REDSTRIKE

RULES OF ENGAGEMENT

GLOBAL FINANCE CORPORATION

JAN 2024

REDSTRIKE

Executive Summary

This document outlines the Rules of Engagement (ROE) for a red team assessment of Global Finance Corporation (GFC). The assessment is designed to evaluate GFC's cybersecurity posture by simulating a sophisticated, real-world threat. This engagement aims to identify vulnerabilities, test defense mechanisms, and improve security resilience within GFC's financial technology ecosystem. Signing of the ROE constitutes acknowledgement and approval of the customer, system owner, and the Red Team's authorities in execution of the engagement. The enagement is scheduled for February 1-18, 2024.

Ojectives include:

- Evaluate GFC's incident detection, response, and recovery capabilities.
- Test the resilience of critical financial systems against advanced persistent threats.
- Assess the effectiveness of security awareness training among GFC employees.
- Identify and exploit vulnerabilities in GFC's network infrastructure, applications, and human elements.

Authorized Target Space:

- Data-center (10.0.0.0/16); Recovery Site (192.168.0.0/16); Corporate (172.16.0.0/12)
- www.globalfinancecorp.com
    - online.globalfinancecorp.com, api.globalfinancecorp.com, mobile.golbalfinancecorp.com

Activities:

- Reconnaissance through OSINT, network scanning, and utilizing social media and public records.
- Vulnerability scanning, port scanning, and web application security testing.
- Phishing campaigns, vishing attacks, and physical social engineering attempts.
- Unauthorized access attempts and testing physical security controls such as card readers.

Restrictions:

- No DoS attacks, system destruction, or disruption of production systems.
- Prohibited from exploiting employee personal information or conducting unauthorized social engineering.
- Cannot access customer financial data or violate financial regulations like SOX and PCI-DSS.
- No testing during trading hours (9:30 AM - 4:00 PM EST) or disrupting business continuity systems.

Table of Contents

01

Scope and Objectives

Defines the specific goals of the assessment and outlines what systems and assets are included or excluded.

1.1 Primary Objectives

- Assess the effectiveness of GFC's security controls across all layers of the technology stack.
- Identify and exploit vulnerabilities in GFC's network infrastructure, applications, and human elements.
- Evaluate GFC's incident detection, response, and recovery capabilities.
- Test the resilience of critical financial systems against advanced persistent threats.
- Assess the effectiveness of security awareness training among GFC employees.

1.2 Scope

- GFC's primary data center (10.0.0.0/16)
- Disaster recovery site (192.168.0.0/16)
- Corporate network (172.16.0.0/12)

Public-facing web applications:

- www.globalfinancecorp.com
- online.globalfinancecorp.com
- api.globalfinancecorp.com
- mobile.globalfinancecorp.com

- Employee workstations (Windows and macOS)
- Mobile devices enrolled in GFC's MDM solution
- Cloud infrastructure (AWS and Azure environments)
- Physical security of the headquarters and two branch offices

1.3 Out of Scope

- Third-party vendor systems not directly managed by GFC.
- Personal devices of employees not enrolled in GFC's BYOD program.
- Satellite offices outside of the continental United States.

02

Authorized Actions

Lists the types of activities and techniques the red team is permitted to perform during the engagement.

The red team is authorized to:

2.1 Reconnaissance

- Conduct extensive open-source intelligence (OSINT) gathering.
- Perform passive and active network reconnaissance.
- Utilize social media and public records for information gathering.

2.2 Scanning and Enumeration

- Conduct network and application vulnerability scanning.
- Perform port scanning and service enumeration.
- Utilize automated and manual web application security testing tools.

2.3 Exploitation

- Attempt exploitation of discovered vulnerabilities.
- Develop and deploy custom exploits if necessary.
- Utilize public and commercial exploit frameworks.

2.4 Social Engineering

- Conduct phishing campaigns (max 3 campaigns, 500 employees per campaign).
- Perform vishing (voice phishing) attacks (max 50 attempts).
- Attempt physical social engineering at specified locations (max 3 attempts per location).

2.5 Post-Exploitation

- Attempt lateral movement within compromised networks.
- Perform privilege escalation on compromised systems.
- Establish persistence mechanisms for extended access.

2.6 Data Exfiltration

- Exfiltrate sample data to demonstrate impact (max 100 records per database).
- Test data loss prevention (DLP) controls.

2.7 Physical Security

- Attempt to gain unauthorized physical access to in-scope facilities.
- Test physical security controls, including card readers and surveillance systems.

03

Restricted Actions

Specifies actions that are explicitly prohibited to prevent unintended damage or disruption. The following actions are strictly prohibited:

3.1 Destructive Actions

- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.
- Destruction, corruption, or alteration of production data.
- Disabling or disrupting production systems or networks.

