To Test or Not to Test

How do you know if the security tools and network configurations you have worked so tirelessly to deploy are effectively protecting your organization's systems and data?

The best way to find out is through a comprehensive penetration test. Below are 10 reasons your organization should consider conducting a network penetration test sooner rather than later:

Real-world Testing

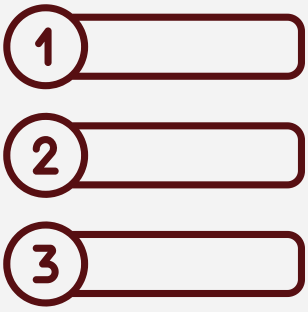
Unlike a vulnerability scan, a penetration test doesn't simply identify potential vulnerabilities, it goes a step further to actively exploit those vulnerabilities and demonstrate the attack vectors that can be used to successfully gain access to your organization's systems, assets, staff, etc.

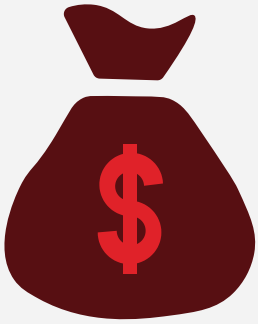
Understanding Your Weaknesses

You will be better positioned to protect your systems if you are able to accurately pinpoint gaps and then remediate those deficiencies.

Prioritizing Risks

A well-written penetration test report will include a measurement of risk that each gap represents, so you can quickly address high-risk areas where breaches are more likely to occur or have a larger impact, and then build plans to address the lower risks items in your long term security strategy.





Preventing Costly Breaches

Resources may be tight so consider segmenting the tests to start – begin with those areas that touch sensitive data, identify and remediate findings there, and then move on to other areas. Remember, hackers aren't going to feel bad for you and give you a pass just because your IT budget is limited.

REDLENS INFOSEC™

Preparing Your Team

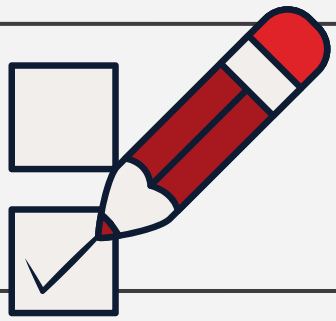
Use the knowledge you gain from a penetration test to develop an incident response plan. You can identify key players, educate them regarding potential risks, and more closely monitor vulnerable systems.

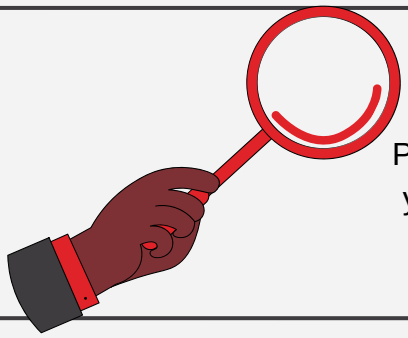
Gaining Executive Support and Buy-in

Time, money, and resources are three things that Information Security departments rarely have enough of, however, a well-conducted penetration test will provide your team with evidence to both demonstrate the value of your current security tools and support increased security investments should the tools prove to be inadequate.

Complying with Regulatory Standards

Penetration testing is necessary for compliance efforts; depending on your environment, it is required by the PCI DSS.





Gaining an alternate perspective

Partnering with a third-party who has not been involved with the implementation of your security tools will allow you to put fresh eyes on your network, helping you to reveal security faults that had previously gone unnoticed during internal reviews.

Industry Benchmarking

A thorough penetration test will provide useful information that will allow you to compare your company's overall security risk with others in your industry.

Saving Money

Investing in a pen test does require upfront costs, but your return on investment will exceed that initial budget request.

REDLENS INFOSEC™