RAPID7

WHAT IS PENETRATION TESTING?

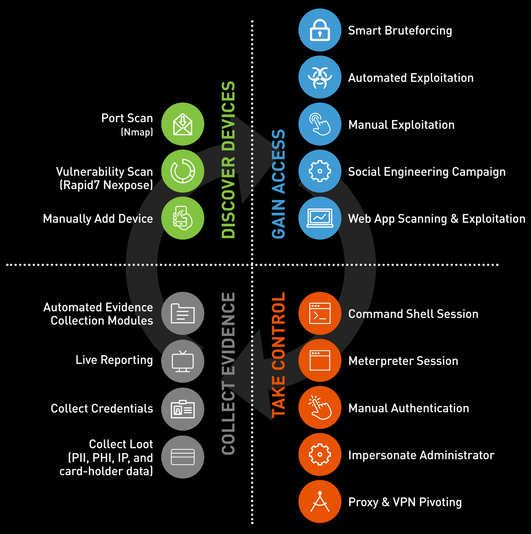
Penetration testing is the process of identifying security gaps in your IT infrastructure by mimicking real world attacks. Think about it as quality assurance for your IT security.

WHY PENETRATION TESTING?

People conduct penetration tests for a number of reasons:

- Prevent data braches
- Check security controls
- Meet compliance requirements
- Get a baseline for your security program
- Ensure security of new applications
- Assess incident detection and response effectiveness

Every penetration tester has a slightly different method, and assessments depend on the environment and goals. That said, here are the stages of a typical security assessment:



KEY CONSIDERATIONS FOR YOUR NEXT PENETRATION TEST

SET THE SCOPE
Ask, "What is the most important digital asset my company needs to protect?" Then instruct the penetration tester to try to access those systems.

CONDUCT THE TEST SAFELY
Ensure that the person carrying out a penetration test on your systems is qualified to do so. Avoid issues with your production environment.

IN-HOUSE VS. OUTSOURCED
Do you have enough work to employ a penetration tester full-time? You may want a truly independent assessment, which means enlisting an external penetration tester with a fresh set of eyes.

SELECT THE RIGHT PERSON
Whether you're hiring an internal penetration tester or a consultant, make sure they are well trained and highly trustworthy.

FOR A MORE DETAILED GUIDE ON PENETRATION TESTING PRINCIPLES AND BEST PRACTICES, DOWNLOAD THE WHITEPAPER:

www.rapid7.com/what-is-penetration-testing

RAPID7

Nasdaq