scp C:\Users\Sila\Desktop\john.conf azure\_user@20.151.89.28:/home/azure\_user/Desktop

Recall that zero trust means not granting access to resources until a device verifies its identity.

1. What is a real world situation that operates on the principle of zero trust?

* One example of a real-world situation that operates on the principle of zero trust is the modern approach to network security. In a traditional network security model, there is a perimeter that separates the trusted internal network from the untrusted external network. Once a user is authenticated and authorized, they are granted access to the internal network and its resources.
* In contrast, the zero-trust model assumes that there is no secure perimeter, and all traffic must be treated as untrusted until proven otherwise. This means that users, devices, and applications must be authenticated and authorized before they are granted access to any resources, even if they are already inside the network.
* This approach is becoming increasingly important as organizations move to cloud-based applications and mobile workforces. By using zero trust principles, organizations can limit the risk of data breaches, reduce the impact of a potential attack, and increase visibility into their network traffic.

2. Two more factors of authentication

1. Location - vpn connection is a risk
2. Time
3. List the apps or sites where you have 2FA enabled.
4. How would you describe the experience of using 2FA?

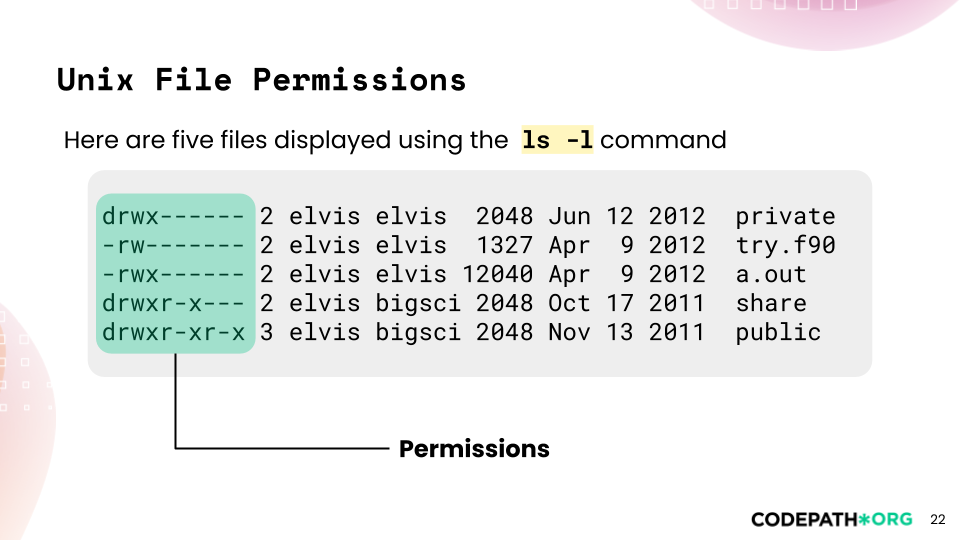
2FA (Two-Factor Authentication) is an additional layer of security that requires users to provide two different forms of authentication before accessing an account or application. These two factors can be something the user knows (such as a password or PIN) and something the user has (such as a smartphone or hardware token).

