

INTRODUCTION TO CYBER SECURITY WITH SURICATA

ELİF ŞAHİNÖZ

Contents

1. Basic Linux Commands
2. Computer Networks Concepts
 - 2.1 Network Types
 - 2.2 Network Devices
 - 2.3 Cable Types
 - 2.4 General Terms
3. Installation VMware
4. Installation Kali Linux on VMware
5. What IPS/IDS?
 - 5.1 What is IPS?
 - 5.2 IPS Classes
 - 5.3 What is IDS?
 - 5.4 IDS Classes
 - 5.5 What is Signature
 - 5.6 Signature Alarms
 - 5.7 What are the differences between IPS and IDS?
 - 5.8 How to Bypass IDS and IPS?
6. What is Suricata?
 - 6.1 What is Suricata?
 - 6.2 What is Suricata used for?
 - 6.3 Why choose Suricata?
7. Suricata vs Snort
 - 7.1 Differences
 - 7.2 Malware Viruses/Test Cases
8. Suricata Installation
9. Suricata Rules
 - 9.1 Rules Format
 - 9.2 Meta Keywords
 - 9.3 IP Keywords
 - 9.4 TCP Keywords
 - 9.5 UDP Keywords
 - 9.6 ICMP Keywords
 - 9.7 Payload Keywords
 - 9.8 Transformations
 - 9.9 Prefiltering Keywords
 - 9.10 Flow Keywords
 - 9.11 Bypass Keyword
 - 9.12 HTTP Keywords
 - 9.13 File Keywords
 - 9.14 DNS Keywords
 - 9.15 SSL/TLS Keywords

- 9.16 SSH Keywords
- 9.17 SIP Keywords
- 9.18 RFB Keywords
- 9.19 MQTT Keywords
- 9.20 HTTP2 Keywords
- 9.21 Generic App Layer Keywords
- 9.22 IP Reputation Keyword
- 10. Testing Suricata with Basic Rules
 - 10.1 Example 1
 - 10.2 Example 2
- 11. Suricata's Command Line Options
 - 11.1 What is pcap?
 - 11.2 Unit Tests
- 12. Packet Profiling
 - 12.1 Update Suricata from GIT Repository
 - 12.2 Wireshark
 - 12.3 Use of Wireshark
 - 12.4 Suriwire
- 13. Using Capture Hardware
 - 13.1 eBPF and XDP
 - 13.2 Setup Bypass
 - 13.3 Setup eBPF Filter
 - 13.4 Setup eBPF Bypass
- 14. Splunk Free for Suricata
 - 14.1 What is Splunk?
 - 14.2 How does it work?
 - 14.3 Splunk installation on Kali
 - 14.4 How to use Splunk?
 - 14.5 Splunk for Suricata
 - 14.6 Search Details and Logs
- 15. Suricata on pfSense
 - 15.1 What is pfSense?
 - 15.2 What is firewall?
 - 15.3 What is router?
 - 15.4 Installing pfSense on VMware
 - 15.5 Setup Suricata on pfSense
 - 15.6 Check Out the Config
- 16. Malware& Malicious Traffic
 - 16.1 What is Malicious Traffic?
 - 16.2 Malicious Traffic Types
 - 16.3 How does Malicious Traffic work?
 - 16.4 Detecting Malicious Traffic
 - 16.5 Any.run
 - 16.6 Monitoring Network Traffic with Suricata and ClamAV
- 17. References

CHAPTER 1

Basic Linux Commands

pwd : print working directory

cd : change directory

cd / : root directory

cd .. : previous directory

ls : to list

ls -l : to list in more detail

cd .. : a parent directory

mkdir : make directory

touch : create file

rm fileName : delete file

rm -f fileName : delete file, f means force. Does not ask questions when deleting.

cp : copy

mv : move file

shred -zuv fileName : wipe out completely

man ls : get information

head -4 : output first 4 lines

tail -4 : output last 4 lines

grep -n "word" fileName : finds the "word" in fileName.

chmod : change mod(read write)

ex: chmod 700 fileName

./fileName : run file

history : shows all commands written in the shell.

su : switch user

Computer Networks Concepts

2.1 Network Types

LAN : Local Area Network

An in-house, in-home network is an example.

There are structures such as Ethernet and token rings,

Switch is used.

WAN : Wide Area Network.

Physical distance is increasing for network.

The largest WAN is the Internet.

Router is used.

There is no physical ownership as the WAN passes over other networks.

WLAN : Wireless Local Area Network

MAN : Metropolitan Area Network

Physical Ranking: LAN < MAN < WAN

CAN: Campus Area Network

More than one LAN.

PAN : Personal Area Network

Network around an individual.

Ex: Bluetooth

SAN :Storage Area Network

Network of data storage devices

Faster than SSD.

SAN: System Area Network (cluster area network)

Coexistence of high speed computers.

POLAN : Passive Optical Local Area Network

2.2 Network devices

Hub : Simples machine for network.

Sends the packet everywhere, not where it needs to be forwarded.

Switch : Not as in the hub, it takes the packet where it needs to be transmitted.

There is control with the MAC table (Media Access Control)

Router : Sending packets from one network to another.

They only receive information about them. It can also be called a gateway.

Modem : It comes without changing the mode.

2.3 Cable Types

UTP: Unshielded Twisted Pair

Electrically conductive copper cables, no shielding (against electromagnetic).

STP: Shielded Twisted Pair

Coaxical

Fiber optic: Communication with light.

Purpose : Avoiding electromagnetic fields

2.4 General Terms

What is log?

Means storage of digital movements and keeping a record.

What is port?

Means input or socket.

Ports can be physical or virtual.

It can send data to a physically attached machine or control its operation.

Virtual ports are logical connection points that are routed over the network and internet or through software while using a computer.

Computers IP addresses are given by the server programs to ensure communication and data exchange in the network environment. When a server on the network wants to connect to the program, the port number is added next to the IP address.

What is protocol?

Protocol is a set of rules that govern communication between computers on a network.

What is IP?

Internet Protocol

IP addresses are at the level of 32 bits, but they are divided into 4 groups of 8 bits for easy reading.

There are two parts of the IP address structure. The first is the number of a private network to which the computer is connected. The second is the computer's private number. While the data passes through routers, only the number of this private network is checked.

What is TCP?

Transmission Control Protocol

Connection-based protocol. Data transmission is guaranteed.

TCP works as a triple handshake.

What is UDP?

User Datagram Protocol

It is used for media, voice, large data transfers.

Data transmission in UDP is not guaranteed, but it is faster than TCP.

DNS resolution happens with UDP.

CHAPTER 3

Installation VMWare

What is Vmware?

Vmware is a virtualization and cloud computing software.

What is Virtualization?

Virtualization is the process of creating a software-based, or virtual, representation of something, such as virtual applications, servers, storage and networks.

Setup Vmware for Suricata

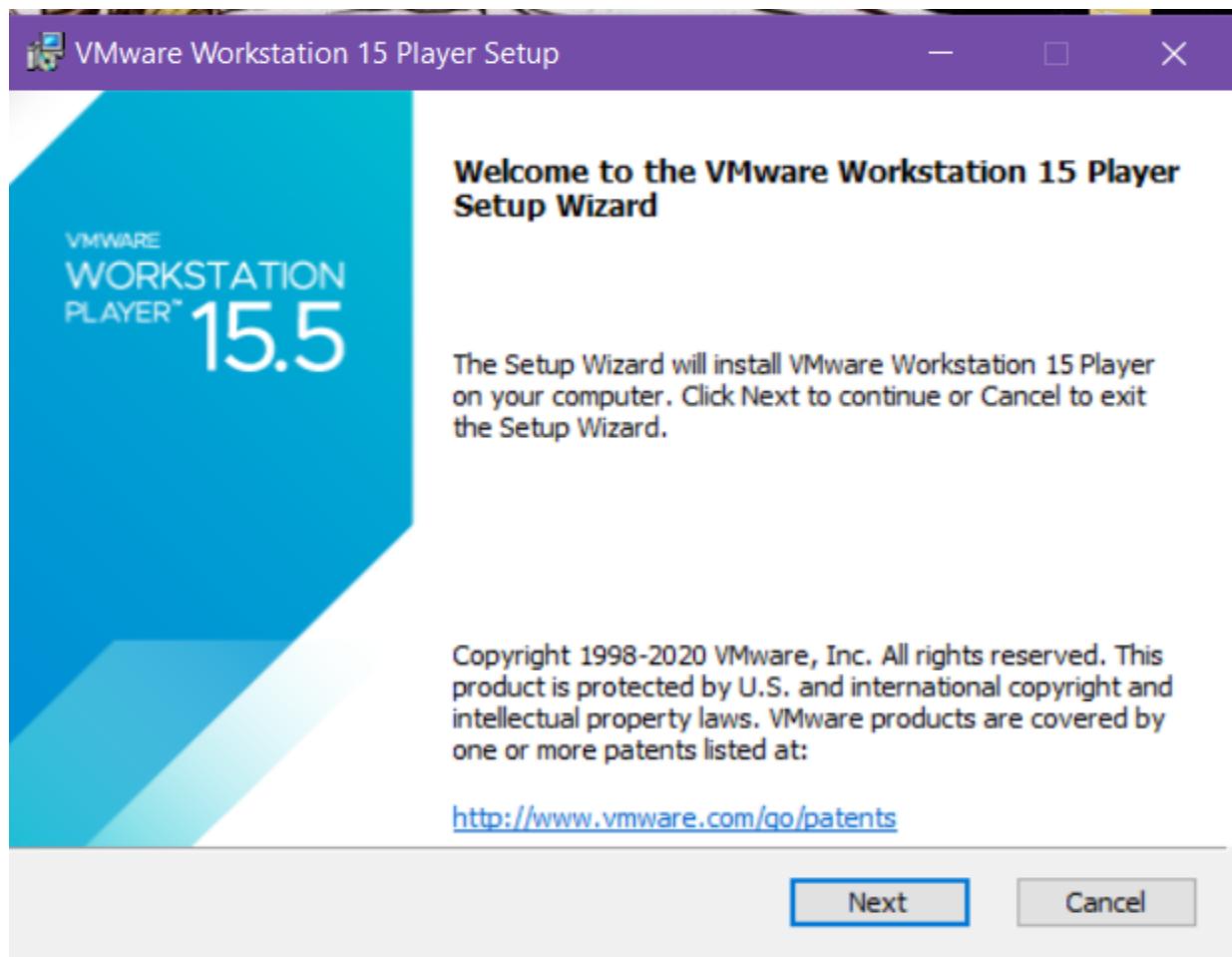
Step 1 : Go to the website and download by operating system.

