InfoSec Ninjas

Croissants

Intrusion Detection and Prevention System (IDPS)

InfoSec Ninjas

Who am I?

Samiux is an Information Security Enthusiast.

- - OSCE, OSCP, OSWP
- - Blogger
- - Linux user

Hobbies :

- - Programming
- - Reading
- - Pentesting

InfoSec Ninjas

What is Croissants?

Croissants is an Intrusion Detection and Prevention System based on Suricata.

- - Developed by Samiux since 2012
- - Open Source under GPLv3
- - Intrusion Prevention System (IPS)
- - High Performance
- - Ultra-low Latency

- - Network based
- - Host based

- - Not Embedded Linux

InfoSec Ninjas

Main components :

- - Suricata
- - Hyperscan
- - Ubuntu Server

InfoSec Ninjas

General Features :

- - Blocks known malicious activities
- - Blocks known malware and virus
- - Easy and straight forward interfaces
- - Compatible with Bittorrent and 4K video streaming
- - Ultra-low latency for demanding online games
- - Compatible with Microsoft Windows, GNU Linux, Apple macOS, Apple iOS, Google Android
- - No subscription fee
- - Automatically update and upgrade
- - Urgent Update Push
- - Plug, Play and Forget!

InfoSec Ninjas

Detailed Features :

- - Emerging Threats (ET) Open Ruleset (Default, Free)
- - ET Pro Ruleset (Optional, Expense)
- - Malware Hashes Ruleset - MD5, SHA1, SHA256
- - Malware SSL/TLS Fingerprints Ruleset - JA3
- - Protocol Ruleset - SSH, DNS, TLS, etc
- - Malicious/Compromised IP Addresses Blacklist
- - TOR (The Onion Router) Exit Nodes Blacklist
- - Malicious URL/Domain Blacklist
- - Malicious SSL/TLS Fingerprints Blacklist
- - Bandwidth Over 10Gbps
- - Drop instead of Reject

InfoSec Ninjas

NON Open Source Features :

- - Not For Sale
- - Blocks Common Scanners
- e.g. nmap, masscan, Shodan, Censys, Zoomeye

InfoSec Ninjas

Minimum Requirements :

(1) Hardware

- - Multi-Core Intel/AMD x86 CPU (at least Intel ATOM D2550)
- - 8GB DDR3 RAM or more
- - 64GB SSD or more
- - 3 Network Interface Cards/Ports (Network Based only)
- - 1 Network Interface Card/Port (Host Based only)
- - CPU with AVX2 or better (at least SSSE3)

- * Intel ATOM D2550 can handle up to 300Mbps traffic only

(2) Software

- Ubuntu Server LTS (64-bit)

InfoSec Ninjas

Demo

Open Source Interfaces (Network Based)

- glances and netdata - https://youtu.be/kVHKU32Mky8

Non Open Source Features

- Shodan - https://youtu.be/OoPS8Au2kAw
- nmap - https://youtu.be/uwcCDcdaRT4

Live Target (Online Time Is Limited)

- Croissants and Longjing (Deep Learning Driven Web Application Firewall)
- Infosec Projects - http://www.infosec-projects.com/

InfoSec Ninjas

Reference

- Suricata - https://suricata-ids.org/
- Hyperscan - https://www.hyperscan.io/
- Ubuntu - https://ubuntu.com/

- Croissants - https://www.infosec-ninjas.com/croissants
- Freenode - #infosec-ninjas (SSL and Port 6697)
- Infosec Ninjas - https://www.infosec-ninjas.com/

InfoSec Ninjas

Thank you!

InfoSec Ninjas

Q&A