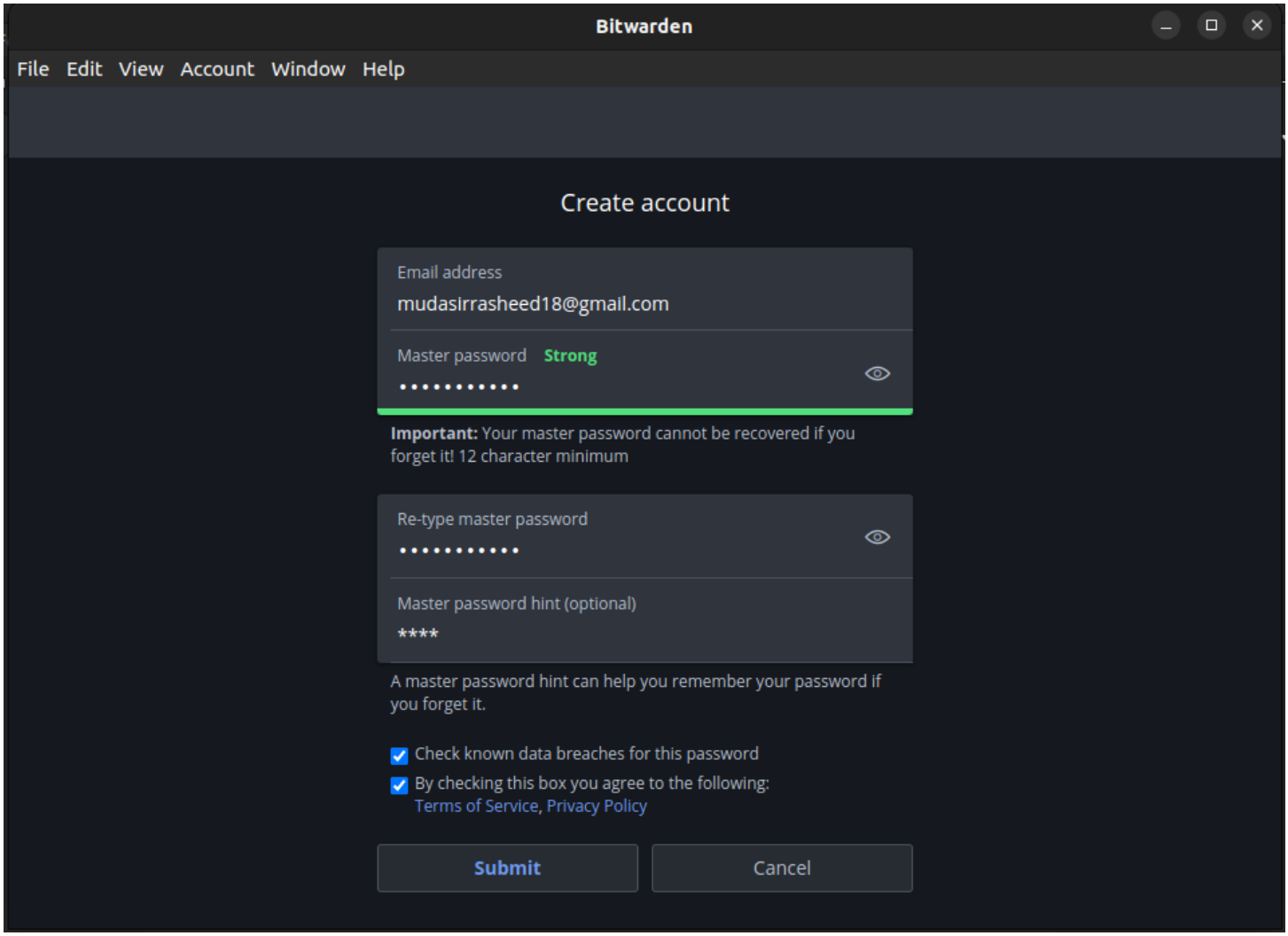
- **Install a Password Manager:**

Bitwarden Installation:

