# Common Network Security Vulnerabilities Discovered in Penetration Tests

The advancement of technology has opened many gateways to development and improvisation in the world's current systems. However, the dark side constitutes information breach, hacking, and system attacks. Thus, it has become essential for agencies to pass their systems through penetration tests. These tests can be called ethical hacking as it confirms the level of security for your system. Penetration testing is conducted by identifying and exploiting vulnerabilities in the system. It returns you a complete report about how an ethical hacker was able to breach your system, how much data was accessed, and what preventions can be taken in the future to avoid these failures.

Let’s have a look at some common network security vulnerabilities that are discovered in penetration tests.

## Hashing Manipulation

Hashing is a process that manipulates the data into a pre-determined length, which appears meaningless to an everyday user. However, an intruder can develop a program to intercept the hashed data and gain authentication to a system. A simple password can be converted into such digits and alphabets that an ordinary user cannot assess, but an intruder can intercept it during the relaying process.

## Reusing of passwords

People who commonly keep the same password to access various applications are likely to fall victim to asecurity breach. If your password gets breached from one platform, all your other applications are at risk. The intruder uses the data loss of one forum to penetrate another.

## Weakness of patches

Another well-known miser-ability of a system found through penetration testing is the weakness of patches. Cyber hackers can uproot the liability for which patches are released. If an IT team does not keep the patches up-to-date, especially if it is a third-party application, you are more open to attacks.

## Encryption and Authentication Flaws

Organizations commonly use data encryption to ensure secure communications for data at rest or in transit. SSL, SSH and TLS are common encryption protocols used for converting plaintext data into unreadable ciphertext. However, in some instances, businesses have actually used encryption methods that are less secure. For instance, in October 2017, the WPA2 protocol used for protecting WiFi connections was actually found to be [breakable](https://www.theguardian.com/technology/2017/oct/16/wpa2-wifi-security-vulnerable-hacking-us-government-warns).

## In-house applications

Penetration testing has also proved that in-house applications are more vulnerable to intruders than third party applications. The primary reason for this is inadequate testing, which can lead to input validation flaws.

## Conclusion

Cybercriminals cannot be let on the loose, and the only way to contain them is by conducting penetration testing for your system and software. You need to explore your application from the perspective of a hacker to build a secure system.