

CYBERSECURITY

ETHICAL HACKING

PENETRATION TESTING

TRAINING

ISGroup
Information Security

Vulnerability Assessment

Map your exposure and prioritise what to fix first



OBJECTIVE

Know exactly what is exposed and what is at risk

A Vulnerability Assessment identifies known vulnerabilities across systems, services and network components.

It provides a clear, verified picture of exposure so the company can prioritise remediation based on real risk, not just severity scores.

METHOD

Fast analysis, verified and **focused on fixing**

Scope

Assets, addresses, services and internal or external analysis mode are defined upfront.

Scanning

Specialised tools identify known vulnerabilities, exposed versions and risky configurations.

Verification

Results are manually checked to reduce false positives and assign concrete priorities.

MODES

From the internet or internal network, on a scheduled basis

An external assessment shows what an attacker can see from the internet.

An internal assessment measures what could happen starting from the corporate network, a branch, a VPN or a specific segment.

The activity can be point-in-time, before a release or an audit, or recurring to keep exposure under continuous control.



Soddisfare i requisiti di Compliance



SPECIFICATIONS

Clear, verified results that are easy to act on

Coverage

Networks, systems, services, VPNs, exposed components and web applications.

Validation

Manual review of the most relevant results and reduction of false positives.

Priorities

Severity, impact and practical guidance to plan remediation activities.



OUTPUT

Executive Summary, technical details and remediation plan

The report turns findings into clear operational priorities.

Executive Summary for Management.

Vulnerability Details for Security Managers and technicians.

Remediation plan with precise instructions to secure systems and services.

Let's **HACK** together



ISGroup
Information Security

Tax ID and VAT 04164220230
www.isgroup.biz

BOOK A MEETING
sales@isgroup.it
+39 045 4853232