Introduction Vulnerability Assessments & Penetration Testing

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 is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint
© Infopercept Consulting Pvt. Ltd.
Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com
www.infopercept.com/knowledge/datasheets