PENETRATION TEST

RULES OF ENGAGEMENT(ROE)

Prepared For:

Samantha Patel, CISO

Legere, Hamilton, ON

spatel2@legere.com

M: 437-636-9290

Prepared By:

Anilsingh Rajpurohit,
Project Manager

anilraj@my.yorku.ca

M: 437-660-2210

DATE

2024-05-28

1. **Introduction**

This document outlines the Rules of Engagement (ROE) for a penetration testing engagement conducted by XYZ company for Legere at their Hamilton, Ontario office subsidiary. The engagement will be performed from **2024-05-28 to 2024-06-03**, with a focus on identifying vulnerabilities in their information security posture.

2. **Objectives and Scope**

Objective:

Identify and assess potential security vulnerabilities within the Legere Hamilton office network infrastructure, physical security measures, and social engineering susceptibility.

Scope:

Leger Consulting Inc. requires a comprehensive security assessment encompassing network penetration testing of their public IP range (24.141.157.10/11) and website (www.legereconsulting.com), along with social engineering testing through email phishing simulations and pretext phone calls (black-box approach). Additionally, a physical security assessment of their Hamilton office building is recommended. Brute-force attacks. Cogeco, Leger's datacentre provider, allows network penetration testing with prior approval.

3. **Off-Limits**

Datacentre:

physical testing of the datacentre is out of scope. (Third Party)

Data:

Human Resources (HR) Server (WVP-LGMHRM-18, 172.16.40.50) & HMHRMA (192.168.0.112) - containing employee PII. City of Ottawa and Toronto project files hosted on servers WPJ-MPRJOTT (172.16.40.10) & WPJ-MPRJTOR (172.16.40.11).

**No data exfiltration is allowed, even for testing purposes. If confidential data is encountered outside excluded servers, document the file path and refrain from retaining evidence.

Activities:

Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks. Physical attacks causing property damage or personnel injury.

4. **Testing Methodology**

Black-box testing methodology will be employed, simulating a real-world attacker's approach. The penetration test will occur 24/7 throughout the engagement week.

5. **Social Engineering**

Spear phishing simulations targeting employee email addresses will be conducted. Pretext phone calling exercises will be implemented without a predefined target list due to the black-box nature of the test.

6. **Physical Security Testing**

Tailgating and dumpster diving on Legere property are permitted. Physical access attempts will be made, including connecting to network ports in conference rooms or offices for reconnaissance activities. Lock-picking activities are allowed for testing locked areas. Placement of hardware (USB drives, mice, keyboards, and netbooks) throughout the building is permitted.

Project Schedule For Activities:

Day 1	*Pre-Engagement:* * Scope Definition: Finalize the specific systems and areas to be included in the test. * Rules of Engagement: Establish guidelines such as testing hours, allowed test types, and procedures for handling critical findings. * Physical Testing: Simulate a break-in to evaluate the building's physical security measures.
Day 2	*Reconnaissance:* Planning & Scoping: * Define the target system (web application, network, etc.) based on the assignment details.

	* Understand the engagement rules and limitations. * Outline the testing methodology and tools. * Information Gathering *Social Engineering *Brute-force attacks Use open-source intelligence (OSINT) techniques to gather information about the target: * DNS records for subdomains and services. * Technology stack identification through website analysis tools. * Social media and public information for potential entry points.
Day 3-4	*Assessment:* * Vulnerability Scanning: Utilize automated tools to scan for known system vulnerabilities. * Manual Testing: Conduct manual tests to identify vulnerabilities that automated scanners might miss.
Day 5-6	*Exploitation:* * Vulnerability Exploitation: Attempt to leverage identified vulnerabilities to gain unauthorized access or disrupt system operations. * Post-Exploitation: Assess the real-world impact of exploiting these vulnerabilities (e.g., data access).
Day 7	*Reporting & Analysis:* Report Preparation: Generate a comprehensive report outlining the findings, exploited vulnerabilities, potential impact, and recommendations for mitigation.

**Please note that this workflow is adaptable based on specific requirements and situations.

7. **Communication**

Twice-daily briefing calls will be held at 8:00 AM and 4:30 PM Eastern Time (ET) via Microsoft Teams (their internal conferencing software).

Samantha Patel, CISO (spatel2@legere.com, 437-636-9290) and Matthew Rodriguez, VP of Operations (mrodriguez@legere.com, 437-636-2748) are the designated points of contact for the client.

Critical vulnerabilities will be reported during briefings. Any additional access or information requests will be raised at the briefings.

8. **Reporting Considerations**

A final report will be delivered as a password-protected PDF on an encrypted USB drive. The report will be presented and delivered in person at the Hamilton office upon completion of the engagement.

9. **Termination of testing or Success Criteria**

Access to any internal systems (server or workstation) will be considered a successful penetration test, with identification of system type and owner (if possible).

10. **Incident Handling Procedures**

The penetration test is designed to minimize disruption to business operations. However, if any unintended disruptions occur, Samantha Patel (spatel2@legere.com, 437-636-9290) will be notified immediately. Samantha Patel, CISO - main contact who commissioned the test, to be called on her mobile in case of 'emergency' (i.e.: network outage, law enforcement, etc)

11. **Disclaimer**

Legere acknowledges that a penetration test may expose security vulnerabilities. XYZ Company will act in an ethical and professional manner throughout the engagement and will not be held liable for any unintended consequences arising from the test. An industry standard level penetration test will be done but there is a possibility that it may not gain any access or identify and address potential security risk.

12. **ROE and Test Plan Approval and Signature**

This ROE constitutes the agreement between XYZ Company and Legere regarding the scope and limitations of the penetration testing engagement. By signing below, both parties acknowledge their understanding and acceptance of these terms.

_____

Samantha Patel, CISO DATE: 2024-05-28

Legere, Hamilton, ON

_____

Anilsingh Rajpurohit, Project Manager DATE: 2024-05-28

XYZ company, Toronto, ON