PENETRATION TESTING

guernsey

What is a penetration test?

Is the process of identifying security gaps in your IT infrastructure by conducting simulated real-world attacks on physically connected infrastructure and network access to computer systems. This simulated attack can happen on the Internet-facing external perimeter or internal systems and networks. Applications can also be included and tested explicitly for vulnerabilities and exploitable services.

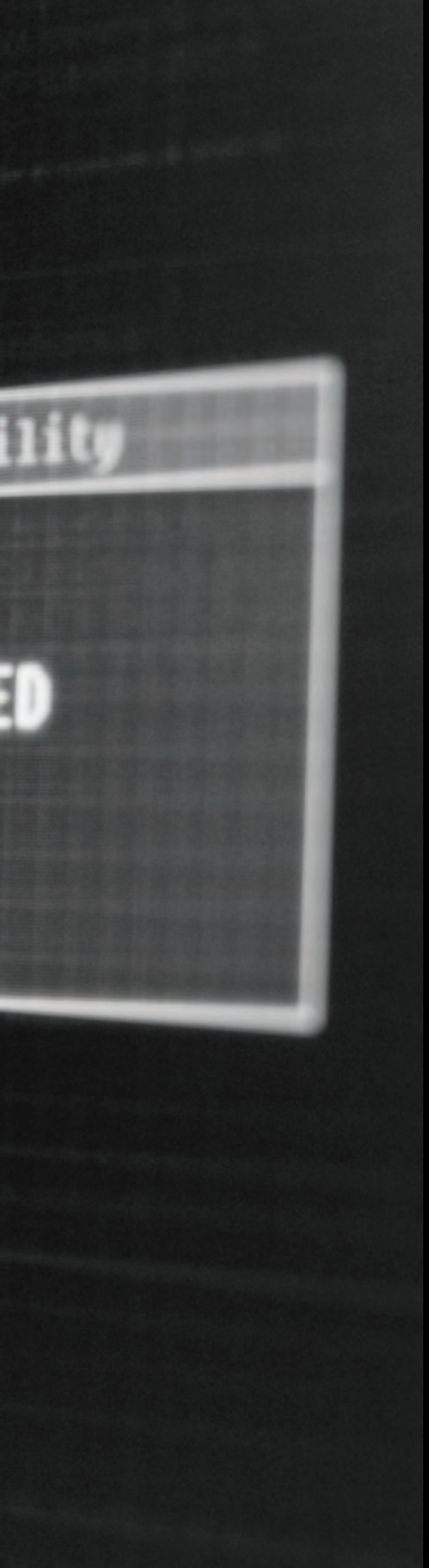
Why do you need a penetration test?

The fact is a "pen test" may not be the best approach to evaluating your cybersecurity posture, but it can be an effective way to gain comfort that your systems and applications are not vulnerable. It may also be necessary for your organization to have a penetration test performed because of regulatory or contractual obligations. Pen testing, in its many forms, may be an essential part of your overall information security program. Our professionals will work with you to understand your environment and risk profile, to design a test that best fits your needs.

What kind of testing does your company need?

Our goal to help you best use your cybersecurity budget by designing a test that mimics the likely threats to your organization. These factors vary based on factors such as your industry, the type of information you maintain, the standards of Internet-facing applications your organization has, and other factors. Our approach includes:

- **External Network Pen Test:** The goal of an external network penetration test is to simulate an attack on your Internet-facing resources. An external network penetration test will attempt to exploit what a bad actor can see from the Internet.
- **Internal Network Pen Test:** An internal network penetration test is like an external attack but is more of a simulated attack from the inside. Assuming a bad actor has gained internal access to the network, penetration testing helps to identify configurations and security weaknesses on your internal network.
- **Red-Team Exercise:** Is a simulated test that includes all or some of the types of penetration tests combined to create a more "real-world" scenario. For example, a bad actor may use phishing to gain access to an external service, then using credentials learned to pivot access to the internal network resources or Internet-facing web application resources. Another example would be gaining physical access to a building to plant a network device to send data back to the bad actor that provides intel for a more focused attack.
- **Physical Penetration Test:** Breaching physical access is when a bad actor tailgates or impersonates another person such as an employee or vendor to gain physical access to the building to steal secrets or achieve some other access such as internal surveillance that can be controlled externally by the bad actor.



What techniques are used during a penetration test?

The Guernsey team will work with you to design a test that meets your goals and addresses your organization's risks using different techniques that are often employed by bad actors. Some of the methods our experts have used include:

- **Open Source Intelligence (OISINT):** All attacks require investigation of an organization using open-source intelligence (OSINT) sources on the Internet. OSINT identifies publicly available information that can be found in sources such as databases of credentials found in past data breaches, social media sites, public records, job postings, company web page Internet, and financial records. The types of data collected include IDs and passwords, email addresses, IP addresses, and the technology used by your organization; this information helps testers target an organization by identifying targets and creating legitimacy.
- **Social Engineering:** Social engineering test uses the art of deception and manipulation to get a person to perform a task compromises the security, such as granting access, opening files, and surrendering logon credentials.
- **Phishing:** Bad actors use phishing to send forged or spoofed emails that appear from a legitimate source. The phishing email uses persuasive techniques to coerce a user to act in a way that could compromise the network.
- **Vishing:** Vishing is very similar to phishing, except this is done by making phone calls to individuals in the organization to perform a task such as reset a password.

5555 N Grand Boulevard
Oklahoma City, OK 73112
405.416.8100
guernsey.us