<https://www.vmware.com/tr/products/workstation-player/workstation-player-evaluation.html>

There are different versions of VMware. This is a free one.

The screenshot shows the VMware website's product page for VMware Workstation Player 15.5. At the top, there's a navigation bar with links for Cloud, Solutions, Products, Support & Services, Downloads, Partners, and Company. Below the navigation is a breadcrumb trail: Products > Workstation Player > Try VMware Workstation Player. The main content area features a large image of the VMware Workstation Player 15.5 software box, which is blue and white with the text "VMWARE WORKSTATION PLAYER™ 15.5". To the right of the box, there's a brief description: "VMware Workstation Player is an ideal utility for running a single virtual machine on a Windows or Linux PC. Organizations use Workstation Player to deliver managed corporate desktops, while students and educators use it for learning and training." It also mentions that the free version is available for non-commercial, personal and home use. Below this, there are links for "Commercial organizations require commercial licenses to use Workstation Player." and "Need a more advanced virtualization solution? Check out Workstation Pro.". At the bottom of the page, there are two download buttons: "Try Workstation 15.5 Player for Windows" and "Try Workstation 15.5 Player for Linux".

Step 2 : Set up the program.





End-User License Agreement

Please read the following license agreement carefully.



VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU

I accept the terms in the License Agreement

Print

Back

Next

Cancel



VMware Workstation 15 Player Setup



Custom Setup

Select the installation destination and any additional features.



Install to:

D:\VMware\VMware Player\

Change...

Enhanced Keyboard Driver (a reboot will be required to use this feature)

This feature requires 10MB on your host drive.

Back

Next

Cancel



User Experience Settings



Edit default settings that can improve your user experience.

- Check for product updates on startup

When VMware Workstation 15 Player starts, check for new versions of the application and installed software components.

- Join the VMware Customer Experience Improvement Program

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical

[Learn More](#)

Back

Next

Cancel



Shortcuts

Select the shortcuts you wish to place on your system.

Create shortcuts for VMware Workstation 15 Player in the following places:

Desktop

Start Menu Programs Folder

Back

Next

Cancel



VMware Workstation 15 Player Setup



Ready to install VMware Workstation 15 Player

Click **Install** to begin the installation. Click **Back** to review or change any of your installation settings. Click **Cancel** to exit the wizard.

Back

Install

Cancel



VMware Workstation 15 Player Setup



Installing VMware Workstation 15 Player



Please wait while the Setup Wizard installs VMware Workstation 15 Player.

Status: Installing virtual network drivers.



Back

Next

Cancel



VMware Workstation 15 Player Setup



VMWARE
WORKSTATION
PLAYER™ 15.5

Completed the VMware Workstation 15 Player Setup Wizard

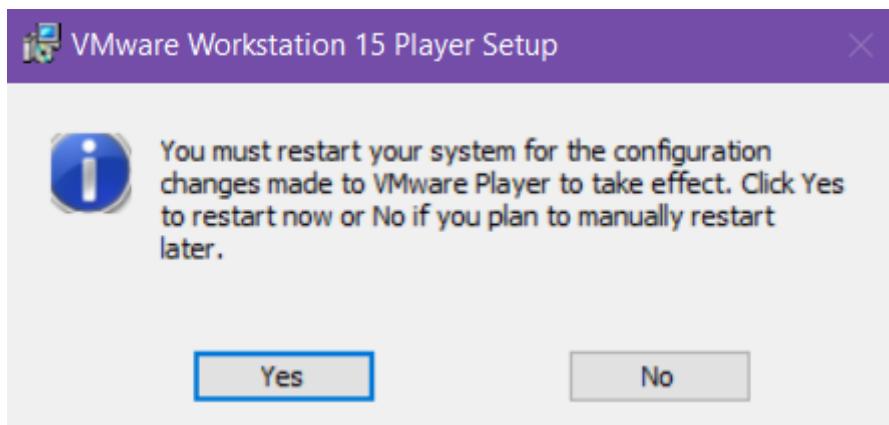
Click the Finish button to exit the Setup Wizard.

Press the License button below if you want to enter a license key now.

License

Finish

Step 3: It is ready for use after restarting the computer.



VMware Workstation 15 Player (Non-commercial use only)

Player ▾ | ▶ ⌂ ⌃ ⌄

 Home

Welcome to VMware Workstation 15 Player

 **Create a New Virtual Machine**
Create a new virtual machine, which will then be added to the top of your library.

 **Open a Virtual Machine**
Open an existing virtual machine, which will then be added to the top of your library.

 **Upgrade to VMware Workstation Pro**
Get advanced features such as snapshots, virtual network management, and more.

 **Help**
View online help.

 This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. [Buy now.](#)

CHAPTER 4

Installation Kali Linux on VMware

I will download Suricata to Kali Linux, so I install Kali Linux on vmware.

Step 1 : Download Kali Linux Vmware Images

DOWNLOAD KALI LINUX VIRTUAL IMAGES

Want to download Kali Linux custom images? We have generated several Kali Linux VMware and VirtualBox images which we would like to share with the community. Note that the images provided below are maintained on a "best effort" basis and all future updates will be listed on this page. Furthermore, Offensive Security does not provide technical support for our contributed Kali Linux images. Support for Kali can be obtained via various methods listed on the [Kali Linux Community](#) page. **These images have a default login/password of "kali/kali" and may have pre-generated SSH host keys.**

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>. Downloads are **rate limited to 5 concurrent connections**.

– KALI LINUX VMWARE IMAGES				
Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VMware 64-Bit	Torrent	2020.2a	2.2G	fc12968c1842bc6583b6c24eed3b6b56baa6f9f2790c20d26d6617ebc93e62aa
Kali Linux VMware 32-Bit	Torrent	2020.2a	1.9G	e5e3a5d41fba8353c69b33d046dfb547cf8e56815ce38926b7c16bb9449535b4

<https://www.kali.org/downloads/>

step 2: Install in VMware after download.

Welcome to VMware Workstation 15 Player



Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.



Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.



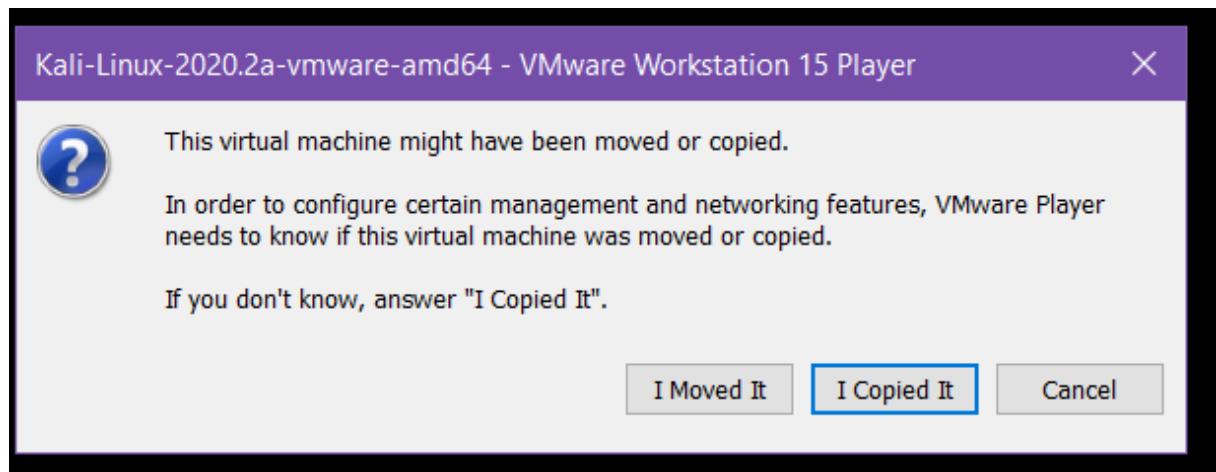
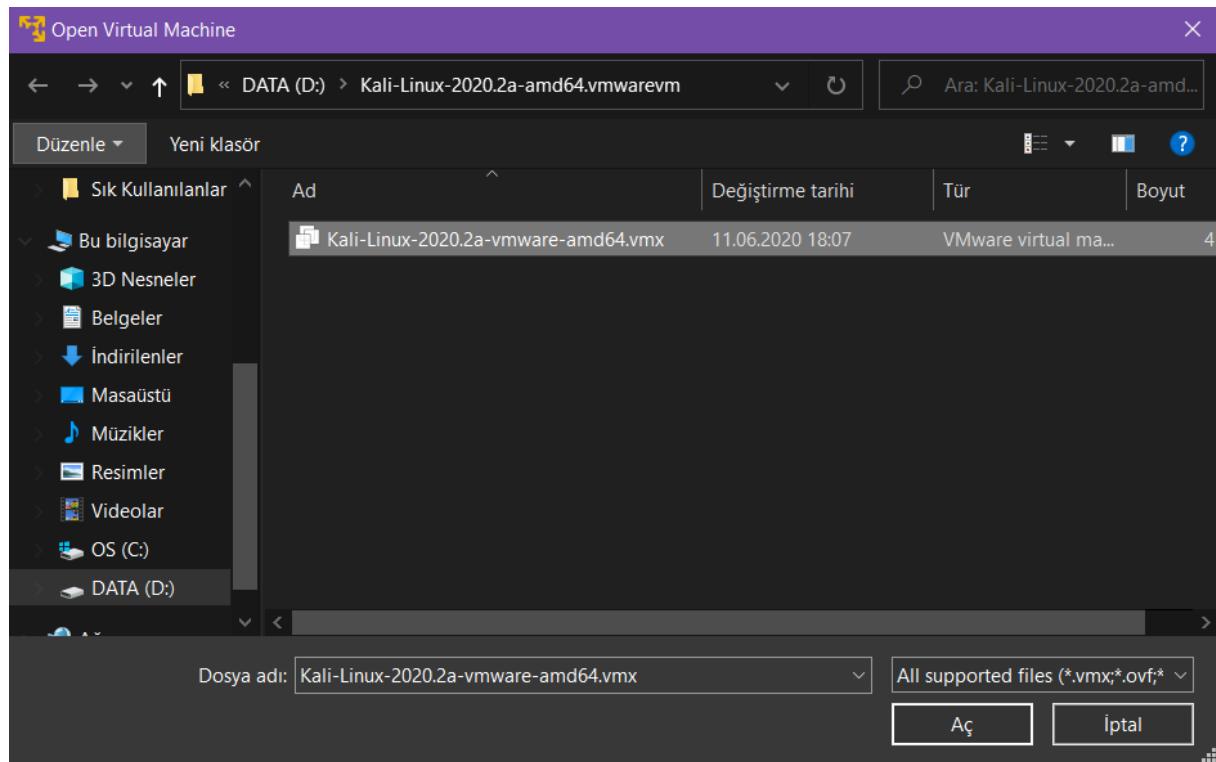
Upgrade to VMware Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.

