## Penetration Testing and Security code review

Businesses and government-related organizations that are serious about their network security hire ethical hackers and penetration testers to help probe and improve their networks, applications, and other computer systems with the ultimate goal of preventing data theft and fraud.

As ethical hackers we are usually employed by an organization who trusts us to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities. Unauthorized hacking (i.e., gaining access to computer systems without prior authorization from the owner) is a crime, but penetration testing done by request of the owner of the targeted system(s) or network(s) is not.

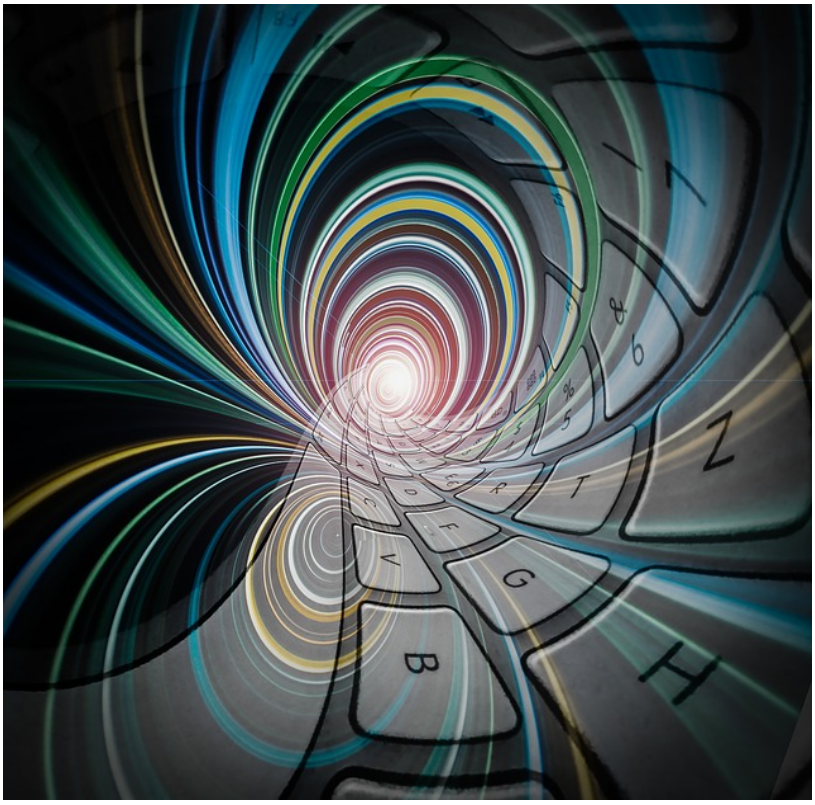
## Penetration Testing – Why Do It?

- Penetration Testing engagements are required by many compliance requirements (such as the Payment Card Industry Data Security Standard)
- Penetration Testing greatly improves your security posture
- Penetration Testing should be performed regularly (at least annually), due to the constant addition / removal of hardware in your environment, code releases, patching requirements, manual environment modification

## Penetration Testing – Areas of Impact?

Penetration Testing is performed against multiple layers of your environment:

- Network Layer – Performed against the network layer of your environment (web servers, file servers, firewalls, routers, email servers). This layer is evaluated for vulnerabilities and configuration issues, with all results validated by a security engineer
- Application Layer – Performed against applications (primarily web applications) looking for application layer vulnerabilities, logical faults, and web server configuration issues.
- Human Layer – Performed against people within the organization using social-engineering

techniques to obtain unauthorized acces.

- External Penetration Testing – testing is performed from outside your environment (similar to a hacker)
- Internal Penetration Testing – testing is performed from inside your environment (similar to a hacker that has breached the outer defenses)
- Firewall and VPN testing
- Mobile applications testing
- Applications security – Source code review
- Web application firewall (WAF) – effectiveness evaluation (false negatives and pozitives)