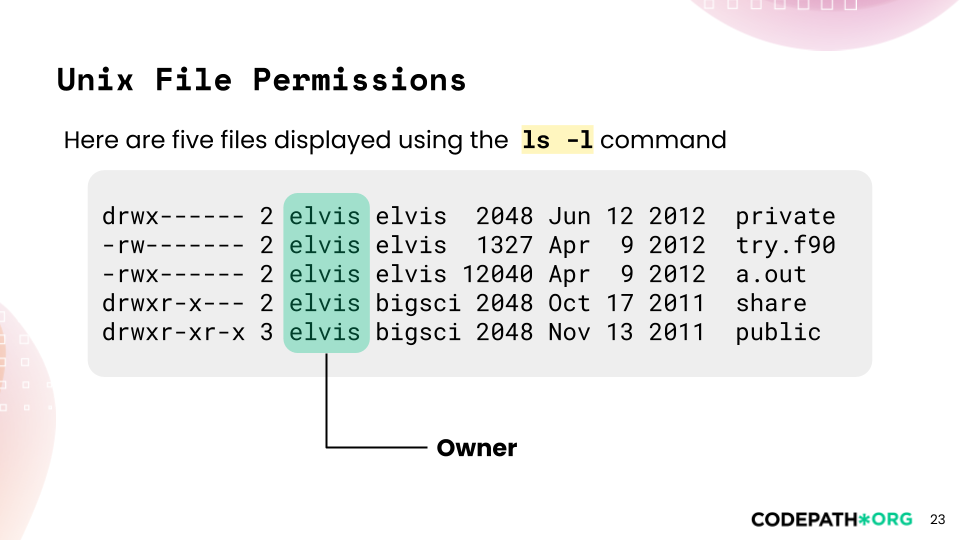
The experience of using 2FA can vary depending on the implementation and the user's preferences. Some common ways of providing the second factor of authentication include receiving a code via SMS or email, using a code generated by an authenticator app, or using a physical security key.

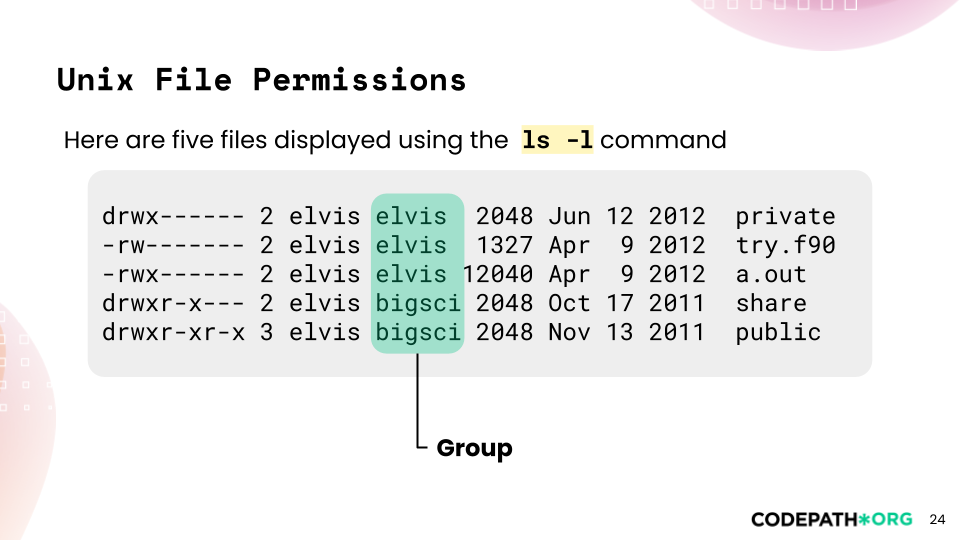
At first, using 2FA may feel like an extra step that slows down the login process. However, it can greatly enhance the security of an account or application by making it much harder for an attacker to gain unauthorized access, even if they have obtained the user's password.