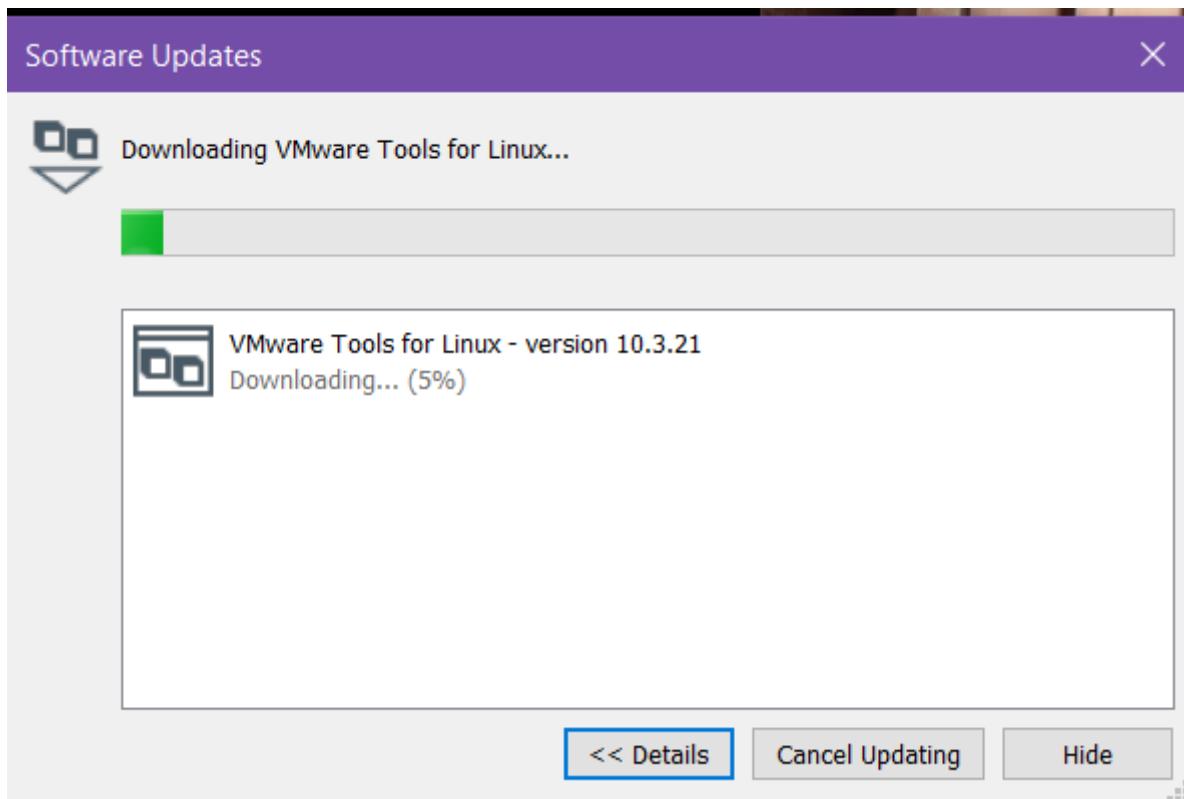
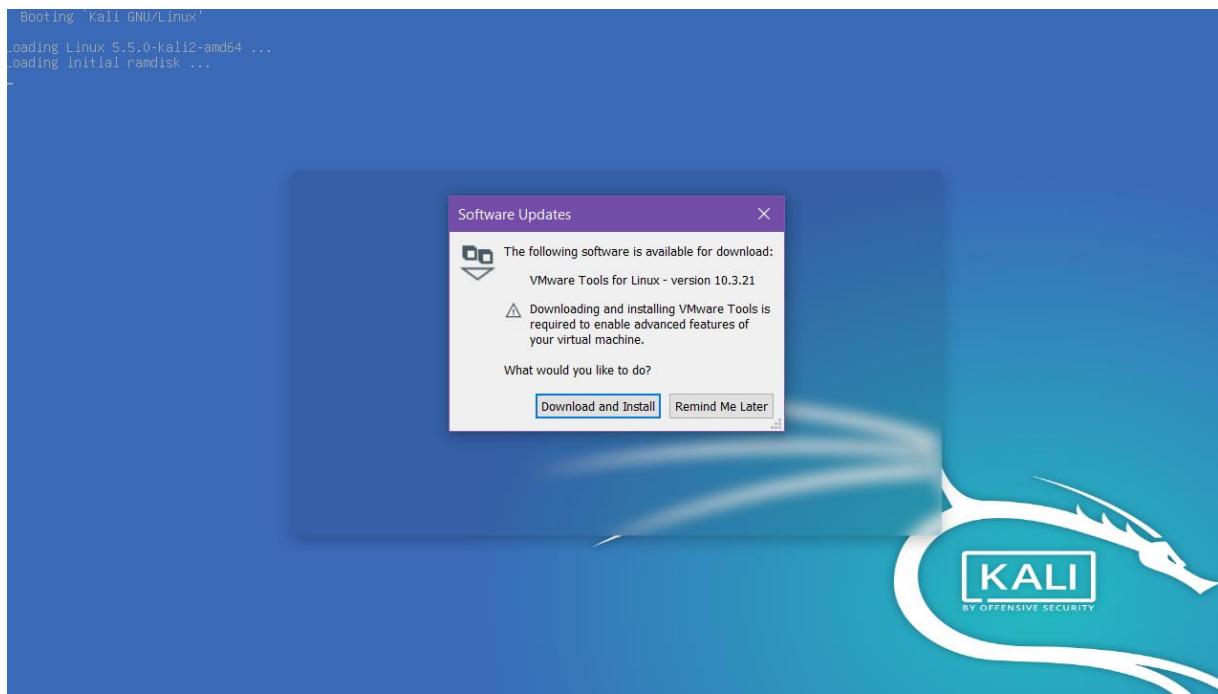


Help

View online help.



```
Booting 'Kali GNU/Linux'  
Loading Linux 5.5.0-kali2-amd64 ...  
Loading initial ramdisk ...
```



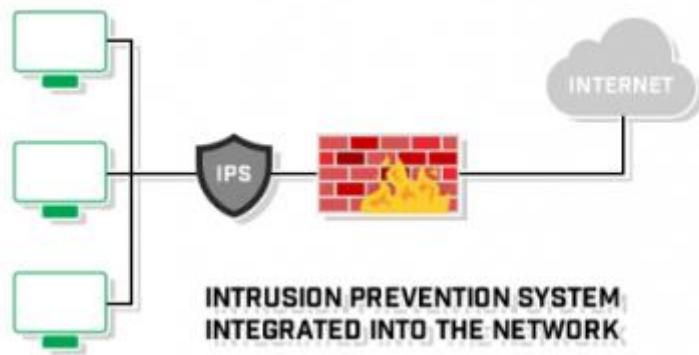
Kali Linux is ready to use.

What is IDS/IPS?

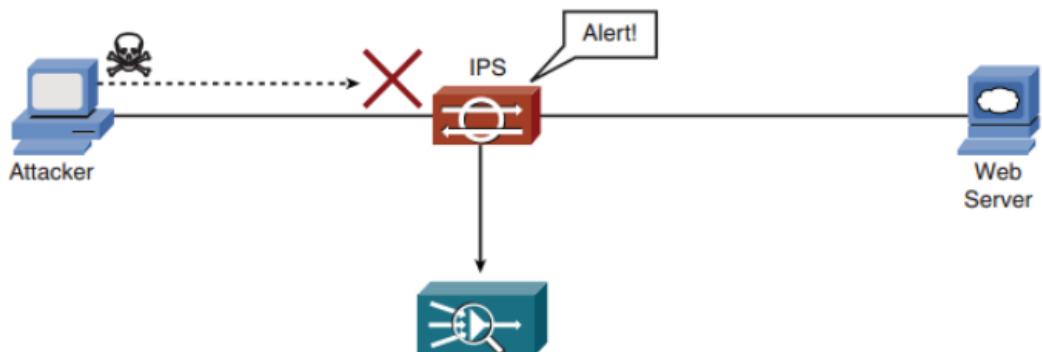
5.1 What is IPS? (Intrusion Prevention System)

It is a network security-threat prevention technology that examines network traffic flows to detect and prevent IPS vulnerability breaches. It provides a complementary layer of analysis that favorably selects dangerous content as negative, reliable content.

IPS is usually located just behind the firewall.

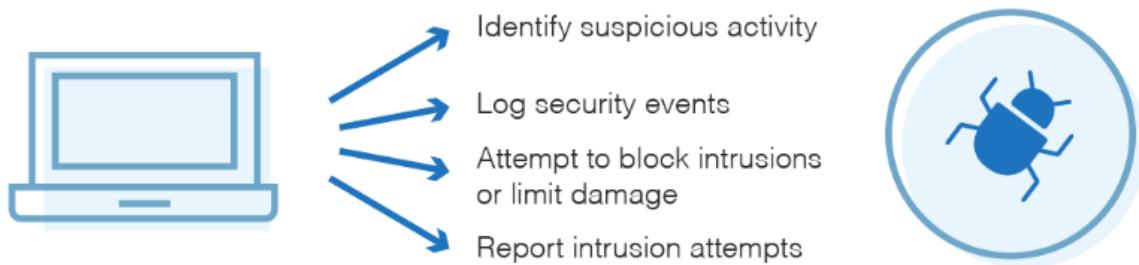


The IPS is placed in the direct communication path between source and destination, packets are actively analyzed and automatic actions are performed.



