Penetration Testing is the method of simulating real-world threats using the same tactics as malicious hackers. For a safety evaluation that goes beyond a basic risk scanner, you need industry experts. Unlike automatic vulnerability tests that just scratch the surface of your network, Infopercept’s network penetration testing gives insights into the safety threats in your environment.

By taking advantage of decades of combined intelligence research, our experts will help determine:

- Where vulnerabilities occur in the network
- Overall damage, probability of abuse, and the possible effect of vulnerabilities
- How privileged accounts may be abused internally
- Which permissions can be escalated on compromised systems?

External Network Assessment

Often straightforward social engineering commitments are fruitful by deliberately exploiting confidential information or access, but not all attacks are so straightforward. In the case of more advanced commitments, operators can request simple office material, such as the organizational structure or who is on vacation. This information serves as building blocks for coercing more prepared users, using common experience to gain trust and credibility.

Conducting a social engineering evaluation with Infopercept will identify the risks and effects of social engineering as well as the potential of the organization to respond to such an attack.

Internal Network Assessment

At Infopercept, each commitment to social engineering implements a validated approach to ensure strongly focused, reliable commitments. Each engagement shall be carried out in the following steps:
ASSESSMENT DETAILS AND METHODOLOGY

At Infopercept, our network penetration testing is aimed at the full spectrum of devices on the network. Using the same tactics as professional hackers, we sometimes intentionally skip automated tools with specific access to security threats. To ensure good quality, repeatable commitments, our process of penetration testing meets the following steps:

Information gathering on the target environment

1. Reconnaissance

As with malicious hackers, any penetration test starts with the collection of information. To identify vulnerabilities, collecting, parsing, and correlating information on the target is essential.

Identify and map vulnerabilities

2. Vulnerability Detection

If the goal has been thoroughly listed, Infopercept uses both vulnerability scanning software and manual inspection to find security vulnerabilities. With decades of experience and custom-built equipment, our security engineers find loopholes that most automatic scanners ignore.

Safe and controlled exploitation of vulnerabilities

3. Attack and Post-Exploitation

At this point of the evaluation, our experts review all prior data to securely leverage known vulnerabilities. Once critical access has been achieved, attention is shifted to an escalation to identify the overall market effect.

During each step of the compromise, we keep client stakeholders updated about progress testing, maintaining asset protection and stability.

Detailed, risk-prioritized report with remediation steps

4. Assessment Reporting

If the engagement has been completed, Infopercept will include a concise review and vulnerability report, including remedial action. Our advisors set industry standards for transparent and succinct reviews, prioritizing the highest risk vulnerabilities.

The appraisal shall contain the following:

- Executive Summary.
- Strategic strengths and weaknesses.
- Identified vulnerability and risk rating.
- Detailed risk remediation.
- Assets and Data Committed during the assessment.
About INFOPERCEPT

Infopercept’s vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners’ cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint
© Infopercept Consulting Pvt. Ltd. 2021

Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

Global Offices
UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 809

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

By accessing/ proceeding further with usage of this platform / tool / site / application, you agree with the Infopercept Consulting Pvt Ltd’s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.