EXCELLIUM

Your first call when it comes to IT and security

INTRUSION TESTS - RED TEAM

SECURITY ASSESSMENTS

The intrusion department is specialized in security assessments and penetration tests. The goal of the missions is to attack the targeted infrastructure and provide a valuable report explaining how to remove the vulnerabilities, enhance the detectability and make the exploitation attempts harder.

> There are two kinds of people: those who know they have experienced a cyber-attack and you.

CUSTOMER CHALLENGES

Each enterprise networks is attacked several times a day. Even if some security strategies are in place, the only way to verify their efficiency is to assess the defences like real attackers. This is why Excellium has developed several scenarios to simulate realistic tests specialized against those targets:

- Web application
- Internal LAN / WI-FI
- Internet perimeter
- Remote access
- SQL/NoSQL databases
- Physical Security and Social Engineering
- Stolen laptop
- Authentication and single sign-on portals
- Mobile (apps, devices, MDM)
- Citrix/VDI environments

OUR APPROACH

For years, classical intrusion tests were limited to vulnerability assessments, no attention was put on the detection capabilities nor on the difficulties to exploit the issues without noise. Our approach at Excellium is different because each scenario can be declined to test specifically the vulnerabilities, the detection capabilities or the hardening effort put on the target. It clearly helps to reproduce an attack in a realistic manner and to provide the best guidance based on the client's strengths and weaknesses.

This approach also helps to enhance the security as a process and not only with products. Our methodology combines:

- Vulnerability identification
- Detection capabilities
- Hardening robustness
- Patching strategy
- Awareness and knowledge transfer

INTRUSION TESTS BENEFITS

For Excellium, a mission is successful when the client understands all the attacks launched against the target, agrees on the remediation plan and knows how to implement the fixes.

The mission helps the security team to prioritize the investments and projects in terms of remediation strategy. The benefits can be summarized by the following:

- Better understanding of the infrastructure strengths and weaknesses
- Learning of new attack technics
- Cost estimation of the fixes
- Compliance
- Rating using standard references (OWASP, CVE, CWE)
- Governance adjustments and security roadmap definition

ABILITY TO DELIVER

Our team is composed by known security experts, involved in notorious projects such as OWASP, Metasploit and MITRE.

RESEARCH & DEVELOPMENT

The team created many tools in order to improve the simulation of realistic attacks. For example, some tools are specialized in phishing, malware distribution, mobile application reverse engineering, and web browser assessment.

DETECTION

The tools are homemade and not recognized by any antivirus nor classical security systems.

CONFIDENTIALITY

Excellium is PSF accredited since 2016.

COLLABORATION

Our CERT-XLM CSIRT, network and security teams help to better understand the attacks and the defences capabilities in order to be more efficient and up to date during the tests.

SERVICES PROVIDED

The mission ends with several documents that help to better understand the attack scenarios, the threats and the recommendations.

The deliverables are the following:

- Executive report
- Technical report
- Vulnerability scan results
- Risk analysis and recommendation for each vulnerability
- Remediation plan
- Benchmark compared to the same market actors
- Closure meeting and pragmatic explanation of the risks
- Document classifying the findings in a task list with owners and technical details

EXCELLIUM

Twin Squares , Culliganlaan 1B
B-1831 DIEGEM
Office: +32 2 403 12 81

5 rue de Goell
L-5326 CONTERN
Office: +352 26 20 39 64