# EXPLAINING PENETRATION TESTING

**A penetration test, or pen-test, is an effort to measure the security of an IT infrastructure by safely attempting to exploit vulnerabilities.**

- These vulnerabilities may exist in OSs, services, and application program defects, improper configurations or insecure end-user behaviour.
- Such appraisals are also useful in confirming the efficacy of protective mechanisms, likewise end-user attachment to protection policies.

vulnerability scanning

social engineering

## Hack

Armed with intel gathered from social engineering and vulnerability scanning, the penetration tester begins bombarding the web application (or infrastructure or wireless system) with hacking attempts


## PENETRATION TESTER

# PENETRATION TESTER

## Gather

Throughout the penetration test, information is gathered, and risks are identified.

## Get Results

The results of the penetration test are prioritized and compiled in an executive report. Risks are labelled and described, and a proposed solution is provided.

## Remediate

The report is used by the IT team to guide the subsequent risk mitigation process. At this time IT staff members and developers work to resolve high and moderate risk findings.

# Remediate

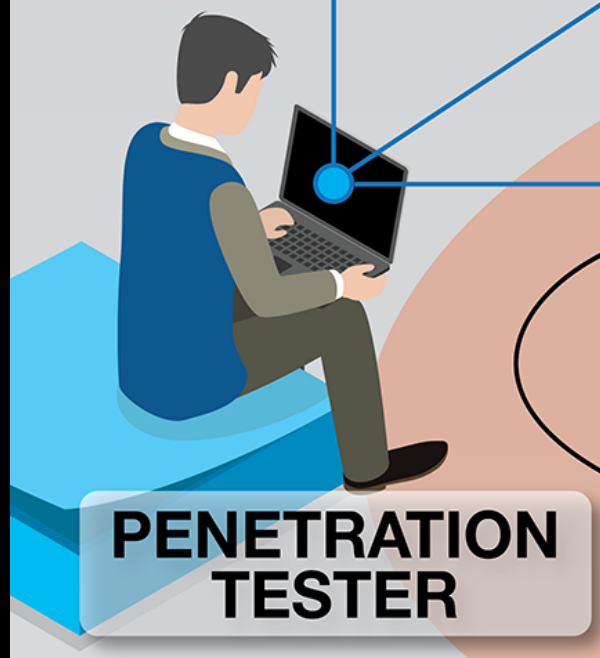
The report is used by the IT team to guide the subsequent risk mitigation process. At this time IT staff members and developers work to resolve high and moderate risk findings.

an executive report. Risks are labelled and described, and a proposed solution is provided.

# Validate

Following the attempt to fix discovered issues found in an external test, the penetration tester will validate remediation efforts. This process will confirm whether or not the remediation was successful.

- Validated Input
- Secure Authentication
- Correct Security Configuration



# PENETRATION TESTER

## Hack

Armed with intel gathered from social engineering and vulnerability scanning, the penetration tester begins bombarding the web application (or infrastructure or wireless system) with hacking attempts


## Gather

Throughout the penetration test, information is gathered, and risks are identified.

## Get Results

The results of the penetration test are prioritized and compiled in an executive report. Risks are labelled and described, and a proposed solution is provided.

## Remediate

The report is used by the IT team to guide the subsequent risk mitigation process. At this time IT staff members and developers work to resolve high and moderate risk findings.

## Validate

Following the attempt to fix discovered issues found in an external test, the penetration tester will validate remediation efforts. This process will confirm whether or not the remediation was successful.