ELEVATE LABS (CYBER SECURITY INTERNSHIP)

Task 2: Operating System Security Fundamentals (Linux & Windows)OS Security & Hardening – Internship Task

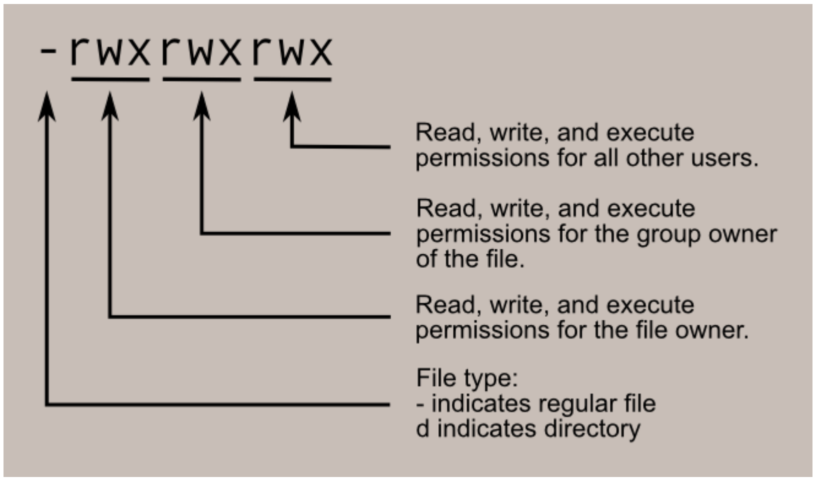
1. Installing a Linux Virtual Machine / Using Windows Security

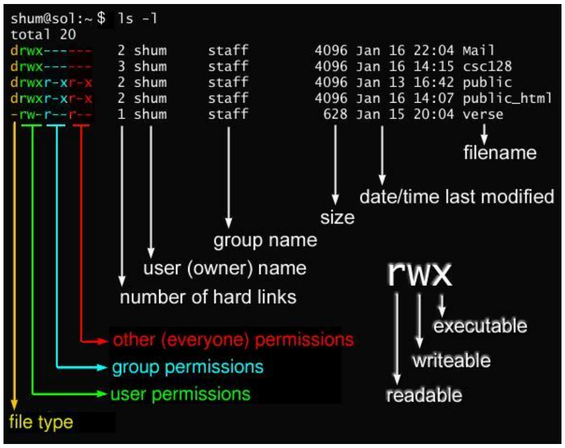
A Linux virtual machine was installed using VirtualBox to safely practice operating system security tasks. This virtual environment allowed system-level configurations without impacting the host system. Basic Windows security settings were also reviewed for comparison.

2. User Accounts, Permissions, and Access Control

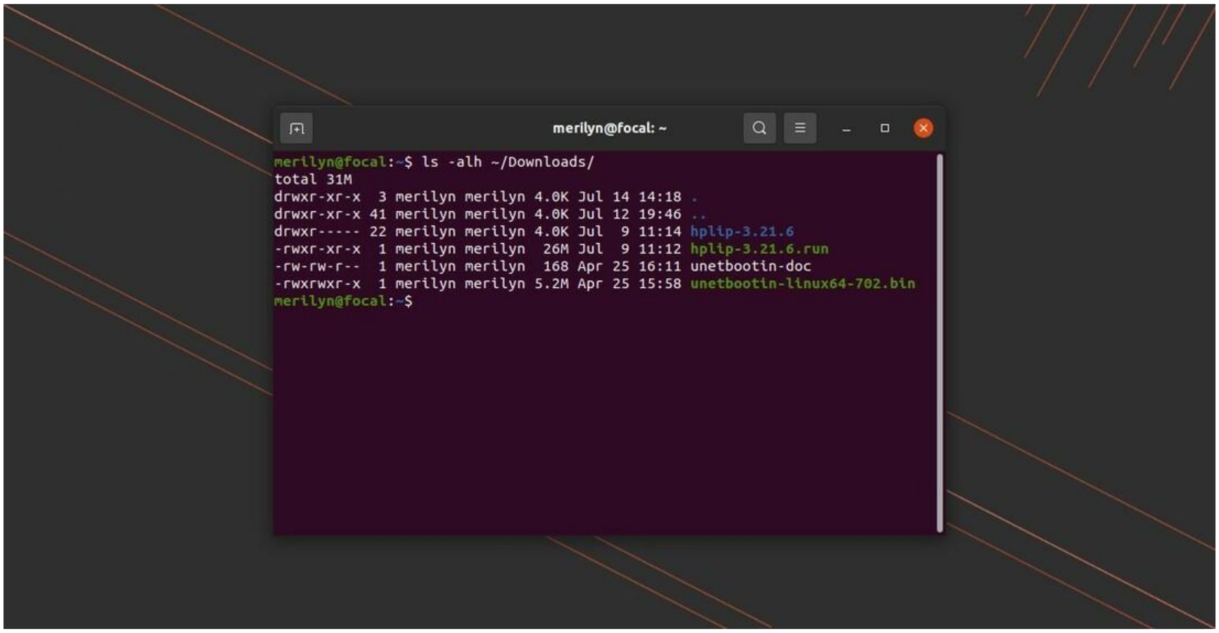
User accounts were explored to understand how the operating system controls access to files and system resources. Different users have different permission levels, and access control ensures that only authorized users can perform specific actions. The importance of limiting user privileges was observed.