3.2 Ethical Constraints

- Exploiting or taking advantage of GFC employees' personal information.
- Conducting social engineering attacks outside of the agreed-upon scope.
- Sharing any information obtained during the engagement with unauthorized parties.

3.3 Regulatory Compliance

- Accessing, exfiltrating, or storing actual customer financial data.
- Violating any financial regulations, including SOX, PCI-DSS, and GDPR.
- Interfering with regulatory reporting or compliance mechanisms.

3.4 Operational Restrictions

- Exploiting vulnerabilities in critical financial systems during trading hours (9:30 AM - 4:00 PM EST, Mon-Fri).
- Conducting loud or disruptive testing during business hours without prior approval.
- Modifying or disrupting any disaster recovery or business continuity systems.

3.5 Third-Party Limitations

- Attacking or attempting to compromise third-party vendors, partners, or service providers.
- Exploiting vulnerabilities in third-party software without explicit permission.

04

Timeframe

Establishes the duration of the engagement and any time-based restrictions on testing activities.

4.1 Duration

The engagement will run from February 1, 2024, to February 18, 2024 (2.5 weeks).

4.2 Testing Windows

- Active testing is permitted 24/7, except for the restrictions noted in section 4.
- Exploitation of critical systems restricted to non-business hours (7:00 PM - 6:00 AM EST, Mon-Fri, and all day Sat-Sun).

4.3 Blackout Periods

- No testing allowed during quarterly financial closing (Feb 16 - Feb 17, 2024).
- Restricted testing during planned system upgrades (dates TBA).

05

Tools and Techniques

Outlines the approved tools and methodologies the red team may employ.

5.1 Approved Tools

The red team may use industry-standard penetration testing tools, including but not limited to:

- Nmap, Nessus, Burp Suite, Metasploit, Cobalt Strike.
- Custom scripts and exploits developed for this engagement.
- Hardware devices for physical security testing (e.g., RF scanners, lock picking tools).

5.2 Approval Process

- All tools must be approved by the trusted agent prior to use.
- A complete inventory of tools must be maintained and updated throughout the engagement.

5.3 Malware and Payloads

- Custom malware or payloads must be fully documented and approved.
- All malware must include a self-destruct mechanism and must not propagate automatically.

5.4 Data Collection

- All data collection tools must encrypt data at rest and in transit.
- Tools must not store raw credentials or sensitive data without explicit approval.

06

Reporting and Communication

Defines the frequency and format of updates, as well as procedures for reporting findings.

6.1 Regular Updates

- Daily status updates to be sent to the trusted agent by 5 PM EST.
- Weekly progress reports due by COB every Friday.
- Bi-weekly briefings with GFC leadership (schedule TBD).

6.2 Critical Findings

- Critical vulnerabilities to be reported to the incident response team within 1 hour of discovery.
- Detailed write-up of critical findings due within 24 hours of initial report.

6.3 Reporting Channels

- Encrypted email for daily updates and non-critical communication.
- Secure messaging app for real-time communication during active exploitation.
- Dedicated hotline for emergency communication.

6.4 Final Report

- Preliminary report due within 25 business days of engagement completion.
- Final report, including executive summary, due within 30 business days.
- In-person debrief (Hot Wash) presentation to GFC leadership within 24 hours of assessment completion.

07

Points of Contact

Lists key personnel involved in the engagement and their contact information.

7.1 Red Team

- Red Team Lead: Jane Doe (jane.doe@redteam.com, 555-0100)
- Technical Lead: Bob Wilson (bob.wilson@redteam.com, 555-0101)
- Social Engineering Specialist: Eve Brown (eve.brown@redteam.com, 555-0102)

7.2 Blue Team

- Blue Team Lead: John Smith (john.smith@gfc.com, 555-0200)
- SOC Manager: David Lee (david.lee@gfc.com, 555-0201)
- Threat Intelligence Analyst: Sarah Chen (sarah.chen@gfc.com, 555-0202)

7.3 GFC Management

- Trusted Agent: Alice Johnson (alice.johnson@gfc.com, 555-0300)
- CISO: Michael Taylor (michael.taylor@gfc.com, 555-0301)
- CIO: Laura Martinez (laura.martinez@gfc.com, 555-0302)

7.4 Emergency Contacts

- Incident Response Team: ir@gfc.com, 555-0400
- Physical Security: security@gfc.com, 555-0500
- Legal Department: legal@gfc.com, 555-0600

08

Incident Response Procedures

Describes the process for handling actual security incidents that may occur during the assessment. In the event of an actual security incident:

8.1 Immediate Actions

- Immediately cease all red team activities.
- Preserve all relevant logs and data.
- Contact the incident response (IR) team and trusted agent.

