OFTG-Ninja User Guide

Get out -- undetected

Version 1.0

Ryan O’Horo

IOActive, Inc. 2015

Contents

[Overview 4](#_Toc420203315)

[About OFTG-Ninja 4](#_Toc420203316)

[How OFTG-Ninja Works 4](#_Toc420203317)

[Technical Requirements 4](#_Toc420203318)

[Prerequisites 4](#_Toc420203319)

[Installation 5](#_Toc420203320)

[Getting Started 5](#_Toc420203321)

[Starting OFTG-Ninja 5](#_Toc420203322)

[Deploying a Server 5](#_Toc420203323)

[Configuring Prerequisite Resources 5](#_Toc420203324)

[Configuring a Client 6](#_Toc420203325)

[Running an Assessment 6](#_Toc420203326)

[Payloads 6](#_Toc420203327)

[Cases 6](#_Toc420203328)

[Plugins 6](#_Toc420203329)

[Configuration File 6](#_Toc420203330)

[Third-Party Licenses 6](#_Toc420203331)

# Overview

## About OFTG-Ninja

OFTG-Ninja’s goal is to be a vulnerability assessment tool for DLP appliances, firewalls and policies that prevent certain types of data from leaving a network. By utilizing a suite of exfiltration methods, a large number of possible exfiltration vectors are tested and actively exploited.

Go ahead and get started.

## How OFTG-Ninja Works

OFTG-Ninja uses a client-server model to move data from one network to another. Using packet capture and forgery, packet transmission over various protocols are simulated without the need for full protocol stacks or bound ports. This frees host ports for other services and allows any protocol to interact with OFTG-Ninja.

# Technical Requirements

OFTG-Ninja is a python application which uses an embedded web server to allow user interaction. Because OFTG-Ninja is a full web server and packet processing application, several dependencies need to be met before running.

Prerequisites  
The following components have been fully tested with OFTG-Ninja:

Windows 7, Linux 2.x

WinPcap 4.1.3 / Libpcap vX.XX

Python 2.7.8

Python Flask 0.10.1

Python Flask-SocketIO 0.6.0 (<http://aka.ms/vcpython27> Microsoft Visual C++ 9.0 Runtimes)

Python Websocket-Client 0.32

Python socketIO-client 0.6.5

Python Impacket 0.9.13

Python PyCrypto / pysodium

Resources

# Installation

OFTG-Ninja can be configured to run unattended at startup. See Configuration File.

# Getting Started

## Starting OFTG-Ninja

python oftg-ninja.py

http://127.0.0.1:7331/

## Deploying a Server

After installing and running OTFG-Ninja on the Server host, open the web interface and navigate to the Server tab. Choose the interface from the drop-down menu which you intend to receive Client traffic on. Click Start Server. A new Server Task will be started.

This will start the packet capture process and load all available plugins for traffic analysis.

The Server host should be such that no firewall, IPS or other appliance will interfere with incoming traffic and should be on a network outside of the network being assessed.

Using a hosted service to run OTFG-Ninja in Server mode is recommended for best results.

## Configuring Prerequisite Resources

Some plugins require ancillary services or configuration values that will allow the plugin to function as intended. See Cases.

**Examples:**

The DNS Plugin requires a valid domain which can receive DNS requests from the Client. A dedicated domain name should be configured with the address of the Server host as the name server for that domain.

The IPv6 Plugin and Plugins which support IPv6 require support by the Client Host, Server host and any intermediate network for IPv6 addressing and routing.

Consider these requirements when choosing a Server host.

## Configuring a Client

After installing and running OTFG-Ninja on the Client host, open the web interface and navigate to the Cases tab. Click Create Case. Name the new case and select the Plugins you wish to use for this Case and customize the Plugin parameters for your environment. Choose from premade or upload custom payloads for testing, if desired. Configure any other desired Case options like Compression and Encryption. Click Save Case.

## Running an Assessment

With the Server Task running on the Server host, open the web interface of the Client host and navigate to the Client tab. Choose a Case and enter the external IP address(s) of the Server host. Click Start Client. One or more Client Tasks will be created. While these Tasks are running, the Client will iterate through each selected Plugin attempting to contact the Server.

As the Client runs, The Server Task will collect any available traffic generated by the Client. The Server host will display data received and details about which Plugin was used to send it.

When the Client completes, the details of the assessment will be available in the Reports tab.

# Payloads

# Cases

# Plugins

# Configuration File

Client Key?

# Third-Party Licenses