3. File Permissions Using `chmod`, `chown`, and `ls -l`


-rwxrwxrwx
Read, write, and execute permissions for all other users.
Read, write, and execute permissions for the group owner of the file.
Read, write, and execute permissions for the file owner.
File type:
- indicates regular file
d indicates directory



```
shum@sol:~$ ls -l
total 20
drwx------  2 shum    staff       4096 Jan 16 22:04 Mail
drwx------  3 shum    staff       4096 Jan 16 14:15 csc128
drwxr-xr-x  2 shum    staff       4096 Jan 13 16:42 public
drwxr-xr-x  2 shum    staff       4096 Jan 16 14:07 public_html
-rw-r--r--  1 shum    staff        628 Jan 15 20:04 verse
```



```
merilyn@focal:~$ ls -alh ~/Downloads/
total 31M
drwxr-xr-x  3 merilyn merilyn 4.0K Jul 14 14:18 .
drwxr-xr-x 41 merilyn merilyn 4.0K Jul 12 19:46 ..
drwxr----- 22 merilyn merilyn 4.0K Jul  9 11:14 hplip-3.21.6
-rwxr-xr-x  1 merilyn merilyn  26M Jul  9 11:12 hplip-3.21.6.run
-rw-rw-r--  1 merilyn merilyn  168 Apr 25 16:11 unetbootin-doc
-rwxrwxr-x  1 merilyn merilyn 5.2M Apr 25 15:58 unetbootin-linux64-702.bin
merilyn@focal:~$
```

Linux file permissions were studied using the `ls -l` command to view permissions. The `chmod` command was used to modify read, write, and execute permissions, while `chown` was used to change file ownership. This helped in understanding how improper permissions can create security risks.

4. Administrator vs Standard User Privileges

The difference between administrator and standard user privileges was analyzed. Administrators have full control over the system, including installing software and changing system configurations, while standard users have limited access. Using a standard user for daily tasks improves system security.

5. Enabling Firewall (UFW / Windows Firewall)

The firewall was enabled to control network traffic and prevent unauthorized access. In Linux, UFW was used to allow or block specific services. Windows Firewall settings were also reviewed. Firewalls play an important role in protecting the system from external threats.

6. Identifying Running Processes and Services

Running processes and background services were identified to understand what is actively running on the system. This helped in recognizing essential system services and detecting unnecessary or suspicious processes.

7. Disabling Unnecessary Services

Unnecessary services were disabled to reduce the system’s attack surface. Reducing the number of running services lowers the risk of exploitation and improves overall system security.

8. Documenting OS Hardening Best Practices

Based on the task, basic OS hardening practices were documented, including:

- Regular system updates
- Strong password usage
- Limited administrative access
- Firewall configuration
- Proper file permissions
- Disabling unused services