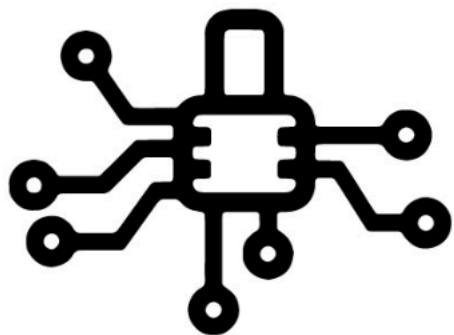


TYPES OF PENETRATION TESTING



BLACK BOX (EXTERNAL)

- No information about the internal systems, applications or source code is provided to the Penetration Tester.
- Is meant to be a true simulation of a real malicious cybersecurity attack.
- Typically it will determine the vulnerabilities in a system that are exploitable from outside the internal network.



WHITE BOX (INTERNAL)

- The Penetration Tester is given unrestricted access to information about the internal systems, applications or source code.
- Is meant to simulate both external and internal malicious cybersecurity attacks.
- Typically it will determine the vulnerabilities in systems that are exploitable for outside or within the internal network.

GREY BOX

- The Penetration Tester is given some information about the internal systems, applications or source code, but not all of it.
- Is meant to simulate both external and internal malicious cybersecurity attacks.
- Typically it will determine the vulnerabilities in systems that are exploitable for outside or within the internal network.

