wizlynx group

Your Cyber Security partner worldwide

Advanced Penetration Testing & Ethical Hacking Services

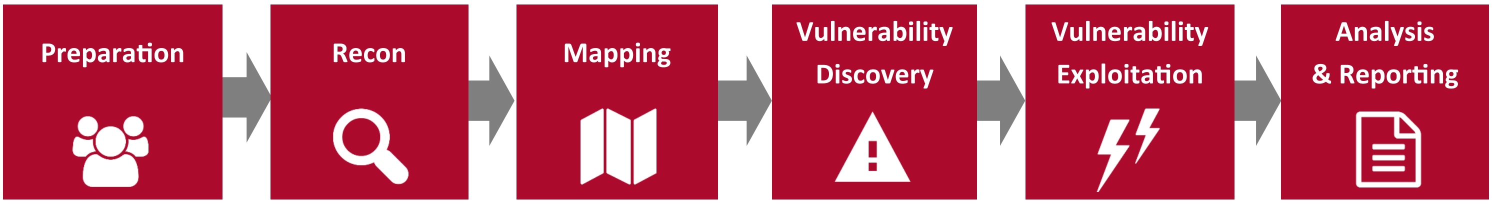
Cybercrime is on the constant rise—this is a fact. More now than ever, companies of any size and industry must verify that all existing applications, networks and systems do not have any vulnerabilities that would result in loss of sensitive information, reputation, revenue and customer loyalty, if exploited.

wizlynx group penetration tests are tailored based on your needs and environment. We leverage a global team of resources, comprised of highly skilled security professionals and penetration testers with extensive experience, both defense and offense. Uniting diverse mindsets better enables us to reach our ultimate goal: **your security**.

All of our penetration tests use a hybrid testing approach which combine the advantages of both automated tools and manual testing for a more controlled and thorough penetration test.

METHODOLOGY

At wizlynx group, our penetration testing methodology builds on the approach outlined in the OWASP Testing Guide, Open Source Security Testing Methodology Manual (OSSTMM) and Penetration Testing Execution Standard (PTES).


Preparation → Recon → Mapping → Vulnerability Discovery → Vulnerability Exploitation → Analysis & Reporting

Preparation: Essential step of a penetration test which determines the assessment's success. This phase consists of building the scope and preparing the rules of engagement, together with the customer and based on it needs.

Reconnaissance: Provides the foundation for a successful, efficient, and informed penetration test. Therefore, this is one of the most important phases where we gather publicly available information regarding the target asset and organization.

Mapping: Active information gathering to identify underlying components such as operating systems, running services, software versions, etc. In this phase, we learn how the application works, its features, and understand the relationship between application components in order to identify attack vectors that can be leveraged, e.g. for privilage escalation.

Vulnerability Discovery: Evaluation of the information assets in scope against 80'000+ vulnerabilities and configuration checks, in addition to CWE/SANS TOP 25 Most Dangerous Software Errors and OWASP Top Ten vulnerabilities.

Vulnerability Exploitation: Attempt to gain privileged access to the target system in a controlled manner by exploiting previously identified vulnerabilities.

Analysis & Reporting: Comprehensive risk analysis with an executive summary, detailed findings, and actionable and prioritized remediation steps.

OUR PENETRATION TEST PORTFOLIO

Web Application

Comprehensive penetration test of your web applications, web services and APIs that may be used to store and access critical business information, with the goal to identify and exploit web-borne vulnerabilities. Our pen-testers will use advanced skills and techniques required to test modern web applications and next-generation technologies.

Network and Server Infrastructure

Evaluation of your internal or external information assets' ability to withstand attacks. Our world-class penetration testers, armed with the same techniques as cybercriminals, will attempt to break into your network, IT infrastructure, and servers to raise awareness about vulnerabilities and the effects of exploitation, as well as end-user adherence to security policies.

Mobile Application

Access to your mobile applications to identify vulnerabilities specific to mobile computing environments, such as those defined by the Open Web Application Security Project (OWASP) and other emerging industry standards.

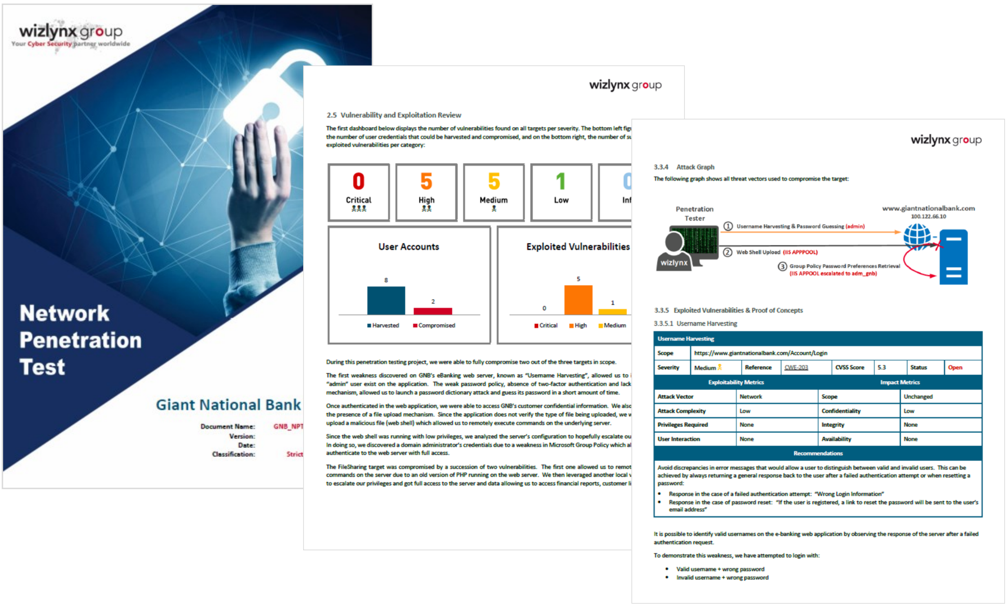
Wireless Networks

Comprehensive wireless penetration testing services, ranging from traditional WiFi networks to specialized wireless systems, which include identifying and exploiting vulnerabilities and providing guidance to strengthen such identified weaknesses.

