HOW PENETRATION TESTING CAN SAVE YOUR COMPANY

CONTENTS

1 What is penetration testing?

How effective would your existing security controls be against a skilled adversary? Discover the answer with penetration testing.

The main difference between a penetration test and an attacker is permission. A hacker will not ask for permission when trying to expose your critical systems and assets, so to protect them, you need to do thorough penetration testing.

A ‘pen’ test is not just a hacking exercise. It is an essential part of your complete risk assessment strategy.

Pen testing is a method of compromising the security of a computer system or network by simulating an attack by a malicious hacker.

2 Malicious Hacker vs. Penetration tester

Agent 007 for your cyber security and how to recognize him in action:

MALICIOUS HACKER	PENETRATION TESTER
No moral restrictions.	Observe strict moral code, NDA.
Unauthorized.	Must be authorized.
It can use any techniques without regard for the consequences.	It should be extended to pre-approved limits.
Trying to avoid / delete chronological records (logs).	Must record all actions.
No report.	Must submit a detailed report.
Taking advantage of vulnerabilities.	Describes the vulnerabilities and recommended approaches for elimination.
With unknown competencies and it is unclear whether it can repeat the attack.	Well-trained, with experience and documenting actions.

3 Security is your business

The security of your systems can be compared to security of your car and how safe it is.

Do you know about OWASAP Top 10 – 2017 chart?

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software and every few years, it posts an updated chart of the top 10 leading security risks.

3 Security is your business

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 - Injection	→	A1:2017 - Injection
A2 - Broken Authentication and Session Management	→	A2:2017 - Broken Authentication
A3 - Cross-Site Scripting (XSS)	↘	A3:2017 - Sensitive Data Exposure
A4 - Insecure Direct Object References (Merged + A7)	U	A4:2017 - XML External Entities (XXE) (NEW)
A5 - Security Misconfiguration	↘	A5:2017 - Broken Access Control (Merged)
A6 - Sensitive Data Exposure	↗	A6:2017 - Security Misconfiguration
A7 - Missing Function Level Access Contr (Merged + A4)	U	A7:2017 - Cross - Site Scripting (XSS)
A8 - Cross-Site Request Forgery (CSRF)	☒	A8:2018 - Insecure Deserialization (NEW, Community)
A9 - Using Components with Known Vulnerabilities	→	A9:2017 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards	☒	A10:2017 - Insufficient Logging&Monitoring(NEW,Comm.)

(Source: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)

Are you secure from any of these?

4 Challenges that penetration testing helps with

Are you familiar how pen testing can help? Here are some examples:

GDPR

- Are you familiar with how your data assets can be protected in the case of a data breach?
- After GDPR entered through our business door and in case of data loss, controllers shall notify the supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours, unless the breach is likely to result in a risk to the rights and freedoms of individuals.

Penetration tests improve your security by testing for data breaches.

PCI-DSS

Every financial institution according to Payment Card Industry Data Security Standard needs to undertake penetration tests at least every 6 months.

The tests help:

- to determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files, logs and/or cardholder data.
- to confirm that the applicable controls, such as scope, vulnerability management, methodology, and segmentation, required in PCI DSS are in place.

4 Challenges that penetration testing helps with

Prioritizes security risks.

- How do you know which security risks your company mostly avoids?
- Are you familiar with how the IT environment in your organization can protect you, and from what type of security risk you are not aware?
- According to the Ponemon Institute, 7 out of 10 organizations agree that their security risk increased significantly in 2017.

Avoid the cost of network downtime

- Do you know the system downtime and theft of information assets have become the second security risk, after loss of IT and end user productivity?
- Penetration tests can provide additional information about which hardware solution can attack first, so an organization can secure them in advance.

Preserve corporate image and customer loyalty

- Carnegie Mellon University confirms there is a clear relationship between security breaches and loss of consumer trust and loyalty.
- Security specialists advise how to review the network security to ensure emerging threats are recognized, and your organization is prepared to defend against them.
- By defending your customers from attacks, you can:
  - Retain customer loyalty and trust for the long term
  - Lower the incurred costs of handling and compensation of customer fraud cases.
  - Protect your brand reputation.

5 Top 5 goals of penetration testing

Make sure your penetration tests will:

- Identify and assess vulnerability checks
- Identify vulnerabilities that have not been found during automatic scans
- Evaluate the effects of potential losses in the case of a successful attack
- Check the network security effectiveness
- Provide additional security of personal and corporate data, preserving corporate image and customer loyalty

6 About Lirex

Lirex has more than 25 years of experience in the IT field, serving customers from six continents. The company is a leading system integrator, adding highly valuable service to companies for chemical, government agencies, banking, and defense industries. Lirex has extensive experience with Western European clients, providing them penetration testing and IT auditing services, IT security patches management, testing & implementation services. The company is a well-known partner with Check Point, Cisco, HP and Microsoft. It is certified by ISO 9001 (Quality); ISO 27001 (Information Security); ISO 20000 (ITIL); ISO 14001 (Environmental management) & BS OHSAS 18001 (Health and Safety).

LIREX BG
IT INNOVATIONS

Trust your security with us:

Richard Leslie
UK Business Development - LirexBG
mobile: +44 7771 787840
rleslie@lirex.com

Kristiyan Mihaylov
International Sales Specialist
mobile: +359 882 720 233
kmihaylov@lirex.com