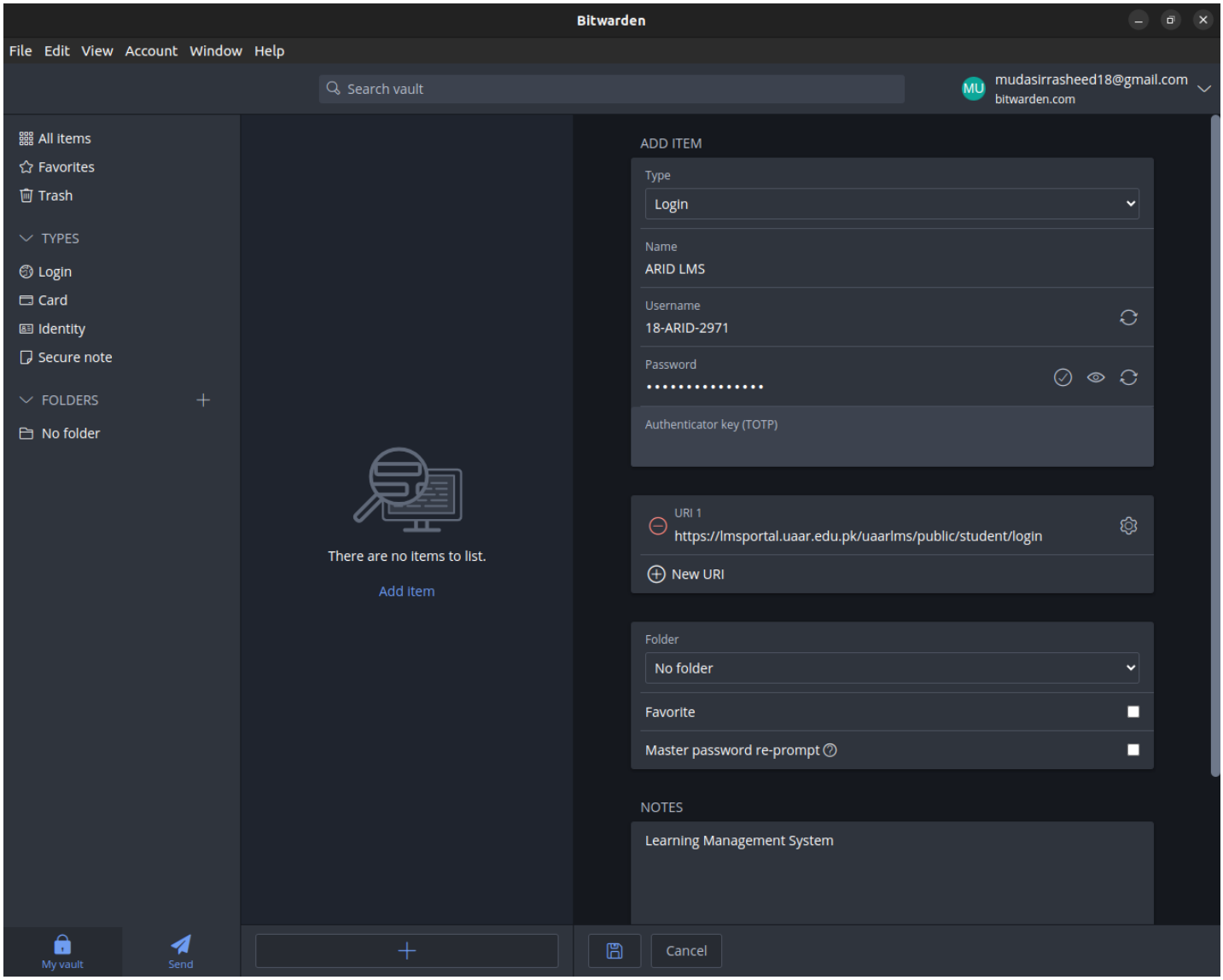


- **Setting Up Bitwarden:**

  Creating an account



Adding Password



Generating Strong Password Using Bitwarden: