THINK SAFE. THINK ICS

OFFENSIVE SECURITY

YOUR PARTNER FOR COMPREHENSIVE IT-& OT-PENETRATION TESTING

Clarification and preparation › Scanning › Penetration › Clean up › Reporting › Catalogue of measures › Implementation system hardening

In a world of increasing cyber threats, security is essential. We protect your company with customised penetration testing, uncover security vulnerabilities and fix them before attackers can strike.

WHY PENETRATION TESTING?

› **Recognising vulnerabilities:** We identify security gaps in your systems and investigate the possibilities for exploiting these vulnerabilities.
› **Proactive security:** By closing the relevant security gaps, you strengthen your systems long before monitoring solutions could report attackers in the network.
› **Protect your data:** By securing your systems and networks, you protect your company from data loss and theft.

OUR SERVICES

TYPES OF SECURITY TESTS

Vulnerability Assessment

› Identification of **vulnerabilities** in the system
› **Automated** using tools such as NMAP, Nessus Pro or Nikto
› **Manual testing** of devices, servers and web applications
› **No** active attack

IT-Penetration Test

› Identification of vulnerabilities in the IT system
› **Verification of found vulnerabilities through active attacks**
› Comprehensive investigation by analysing various **attack possibilities**

OT-Penetration Test

› Identification of weak points in the **OT system**
› OT experts with knowledge of sensitive components and special protocols
› Comprehensive investigation by analysing various attack possibilities

Physical Penetration Test

› Identification of physical security gaps **(access and entry)**
› Checking the security of **buildings and systems**
› Specialist attempts to gain unautho-rised entry or access
› Use of **social engineering**

Red Team Assessment

› Application of tactics, techniques and procedures (TTPs) of a **real attacker**
› Verification of the Blue Team
› Red Team has high priority to remain **unnoticed**
› Detailed debriefing

Phishing Campaign

› Checking the security awareness of employees
› Various options, with and without recording access data
› **Anonymised evaluation**

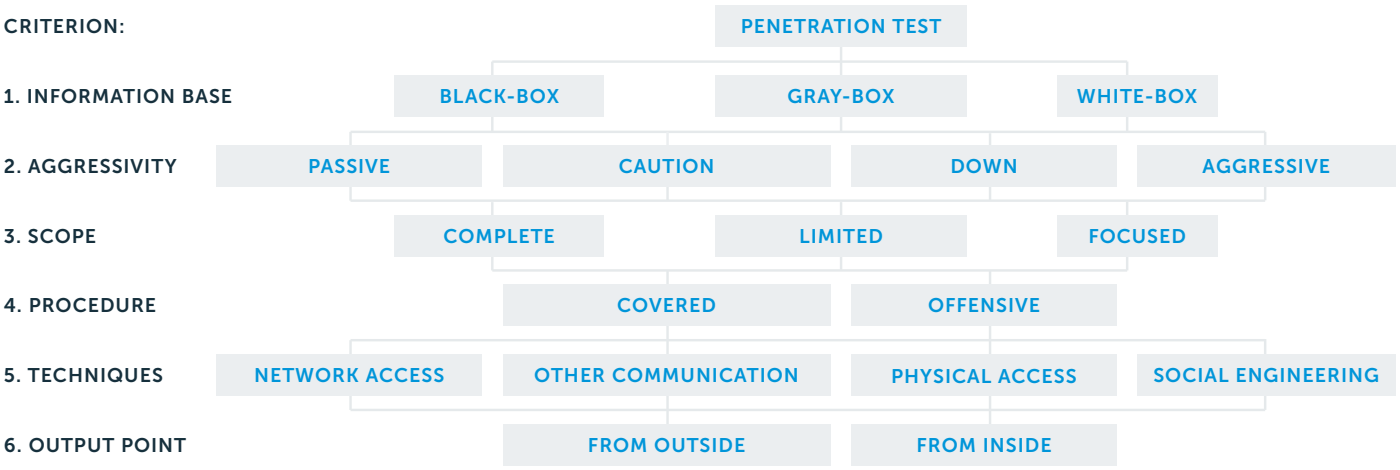
WHY ICS?

› **Expert knowledge:** Comprehensive experience in IT- and OT-Penetration testing, also for KRITIS companies.
› **Customised solutions:** Any configuration of the project according to BSI classification.
› **Highest quality:** Penetration tests with a fixed scope definition to maintain your value chains.
› **Confidentiality:** Maximum protection of your sensitive data.

OFFENSIVE SECURITY

INDIVIDUAL ADJUSTMENT OF PENETRATION TEST CONFIGURATION

CLASSIFICATION ACCORDING TO BSI



PROCESS FLOW

Information Procurement

1 EDUCATE & SCAN

› Internet and server addresses and components
› Checking the IP address for activities
› Recording domains of the website
› Analysing operating systems, protocols and ports
› Identify vulnerabilities

Penetration Test

2 PENETRATE & CLEAN UP

› Attack the target system
› Gain access to the system
› Extend access rights in the system

After completion of the tests:

› Restore the original state
› Delete created accounts
› Reset configurations
› Acceptance report

PenTest Report

3 REPORTING & CATALOGUE OF MEASURES

› Procedure and test cases
› Identified security vulnerabilities
› Risk assessment per vulnerability
› Assessment with CVSS
› System hardening measures

Optional: Closing the gaps

4 IMPLEMENTATION SYSTEM HARDENING

› Support in closing the security gaps
› If required: definition of alternative measures (e.g. for existing technology)

ICS GmbH
+49 711 21037-42
vertrieb@ics-gmbh.de
think-safe-think-ics.de