KOMODOSEC

MAKING CYBERSECURITY SIMPLE

RULES OF ENGAGEMENT FOR RED-TEAM

www.komodosec.com

EXECUTIVE SUMMARY

Cyber Security is an Exponential Problem

Red team assessments help you understand your organization's detection and investigative capabilities. Not setting the right rules and expectations when starting a Red team or Penetration Testing exercise may lead to less-than-great outcomes.

This document is an example of the rules of engagement between the Komodo Consulting Team and the Customer Teams for the Red team and Pentest exercises which will help you understand the rules of engagement for Red team exercise.

FRAMEWORK

- ### Contacts

	Name	Email	Phone

- ### Timeline
  - Activity Start Date:
  - Activity End-Date:
  - A red-team activity usually takes about 60 days start to end.

- ### Locations

Komodo Offices

Customer Europe Site

Customer US Site

- ### Status Updates

Weekly conference will take place on Mondays &, Thursdays OR specify the days you want the status updates

Critical findings will be notified on a daily basis.

- ### Testing Time Frame

During Business Hours?

After Business Hours? E.g. Israeli GMT+2 daytime hours (PST night time)

On Weekends?

Doesn't Matter

- Our assumptions are that 90% of testing will be performed on Israeli daytime hours

- **Stealth/Shunning**

  Testing should be performed in stealth mode

  - Note that this limits the pentesters capabilities but reflects a closer to 'real life' attack simulation.

- **Permission To Test**

  The Customer hereby acknowledges that Komodo's team will perform penetration testing on systems in scope (see IP range and domain lists below).

  Testing may lead to system instability and all due care will be given by the tester to not crash systems in the process. However, because testing can lead to instability, and the connection between testing and system instability is sometimes loosely coupled and wrongly connected, The Customer shall not hold the tester liable for any system instability or crashes.

- **Legal Approval**

  The Customer hereby approves that testing the systems in scope is approved to be legal in the state they are performed.

PROJECT SPECIFIC

- **List IP Range and Domains in Scope**

  Here follows is the list of IP ranges identified by Komodo at the preliminary information gathering stage. These IP addresses will define the scope for the project. Each range is attached with its Physical GEO location.

IP/Domain	GEO	Zone

- **Leverage**

  In the case that a system is penetrated, how should the testing team proceed? (Check all that apply)

  Perform a local vulnerability assessment on the compromised machine?

  Attempt to gain the highest privileges (root on UNIX machines, SYSTEM or Administrator on Windows machines) on the compromised machine?

  Attempt to proceed with the attack towards internal reachable servers

  Stop and notify

- **Available Testing Environment (Check All That Apply)**

  Production Environment

  Staging Environment

  Test Environment

  Development Environment

- **Effectiveness of Defense**

  Can be defined as required

- **Exceptions**

  Modules to exclude, e.g. Mainframe server is not part of the scope.

  1.
  2.
  3.

  Tests to exclude, e.g. Do not run RCE exploits in production.

  1.
  2.
  3.

  Tools to exclude

  1.
  2.
  3.

ABOUT KOMODOSEC

Cybersecurity consulting firm established 2011 by security experts and military intelligence veterans serving finance, healthcare, tech, and critical infrastructure sectors.

SERVICES

- Advanced penetration testing (infrastructure, applications, cloud)
- Red team assessments
- Cloud security architecture assessment
- Mobile/API security testing
- Supply chain risk assessment
- Compliance advisory
- Security architecture for startups

OUR ADVANTAGE

- Deep technical expertise from operational experience
- Business-aligned security recommendations
- Professional, discreet, and trustworthy approach

TRUSTED BY INDUSTRY LEADERS

SAFECHARGE

"Komodosec provides us with peace of mind by securing our applications before they go into production and supporting us during critical incidents."
— *Amnon Cohen, CIO, Safecharge*

Trusteer
an IBM Company

"Komodo presents valuable insights and advice. Work with Komodo Consulting has always been a streamlined, efficient process. Results are always to the point and right on time, accompanied by valuable insights and advice."
— *Eldan Ben-Haim, CTO, Trusteer (IBM)*

Enhance Your Security with
Actionable Customized Recommendations

REQUEST FREE CONSULTATION

New Castle, DE 19899
USA
+1 917 5085546

1 Golders Green Road
London NW11 8DY
+44 20 37694351

Ariel Sharon 4, Giv'atayim
Israel
+972 9 955 5565

info@komodosec.com | www.komodosec.com