Rules Of Engagement For Red-Team

Executive Summary

The nature of this document is to portray in broad strokes the rules of engagement between Komodo Consulting Team and The Customer Teams for the Red-Team and Pentest exercises.

Framework

Contacts

	Name	Email	Phone
Komodo – Point of contact	Komo Dosec	info@komodosec.com	+972-9-9555565
The Customer - Manager			

Timeline

Activity Start Date: January 1st 2020

Activity End-Date: March 31st 2020

- 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_____

☐ 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

1. Mainframe server is not part of the scope.
2.

Tests to exclude

1. Do not run RCE exploits in production.
2.

Tools to exclude

1.
2.