# Rules of Engagement

National Cyber Security Student Association and THE COMPANY X, Inc.

*THE COMPANY X*

*September 2021 – December 2021*

## EXECUTIVE SUMMARY

A penetration test with Rules of Engagement is a process of determining how effectively THE COMPANY's Product meets specific security objectives. The post-event analysis and technical activities from engagement will encourage THE COMPANY to develop information security policies, methodology, and individual responsibilities related to the technical findings of the assessment. THE COMPANY will determine which systems to assess and develop an assessment plan. THE COMPANY will document the selected partner for conducting technical penetration testing using methods and techniques expressed to THE COMPANY. THE COMPANY will coordinate and respond to any incidents that may occur during the test outside of the scope.

The purpose of penetration testing on THE COMPANY’s System Under Test (further referred to as SUT), is to understand the current threat of actors' tactics for accessing the system in a particular environment with no front-end protection. Software is standalone protection. Results will allow THE COMPANY to understand any vulnerabilities present. The outcome of the test is to be able to mitigate vulnerabilities, collect data on the actors' processes, and align objectives of security with business goals and mission. The tests will serve as a supplement to other testing performed for THE COMPANY from a different perspective.

The purpose of engagement for National Cybersecurity Student Association is to encourage students to test their knowledge on a real-world application and report their findings, promoting the learning of proper network attacks and benefits.

**Explicit Restrictions**:

• Internal Networks of THE COMPANY X

• Social Engineering Attempts to Personnel of THE COMPANY X

**Authorized Target Space**:

• 45.76.18.211

**Activities**:

• Reconnaissance

• Access Types

• Positioning

• Impacts

Table of Contents

# 1 RULES OF ENGAGEMENT INTRODUCTION

## 1.1 PURPOSE

This document establishes the Rules of Engagement (ROE) for cybersecurity assessments requested by THE COMPANY X from the National Cyber Security Student Association (further referred to as NCSA Participant).

The purpose of the security test is multifaceted. The main objectives are to identify the threats to the system, measure the potential vulnerabilities of the system, detect possible security risks in the system, and help developers in fixing the security problems through coding.

## 1.2 SCOPE

The scope of the agreement includes allowed hosts for NCSA Participant testing, under an unrestricted penetration testing scenario for the purpose of data collection of security weaknesses in a THE COMPANY system, and a learning experience for NCSA Participant in a real-world environment.

Real-World penetration testing for students gains practice into skills acquired. Good research skills are extremely important for a pen tester who wants to continuously improve. Soft skills or personal skills are important, as well. The most important of these is determination and a willingness to keep going in the face of adversity the ability to ask for help when you need it, Adaptability and the ability to learn on the fly.

This agreement is applicable for the receipt of activities. This document will establish the guidelines, limitations, and restrictions for conducting an engagement.

## 1.3 DEFINITIONS

**Network Discovery**: The process of discovering active and responding hosts on a network, identifying weaknesses, and learning how the network operates.

**Penetration Testing**: Security testing in which evaluators mimic real-world attacks to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data with the same tools and techniques used by actual attackers.

**Port Scanner**: A program that can remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

**Rules of Engagement (ROE):** Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test and gives the test team authority to conduct defined activities without the need for additional permissions.

**Target Vulnerability Validation Techniques**: Active information security testing techniques that corroborate the existence of vulnerabilities. They include password cracking, remote access testing, penetration testing, social engineering, and physical security testing.

**Vulnerability**: Weakness in an information system, or in system security procedures, internal controls, or implementation, that could be exploited or triggered by a threat source.

**Vulnerability Scanning**: A technique used to identify hosts/host attributes and associated vulnerabilities.

## 2 RULES OF ENGAGEMENT AND SUPPORT AGREEMENT

**a.** THE COMPANY X has agreed to be the target of attack for engagement and supporting activities. High-Level Description of Company for testing can be found in Appendix C. This document provides the ground rules for planning, executing, and reporting the engagement.

**b.** The Network Penetration Test on Publicly Facing SUT will include a write up from infiltrators that includes a description of activities to gain access and activities performed while inside of said system. Activities and Methodologies listed in Appendix B The following systems, networks, and/or assets will be included:

- THE COMPANY X SUT (https://45.76.18.211/)
- Any port access through means of this system to other systems will be included in the report but not acted upon if result is an internal network system.

