

Vulnerability Scanning and Penetration Testing

The background of the top half of the page is a dark blue field with a complex, futuristic pattern of glowing lines, circles, and dots, resembling a digital or cybernetic interface.

Safeguarding the Network

In an increasingly uncertain world that relies more on data and communication, organisations need to be more careful than ever that their security is up to the task of protecting their assets and to also safeguard their customers, suppliers and the general public.

Testing Your Security Posture

There are many good reasons to book a penetration test for your organisation, carried out by a qualified ethical hacker who has the skills to test your security but the knowledge to make sure your information remains safe and no real damage is caused to your organisation. Your remediation report will be devised by someone who knows everything there is to know about security and can handle any serious vulnerabilities with the utmost discretion and calm. They are able to make sensible recommendations that are tailored to your business.

Apstorm offers a comprehensive range of security testing services that test all aspects of an organisation's security. Your security solutions are an important investment for your business and it is crucial that you can show that they are up to the task of protecting your sensitive data. You may also have to prove to directors and stakeholders that your investment is being placed in the best solutions.

At a Glance

External Vulnerability Test

External Vulnerability Scanning seeks out security flaws on public facing services and network equipment to see if and where a system or service could be exploited or threatened.

External Penetration Test

External Penetration Tests take Vulnerability Scanning to the next level. Not only does a Penetration Test look for security flaws in public facing services and network equipment like vulnerability scans but a highly skilled penetration tester checks to see if these flaws can be exploited.

Internal Penetration Test

Internal Penetration Tests are designed to emulate the risk of an attacker who has breached the network defences from inside the business premises or connecting to the WiFi from outside the building.

Web Application Test

Web Application Testing involves an active analysis of the application for any weaknesses, technical flaws or vulnerabilities.

Types of Security Testing

What Does a Full Penetration Test Cover

What Does the Full Penetration Test Cover? A full Penetration Test from Apstorm comprises a number of parts. It starts with our team searching public domains, such as the internet, to see what sensitive information may be widely available and vulnerable to attack. This is followed by an automated scan on target networks. The enumeration phase looks into the operating systems, applications and services that are used by the organisation which provides a basis for the exploitation phase.

The analyst will gather everything they have learnt in an effort to actually breach the network, but take steps to ensure that any exploits carried out do not result in a denial of service or corruption of data. The tester then clears their tracks, making sure any changes that were made during the test are undone and they make a full report on what they have found, marking vulnerabilities as either CRITICAL, HIGH, MEDIUM or LOW. Organisations can then request help with the remediation process. Our vulnerability and Penetration Tests can include the following:



External Vulnerability Scanning

Nearly all organisations will have at least one internet connection, often running multiple services such as VPNs, email, cloud services, etc. Having your servers and network available over the internet is important for communication, business services and data transfer. However, they do open the door to potential security threats and hackers.

Apstorm's External Vulnerability Scanning seeks out security flaws on public facing services and network equipment to see if and where a system or service could be exploited or threatened. The service is provided remotely by a highly trained consultant and using a recognised methodology we generate a report so that the organisation can confirm the status of the security and make any needed changes.



External Penetration Testing

External Penetration Tests take Vulnerability Scanning to the next level. Not only does a Penetration Test look for security flaws in public facing services and network equipment additionally our highly skilled consultants test to see if these flaws can be exploited.

Penetration Tests use different techniques and work in a very similar way to an actual hacker but with agreed parameters and boundaries so not to disrupt or compromise the organisation being tested. Apstorm's External Penetration Test uses recognised methodologies.



Internal Penetration Testing

Internal Penetration Tests are designed to emulate the risk of an attacker who has breached the network defences from inside the business premises or connecting to the WiFi from outside the building. The test is designed to analyse how easy it is to compromise the network or system and what information they could access and take. Further testing includes escalated permission, which emulates the malicious insider and what they could do.

Apstorm provides Internal Penetration Testing through their highly trained consultants and a scope is agreed before a test is undertaken to ensure its success. A report is produced that details if and where any issues exist and addresses them.



Web Application Testing

Nearly all organisations have a website and many have public facing Web Applications for providing services or trading online. Apstorm's Web Application Testing involves an active analysis of the application for any weaknesses, misconfigurations, or vulnerabilities. Our Penetration Testers will look for web application vulnerabilities including the top ten as identified by OWASP (Open Web Application Security Project), a list showing what security professionals broadly believe to be the most critical flaws for web applications. Any security issues that are found will be presented in a report to the system owner together with an assessment of their impact and a technical solution.