GLOBALCOM
DATA SERVICES

SECURITY ASSESSMENT PENETRATION TESTING

IMPROVE THE SECURITY OF YOUR NETWORK BY DISCOVERING ITS WEAKNESSES

Penetration testing's purpose is to highlight the strengths and weaknesses of the targeted asset on your network as well as your security protocols and team's readiness.

GDS will work with your IT or security team to customize the assessment based on several options, conduct the penetration test and provide you with a comprehensive report that highlights the findings.

SERVICE OPTIONS

Penetration testing can be conducted in different ways using several techniques.
The purpose of these options is to provide you with the most adequate result with regards to the purpose of the test and the assets to be tested.

BENEFITS

- Discover risks before they affect your business.
- Validate security procedures and security team response protocols.
- Improve security awareness.
- Assess the security of applications and systems.
- Get an overall security score.

DELIVERABLES

- Executive summary C-level report.
- Technical assessment details including steps to understand and reproduce the findings.
- Scoring and risk analysis of the discovered threats on your network.
- General recommendations for increasing resilience against cyber-attacks.

PENTEST PROCEDURE

PENETRATION TESTING IS A SIX-STEP PROCEDURE

STEP 1 PLANNING & PREPARATION

Start by defining the goals and objectives of the penetration testing with the customer:

- Identification of the vulnerability to improve the security of the technical systems.
- Increase the security of the organizational/personnel infrastructure.

STEP 2 RECONNAISSANCE

Includes an analysis of the preliminary information. We start by analyzing the available information and, if required, request system information from the client such as system descriptions, network plans and others. This step is defined by the customer based on the selected awareness option (Black, grey or white box).

STEP 3 DISCOVERY

Automated tools are used to scan the vulnerabilities to list the active assets on the network:

- Network Discovery – Discover additional systems, servers, and other devices.
- Host Discovery – Determine open ports on these devices.
- Service Interrogation – Interrogate ports to discover actual services running on them.

STEP 4 ANALYZING INFORMATION & RISKS

Analysis and assessment of the information gathered before the test steps for dynamically penetrating the system:

- Defined goals of the penetration test.
- Potential risks to the system.
- Estimated time required for evaluating potential security flaws for the subsequent active penetration testing.

From the list of identified systems, we may choose to test only those which contain potential vulnerabilities.

STEP 5 ACTIVE INTRUSION TESTING

We use several attack techniques to exploit the targeted asset agreed upon in the contract.

STEP 6 REPORT

- Overall summary of penetration testing.
- Details of each step and the information gathered during the penetration testing.
- Details of all the discovered vulnerabilities and risks.
- General recommendations for eradication.
- Suggestions for improving the security.

STANDARD SERVICE OPTIONS FOR PENETRATION TESTING

AWARENESS	OBJECTIVES	BENEFITS
BLACK BOX	Identify the vulnerabilities of systems exposed to the Internet	Understand the risks on assets exposed to the Internet
GREY BOX	Simulate an intruder that gained access to your inside network and try to perform hacking through different techniques	Understand the risks on assets due to breach
WHITE BOX	Simulate an intruder that has knowledge of the application source code and network and try to perform internal hacking	Understand the risks of data exfiltration due to application and network breach

AGGRESSIVENESS		
PASSIVE	Discover the vulnerabilities through passive scan	Identify unknown vulnerable assets that are not identified by the management systems
CALCULATED	Perform assessment of the targeted asset	Identify if the targeted asset is vulnerable
AGGRESSIVE	Perform assessment until a vulnerability is detected	Assess the level of security protection

EXTENT		
FULL	Assess all parts of the targeted asset	Assess the security of the asset from all perspectives
REDUCED	Assess within a defined extent	Understand the possibility to perform intrusion up to a certain level
SPECIFIC	Assess a specifically defined part of an asset	Understand the security level of specific parts of the asset

APPROACH		
STEALTHY	Conduct the test without prior knowledge of the security team	Understand the risk of threat in normal conditions
OVERT	Conduct the test while the security team is informed	Assess the response level and capabilities of the security team

TECHNIQUE		
NETWORK BASED	Conduct the test through the Internet or using a network technology	Understand the risk coming from a typical connected environment
SOCIAL ENGINEERING	Conduct the test using techniques that exploit the personnel	Assess resilience to phishing techniques or personnel exploitation
PHYSICAL ACCESS	Conduct the test using physical access to the systems	Assess the resilience to attacks when physical presence is ensured

STARTING POINT		
OUTSIDE	Conduct the test from an external network location	Simulates an attack from a typical point of view
INSIDE	Conduct the test from an internal network location	Assess resilience of the second line defenses after a breach has happened

METHODOLOGY

Penetration testing follows different methods for assessing the vulnerabilities of the target. Depending on the type of each asset, a certain technique is adopted. Multiple techniques can also be utilized on a single asset depending on the end-goal.

Web applications along with mobile applications are inspected and tested for vulnerabilities that can lead to unauthorized access or data exposure. Methods of testing include reconnaissance for information leakage, SQL/xml/code/command injection or application misuse. Our team will test for weaknesses in transit protection, unnecessary permissions, weak server-side controls and weak protection in stored data. Our team will also conduct tampering and reverse engineering to get a deeper understanding of the vulnerabilities.

Network infrastructure is assessed for security by gathering information, exploiting vulnerable devices, conducting lateral movement, achieving persistency on devices and finally exfiltrating data.
For WiFi networks, our team will assess the security of the deployed solution: 802.x, Bluetooth, ZigBee or others. We will conduct access control, wireless integrity, wireless confidentiality and post-authentication attack testing.

Our teams are also able to conduct social engineering testing. The purpose is to assess security awareness and general security controls with respect to human manipulation. Approach vectors are as varied as emails, phone calls, media drops and physical access. We build on the potential of search engine discovery, email harvesting, spear phishing, social media harvesting and email spoofing to achieve our purpose.

To learn more about GDS and our security portfolio, visit **https://www.gds.com.lb/security-services.html**

Globalcom Data Services sal
Holcom Bldg., 4th floor
Corniche Al Nahr, Beirut, Lebanon
Tel: +961 1 59 52 59
info@gds.com.lb

About Globalcom Data Services sal
Operating since 1996, GDS is widely regarded as being one of the first Data Service Providers in Lebanon to bring modern and fast connectivity to the country. Always leading the way to the future for individuals and businesses, GDS has been continuously supporting new technologies for more than 20 years.
Building on its extensive network and security expertise, GDS provides a comprehensive security services portfolio. A team of security experts is available to assist customers with facing the complex security threats and cyber attacks that might affect their business.