Our penetration tests can be performed black box (no knowledge of the environment), grey box (limited information of the environment, or white box (with full knowledge of the environment).

WHAT YOU WILL GET

wizlynx group's penetration test results will be documented in a detailed technical report of observations, which will include security vulnerabilities, weaknesses and misconfigurations. These observations will have actionable and prioritized technical recommendations, along with a summary of the key findings discovered during the penetration test.



wizlynx group
Your Cyber Security partner worldwide

Network Penetration Test

Giant National Bank

Document Name: GNB_NPT
Version:
Date:
Classification: Strict

wizlynx group

2.5 Vulnerability and Exploitation Review

The first dashboard below displays the number of vulnerabilities found on all targets per severity. The bottom left fig
the number of user credentials that could be harvested and compromised, and on the bottom right, the number of su
exploited vulnerabilities per category:

During this penetration testing project, we were able to fully compromise two out of the three targets in scope.

The first weakness discovered on GNB's eBanking web server, known as "Usemame Harvesting", allowed us to i
"admin" user exist on the application. The weak password policy, absence of two-factor authentication and lack
mechanism, allowed us to launch a password dictionary attack and guess its password in a short amount of time.

Once authenticated in the web application, we were able to access GNB's customer confidential information. We also
the presence of a file upload mechanism. Since the application does not verify the type of file being uploaded, we w
upload a malicious file (web shell) which allowed us to remotely execute commands on the underlying server.

Since the web shell was running with low privileges, we analyzed the server's configuration to hopefully escalate ou
In doing so, we discovered a domain administrator's credentials due to a weakness in Microsoft Group Policy which al
authenticate to the web server with full access.

The FileSharing target was compromised by a succession of two vulnerabilities. The first one allowed us to remot
commands on the server due to an old version of PHP running on the web server. We then leveraged another local v
to escalate our privileges and got full access to the server and data allowing us to access financial reports, customer li

wizlynx group

3.3.4 Attack Graph

The following graph shows all threat vectors used to compromise the target:

Penetration Tester
wizlynx
www.giantnationalbank.com
100.122.66.10
① Username Harvesting & Password Guessing (admin)
② Web Shell Upload (IIS APPPOOL)
③ Group Policy Password Preferences Retrieval (IIS APPOOL escalated to adm_gnb)

3.3.5 Exploited Vulnerabilities & Proof of Concepts

3.3.5.1 Username Harvesting

Username Harvesting							
Scope	https://www.giantnationalbank.com/Account/Login						
Severity	Medium	Reference	CWE-203	CVSS Score	5.3	Status	Open
Exploitability Metrics				Impact Metrics			
Attack Vector	Network	Scope	Unchanged				
Attack Complexity	Low	Confidentiality	Low				
Privileges Required	None	Integrity	None				
User Interaction	None	Availability	None				
Recommendations							
Avoid discrepancies in error messages that would allow a user to distinguish between valid and invalid users. This can be achieved by always returning a general response back to the user after a failed authentication attempt or when resetting a password: • Response in the case of a failed authentication attempt: "Wrong Login Information" • Response in the case of password reset: "If the user is registered, a link to reset the password will be sent to the user's email address"							

It is possible to identify valid usernames on the e-banking web application by observing the response of the server after a failed authentication request.

To demonstrate this weakness, we have attempted to login with:

- Valid username + wrong password
- Invalid username + wrong password

BENEFITS

- Discover if your critical information assets are at risk
- Identify and address vulnerabilities before they can be utilized by cybercriminals
- Meet compliance requirements
- Quickly remediate discovered vulnerabilities with actionable recommendations

CREST APPROVED

wizlynx group is an approved CREST penetration testing service provider globally with CREST certified penetration testers.

ABOUT WIZLYNX GROUP

wizlynx group is an ethical, trustworthy, and vendor agnostic Swiss Cyber Security provider, who you can rely on to effectively guard your business and trade secrets. Our services are designed to protect against any form of cybercrime, such as malware outbreak, malicious insiders, cyberattacks, cyber espionage, data leakage, and more...

We live and breathe Cyber Security! For this reason, we have designed a service portfolio that covers the entire risk management lifecycle to ensure our customer benefits the most from our passion and experience, but primarily to maximize their protection. It starts with security assessment, such as penetration testing and ethical hacking for mobile applications, web applications, networks, and systems, but also vulnerability assessments and secure code review. With our Information Security Assessments, we evaluate the IT processes, governance and compliance (GRC), so that an integral security can be succeeded. We also provide design and integration of security products spanning all layers (i.e. network, host, system, and application) for a 360° protection. Finally, we offer managed security services (MSS) and emergency breach response for cyber security incidents with our cyber SWAT team.