IPS performs these:

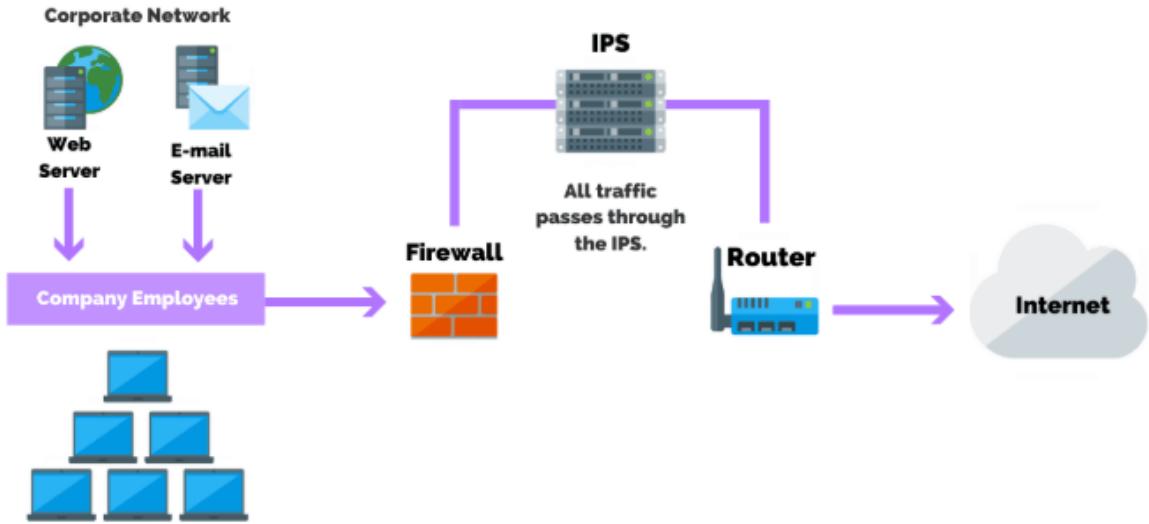
- Send a warning to the administrator in case of an attack
- Dropping malicious packages
- Blocking traffic on the source address
- Resetting the connection
- Correcting CRC errors
- Merge packet flow
- Sorting the incoming segments by looking at the Sequence Number in the TCP layer and notifying any missing segments.



As a security component, IPS must work efficiently to avoid attacks that degrade network performance. It should also work fast because exploits can happen in real time. IPS must accurately detect and respond to eliminate threats and false positives (false detection of trusted packets as threats).

5.2 IPS Classes

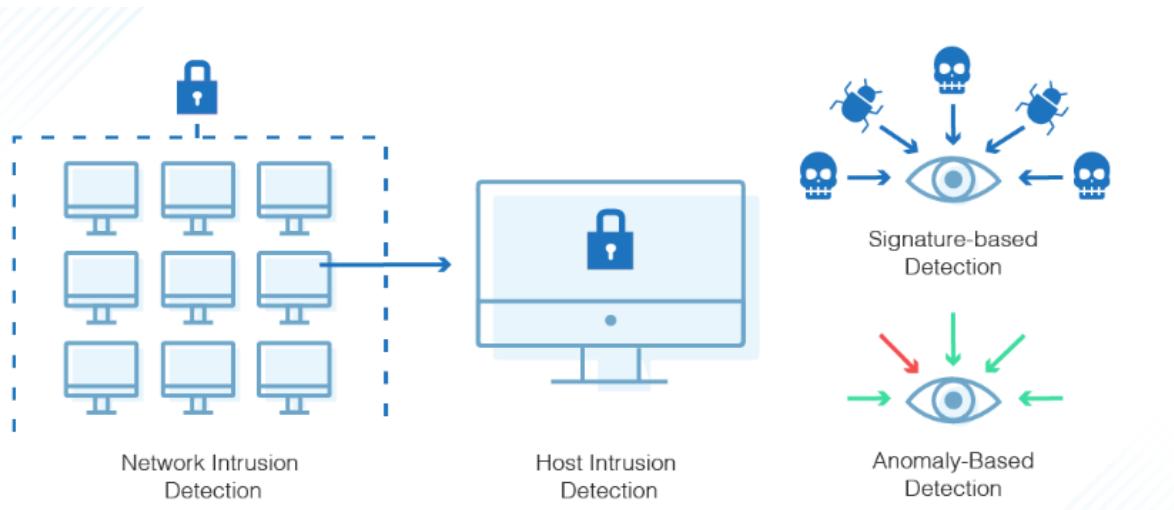
1. **Network-Based Intrusion Prevention (NIPS):** Monitors using the protocol analysis method to detect suspicious situations in the entire network.



2. **Wireless Intrusion Prevention Systems (WIPS)**: Monitors with wireless network protocol to detect suspicious situations on the wireless network.
3. **Network Behavior Analysis (NBA)**: It is used to analyze behaviors in network traffic.
4. **Host-Based Intrusion Prevention (HIPS)**: Used to prevent attacks on the host computer.

5.3 What is IDS? (Instrusion Detection System)

IDS is basically a system configured to monitor and analyze network traffic activity and alert a user / organization to potential vulnerabilities and attacks. IDS like IPS is usually located just behind the firewall.



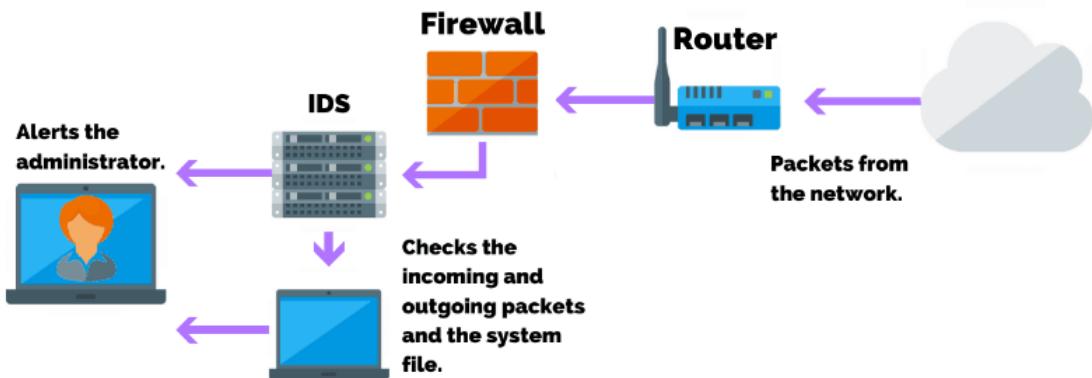
IDS does:

- Detects attacks originating from a program or a person.
- Records attack patterns to continually improve detection logic.
- Provides alerts and reports using a powerful control panel and boost mechanism.
- Records and activates all possible and occurring attacks in the database for future forensic evidence.
- Quarantine the damaged system.
- Ensures data integrity, accessibility and confidentiality.

5.4 IDS Classes

IDS is divided into two categories under security methods for computers and networks:

1. **Network Intrusion Detection Systems (NIDS)** consists of a Network Interface Card (NIC) operating in a different mode and a network device with a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment. Performs traffic passing analysis across the entire subnet and matches traffic passed across subnets to a library of known attacks. Warns when an attack is detected or abnormal behavior is detected.
2. **Host Intrusion Detection Systems (HIDS)** monitors the operating system with the agent on it and writes the data to the log files. HIDS can only monitor individual workstations where agents are installed and cannot monitor the entire network. Often used to monitor any intrusion attempts on critical servers. HIDS is not used much because it is difficult to analyze intrusion attempts on multiple computers. It can be very difficult to maintain in large networks with different operating systems and configurations. Once the system is compromised, it can be disabled by attackers.



IDS is divided into 5 under the title of detection method use:

1. **Signature-Based IDS** is based on searching for "known patterns (signature)" of harmful activities. All he has to do is to search for the list of known attack signatures and if he found a match report, he will do so to the user / institution etc. to report. It is fast simply because it makes a comparison between what it sees and a predetermined rule. On the downside, when a new attack is carried out, it won't be able to protect as it won't match any pattern from its database. Attacks can camouflage themselves by splitting messages. After a new attack is recorded, the data files must be updated before the network is secure.
2. **Anomaly-Based IDS** is based on tracking the unknown unique behavior pattern of malicious activity. It provides protection against a new attack or unknown threats. Network traffic is looked at and compared to identify abnormal and potentially harmful behavior. Negatively, false positives catch a lot because NIDSs follow a system based on behavioral patterns. If the right person uses too many resources or resources, it can be detected as an anomaly and become a signature.
3. **Pattern Matching IDS** searches for a fixed sequence of bytes within a single packet. To filter traffic inspection, the model is usually associated with a specific service and source or destination port. However, many protocols and attacks do not take advantage of well-known ports, and thus Pattern Matching has difficulty detecting such attacks. Also, if the match is based on a non-unique pattern, multiple false-positives can result. Stateful Pattern Matching IDS offers a slightly more sophisticated approach as it takes into account the context of the established session rather than basing its analysis on a single package. It does the template mapping by searching for strings that can be distributed among several packages in a stream.

4. **Protocol Decode-Based Analysis** as a smart extension of Protocol-based signatures Pattern Matching. With this type of signature, IDS searches for protocol violations defined by RFCs and can include pattern matches for a particular field. Although this method is effective in reducing false positives for well-defined protocols, it is easily overlooked by IDS if the protocol is ambiguous or loosely defined.
5. **Heuristic-Based Analysis** uses a heuristic-based signature algorithm to determine whether an alarm should be triggered. An example of this type of analysis and warning would be a signature that generates an alarm if the threshold number of thresholds is scanned on a particular host. Signature can also be restricted to SYN packets from a specific source, such as a perimeter router. While heuristics-based signatures are the only way to detect certain types of attacks, they require tuning and modification to better adapt to unique network environments. However, it uses a lot of memory, CPU and system resources.

