arco
IT SECURITY SERVICES

Penetration Testing

Every day hackers uncover potential weaknesses in an IT environment. In 2022, over 22,500 vulnerabilities were published. Many of these get used by attackers within days, before IT units have started patching.

With a penetration test, you will be aware of security gaps that may leave your organization hackable and open to cyber attacks. To make sure your IT is safe, our dedicated team of PenTest experts conduct best-in-class white, black or grey box penetration tests with a combination of automated, semi-automated and manual tools.

While an automated penetration test is a process that uses specialized software tools or scripts to automatically scan a system for potential weaknesses, a semi-automated works with manual verification. A human security analyst reviews and validates the generated results. This multi-approach to pentesting takes intervaled, comprehensive snapshot of your company's exposure, which identifies potential security weaknesses and providing actionable insights to mitigate risks.

HOW IT WORKS

With the help of our PenTest Team, we test your systems from the outside for a classical check of your perimeter security. We can also test within your IT environment, to validate your "defense-in-depth" security.

1. DISCOVER

Our penetration testing team uses discovery tools (and probes inside your network, if we test "defense-in-depth") to identify the scope of systems, collect initial data, i.e. reachable hosts, open ports, fingerprinting of active services, versions of web-servers, etc. In addition to classic IT devices that are well-managed by most infrastructure groups, we also discover network equipment, IoT devices, IT systems, and other hardware that may have been left out of your internal management processes. The result is a comprehensive inventory of networked devices.

2. SCAN

The data is then carefully analyzed to identify potential routes for exploitation. This process is essential for understanding the target system's vulnerabilities and determining the best approach to conduct a thorough and effective penetration test. During this step, our PenTest Team search for vulnerabilities using automated tools. We use comprehensive databases of known vulnerabilities to feed the engines of our scanning tools. With these, we have a list of prioritized vulnerabilities to exploit.

3. PENETRATE

Once the PenTest Team has a clear picture of the environment, they can focus on breaching the security perimeter or exploiting a target device. We use advanced techniques to gain continual access or move laterally within threat. For any system we manage to penetrate, we collect evidence and a description of how the breach was possible.

For continued vulnerability and patch management, when known vulnerabilities are fixed by the provider, we can validate that your systems are up-to-date by performing a re-test. Our Team can also set up periodic scans to check then alert you when new vulnerabilities appear.

WHAT YOU CAN EXPECT

Your business relies on a solid foundation, without cracks or weaknesses. We'll help lay that foundation, as well as regularly reinforce it to ensure your IT infrastructure is strong. Moreover, with our continuous vulnerability scans, you can be confident that your security standards and patch management process slam the door on attackers.

YOU BENEFIT FROM

- ✓ An inventory of the services & infrastructure you have: This benefit helps you gain a clear understanding of your infrastructure and services, and allows you to get proactive on systems that you may have not been aware of.
- ✓ A list of security vulnerabilities with a risk rating for your internet-facing or internal systems, to help you prioritize your security efforts and address the most important vulnerabilities first, reducing your risk of a successful cyber-attack quickly.
- ✓ Expert advice on how to fix the identified issues; helping you to keep your defenses strong and your systems protected from cyber threats.