**c.** The explicit responsibilities are as follows:

- Perform Gray Box Testing including:
  - Web application test: The pen test uses software to assess the security vulnerability of web apps and software programs.
  - Network services test: A user tries to either locally or remotely identify openings in the network.
  - Client-side test: Exploit vulnerabilities in client-side programs of the application such as Java, CSS, JSON, REST, XML, etc.
- Monitor access to the systems to determine entry and to determine a "winner" (as defined in Appendix E) of the attack event.
- Provide to THE COMPANY X the results of the Vulnerability Assessment scans performed to create the effects of intelligence gathering background efforts expected of a malicious entity. These results should include tools used by students and methods.
- Provide monthly updates (during the duration of the test):
  - Update 1: Student Report of Findings and Access
  - Update 2: Number of Reported Students to Access System (if applicable)

**d.** The explicit responsibilities of THE COMPANY X are as follows:

- Provide background information on company, mission, and goals for the deliverable.
- Provide IP address ranges and administrative support for target of engagement.
- Coordinate support of activities with the appropriate stakeholders.
- Provide contact information (i.e., names, job titles, phone & email address) to the signatories of this document.
- Provide to the NCSA POC the results of the Vulnerability Assessment scans performed prior to the engagement to create the effects of intelligence gathering background efforts expected of a malicious entity; Known Open Ports for NCSA Participant knowledge to compare against NCSA findings.

**e.** The following details of activity shall be agreed upon by all parties and NCSA Participants.

- The engagement is designed to test the software application against open threats without using any front-end protections such as an SBC or firewall in the field.
- The intention of the system is to withstand attacks, report any threats, monitor access, and perform the duties of its nature.

- An open network will be utilized. An open network is defined as a network with access to the Internet.
- There will be complete and open coordination with all stakeholders required for engagement execution.
- Activities are limited to the target of engagement.
- Tools and activities may be intrusive but will not intentionally disrupt services outside the authorizations of these Rules of Engagement.

**f.** Efforts will be coordinated by NCSA POC and THE COMPANY POC for the duration of the engagement. The target is only those hosts and internet protocol (IP) addresses within the confines and control of the target of engagement network.

**g.** Methods may be intrusive, but should not be destructive, and will be terminated if information is shared outside of the parties within the agreement pertaining to an actual intrusion. THE COMPANY X is responsible for informing the NCSA POC if an actual intrusion is discovered. The NCSA Participant will report the actual intrusion to the appropriate representative, along with any substantiating information regarding the detected intrusion within the given subset of time agreed upon for the event to occur.

**h.** THE COMPANY X systems contain code and technical references which are not to be viewed, distributed, or evaluated by external organizations without proper authorization given. Neither party shall use the name of the other in connection with any products, promotions, or advertising without the prior written permission of the other party. Disclaimer for Company X provided in Appendix D.

**i.** The attempt is to gain access to the target of engagement.

**j.** An off-limits IP list is provided in Appendix A. This list should only include those IP ranges within the network that are not part of the engagement.

**k.** 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 POC Team to review these notice procedures and certify they provide sufficient notice.

**l.** Sensitive information reporting:

- 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.
- Reporting is otherwise conducted in a way that does not attribute information or activity to an individual.
- Activities may not be conducted in support of law enforcement or criminal investigation purposes.

**m.** Cease operations process:

- Suspension of activity is required upon detection of computer anomalies that could potentially be unauthorized intrusions into target of environment networks.
- Suspension of activity is required 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 and contact THE COMPANY X for any of these cases.

**n.** Information usage:
- No intentional modification or deletion of any operational user data.
- During the timeframe of test (September to December) Denial of Service attacks and such is outside the bounds of test.
- Reporting is conducted in a way that does not attribute information or activity to a specific individual.

**o.** Deconfliction process:
- All detected information assurance incidents, whether real-world or alleged activity, should immediately be reported using normal incident reporting processes.
- The COMPANY X POC may contact the POC to determine if discovered activities are the result of the test.

**p.** Deliverables:
- THE COMPANY X will provide a written summary of the engagement results to the representatives within 30 days following completion of the test for test comparison and winner determination. Reports and findings will belong to THE COMPANY and should not be distributed without the written consent of THE COMPANY.

## 2.1 ROE PROVISIONS

The following additional provisions apply to this memorandum:

- **a.** All operations will be conducted within guidelines established within the Rules of Engagement.
- **b.** All contact with computer networks/subnets will be from within the 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 COMPANY X, and signors.

## 2.2 REQUIREMENTS, RESTRICTIONS, AND AUTHORITY

**a.** Test 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.).
- Provide contact information (i.e., names, job titles, phone & email address) to the COMPANY X 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.
- NOT damage internal 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.
- Social Engineering and Phishing Attempts to personnel of THE COMPANY X are off limits.

