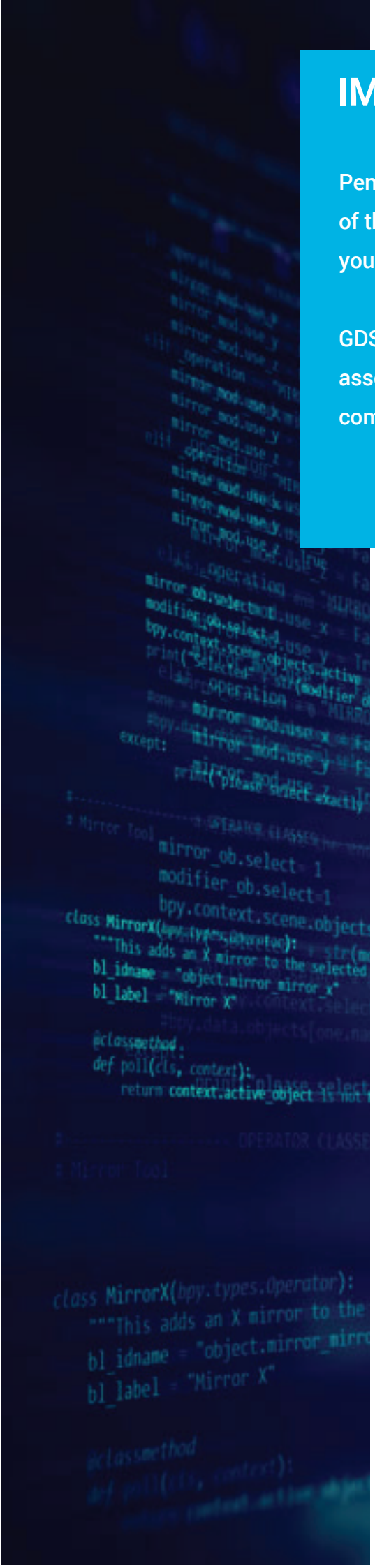
GLOBALCOM
DATA SERVICES

SECURITY ASSESSMENT
PENETRATION TESTING



IMPROVE YOUR NETWORK SECURITY

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

GDS will work with your IT or security team to customize the assessment, conduct the penetration test, and provide you with a comprehensive report highlighting the results.

SERVICE OPTIONS

Penetration testing can be conducted in different ways using various techniques.

The purpose of these options is to provide you with the most adequate result – this includes the purpose of the test and the assets to be tested.

BENEFITS

- Discover potential risks
- Validate security procedures and security team response protocols
- Improve security awareness
- Assess the security of applications and systems
- Achieve overall security score

DELIVERABLES

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

PENTEST PROCEDURE

PENETRATION TESTING IS A SIX-STEP PROCEDURE

STEP 01

PLANNING & PREPARATION

Define goals and objectives of penetration testing with the customer:

- Identify vulnerabilities to improve security of technical systems
- Increase security of organizational/personnel infrastructure

STEP 02

RECONNAISSANCE

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

STEP 03

DISCOVERY

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

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

STEP 04

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 that contain potential vulnerabilities.

STEP 05

ACTIVE INTRUSION TESTING

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

STEP 06

REPORT

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

STANDARD SERVICE OPTIONS

FOR PENETRATION TESTING

AWARENESS	OBJECTIVES	BENEFITS
Black Box	Identify vulnerabilities of systems exposed to the Internet	Understand the risk on assets performed to the Internet
Grey Box	Simulate an intruder that gained access to your inside network, and try to perform hacking through different techniques to your system	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 vulnerabilities through passive scan	Identify unknown vulnerable assets unidentified by management systems
Calculated	Perform assessment of targeted asset	Identify a potential vulnerability in targeted asset
Aggressive	Perform assessment until a vulnerability is detected	Assess level of security protection
EXTENT		
Full	Assess all parts of targeted asset	Assess security of the asset from all perspectives
Reduced	Assess defined level of extent	Understand possibility to perform intrusion [up to a certain level]
Specific	Assess specific section of the asset	Understand security level of specific parts of the asset
APPROACH		
Stealthy	Conduct test without prior knowledge of the security team	Understand risk of threat in normal conditions
Overt	Conduct test when the security team is informed	Assess the response level and capabilities of the security team
TECHNIQUE		
Network Based	Conduct test using the Internet or a network technology	Understand the risk coming from a typical connected environment
Social Engineering	Conduct test using techniques that exploit the personnel	Assess resilience to phishing techniques or personnel exploitation
Physical Access	Conduct test using physical access to the systems	Assess resilience to attacks when physical presence is ensured
STARTING POINT		
Outside	Conduct test from an external network location	Simulate an attack from a typical point of view[MR1]
Inside	Conduct test from an internal network location	Assess resilience of the second line defences after a breach has occurred

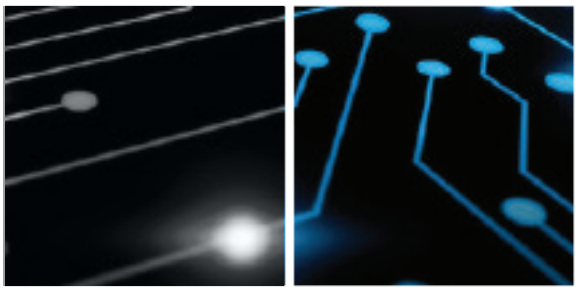
METHODOLOGY

Penetration testing follows different methods for assessing the vulnerabilities of the target. A specific technique is adopted depending on asset type – however, multiple techniques can be used on a single asset depending on the end-goal.

Web and mobile applications are inspected and tested for vulnerabilities – this 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 exfiltrating data.

With regard to WiFi networks, our team will assess the security of the deployed solution – i.e., 802.x, Bluetooth, ZigBe. We will also conduct access control, wireless integrity, wireless confidentiality and post-authentication attack testing.



Our team also conducts social engineering testing: the purpose of testing is to assess security awareness and general security controls with respect to human manipulation. Approach vectors may include emails, phone calls, media drops and physical access. By building opportunity for potential search engine discovery, email harvesting, spear phishing, social media harvesting and email spoofing, we are able to achieve our purpose and objectives.

To learn more about GDS and our security portfolio, visit **www.gds.com.lb**

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 deemed one of the first Data Service Providers in Lebanon to provide modern and fast connectivity across the country.
GDS leads the way to the future by consistently supporting new technologies for over 20 years.
GDS provides a comprehensive security services portfolio by building on its extensive network and security expertise.
A team of security experts is available to assist customers with complex security threats and cyber-attacks that may potentially affect their businesses long-term.