Rules of Engagement

Chippy’s Corner
08/02/2025

Executive Summary

The Rules of Engagement (ROE) document the approvals, authorizations, and critical implementation details necessary to execute this Red Team engagement. Signing of this ROE constitutes acknowledgement and approval by the customer (Chippy's Corner), the system owner (Colin Parker), and the Red Team (Bah Red Labs) of the Red Team's authorities and agreed-upon boundaries for execution of the engagement.

The engagement will focus on assessing Chippy's Corner's employee subnet to identify vulnerabilities, evaluate potential attack paths, test persistence mechanisms, and demonstrate risks related to unauthorized access and data exfiltration. The engagement will be executed from Bah Red Labs' controlled environment, targeting only the approved IP space defined in Appendix A.

The objectives include:

- Identify exposed services and potential attack vectors within the authorized subnet.
- Attempt controlled exploitation of identified vulnerabilities to gain initial access.
- Establish persistence on compromised systems and test the ability to maintain access post-reboot.
- Simulate data exfiltration of sensitive employee information to demonstrate business impact.

Authorized Target Space:

- IP Range: 192.168.110.100 – 192.168.110.200 (/24)
- Domains: Internal Chippy's Corner employee network only (no external domains).
- URLs: Any web interfaces hosted within the approved subnet.
- Network Segments: Only systems within the employee subnet; all other networks are strictly out of scope.

Activities:

- Reconnaissance and enumeration of in-scope hosts and services.
- Controlled exploitation and initial access attempts.
- Establishment of persistence via custom C2 payload.
- Lateral movement to an additional endpoint containing employee data.
- Simulated data exfiltration to Red Team infrastructure for impact demonstration.

TABLE OF CONTENTS

Section Page

1 Rules of Engagement Introduction

1.1 Purpose

To establish the responsibilities, relationships, and guidelines between the Bah Red Labs Red Team, hereafter referred to as “Red Team”, Chippy's Corner, hereafter referred to as “Customer”, Colin Parker, hereafter referred to as “System Owner”, for conducting a Red Team engagement on Chippy's Corner employee subnet, hereafter referred to as “Target of Engagement”.The engagement will be conducted at Chippy’s Corner HQ on target systems located at 192.168.110.100-192.168.110.200.

1.2 References:

a. MITRE ATT&CK® Framework – Adversary Tactics and Techniques Knowledge Base.

1.3 Scope

This agreement applies to Chippy's Corner employee network for the receipt of Red Team activities. This document will establish the guidelines, limitations, and restrictions for conducting a Red Team engagement.

2 Rules of Engagement and Support Agreement:

a. Bah Red Labs has agreed to conduct a Red Team engagement and support Red Team activities. This document provides the ground rules for planning, executing, and reporting the engagement.

b. Chippy's Corner has requested a Red Team engagement to assess the security posture and resilience of their internal employee network against real-world adversary tactics, techniques, and procedures (TTPs). The purpose of this engagement is to simulate potential attacker behavior, evaluate detection and response capabilities, and identify areas for security improvement within the organization's infrastructure.

   The following systems, networks, and/or assets will be included:

   - Chippy's Corner employee subnet: 192.168.110.100 – 192.168.110.200
   - All associated software, hardware, endpoints, and services within this subnet that are in scope for this engagement.

c. The Red Team will perform reconnaissance, vulnerability discovery, targeted exploitation, persistence establishment, credential brute forcing, and controlled data exfiltration on the in-scope Chippy's Corner employee subnet.

   - The engagement is designed to simulate realistic attacker behavior to evaluate Chippy's Corner's detection, response, and security control effectiveness. This means the system must withstand unauthorized access attempts, detect malicious activity, prevent privilege escalation, and safeguard sensitive employee information from exfiltration.
   - For the Red Team, a closed network will be utilized. A closed network is defined as a network without access to the Internet.
   - There will be complete and open coordination with all stakeholders required for the execution of the engagement. Stakeholders are the parties represented by the signatories of this document.
   - Red Team activities are limited to the target of engagement.
   - Red Team tools and activities may be intrusive, but will not intentionally disrupt services outside the authorizations of these Rules of Engagement.
   - The Red Team will provide two updates as follows:
     - Update 1: Upon successful initial access to the first in-scope system.