5.5 What is Signature?

Signature is a set of rules used by IDS and IPS to detect known attacks and respond with predefined actions.

5.6 Signature Alarms

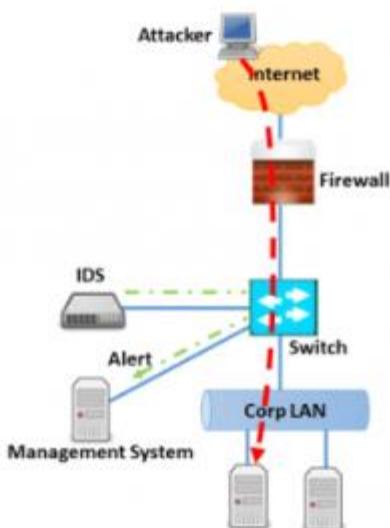
In case of an attack or violation in the system, the response of the system creates the signature type.

- **A false-positive** is an alarm triggered by normal traffic or a positive action.
- **False-negative**, false traffic, etc. It is the alarm that occurs when the situation is detected and a signature is not triggered against it.
- **True-positive** is the alarm that occurs when the signature against the attack is correctly triggered and annoying traffic is detected.
- **True-negative** is an alarm when a false attack is caught and a signature is not taken when analyzed.

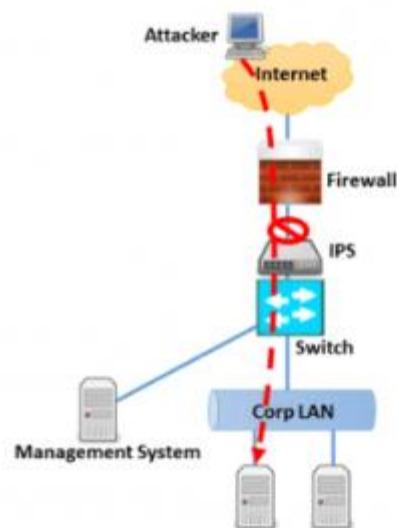
5.7 What are the differences between IPS and IDS?

- **As the system type**, IPS can be active (tracking and self-defense), while IDS is passive. IDS only provides monitoring and notification. (IDS only displays the attack, IPS monitors and prevents the attack.)
- **As detection mechanisms**, IPS detects statistical anomaly-based detection, signature-based detection, the signature facing the exploit and the signature facing the vulnerability, while IDS performs signature-based detection and signature-based detection that looks at the exploit.

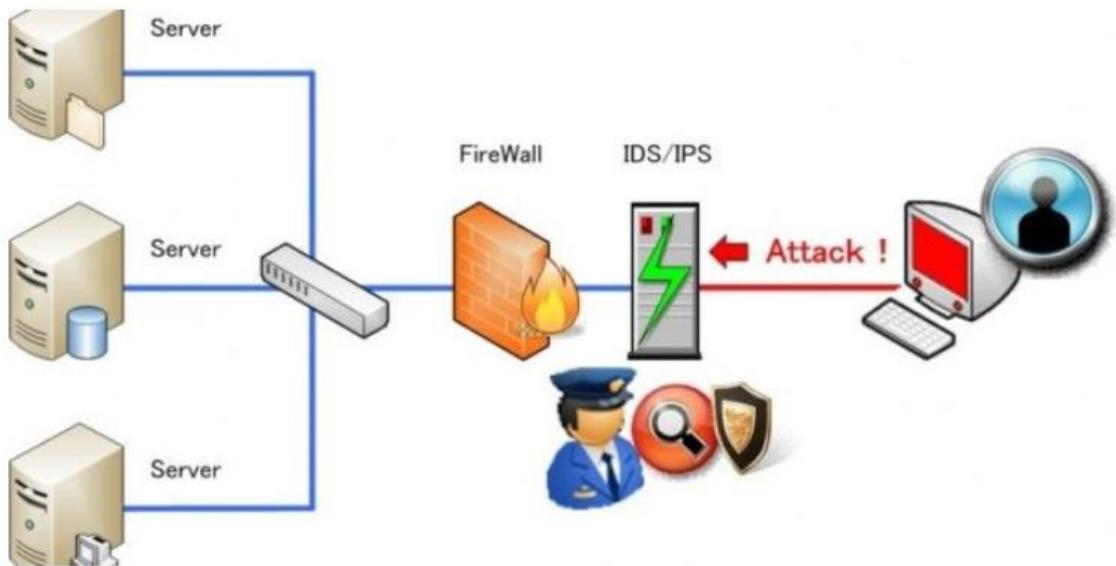
Intrusion Detection System



Intrusion Prevention System



They must be used with IDS and IPS firewalls. In this way, more efficient results are obtained in terms of performance by taking the load through the firewall.



5.8 How to Bypass IDS and IPS?

There are many ways to bypass IPS and IDS systems. One of them is the Packet Fragmentation way. When using this route, we use MTU (Maximum Transfer Unit) operation.

MTU is simply the maximum capacity to enter the network. This value is 1500 bytes in Ethernet networks. For example, when the size of the sent packet is 1800 bytes, the packet is sent by being fragmented as 1500 + 300 and reassembled in the firewall. Packets sent in fragmentation are dangerous for firewall and ips / ids systems. The reason for this is that, for example, if the first packet of a 1500 + 300 byte packet passes through the firewall, the contents of the other packet will not be checked, the packet will be filtered.

CHAPTER 6

What is Suricata?

6.1 What is Suricata?

Suricata is a free and open source, mature, fast and robust network threat detection engine.

The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing.

Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats.

Features:

- Multi-threading
- Automatic protocol detection
- Gzip decompression
- Independent HTTP library
- Standard input methods
- Unified2 output
- Flow variables
- Fast IP matching
- HTTP log module
- JSON standard outputs
- Windows binaries
- Lua scripting
- Prelude output
- file matching, logging, extraction, md5 checksum calculation
- IP reputation
- DNS logger
- VXLAN support since 4.1.5

6.2 What is Suricata used For?

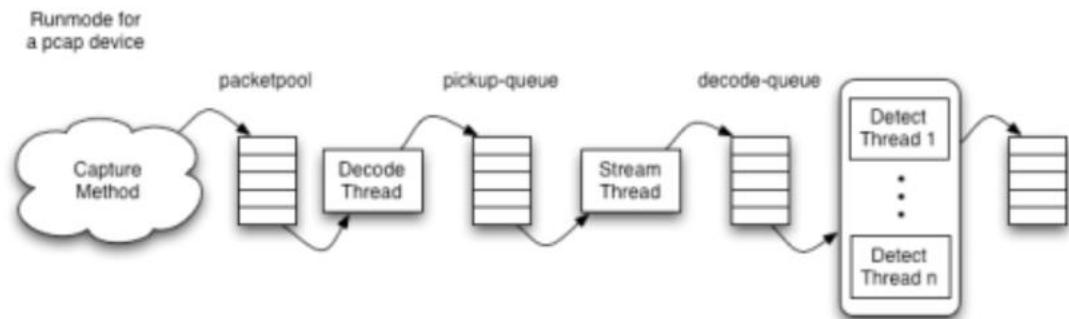
- To set it up as a host-based IDS, which monitors the traffic of an individual computer.
- As a passive IDS, Suricata can monitor all of the traffic through a network and notify the administrator when it comes across anything malicious.
- When Suricata is set up as an active, inline IDS and IPS, it can monitor inbound and outbound traffic. It can stop malicious traffic before it enters the network, as well as alert the administrator.

6.3 Why Choose Suricata?

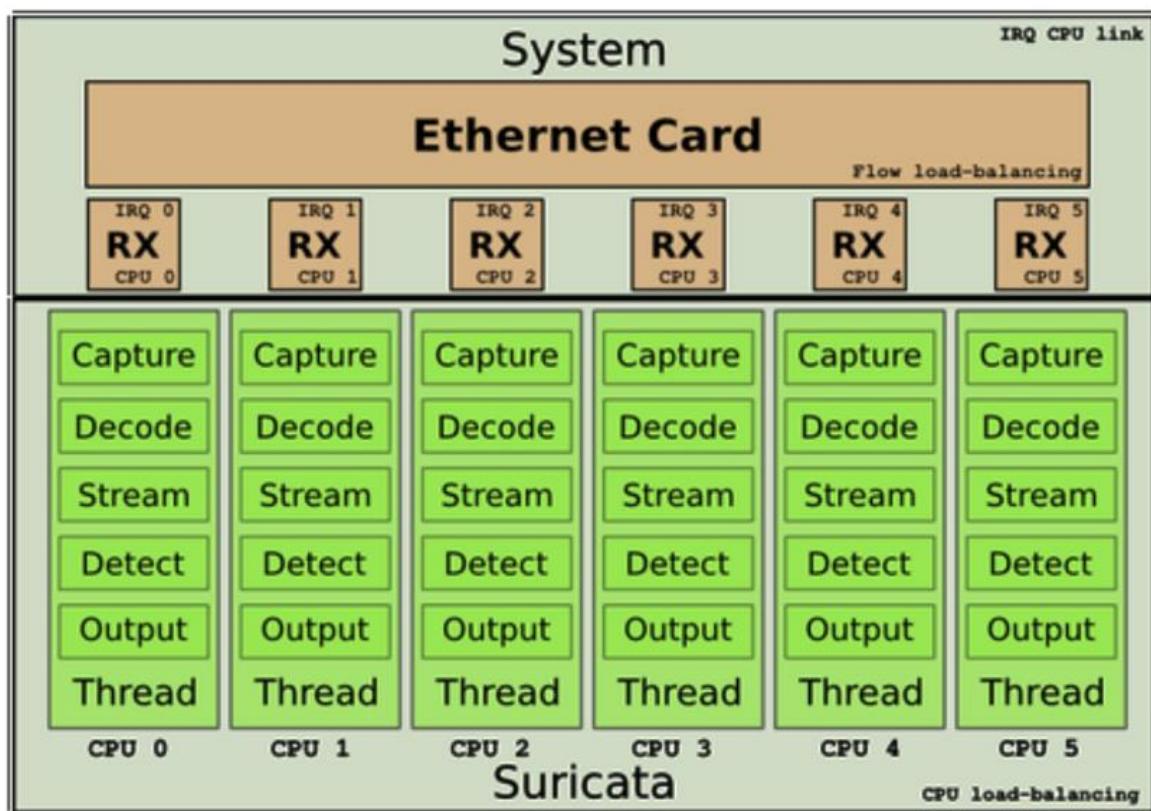
Suricata is a low-cost tool that helps to give greater insight into a network. Despite this, it needs to be viewed as a single layer in a comprehensive security plan, rather than a complete solution to security issues.