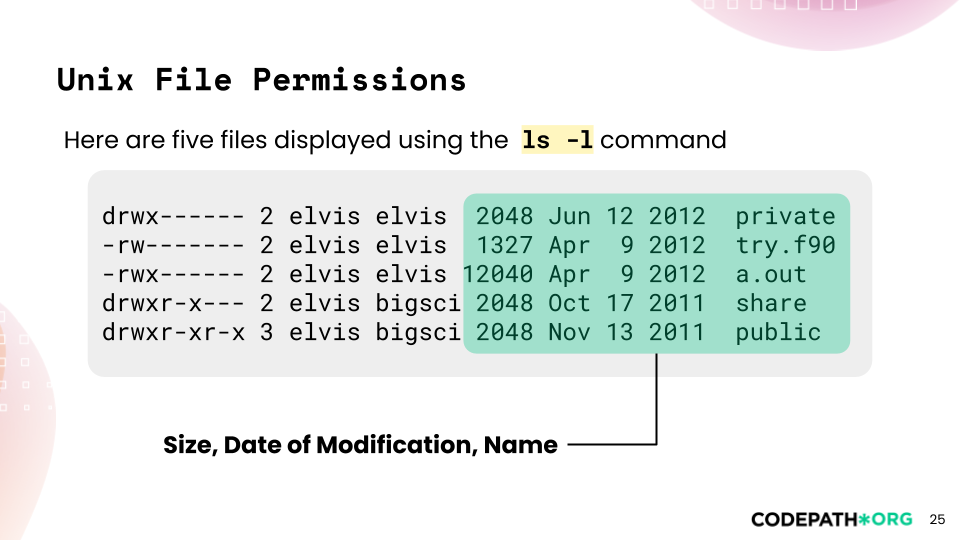
Overall, the experience of using 2FA can be seen as a small inconvenience that provides a big boost in security. It is becoming increasingly popular as more and more services and applications implement it as a standard security measure.

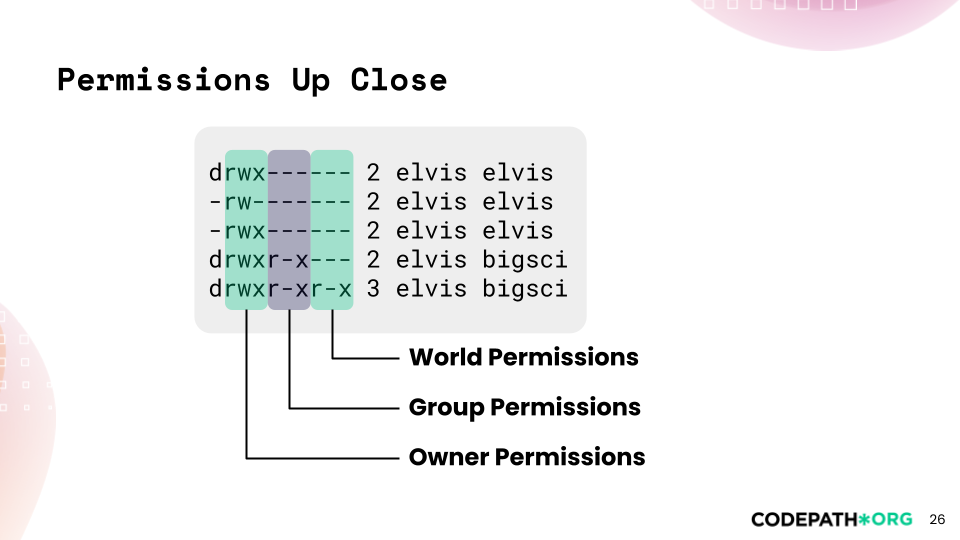
1. ls -l command which means long listing
   1. Drwx- - - -2 elvis elvis 2048 Jun 12 2012 private -> d identifies whether it’s a directory or a regular file, r means read, w means write and x means execute. Rwx are user permissions. 2 means how many links to the file there are. Elvis is the owner, elvis is group name, 2048 is file size, Jun 12 2012 is the last time the file was modified, private is the actual filename or directory name











1. Describe the owner, group, and world permissions for the **narwhals** directory:

drwxr-x--- 4 arvind zoo 2048 Oct 22 2024 narwhals

The owner of the "narwhals" directory is "arvind", the group owner is "zoo", and the directory has the following permissions:

* The owner ("arvind") has read, write, and execute permission, indicated by the "rwx" in the first three characters of the permission string.
* The group owner ("zoo") has read and execute permission, indicated by the "r-x" in the middle three characters of the permission string.
* The world (anyone else) has no permission, indicated by the "---" in the last three characters of the permission string.

Therefore, the owner ("arvind") has full access to the directory, the group owner ("zoo") can read and execute files in the directory, and anyone else has no access to the directory.