- Update 2: Upon successful data exfiltration or conclusion of lateral movement activities.

d. Red Team efforts will be coordinated with Colin Parker for the duration of the engagement. The Red Team will target only those hosts and Internet Protocol (IP) addresses within the confines and control of the target engagement network.

e. Red Team methods may be intrusive, but should not be destructive, and will be terminated if information is gathered pertaining to an actual intrusion. Red Team is responsible for informing Colin Parker if an actual intrusion is discovered. Colin Parker will report the actual intrusion to the appropriate representative, along with any substantiating information regarding the detected intrusion.

f. Red Team operations require the use of exploitation and attack tools and techniques. All tools employed by the Red Team have been extensively tested by the team to ensure they are non-destructive and are under positive control when employed.

g. Red Team systems contain exploit tools, code, and technical references, which are not to be viewed, distributed, or evaluated by external organizations.

h. The Red Team will attempt to gain access to the target of engagement.

i. The Red Team may only conduct activities against client networks that provide sufficient notice to system users that their use of those systems constitutes consent to monitoring. It is the responsibility of the target of engagement legal counsel to review these notice procedures and certify that they provide sufficient notice.

j. Sensitive information reporting:
   - Vulnerabilities discovered during the engagement that present an immediate risk to life, limb, or eyesight will be reported promptly to Colin Parker to enable immediate response or action. Representatives of the signatories of this ROE will receive follow-up notification as appropriate.
   - Incidental discovery of information that relates to serious crimes such as sabotage, threats, or plans to commit offenses that threaten a life or could cause significant damage to or loss of customer property, and which does not present an immediate risk, will be reported to the applicable local authorities for action.
   - The Red Team reporting is otherwise conducted in a way that does not attribute information or particular activity to an individual.
   - Red Team activities may not be conducted in support of law enforcement or criminal investigation purposes.

k. Cease operations process:

- The Red Team will suspend activity upon detection of computer anomalies that could potentially be unauthorized intrusions into target of environment networks.
- The Red Team will suspend activity when unintentional information as described above is encountered, and until the appropriate reporting has taken place.
- All engagement activities operate under the direction of the Engagement Director, who may alter or cease activities as necessary.

l. Information usage:

- The Red Team will not intentionally compromise Privacy of Information Act (PIA), medical, justice, worship or religious pursuit, or any other protected or privileged information. If a compromise does occur, it will be handled through normal procedures. The proper security personnel will be notified immediately.
- The Red Team is authorized to exploit files, email, and/or message traffic stored on the network, as well as communications transiting the network for analysis specifically related to the accomplishment of their objectives. (e.g., identifying user ID's, passwords and/or network IP addresses in order to gain further access).
- The Red Team will not intentionally modify or delete any operational user data, or conduct any Denial of Service attacks. The Red Team will not otherwise intentionally degrade or disrupt normal operations of the targeted systems.
- The Red Team reporting is conducted in a way that does not attribute information or particular activity, to a specific individual.

m. Deconfliction process:

- All detected information assurance incidents, whether real-world or alleged Red Team activity, should immediately be reported using normal incident reporting processes.
- Chippy's Corner, Colin Parker may contact the Red Team's POC to determine if discovered activities are the result of the Red Team.

n. Deliverables:

- The Red team will provide an engagement summary presentation for the target of engagement representatives at the completion of the engagement.
- The Red Team will provide a written summary of the engagement results to Colin Parker within 30 days following completion of the test.

2.1 ROE Provisions

The following additional provisions apply to this memorandum:

a. All operations will be conducted within guidelines established by applicable policy, regulations and laws.

b. All contact with computer networks/subnets will be from within the Red Team or target of engagement environment.

c. During the engagement, any deviations from these ROE must be mutually agreed to and approved in writing by the senior representatives for the Red Team, Chippy's Corner, and Colin Parker.

2.2 Requirements, Restrictions, and Authority

a. The Red Team will:

- Provide the appropriate support and input for the planning of the engagement.
- Coordinate engagement approval and support via this Rules of Engagement (ROE).
- Inform target of engagement POCs of all team requirements (logistics, administrative, etc.).
- Coordinate team personnel and administrative issues/concerns with Colin Parker. names, job titles, phone & email address) to the Chippy Corner's representatives.
- Escalate problems and issues to the appropriate representatives.
- Upload, where appropriate, indicators on systems to demonstrate a compromised state.
- When necessary, add/modify/disable accounts (not delete them) on compromised systems.
- Conduct exploitation with the intent of emulating threat techniques, tactics and procedures.
- May view/read or modify personal data files, PII, or emails.
- NOT use unapproved tools.
- NOT damage systems or networks.
- NOT conduct denial of service (DOS), except as explicitly approved.

2.3 Ground Rules

This section identifies specific rules associated with the execution of this event.

a. Network Operations

- All systems outside the IP ranges provided under separate cover are off limits

3 Authorization

This agreement becomes effective upon the date of the last approving official's signature.

Termination of this agreement can be directed by any of the stakeholders listed in this document at any time by giving notice in writing to the non-terminating parties. This agreement can only be modified by mutual written consent of the signatories. Changes must be coordinated by means of an exchange of memoranda between the signatories. This agreement will undergo a review in its entirety with each modification request or by the request of either party after giving notice in writing at least 7 days prior to the review.

