Ethical Hacking

A2SECURE

Check the efficiency of your security countermeasures by simulating real attacks

The A2SECURE team, by means of the expertise in simulating security attacks, provides organizations with the global perspective for the strengthening of IT comprehensive security and operational efficiency, risk mitigation and compliance of specific regulations.

Thinking Offensive to strengthen the Defense

The exploitation of existing vulnerabilities has become the most frequent cause of security breaches. It is essential to be able to verify that applications, networks and systems are not vulnerable and exposed to a security risk to avoid those vulnerabilities to be exploited by non-authorized or malicious users. A vulnerability analysis would not suffice though. It is also necessary to weigh the true impact of their exploitation and what effective actions need to be put in place.

A2SECURE: the solution

A2SECURE combines the singularity of every specific client with a systematic methodology which guarantees a global high-quality security service. On top of following the best industry standards A2SECURE adds value by including our next generation in-house designed tactics, in continuous development by our pentesting team.

We are conscious that one of the keys of our success lies in being able to transmit and add value to our activity. The final report of result compilation together with a personalized meeting, facilitates the understanding of the findings and the start of the mitigation phase continuously supported by the expertise of our team.

Ethical Hacking: the method

Ethical Hacking is the answer to your concern "can a hacker penetrate my network?" Intrusion tests identify vulnerabilities that a malicious user would use to enter your organization enabling it to proceed with vulnerability mitigation. Your organization obtains a greater understanding of the current security environment and would allow you to define a hardening strategy for the potential most common or specific cyber attacks which could benefit from the existing vulnerabilities in your organization.

We emulate similar tests to the ones commonly used by attackers to show how they could get access to the non authorized areas of your organization. From the search of the public information through OSINT, compromised user credentials, exploitation of vulnerabilities, pivoting to the point of reaching persistence. We take advantage of the smallest weakness within all of your network to compromise those assets which should really concern you.

Benefits

- Gaining insight of the real risks threatening your organization
- Developing an action plan with the countermeasures and actions to mitigate and reduce the risk
- Increasing the global security by defying the defensive measures in place under controlled conditions
- Achieving compliance in line with standard and legal regulations such as HIPAA, PCI-DSS, FFIEC, among others
- Remediating the vulnerabilities thanks to a structured action plan based on prioritization side-by-side with A2SECURE

WE ARE CYBERSECURITY

Customized and business oriented perspectives

A2SECURE pentests can be performed from an external perspective, that is to say, to evaluate network perimeter threats or, on the other side, within the network, at an internal level.

The audits of WiFi networks identify which wireless devices are accessing your network, determine the existing unauthorized access points and evaluate the security infrastructure of the WiFi.

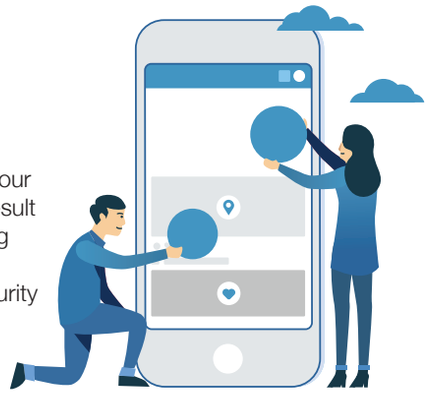
Intrusion tests of iOS applications as well as the ones for IoT devices identify security breaches in the application code, potential leaks or data exfiltration, and vulnerabilities that could be exploited or alter the performance of the application.

What to expect in your report

- **Executive Summary**, directed to the non technical audience: management, auditors, board of directors or others
- **Technical Summary**,it describes the identified issues altogether with the implied risk and our recommendations to fix or mitigate.
- **Technical Report**, directed to the technical personnel within the organization. It provides the findings with specific details and evidence for:
  - Methodology: detail of the activities and the tests performed following standard procedures of the industry and the sequence of specific actions taken by the cybersecurity and ethical hacking professionals to achieve the objectives of the project.
  - Description: it shows every vulnerability and potential security failures with the steps to be replicated in order to locate and reproduce them. It also indicates the risk and threat implied, and correlation between them.
  - Recommendations: to proceed with the remediation every vulnerability goes with adequate instructions to solve them. They also include links to additional knowledge sources so that you can get more information or additional recommendations to remediate or reduce their risks even further. Also any additional information for the understanding of the existing risk or its possible mitigation.
  - Social Engineering Results: description of the social engineering attacks which have been performed, success rate and possible consequences.

Human Factor

People are the weakest link. Your team can be vulnerable and result in a risk. Our social engineering tests are key to identify if the personnel need training in security and best practices such as:



- Enforcing a cybersecurity program and evaluating security and awareness of the employees and systems
- Executing social engineering attacks such as phishing, smishing, vishing, or physical intrusions in your premises which make the employees aware of potential real attacks
- Aligning the benefits of intrusion tests with the continuous improvement in awareness

Key Points

- Customized projects focusing on the review of the critical systems for your business
  Protect your assets
- Detailed reports containing not only the findings but also the analysis of the causes, the way in which they could be exploited and the instructions to solve them
  Combat the threats
- Executive summary with the description of the vulnerability and its possible impact on the different areas of your business
  Gather efforts in security
- Analysing and exploiting vulnerabilities using manual techniques always under control of our ethical hacking experts
  Cooperation and involvement
- Methodology for the assessment and testing of the systems in line with the functional structure of your organization
  Passion for what we do

For more information,
to reach our experts at A2SECURE contact us at +34 933 045 600

info@a2secure.com
www.a2secure.com

A2SECURE

A2SECURE is a company devoted to cybersecurity. Our objective is helping to prevent and manage the risk in our clients facing threats caused by electronic communications. To reach our objective we offer a variety of solutions and services able to satisfy the needs of our clients adapting your requirements resources and availability.