Suricata is multi-threaded, which means that it can use multiple cores at once. Engaging multiple CPUs allows Suricata to process multiple events at the same time without having to interrupt other requests. Multi-threading also enables Suricata to load balance across the CPUs, as well as improve overall performance in network traffic analysis.

Structure of suricata working:



Multi-thread suricata:



Suricata works by getting one packet at a time from the system. These are then pre-processed, after which they are passed to the detection engine. Suricata can use pcap for this in IDS mode, but can also connect to a special feature of Linux, named nfnetlink_queue.

Suricata works with rules. These rules can have actions like 'alert', 'log', etc. Suricata IPS introduces three new actions specific to IPS mode, 'drop', 'sdrop' and 'reject'.

CHAPTER 7

Suricata vs Snort

Suricata is a competitor software to Snort.

Snort has been used as an IDS engine for years. Although the suricata may not be that long, it is a modern answer or alternative to Snort with its multi-threading capabilities.

Both engines have proven success records and are popular.

	Snort	Suricata
Developer	Sourcefire, Inc. (now Cisco)	Open Information Security Foundation (OISF)
Availability	Since 1998	Since 2009
Coded Language	C	C
Operating System	Cross-platform	Cross-platform
Threads	Single-threaded	Multi-threaded
IPv6 Support	Yes	Yes
Snort (VRT) Rules	Yes	Yes
Emerging Threats Rules	Yes	Yes
Logging Format	Unified2	Unified2
Aanval Compatible	Yes	Yes

7.1 Differences:

Param	Suricata	Snort
IPS feature	optional while compiling (--enable-nfqueue)	Snort_inline or snort used with -Q option
Rules	<ul style="list-style-type: none"> VRT:Snort rules EmergingThreats rules 	<ul style="list-style-type: none"> VRT:Snort rules SO rules EmergingThreats rules
Threads	Multi-thread	Single-thread
Ease of install	Not available from packages. Manual installation.	Relatively straightforward. Installation also available from packages.
Documentation	Few resources on the Internet	Well documented on the official website and over the Internet
Event logging	Flat file, database, unified2 logs for barnyard	
IPv6 support	Fully supported	Supported when compiled with --enable-ipv6 option.
Capture accelerators	PF_RING, packet capture accelerator	None, use of libpcap
Configuration file	suricata.yaml , classification.config, reference.config, threshold.config	snort.conf, threshold.conf
Offline analysis (pcap file)	yes	
Frontends	Sguil, Aanval, BASE, FPCGUI (Full Packet Capture GUI), Snortsnarf	

7.2 Malware Viruses/ Test Cases

Test	Suricata	Snort
Packed.Generic.187	1	1
W32.Spybot.Worm	-	-
W32.Sality.AE (1)	1	1
W32.Sality.AE (2)	0	0
W32.Sality.AE (3)	-	-
W32.Sality.AE (4)	-	-
Trojan Horse	0	1
Trojan-Spy.Win32.Zbot	1	0
Trojan.Win32.Spyeye	1	1
Generic Trojan Downloader	1	1
Generic IRC Bot	1	1
Win32/SpamTool	1	1
Dropper with BlackEnergy	1	0
Zango Spyware	1	0
TOTAL	9	7

CHAPTER 8

Suricata Installation

https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Installation

Suricata »

Suricata Installation

For basic Suricata installation instructions, please refer to the [installation chapter](#) in the [Suricata User Guide](#).

The following installation guides may be of use if the basic installation instructions don't work for you, or you have a special use case.

On this page you can find installation-guides for several operating systems. Please, feel free to add information.

Supported Platforms

[Ubuntu Installation - Personal Package Archives \(PPA\) \(using a package\)](#)

[Ubuntu Installation \(compilation\)](#)

[Debian Installation](#)

[CentOS Installation - CentOS 7, 6 and Fedora](#)

[RedHat Enterprise Linux 8 from Source](#)

[Fedora Installation](#)

[OpenSuse Installation](#)

[FreeBSD 8, 9 and 10 Installation](#)

[Mac OS X 10.11 w/Homebrew Installation - Should work with 10.10 as well.](#)

[Windows Installation](#)

[https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Windows](#)
or

[https://redmine.openinfosecfoundation.org/attachments/download/1175/SuricataWinInstallationGuide_v1.4.3.pdf](#)

Step 1: Before installing Suricata in the system:

```
apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev \
build-essential autoconf automake libtool libpcap-dev libnet1-dev \
libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libmagic-dev libcap-ng-dev \
libjansson-dev pkg-config rustc cargo
```

```
kali㉿kali:~$ sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package libpcre3-dev is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

E: Unable to locate package libpcre3-dbg
E: Package 'libpcre3-dev' has no installation candidate
```

```
kali㉿kali:~$ sudo apt-get update
0% [Working]
```

```
kali㉿kali:~$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [16.7 MB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [96.4 kB]
Fetched 17.0 MB in 35s (493 kB/s)
Reading package lists... Done
```

```
kali㉿kali:~$ sudo apt-get update --fix-missing
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
```

NOTE : It may be necessary to update before installing the program.

```
kali㉿kali:~$ sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpcre16-3 libpcre32-3 libpcrecpp0v5
The following NEW packages will be installed:
  libpcre16-3 libpcre3-dbg libpcre3-dev libpcre32-3 libpcrecpp0v5
The following packages will be upgraded:
  libpcre3
1 upgraded, 5 newly installed, 0 to remove and 774 not upgraded.
Need to get 3,117 kB of archives.
After this operation, 5,125 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libpcre3 amd64 2:8.39-13 [343 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libpcre16-3 amd64 2:8.39-13 [259 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libpcrecpp0v5 amd64 2:8.39-13 [152 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libpcre3-dbg amd64 2:8.39-13 [1,464 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libpcre32-3 amd64 2:8.39-13 [250 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libpcre3-dev amd64 2:8.39-13 [650 kB]
Fetched 3,117 kB in 23s (137 kB/s)
apt-listchanges: Reading changelogs...
(Reading database ... 269079 files and directories currently installed.)
Preparing to unpack .../libpcre3_2%3a8.39-13_amd64.deb ...
Unpacking libpcre3:amd64 (2:8.39-13) over (2:8.39-12+b1) ...
Setting up libpcre3:amd64 (2:8.39-13) ...
Selecting previously unselected package libpcre16-3:amd64.
(Reading database ... 269078 files and directories currently installed.)
Preparing to unpack .../libpcre16-3_2%3a8.39-13_amd64.deb ...
Unpacking libpcre16-3:amd64 (2:8.39-13) ...
Selecting previously unselected package libpcrecpp0v5:amd64.
Preparing to unpack .../libpcrecpp0v5_2%3a8.39-13_amd64.deb ...
Unpacking libpcrecpp0v5:amd64 (2:8.39-13) ...
Selecting previously unselected package libpcre3-dbg:amd64.
Preparing to unpack .../libpcre3-dbg_2%3a8.39-13_amd64.deb ...
Unpacking libpcre3-dbg:amd64 (2:8.39-13) ...
Selecting previously unselected package libpcre32-3:amd64.
Preparing to unpack .../libpcre32-3_2%3a8.39-13_amd64.deb ...
Unpacking libpcre32-3:amd64 (2:8.39-13) ...
Selecting previously unselected package libpcre3-dev:amd64.
Preparing to unpack .../libpcre3-dev_2%3a8.39-13_amd64.deb ...
Unpacking libpcre3-dev:amd64 (2:8.39-13) ...
Setting up libpcrecpp0v5:amd64 (2:8.39-13) ...
Setting up libpcre16-3:amd64 (2:8.39-13) ...
Setting up libpcre32-3:amd64 (2:8.39-13) ...
Setting up libpcre3-dbg:amd64 (2:8.39-13) ...
Setting up libpcre3-dev:amd64 (2:8.39-13) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for kali-menu (2020.2.2) ...
Processing triggers for libc-bin (2.30-4) ...
```

```
kali㉿kali:~$ sudo apt-get -y install build-essential autoconf automake libtool libp
cap-dev libnet1-dev
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
build-essential is already the newest version (12.8).
The following additional packages will be installed:
  autotools-dev libltdl-dev libpcap0.8-dev m4
Suggested packages:
  autoconf-archive gnu-standards autoconf-doc gettext libtool-doc gfortran
  | fortran95-compiler gcj-jdk m4-doc
The following NEW packages will be installed:
  autoconf automake autotools-dev libltdl-dev libnet1-dev libpcap-dev
  libpcap0.8-dev libtool m4
0 upgraded, 9 newly installed, 0 to remove and 774 not upgraded.
Need to get 2,516 kB of archives.
After this operation, 7,842 kB of additional disk space will be used.
0% [Working]
```

```
kali㉿kali:~$ sudo apt-get -y install libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libma
gic-dev libcap-ng-dev
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
libyaml-0-2 is already the newest version (0.2.2-1).
libyaml-0-2 set to manually installed.
zlib1g is already the newest version (1:1.2.11.dfsg-2).
zlib1g-dev is already the newest version (1:1.2.11.dfsg-2).
zlib1g-dev set to manually installed.
The following additional packages will be installed:
  file libcap-ng0 libmagic-mgc libmagic1
Suggested packages:
  libyaml-doc
The following NEW packages will be installed:
  libcap-ng-dev libyaml-dev
The following packages will be upgraded:
  file libcap-ng0 libmagic-dev libmagic-mgc libmagic1
5 upgraded, 2 newly installed, 0 to remove and 769 not upgraded.
Need to get 684 kB of archives.
After this operation, 332 kB of additional disk space will be used.
0% [Working]
```

```
kali㉿kali:~$ sudo apt-get -y install libjansson-dev pkg-config rustc cargo
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  gdb libbabeltrace1 libboost-regex1.71.0 libc-dev-bin libc6 libc6-dbg libc6-dev
  libc6-i386 libgit2-28 libhttp-parser2.9 libicu67 libipt2 libjansson4
  libmbcrypto3 libmbedtls12 libmbedx509-0 libsourc-highlight-common
  libsourc-highlight4v5 libstd-rust-1.43 libstd-rust-dev rust-gdb
Suggested packages:
  cargo-doc gdb-doc gdbserver glibc-doc rust-doc rust-src lld-9
Recommended packages:
  cargo
The following NEW packages will be installed:
  cargo gdb libbabeltrace1 libboost-regex1.71.0 libc6-dbg libgit2-28
  libhttp-parser2.9 libicu67 libipt2 libjansson-dev libmbcrypto3 libmbedtls12
  libmbedx509-0 libsourc-highlight-common libsourc-highlight4v5 libstd-rust-1.43
  libstd-rust-dev pkg-config rust-gdb rustc
The following packages will be upgraded:
  libc-dev-bin libc6 libc6-dev libc6-i386 libjansson4
5 upgraded, 20 newly installed, 0 to remove and 764 not upgraded.
Need to get 80.3 MB of archives.
After this operation, 249 MB of additional disk space will be used.
0% [Working]
```

```
The following packages will be upgraded:
  libc-dev-bin libc6 libc6-dev libc6-i386 libjansson4
5 upgraded, 20 newly installed, 0 to remove and 764 not upgraded.
Need to get 80.3 MB of archives.
After this operation, 249 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libc6-i386 amd64 2.30-8 [2,9
28 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libc6-dev amd64 2.30-8 [2,63
1 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libc-dev-bin amd64 2.30-8 [2
81 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libc6 amd64 2.30-8 [2,818 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libhttp-parser2.9 amd64 2.9.
2-2 [21.3 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libmbcrypto3 amd64 2.16.5-
1 [214 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libmbedx509-0 amd64 2.16.5-1
[105 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 libmbedtls12 amd64 2.16.5-1
[134 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 libgit2-28 amd64 0.28.5+dfsg
.1-1 [427 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libstd-rust-1.43 amd64 1.43
.0+dfsg1-1 [15.3 MB]
Get:11 http://kali.download/kali kali-rolling/main amd64 libstd-rust-dev amd64 1.43.
0+dfsg1-1 [25.9 MB]
56% [11 libstd-rust-dev 23.7 MB/25.9 MB 91%] 1,155 kB/s 27s
```

