PEACH
FUZZER

TCPv4 Peach Pit Data Sheet

Peach Fuzzer, LLC

v3.6.94

Peach Fuzzer, LLC
1122 E Pike St
Suite 1064
Seattle, WA 98112

Transmission Control Protocol for Internet Protocol Version 4 (TCPv4)

- Peach Pit: TCPv4
- Direction: Client
- Supported Platforms: Windows, Linux, OS X

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol suite (IP), and is so commonly used together that the entire suite is often called TCP/IP. TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to a local area network, Intranet or the public Internet.

Specifications

Specification	Title
RFC793	Transmission Control Protocol

Use Cases

Messages	Specification
MaximumSegmentSize	RFC793 Section 3.1 page 17

Supported Features	Specification
Establishing a connection (Async, Client)	RFC793 Section 3.4
Closing a Connection (Async)	RFC793 Section 3.5 Case 2
Data Communication	RFC793 Section 3.7

Configuration

Target Configuration

A TCP listener listening on the port defined in configuration file is required. The network tool socat can be used as the listener.

To use this pit, disable outgoing RST packets; Peach manages TCP states outside of the kernel context.

Required Pit Configuration Changes

TargetIPv4

IP address of the target host machine.

SourceIPv4

IP address of the interface on the local machine.

TargetIPBytes

IP address of the target host machine in hexadecimal.

SourceIPBytes

IP address of the interface on the local machine in hexadecimal.

SourcePort

TCPv4 port number of the local machine.

TargetPort

TCPv4 port number of the target host machine.

Optional Pit Configuration Changes

Strategy

Fuzzing strategy Peach will use for testing.

LoggerPath

Path to folder where logs will be stored.

PitLibraryPath

Path to the relative base directory where all pits are located.

Timeout

Timeout in milliseconds to wait for incoming data.

Configure Monitoring

Monitoring must be configured to provide fault detection, data collection, and automation as needed.

Running

Single test debug run

```
peach -1 --debug TCPv4.xml
```

Full test run

```
peach TCPv4.xml
```

Examples

Example 1. Sample TCPv4 Configuration File

Example configuration using socat on Linux.

First we must configure the firewall then install and run socat; for this example we assume you are running Linux. For other platforms follow the platform specific installation instructions for socat and firewall configuration.

```
#Disable outgoing RST on the node running Peach
sudo iptables -A OUTPUT -p tcp -m tcp --tcp-flags RST RST -j DROP

#Install socat

sudo apt-get install socat

#Set up TCPv4 listener
socat tcp4-l:12345,fork,reuseaddr STDIO
```

```
<?xml version="1.0" encoding="utf-8"?>
<PitDefines>
<All>
<Ipv4 key="SourceIPv4"
value="127.0.0.1"
name="Source IPv4 Address"
description="The IPv4 address of the machine running Peach Fuzzer. The IPv4 address
can be found on Windows by running 'ipconfig' and looking for the 'IPv4 Address'
field. For Linux run 'ifconfig' and look for 'inet addr' field. For OS X run
'ifconfig' and look for the 'inet' field."/>

<Range key="SourcePort"
value="1234"
min="0" max="65535"
name="Source Port"
description="The source port the network packet originates from."/>

<Ipv4 key="TargetIPv4"
value="127.0.0.1"
name="Target IPv4 Address"
```

```
description="The IPv4 address of the target machine or device. The IPv4 address can
be found on Windows by running 'ipconfig' and looking for the 'IPv4 Address' field.
For Linux run 'ifconfig' and look for 'inet addr' field. For OS X run 'ifconfig' and
look for the 'inet' field." />

<Range key="TargetPort"
value="12345"
min="0"
max="65535"
name="Target Port"
description="The target or destination port the network packet is sent to."/>


<String key="LoggerPath"
value="logs/tcpv4/"
name="Logger Path"
description="The directory where Peach will save the log produced when fuzzing." />

<Strategy key="Strategy"
value="Random"
name="Mutation Strategy"
description="The mutation strategy to use when fuzzing." />

<String key="PitLibraryPath"
value="."
name="Pit Library Path"
description="The path to the root of the pit library."/>
</All>
</PitDefines>
```