Penetration Testing Services

The Types Of Penetration Test We Offer:

- Infrastructure Testing.
- Web Application Testing.
- Mobile Application Testing.
- Wireless Network Testing.
- Cloud Service Testing.
- Embedded Device / IoT Testing.
- Industrial Control System (ICS) Testing.
- Agile Development Testing.

M360 SECURITY

Brochure Index

M360 SECURITY

INDEX

Methodologies of a Penetration Testing

Blackbox Penetration Testing

Execution of intrusion tests on the Client's "On-Site" site, with 0 level of pre-consented information for:

1. Present a scheme of the vulnerabilities found in relation to their difficulty of remediation and their impact on the organization's information assets.
2. Recommend the most effective solutions for your organizational structure and/or information assets in particular, defined in the scope; that maximize efficiency in the investment to maintain optimal levels of security in the short and medium term.
3. That the scheme of recommended solutions based on the vulnerabilities found, allows strategic and tactical decisions to be taken in relation to the information assets of the segment being analyzed.
4. Recommend optimal strategies for information asset security, taking into account the characteristics of the organization's own business.

Greybox Penetration Testing

Execution of intrusion tests on the Customer's ONSITE site, with at least 1 (one) prior information regarding the target system, this information would be obtained in the first instance through some satisfactory attempt of the Back Box stage or otherwise, by consensus with the work team.

The objective is to detect vulnerabilities, identify them and assign them an approximate criticality level in order to know the associated risks and draw up a remediation plan.

Depending on what is detected in the discovery and evaluation stages, the services and IP addresses to be analyzed and the level of depth reached for each case will be agreed with the contract manager. In some cases, vulnerabilities may be exploited.

Methodologies of a Penetration Testing

Whitebox Penetration Testing

This type of evaluation corresponds to the Internal perspective, where the client provides a detailed structure of its Network infrastructure and through Internal Hacking techniques, the necessary information is obtained to continue with the evaluation. It prevents internal attacks by employees, guests, etc. An evaluation is made with valid and authorized credentials, to analyze all the sensitive information and privileges that the internal structure of the organization has.

The objective is to detect vulnerabilities, identify them and assign them an approximate criticality level in order to know the associated risks and draw up a remediation plan.

Passive Recognition Stage.

Although the client will provide information about the objectives, in order to give an added value we will try to obtain information related to them through the interaction with known search engines, query groups, dns records information, information in whois bases and all that information container that does not have a direct relation with any of the objectives.

In this stage permit, the client is informed of the level of visibility that the targets have from the outside in the eyes of a potential attacker. It should be noted that a high level of visibility does not necessarily imply a vulnerability, but the aim of this stage is to provide all available information about them so that the client can later determine and expose only the strictly necessary information.

Stages of Recon

M3 60 SECURITY

Surface Active Recon Stage

In this stage and contrary to the previous one, it will begin to identify points directly related to the objectives and interacting with them, in this way this stage seeks to identify in principle the active objectives and then practice in the same deeper analysis as those described in the stages following this one.

Active In-Depth Recon Stage

The objective of this critical stage is to practice a much deeper analysis of the objectives detected in the previous stage.
The tests performed in this stage aim to identify all open ports both TCP and UDP, list and identify as precisely as possible all services running on the open ports, identify versions of operating systems on which applications run.
Identify the network topology in which the targets live, in order to analyze the correct implementation of the filtering and detection devices that may exist.

Vulnerability Analysis Stage

With the information obtained in the previous stage, the objective of this stage is to detect potential vulnerabilities that the objectives may have both at the infrastructure and application level.

This stage can be considered sensitive, as appropriate work must be done to eradicate false positives that may be misreported.

Phases of a Penetration Test

The different phases of the analysis are described below

Recon:

Objectives are defined and as much information as possible is collected and then used throughout the following phases. The information sought ranges from names and e-mail addresses of the organization's employees, to network topology, IP addresses, among others. It includes, but is not limited to, the following activities (always depending on the defined scope):

- Identify the network topology.
- Identify the logical network domain used and its configuration.
- Identify network devices (Firewalls, UTMs, Routers, etc.) and filtered ports.
- Analysis of all ports (1 to 65535) open at TCP level, in the different systems of the Company that are detected in the scanning of the IP addresses on the Internet.
- Scanning of all ports (1 to 65535) open at UDP level, in the different systems of the Company that are detected in the scanning of the IP addresses on the Internet.
- Analysis of the security of the links that the Company has to the outside.

Phases of a Penetration Test

The different phases of the analysis are described below

- Analysis of connections with third parties.
- Detection of active services.
- Detection of protocols in use.
- Identify versions and models of Routers, Switches, Firewalls and/or UTMs.
- Analysis of responses to different protocols and packets.
- Detection of used servers and their versioning.
- Remote detection of Server base Operating Systems.

Platform logic survey, trying to detect:

- Routers.
- Switches.
- Firewalls/UTMs.
- Load balancers.
- E-mail Servers.
- DNS servers.
- Proxy servers.
- FTP servers.
- WEB servers.
- VPN Terminators and Remote Access systems.
- Database Systems (SQL Server, Oracle, MySQL, PostgreSQL, etc)..

WHO WE ARE

A Team Of Highly Qualified Professionals With:

Advanced Penetration Skills And Ethical Profile.
Internationally Recognized Professional Certifications.
Years Of Proven Experience In The Field.
Advanced Attacking Skills On Different Aspects Of Security.

What sets us apart from traditional consulting firms is that we think like cybercriminals do.

World Class Penetration Testing

M360 SECURITY