Pre-installation requirements is done.

Step 2 : HTP library installation

NOTE : HTP is found in Suricata by default.

```
wget https://github.com/OISF/libhttp/archive/0.5.21.tar.gz  
tar -xzvf libhttp-0.5.21.tar.gz  
cd libhttp-0.5.21  
../configure  
make  
make install
```

```
kali㉿kali:~$ sudo wget https://github.com/OISF/libhttp/archive/0.5.21.tar.gz  
--2020-08-05 07:12:24-- https://github.com/OISF/libhttp/archive/0.5.21.tar.gz  
Resolving github.com (github.com) ... 140.82.118.4  
Connecting to github.com (github.com)|140.82.118.4|:443 ... connected.  
HTTP request sent, awaiting response ... 302 Found  
Location: https://codeload.github.com/OISF/libhttp/tar.gz/0.5.21 [following]  
--2020-08-05 07:12:29-- https://codeload.github.com/OISF/libhttp/tar.gz/0.5.21  
Resolving codeload.github.com (codeload.github.com) ... 140.82.113.10  
Connecting to codeload.github.com (codeload.github.com)|140.82.113.10|:443 ... connected.  
HTTP request sent, awaiting response ... 200 OK  
Length: unspecified [application/x-gzip]  
Saving to: '0.5.21.tar.gz'  
  
0.5.21.tar.gz [=====] 5.50M 1.52MB/s in 3.6s  
  
2020-08-05 07:12:38 (1.52 MB/s) - '0.5.21.tar.gz' saved [5770751]
```

Step 3 : Activate IPS

Suricata runs as IDS by default. To activate it also as IPS:

```
apt-get -y install libnetfilter-queue-dev
```

```
kali㉿kali:~$ sudo apt-get -y install libnetfilter-queue-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libnfnetlink-dev
The following NEW packages will be installed:
  libnetfilter-queue-dev libnfnetlink-dev
0 upgraded, 2 newly installed, 0 to remove and 764 not upgraded.
Need to get 14.7 kB of archives.
After this operation, 64.5 kB of additional disk space will be used.
0% [Working]
```

Step 4: Compile and install the program

```
 wget http://www.openinfosecfoundation.org/download/suricata-5.0.0.tar.gz
 tar -xvzf suricata-5.0.0.tar.gz
 cd suricata-5.0.0
```

```
kali㉿kali:~$ sudo wget http://www.openinfosecfoundation.org/download/suricata-5.0.0.tar.gz
--2020-08-05 08:48:48--  http://www.openinfosecfoundation.org/download/suricata-5.0.0.tar.gz
Resolving www.openinfosecfoundation.org (www.openinfosecfoundation.org)... 52.14.249.179, 2600:1f16:db2:4f00:da9d:37d6:e8b9:9802
Connecting to www.openinfosecfoundation.org (www.openinfosecfoundation.org)|52.14.249.179|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://openinfosecfoundation.org/download/suricata-5.0.0.tar.gz [following]
--2020-08-05 08:48:49--  https://openinfosecfoundation.org/download/suricata-5.0.0.tar.gz
Resolving openinfosecfoundation.org (openinfosecfoundation.org) ... 52.14.249.179, 2600:1f16:db2:4f00:da9d:37d6:e8b9:9802
Connecting to openinfosecfoundation.org (openinfosecfoundation.org)|52.14.249.179|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23689051 (23M) [application/x-gzip]
Saving to: 'suricata-5.0.0.tar.gz'

suricata-5.0.0.tar.g 5%[>] 1.23M 420KB/s
```

```
kali㉿kali:~$ sudo tar -xvzf suricata-5.0.0.tar.gz
```

```
./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var
```

```
kali㉿kali:~/suricata-5.0.0$ cd suricata-5.0.0
kali㉿kali:~/suricata-5.0.0$ sudo ./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var
checking whether make supports nested variables ... yes
checking for a BSD-compatible install ... /usr/bin/install -c
checking whether build environment is sane ... yes
checking for a thread-safe mkdir -p ... /usr/bin/mkdir -p
checking for gawk ... gawk
```

```
File Actions Edit View Help
kali@kali:~/suricata-5.0.0

checking for nfq_set_queue_maxlen in -lnetfilter_queue ... yes
checking for nfq_set_verdict2 in -lnetfilter_queue ... yes
checking for nfq_set_queue_flags in -lnetfilter_queue ... yes
checking for nfq_set_verdict_batch in -lnetfilter_queue ... yes
checking for signed nfq_get_payload payload argument ... no
checking whether OS_WIN32 is declared ... no
checking for libnet.h version 1.1.x ... yes
checking for libnet_write in -lnet ... yes
checking for libnet_build_icmpv6_unreach in -lnet ... yes
checking libnet_init dev type ... yes
checking pcap.h usability ... yes
checking pcap.h presence ... yes
checking for pcap.h ... yes
checking for pcap.h ... (cached) yes
checking pcap/pcap.h usability ... yes
checking pcap/pcap.h presence ... yes
checking for pcap/pcap.h ... yes
checking pcap/bpf.h usability ... yes
checking pcap/bpf.h presence ... yes
checking for pcap/bpf.h ... yes
checking for PCAP ... yes
checking for pcap_open_live in -lpcap ... yes
checking for pcap_activate in -lpcap ... yes
checking for pcap-config ... /usr/bin/pcap-config
checking for pcap_set_buffer_size in -lpcap ... yes
checking whether TPACKET_V2 is declared ... yes
checking whether TPACKET_FANOUT_QM is declared ... yes
checking whether TPACKET_V3 is declared ... yes
checking whether SOF_TIMESTAMPING_RAW_HARDWARE is declared ... yes
checking for ./suricata-update/setup.py ... yes
checking that generated files are newer than configure... done
configure: creating ./config.status
config.status: creating suricata-update/Makefile
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing libtool commands
checking iconv.h usability ... yes
checking iconv.h presence ... yes
checking for iconv.h ... yes
checking for libiconv_close in -liconv ... no
checking cap-ng.h usability ... yes
checking cap-ng.h presence... yes
checking for cap-ng.h ... yes
checking for capng_clear in -lcap-ng ... yes
checking for libnspr ... no
checking nspr.h usability ... no
checking nspr.h presence ... no
checking for nspr.h ... no
```

```
Suricata Configuration:
AF_PACKET support: yes
eBPF support: no
XDP support: no
PF_RING support: no
NFQueue support: yes
NFLOG support: no
IPFW support: no
Netmap support: no
DAG enabled: no
Napatech enabled: no
WinDivert enabled: no

Unix socket enabled: yes
Detection enabled: yes

Libmagic support: yes
libnss support: yes
libnspr support: yes
libjansson support: yes
hiredis support: no
hiredis async with libevent: no
Prelude support: no
PCRE jit: yes
LUA support: no
libluajit: no
GeoIP2 support: no
Non-bundled http: no
Old barnyard2 support: no
Hyperscan support: no
Libnet support: yes
liblz4 support: yes

Rust support: yes
Rust strict mode: no
```

```

Rust support: yes
Rust strict mode: no
Rust compiler path: /usr/bin/rustc
Rust compiler version: rustc 1.43.0
Cargo path: /usr/bin/cargo
Cargo version: cargo 1.42.1

Python support: yes
Python path: /usr/bin/python3
Python distutils: yes
Python yaml: yes
Install suricatactl: yes
Install suricatasc: yes
Install suricata-update: yes

Profiling enabled: no
Profiling locks enabled: no

Development settings:
Coccinelle / spatch: no
Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no

Generic build parameters:
Installation prefix: /usr
Configuration directory: /etc/suricata/
Log directory: /var/log/suricata/

--prefix /usr
--sysconfdir /etc
--localstatedir /var
--datarootdir /usr/share

Host: x86_64-pc-linux-gnu
Compiler: gcc (exec name) / gcc (real)
GCC Protect enabled: no
GCC march native enabled: yes