* If instead of d, there is a dash then it is a file instead of a directory

1. Unzip files in kali linux
   1. Go to terminal
   2. Write command unzip filename.zip
2. What kinds of passwords were easy to crack?

Passwords that are easy to crack are usually those that are short, simple, common, or predictable. [Some of the password cracking techniques that hackers use are1](https://bing.com/search?q=easy+to+crack+passwords)[2](https://resources.infosecinstitute.com/topic/easy-hacker-crack-password/)[3](https://cybernews.com/best-password-managers/password-cracking-techniques/):

* Dictionary attack: This method involves the use of a wordlist to compare against user passwords. If the password is a common word or phrase, it can be easily cracked by this method.
* Brute force attack: This method is similar to the dictionary attack, but it tries all possible combinations of letters, numbers, and symbols until it finds the correct one. This method can take a long time depending on the length and complexity of the password.
* Rainbow table attack: This method uses pre-computed hashes of common passwords and compares them with the hashed password of the user. This method can be faster than brute force, but it requires a large amount of storage space for the rainbow tables.
* Guessing: This method involves guessing the password based on personal or public information about the user, such as their name, birthday, hobbies, etc. This method can be effective if the user chooses a password that is related to themselves or their interests.
* Spidering: This method involves collecting information from a website or an organization and using it to create a wordlist for dictionary attacks. For example, if a hacker wants to crack passwords of employees of a company, they can spider their website and look for words related to their products, services, values, etc.

To avoid having your passwords cracked by these methods, you should use strong passwords that are long (at least 12 characters), random (not based on words or personal information), unique (not reused for different accounts), and varied (using different types of characters). [You can also use a password manager like Bitwarden4](https://bitwarden.com/password-strength/) to generate and store your passwords securely.

1. What kinds of passwords did you think avoided your dictionary attack?

* [A dictionary attack is a type of brute force attack that tries to guess your password by using common words and their variations1](https://www.techradar.com/features/dictionary-attack)[2](https://en.wikipedia.org/wiki/Dictionary_attack). [To avoid a dictionary attack, you should use passwords that are not based on words from a dictionary or other lists of common passwords3](https://nordpass.com/blog/what-is-a-dictionary-attack/)[4](https://www.geeksforgeeks.org/what-is-a-dictionary-attack/). You should also use a combination of uppercase and lowercase letters, numbers and symbols to make your password more complex and harder to guess

1. john --restore : restores the last command run results

## Project Command List

| SN | Command | Count |
| --- | --- | --- |
|  | john --format=md5crypt-long -single CPLeak.txt | cracked 22, 978 left |
|  | john --format=md5crypt-long --wordlist=/usr/share/wordlists/john.lst CPLeak.txt --rules=l33t | 0, 978 left  (took too long quitted in the middle) |
| 3. | john --format=md5crypt-long --incremental=digits --max-length=8 CPLeak.txt | 0, 978 left  (took too long, quitted in the middle) |
| 4. | john --format=md5crypt-long --incremental=Alnum --max-length=8 CPLeak.txt | 48, 952 left - left in the middle |
| 5. | john --format=md5crypt-long --wordlist=/usr/share/wordlists/rockyou.txt --min-length=3 --max-length=8 --mask=?w?d CPLeak.txt | Took too long |
| 6 | john --format=md5crypt-long --max-length=4 --incremental=ASCII CPLeak.txt | 70, 930 left |
| 7 | john --format=md5crypt-long --max-length=3 --incremental=ASCII CPLeak.txt | 85 password hashes cracked, 915 left - left in the middle |
| 8 | john --format=md5crypt-long --max-length=1 --incremental=alpha CPLeak.txt | 0 |
| 9 | john --format=md5crypt-long --max-length=2 --incremental=alpha CPLeak.txt | 94 cracked, 906 left- completed the run |
| 10 | john --max-length=5 --min-length=4 --incremental=Lower CPLeak.txt | 203 cracked, 797 left |