8.2 Communication

Provide a full briefing to the IR team, including:

- Nature of the incident.
- Systems and data potentially affected.
- Actions taken by the red team.

Remain available to assist in incident investigation and resolution.

8.3 Documentation

- Prepare a detailed incident report within 24 hours.
- Participate in post-incident review and lessons learned sessions.

8.4 Resumption of Activities

Do not resume red team activities until explicitly authorized in writing by the CISO or Trusted Agent.

09

Approval Process

Outlines how changes to the ROE can be requested and approved.

9.1 Changes to ROE

- Minor changes can be approved by the trusted agent and Red Team Lead.
- Significant changes require approval from the CISO and CIO.

9.2 Approval Workflow

- Submit change request in writing, detailing the proposed modification.
- Trusted Agent reviews and provides initial approval.
- CISO and CIO review for final approval.
- All approvals must be documented and distributed to all relevant parties.

9.3 Emergency Changes

- In urgent situations, verbal approval may be obtained from the trusted agent or CISO.
- Written documentation must follow within 24 hours.

10 Legal and Compliance

Addresses relevant legal and regulatory requirements impacting the engagement.

10.1 Regulatory Compliance

- This engagement will comply with all relevant financial regulations, including but not limited to SOX, PCI-DSS, GDPR, and applicable state laws.
- The red team will not access, exfiltrate, or store actual customer financial data.

10.2 Legal Safeguards

- All red team members must sign non-disclosure agreements.
- GFC will provide written authorization for the engagement, to be carried by team members at all times.
- Local law enforcement should be notified of physical penetration testing activities.

10.3 Liability

- GFC agrees to indemnify the red team against any claims arising from authorized activities conducted within the scope of this ROE.
- The red team is responsible for any damages resulting from unauthorized actions or gross negligence.

11 Data Handling

Specifies procedures for managing sensitive data encountered during the assessment.

11.1 Data Classification

- All data discovered or generated during the engagement must be classified according to GFC's data classification policy.

11.2 Data Protection

- All data must be encrypted at rest using AES-256 encryption.
- Data in transit must use TLS 1.3 or approved VPN solutions.

11.3 Data Storage

- Engagement data may only be stored on approved, encrypted devices.
- Cloud storage is prohibited unless explicitly approved and properly secured.

11.4 Data Destruction

- All data must be securely deleted at the conclusion of the engagement.
- A certificate of destruction must be provided to GFC within 5 business days of engagement completion.

12

Operational Security (OPSEC)

Defines measures to maintain the confidentiality and integrity of the red team operation.

12 .1 Team Member Identification

- Red team members must carry GFC-issued identification at all times.
- When conducting social engineering, approved false identities may be used.

12 .2 Communication Security

- All team communications must be encrypted.
- Use of code names for sensitive aspects of the operation.

12 .3 Physical Security

- All physical tools and documentation must be secured when not in use.
- Hotel safes or approved secure storage must be used when traveling.

13

Health and Safety

Outlines protocols to ensure the physical safety of all participants during the engagement.

13 .1 Risk Assessment

- A health and safety risk assessment should be conducted for all physical aspects of the engagement.

13 .2 Safety Protocols

- Red team members must adhere to all GFC safety policies when on-site.
- Any potentially dangerous activities must be approved in advance and properly supervised.

14

Debriefing and Lessons Learned

Describes the post-engagement process for reviewing findings and transferring knowledge.

14.1 Engagement Wrap-up

- A Hot Wash debriefing occurs within 24 hours post-engagement to capture fresh insights while details remain clear ensuring critical findings are quickly documented and actionable to GFC.

14.2 Knowledge Transfer

- An assessment report will be provided to GFC within 30 days providing a comprehensive analysis of the engagement findings, documenting vulnerabilities, attack paths, and recommendations.
- The red team will provide a knowledge transfer session to GFC's security team on request.

15 Threat Profile and Replication

Specifies the threat actors, tactics, and scenarios the red team will emulate to provide a realistic assessment.

15.1 Threat Actors to Emulate

The red team will simulate the following threat actors:

A. Nation-State APT Group

- Codename: “Jade Banker”
- Characteristics: Highly sophisticated, patient, and well-resourced.
- Primary objectives: Intellectual property theft, financial fraud, and strategic intelligence gathering.

B. Organized Cybercrime Syndicate

- Codename: “BlackLedger”
- Characteristics: Profit-driven, technically proficient, and persistent.
- Primary objectives: Large-scale financial theft, ransomware deployment, and data exfiltration for sale.

C. Hacktivist Collective

- Codename: “EqualAccess”
- Characteristics: Ideologically motivated, varying skill levels, and publicity-seeking.
- Primary objectives: Service disruption, data leaks, and reputational damage.