## 3 AUTHORIZATIONS

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.

**APPENDIX A – TARGET ENVIRONMENT**
List of assets, systems, and data

Restricted IP Addresses:

- All Other Internal Networks Found

Authorized IP Space:

- 45.76.18.211

Restricted Hosts:

- *. The Company.com

Authorized Hosts:

- Demo. The Company.com (45.76.18.211)

## APPENDIX B – NSCA PARTICIPANT METHODOLOGY

Example Test Methodology

Get-In:

- Reconnaissance
  - Perform Open-Source Intelligence (OSINT) against the target
  - Search using open unauthenticated sources.
  - Target web sites
  - Social Media
  - Search engines
  - Public Code repositories
- Enumeration
  - Identify external assets.
  - Perform reverse DNS scan to identify registered hosts.
  - Identify URLs and other external touch points from scan and OSINT.
  - Web presence evaluation
  - Browse as a normal user through a web proxy to capture intelligence and understanding.
  - Identify known vulnerabilities and vulnerable conditions.
- Exploitation
  - Attempt to exploit targets based on current knowledge.
  - Perform situational awareness on target.
  - Attempt Local Privilege Elevation
  - Attempt Domain or other system level Privilege Elevation
- Stay-In:
  - Post Exploitation
    - Identify domain user/groups/memberships.
    - Identify IP space
    - Identify file shares.
    - Establish persistence.
    - Use persistence plan to place agents on target systems.
    - Move Laterally
  - Continued Lateral Movement
  - Continued Enumeration
- Act:
  - Impact
    - Modification of Transaction Records
  - Impact
    - Modification of customer order database

## APPENDIX C – BACKGROUND INFORMATION THE COMPANY X AND OBJECTIVES FOR TEST

Who We Are:

- 40+ years focusing on innovative communications solutions.
- Develop Hardware and Software Products for secure and reliable communications technologies to fit various customer needs.
- THE COMPANY bridges years of technological advancements, including landlines, VoIP phones, smartphones, radios, satellite phones, and magneto crank phones.
- U.S.-based development & manufacturing
- Government & Military Communications
- Service Provider Solutions
- Public Safety Communications
- Electronics Manufacturing Services

What We are Looking to Achieve:

- Security deficiencies which exist in Software today
- What adversaries can potentially do to the system before AND after illegitimate access is attained?
- Techniques and capabilities of lateral movement
- Software's current capability to detect/deter/log illegitimate access and attack attempts.
- The rigidity and practical implications of different fill levels
- Students will be able to work off a real-world instance of a web application in the field with no security protections to test what they have learned in Cyber Security.
- Partnership with NCSA means continued events to test Software® strengths.

## APPENDIX D – BACKGROUND INFORMATION SOFTWARE SUT AND QUICK REFERENCE TO SERVICES

Disclaimer:

THE COMPANY X owns the Software of SUT for attack, THE COMPANY X does not own the service or architecture hosting it.

THE COMPANY Software® is a flexible Unified Communications (UC) platform. The software is based on open standards with a focus on interoperability, reliability, and security. THE COMPANY Software offers features, including voice, video, and chat communications, IP trunking, conferencing, and encryption.

THE COMPANY Software® is designed to increase flexibility while reducing size, weight, and power (SWaP) requirements. Designed specifically for government and military users, Software's feature set includes VoIP, Video (P2P), Chat/XMPP with Presence, Voice Conferencing, Unified Messaging, and full Multi-Level Precedence and Preemption (MLPP) support.

THE COMPANY Software is a web application front end of a database server residing on FreeBSD. The entire application is virtualized.

Upon login to the system, users can register a SIP phone to the system, add users, create announcements, etc.

## APPENDIX E – DETERMINATION OF WINNERS AND WRITE UP REQUIREMENTS

Winners will be determined collectively between THE COMPANY X and National Cybersecurity Student Association. Top Choice will be for best method of attack, most targeted approach, and most creative exploitation of resources and report methodology for testing.

As part of the learning process for THE COMPANY X and the students, emphasis will be placed on the report detail of findings and methods of attack when determining a winner. This report is optional but encouraged.

The write up will include at minimum participants name and email address for method of contact. As this is a real-world scenario, attention to detail, critical thinking, and proper report templating will be encouraged. Participant who chooses to submit an after-action report of their kill chain processes as well as infiltration methods well documented and formatted will have the chance to be recognized for their achievements by THE COMPANY X.