

# Security risk assessment report

## Part 1: Select up to three hardening tools and methods to implement

We majorly have three issues currently :

- Weak password policy
- Firewall misconfiguration
- No MFA

For the issues we have these are the hardening techniques that will help us to prevent future attacks

First we should make a strict password policy which restricts the employees from password sharing. Also the password should be harder also no default passwords should be allowed and the passwords should be frequently updated as well.

The second hardening tool that we can use is regular firewall updates also configuring the firewall to properly filter traffic. Rules for the firewall should be checked and changed according to the situation or in consideration of the previous events.

And the third tool we should use is to add MFA (Multi Factor Authentication).

## Part 2: Explain your recommendations

1. A strong password policy will help us in safeguarding our network from attacks like this as the password will not be that easy to guess that will significantly reduce the chances of a brute force attack.
2. Regular firewall maintenance will help us filter unnecessary traffic on the network but can also help us by filtering ports and preventing any malicious traffic from entering the network. It will also notify the network admin if it detects any suspicious activity on the network further hardening our network security . Firewalls should be kept updated according to the latest standards to make them more secure.
3. Using MFA will make sure that only authorized personals can access the network as it will require each individual to provide identity proof in at

least 2 ways or more so even if someone gets the password they still won't be able to login as they will require to prove their identity in other ways as well , it is only needed to be setup once .

Overall these measures will make sure that event like this not happen again these should be maintained on regular basis will help protect the organisation from any future attacks.