D. Malicious Insider

- Codename: “Disgruntled Employee”
- Characteristics: Internal knowledge, legitimate access, and potentially sophisticated.
- Primary objectives: Data theft, sabotage, and financial fraud.

15.2 Tactics, Techniques, and Procedures (TTPs)

The red team will employ the following TTPs, mapped to the MITRE ATT&CK framework:

A. Initial Access

- Phishing (T1566)
- Valid Accounts (T1078)
- Exploit Public-Facing Application (T1190)
- Hardware Additions (T1200) for the insider
- threat scenario

B. Execution

- Command and Scripting Interpreter (T1059)
- User Execution (T1204)
- Exploitation for Client Execution (T1203)

C. Persistence

- Create Account (T1136)
- Bootkit (T1067)
- Office Application Startup (T1137)

D. Privilege Escalation

- Exploitation for Privilege Escalation (T1068)
- Access Token Manipulation (T1134)
- Process Injection (T1055)

E. Defense Evasion

- Obfuscated Files or Information (T1027)
- Indicator Removal on Host (T1070)
- Masquerading (T1036)

F. Credential Access

- Brute Force (T1110)
- Credential Dumping (T1003)

G. Discovery

- Network Service Scanning (T1046)
- File and Directory Discovery (T1083)
- Account Discovery (T1087)

H. Lateral Movement

- Lateral Tool Transfer (T1570)
- Remote Services (T1021)
- Internal Spearphishing (T1534)

I. Collection

- Data from Local System (T1005)
- Data Staged (T1074)
- Screen Capture (T1113)

J. Command and Control

- Application Layer Protocol (T1071)
- Encrypted Channel (T1573)
- Ingress Tool Transfer (T1105)

K. Exfiltration

- Exfiltration Over C2 Channel (T1041)
- Exfiltration Over Alternative Protocol (T1048)
- Scheduled Transfer (T1029)

L. Impact

- Data Destruction (T1485)
- Data Encrypted for Impact (T1486)
- Defacement (T1491)

15.3 Threat Scenarios

The red team will execute the following specific threat scenarios:

A. APT Campaign

- Simulate a long-term, low-and-slow campaign targeting GFC's intellectual property and strategic financial data.
- Establish persistent access and attempt to evade detection for the duration of the engagement.
- Mimic the TTPs associated with the "Jade Banker" threat actor.

B. Ransomware Attack

- Simulate the initial compromise, lateral movement, and encryption phases of a sophisticated ransomware attack.
- Target both on-premises and cloud-based systems.
- Emulate the tactics of the "BlackLedger" cybercrime syndicate.

C. Insider Threat

- Simulate actions of a disgruntled employee with mid-level access.
- Attempt to escalate privileges, access restricted systems, and exfiltrate sensitive data.
- Blend in with normal user activity to test GFC's insider threat detection capabilities.

15.4 Custom Malware and Tools

The red team is authorized to develop and use custom malware and tools that mimic the capabilities of the specified threat actors. This includes:

- Custom backdoors and implants.
- Simulated ransomware (with safeguards to prevent actual encryption of production data).
- Social engineering lures specific to GFC.

All custom tools must be approved by the Trusted Agent and documented thoroughly.

15.5 Threat Intelligence Integration

The red team will incorporate the latest threat intelligence relevant to the financial sector to ensure the simulated attacks reflect current real-world threats. This includes:

- Utilizing recent IOCs (translated to the GFC environment).
- Emulating newly discovered TTPs.
- Adapting the attack scenarios based on emerging threats throughout the engagement.

15.6 Attack Infrastructure

The red team will set up and utilize attack infrastructure that mimics that of the simulated threat actors, including:

- Bulletproof hosting in relevant geographies.
- Domain registration patterns consistent with the threat actors.
- Malware C2 infrastructure reflective of APT and cybercrime operations.

15.7 Measurement and Evaluation

For each simulated threat scenario, the red team will measure and report on:

- Time to initial compromise.
- Time to detection (if detected).
- Time to containment/eradication (if contained).
- Extent of potential damage (e.g., data accessed, systems compromised).
- Effectiveness of GFC's controls at each stage of the attack lifecycle.

15.8 Coordination with Blue Team

To maximize the training value of the engagement:

- The blue team will be notified of the general threat actors being simulated, but not specific attack details.
- Certain scenarios may be coordinated to allow for blue team detection and response practice.
- Joint red team/blue team debriefs will be conducted after significant milestones.

16 Signatures

By signing below, all parties acknowledge that they have read, understood, and agree to abide by these Rules of Engagement.

Red Team Lead		Date	
Trusted Agent		Date	
GFC CISO		Date	
GFC CIO		Date	
GFC Legal Counsel		Date	


REDSTRIKE