4 Approval

The signatures below denote that all parties have read and agree to this Memorandum of Agreement.

_____	_____
(NAME)	(NAME)
Red Team Lead	Chief Information Officer
Bah Red Labs	Chippy's Corner
_____	_____
(Date)	(Date)
_____	_____
(NAME)	(NAME)
Engagement Directory	Chief Executive Officer
Chippy's Corner	Chippy's Corner

_____	_____
(Date)	(Date)

APPENDIX A – TARGET ENVIRONMENT

List of assets, systems, and data

Restricted IP Addresses:

- Any IP ranges outside of the authorized IP space

Authorized IP Space:

- 192.168.110.100 (/24) - 192.168.110.200 (/24)

Restricted Hosts:

- Any hosts outside of the IP ranges.

Authorized Hosts:

- All hosts not expressly restricted

APPENDIX B - Points of Contact

Engagement Director:

- Name: Enzo Fernburger
- Phone: +1 888-888-8888
- Email: enzo.fernburger@bahredlabs.com
- Office Location: Bah Red Labs HQ, 1400 Bridge Lane, Little Rock, AR, USA

Trusted Agent:

- Name: Colin Parker
- Title: Chief Information Officer
- Phone: +1 101-010-1010
- Email: colin.parker@chippyscorner.com
- Office Location: Chippy's Corner Corporate Office, 221 Blue Lion Street, Little Rock, AR, USA

White Cell Lead:

- Name: Rhys Jambalaya
- Title: Chief Executive Officer
- Phone: +1 242-424-2424
- Email: rhys.jameston@chippyscorner.com
- Office Location: Chippy's Corner Headquarters, 221 Blue Lion Street, Little Rock, AR, USA

Emergency Contact:

- Name: Didier Drumstick
- Title: Executive Assistant
- Phone: +1 111-111-1111
-
- Email: didier.drumstick@chippyscorner.com
- Office Location: Chippy's Corner Headquarters, 221 Blue Lion Street, Little Rock, AR, USA

Red Team Lead:

- Name: Mamadu Bah
- Phone: +1 333-333-3333
- Email: mb03@brl.com
- Office Location: Remote

APPENDIX C – RED TEAM METHODOLOGY

Get-In:

- Reconnaissance:
  - The Red Team will scan the 192.168.110.100–200 subnet to identify active hosts and running services.
  - Enumeration of open ports and basic service information will be conducted to identify potential attack vectors.
- Enumeration:
  - The Red Team will attempt to identify any vulnerable web servers or services within the in-scope subnet.
- Exploitation:
  - If a vulnerable service is identified, the Red Team will attempt to exploit it to gain remote code execution.
  - A TCP reverse shell will be used to establish an initial foothold on the compromised host.
  - If weak credentials are discovered on additional endpoints, the Red Team may perform controlled brute-force attempts to gain access.

Stay-In:

- Post-Exploitation:
  - The Red Team plans to deploy a custom-made Command and Control (C2) payload on the initially compromised web server host.
  - The C2 will be configured to persist via startup applications, ensuring that it automatically reconnects to the Red Team infrastructure upon device reboot.
- Lateral Movement:
  - Using the foothold on the web server host, the Red Team will attempt to move laterally to another endpoint containing employee information using discovered or brute-forced credentials.

Act:

- Impact
  - The Red Team intends to simulate data exfiltration by copying employee data from the secondary endpoint to the Red Team host for demonstration purposes only.
- Impact
  - Persistence on the initially compromised machine will be maintained to emulate a real attacker's ability to stay undetected within the environment.

APPENDIX D – ENGAGEMENT OBJECTIVES

Objective 1:

- Integrity of critical employee data
    - Determine the ability of Chippy's Corner to detect and respond to unauthorized access attempts targeting employee systems.
    - Determine the system's ability to prevent tampering or modification of sensitive employee data during an attack.
    - Assess whether an attacker could gain persistence and remain undetected while accessing employee information

Objective 2:

- Exploitation of a vulnerable web server via Remote Code Execution (RCE)
    - Determine the ability of Chippy's Corner to detect and block RCE exploitation attempts against a web-facing service within the employee subnet.
    - Determine the system's ability to prevent unauthorized execution of attacker-supplied commands on the targeted host.
    - Assess whether RCE can be leveraged to gain persistence, escalate privileges, and establish unauthorized access to additional internal systems.

Objective 3:

- Evaluation of Incident Response Procedures
    - Determine the ability of Chippy's Corner to detect, analyze, and escalate alerts triggered by Red Team activities in a timely manner.
    - Determine the system's ability to isolate compromised endpoints to prevent lateral movement and additional data compromise.
    - Identify potential entry vectors into the employee subnet and customer database that may bypass current detection and response controls.