```

```

GCC Profile enabled: no
Position Independent Executable enabled: no
CFLAGS -g -O2 -march=native -I${srcdir}/../rust/
gen/c-headers
PCAP_CFLAGS
SECCFLAGS -I/usr/include

```

```

./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
make
make install

```

```
kali㉿kali:~/suricata-5.0.0$ sudo ./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
```

```
kali㉿kali:~/suricata-5.0.0$ sudo make
make all-recurse
make[1]: Entering directory '/home/kali/suricata-5.0.0'
Making all in libhttp
make[2]: Entering directory '/home/kali/suricata-5.0.0/libhttp'
make all-recurse
make[3]: Entering directory '/home/kali/suricata-5.0.0/libhttp'
Making all in http
make[4]: Entering directory '/home/kali/suricata-5.0.0/libhttp/http'
Making all in lzma
make[5]: Entering directory '/home/kali/suricata-5.0.0/libhttp/http/lzma'
/bin/bash ..../libtool --tag=CC --mode=compile gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT LzFind.lo -MD -MP -MF .deps/LzFind.Tpo -c -o LzFind.lo LzFind.c
```

```
mv -f .deps/htp_request_apache_2_27.Tpo .deps/htp_request_apache_2_27.Plo
/bin/bash ..../libtool --tag=CC --mode=compile gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_request_generic.lo -MD -MP -MF .deps/htp_request_generic.Tpo -c htp_request_generic.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_request_generic.lo -MD -MP -MF .deps/htp_request_generic.Tpo -c htp_request_generic.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_request_generic.lo -MD -MP -MF .deps/htp_request_generic.Tpo -c htp_request_generic.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_request_generic.lo -MD -MP -MF .deps/htp_request_generic.Tpo -c htp_request_generic.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_request_parsers.lo -MD -MP -MF .deps/htp_request_parsers.Tpo -c htp_request_parsers.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_request_parsers.lo -MD -MP -MF .deps/htp_request_parsers.Tpo -c htp_request_parsers.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_request_parsers.lo -MD -MP -MF .deps/htp_request_parsers.Tpo -c htp_request_parsers.c
libtool: compile: gcc -DHAVE_CONFIG_H -I. -I.. -O2 -I.. -I.. /htp -D_GNU_SOURCE -g -Wall -Wextra -std=gnu99 -pedantic -Wextra -Wno-missing-field-initializers -Wshadow -Wpointer-arith -Wstrict-prototypes -Wmissing-prototypes -Wno-unused-parameter -O2 -Wstrict-overflow=1 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security -fPIC -MT htp_response.lo -MD -MP -MF .deps/htp_response.T
```

```
Compiling autocfg v0.1.6
Compiling rand_core v0.4.2
Compiling version_check v0.1.5
Compiling memchr v2.2.1
Compiling libc v0.2.62
Compiling siphasher v0.2.3
Compiling proc-macro2 v0.4.30
Compiling unicode-xid v0.1.0
Compiling byteorder v1.3.2
Compiling build_const v0.2.1
Compiling syn v0.15.44
Compiling num-derive v0.2.5
Compiling bitflags v1.2.1
Compiling cookie-factory v0.2.4
Compiling widestring v0.4.0
Compiling rand_core v0.3.1
Compiling rand_jitter v0.1.4
Compiling phf_shared v0.7.24
Compiling num-traits v0.2.8
Compiling num-integer v0.1.41
Compiling rand_chacha v0.1.1
Compiling num-bigint v0.2.3
Compiling rand_pcg v0.1.2
Compiling rand v0.6.5
Compiling num-complex v0.2.3
Compiling num-rational v0.2.2
Compiling num-iter v0.1.39
Compiling nom v4.2.3
Compiling crc v1.8.1
Compiling rand_isaac v0.1.1
Compiling rand_hc v0.1.0
Compiling rand_xorshift v0.1.1
Compiling phf v0.7.24
Compiling rand_os v0.1.3
Compiling time v0.1.42
Compiling base64 v0.10.1
Compiling quote v0.6.13
```

```
Compiling num-traits v0.1.43
Compiling rusticata-macros v1.1.0
Compiling ntp-parser v0.3.0
Compiling enum_primitive v0.1.1
Compiling ipsec-parser v0.4.1
Compiling phf_generator v0.7.24
Compiling der-parser v1.1.1
Compiling phf_codegen v0.7.24
Compiling snmp-parser v0.3.0
Compiling x509-parser v0.4.3
Compiling kerberos-parser v0.2.0
Compiling num v0.2.0
Compiling tls-parser v0.8.1
Building [=====>] 87/89: num-derive
```

```
Finished release [optimized + debuginfo] target(s) in 2m 50s
make[2]: Leaving directory '/home/kali/suricata-5.0.0/rust'
Making all in src
make[2]: Entering directory '/home/kali/suricata-5.0.0/src'
CC      alert-debuglog.o
CC      alert-fastlog.o
CC      alert-prelude.o
CC      alert-syslog.o
CC      alert-unified2-alert.o
CC      app-layer.o
CC      app-layer-dcerpc.o
CC      app-layer-dcerpc-udp.o
CC      app-layer-detect-proto.o
CC      app-layer-dnp3.o
```

```
CC      ippair.o
CC      ippair-bit.o
CC      ippair-queue.o
CC      ippair-storage.o
CC      ippair-timeout.o
CC      log-droplog.o
CC      log-filestore.o
CC      log-cf-common.o
CC      log-httplog.o
CC      log-pcap.o
CC      log-stats.o
CC      log-tcp-data.o
CC      log-tlslog.o
CC      log-tlsstore.o
CC      output.o
CC      output-file.o
CC      output-filedata.o
CC      output-filestore.o
CC      output-flow.o
CC      output-json-alert.o
CC      output-json-anomaly.o
CC      output-json-dns.o
CC      output-json-dnp3.o
CC      output-json-dnp3-objects.o
CC      output-json-drop.o
CC      output-json-email-common.o
CC      output-json-file.o
CC      output-json-flow.o
CC      output-json-ftp.o
CC      output-json-netflow.o
CC      output-json-http.o
CC      output-json-sip.o
CC      output-json-smtp.o
CC      output-json-ssh.o
CC      output-json-stats.o
CC      output-json-tls.o
CC      output-json-nfs.o
CC      output-json-tftp.o
CC      output-json-smb.o
CC      output-json-ikev2.o
CC      output-json-krb5.o
CC      output-json-dhcp.o
CC      output-json-snmp.o
```

```
copying suricata/update/loghandler.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update
copying suricata/update/sources.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update
creating /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/removesource.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/addsource.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/__init__.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/listsources.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/enablesource.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/disablesource.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/checkversions.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/listenablesources.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
copying suricata/update/commands/updatesources.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/commands
creating /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/configs
copying suricata/update/configs/__init__.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/configs
creating /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/compat
copying suricata/update/compat/__init__.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/compat
copying suricata/update/compat/ordereddict.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/compat
creating /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/compat/argparse
copying suricata/update/compat/argparse/__init__.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/compat/argparse
copying suricata/update/compat/argparse/argparse.py → /home/kali/suricata-5.0.0/suricata-update/lib/suricata/update/compat/argparse
```

```
kali@kali:~/suricata-5.0.0$ sudo make install
```

```
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/commands/updatesources.py to update
sources.cpython-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/net.py to net.cpython-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/util.py to util.cpython-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/main.py to main.cpython-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/engine.py to engine.cpython-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/rule.py to rule.cpython-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/config.py to config.cpython-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/exceptions.py to exceptions.cpython
-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/loghandler.py to loghandler.cpython
-38.pyc
byte-compiling /usr/lib/python3.8/site-packages/suricata/update/sources.py to sources.cpython-38.py
c
running install_scripts
copying /home/kali/suricata-5.0.0/suricata-update/scripts-3.8/suricata-update → /usr/bin
changing mode of /usr/bin/suricata-update to 755
running install_egg_info
Writing /usr/lib/python3.8/site-packages/suricata_update-1.1.0-py3.8.egg-info
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/kali/suricata-5.0.0/suricata-update'
make[1]: Leaving directory '/home/kali/suricata-5.0.0/suricata-update'
make[1]: Entering directory '/home/kali/suricata-5.0.0'
make[2]: Entering directory '/home/kali/suricata-5.0.0'
make[2]: Nothing to be done for 'install-exec-am'.
Run 'make install-conf' if you want to install initial configuration files. Or 'make install-full'
to install configuration and rules
```

To make sure the existing list with libraries will be updated with the new library.

```
kali@kali:~/suricata-5.0.0$ sudo ldconfig
```

Installation is done.

Step 5 : Setup

```
kali@kali:~/suricata-5.0.0$ sudo chmod 777 configure
kali@kali:~/suricata-5.0.0$ sudo ./configure && make && make install-full
checking whether make supports nested variables ... yes
checking for a BSD-compatible install ... /usr/bin/install -c
checking whether build environment is sane ... yes
checking for a thread-safe mkdir -p ... /usr/bin/mkdir -p
checking for gawk ... gawk
checking whether make sets $(MAKE) ... yes
checking whether UID '0' is supported by ustar format ... yes
checking whether GID '0' is supported by ustar format ... yes
checking how to create a ustar tar archive ... gnutar
checking for style of include used by make ... GNU
checking for gcc ... gcc
```

```
kali@kali:~/suricata-5.0.0$ sudo ./configure && make && make install-full
checking whether make supports nested variables ... yes
checking for a BSD-compatible install ... /usr/bin/install -c
checking whether build environment is sane ... yes
checking for a thread-safe mkdir -p ... /usr/bin/mkdir -p
checking for gawk ... gawk
checking whether make sets $(MAKE) ... yes
checking whether UID '0' is supported by ustar format ... yes
checking whether GID '0' is supported by ustar format ... yes
checking how to create a ustar tar archive ... gnutar
checking for style of include used by make ... GNU
checking for gcc ... gcc
```

```
kali@kali:~/suricata-5.0.0$ sudo mkdir /var/log/suricata
```

```
kali@kali:~/suricata-5.0.0$ sudo mkdir /etc/suricata
```

```
kali@kali:~/suricata-5.0.0/etc$ sudo cp classification.config /etc/suricata
kali@kali:~/suricata-5.0.0/etc$ sudo cp reference.config /etc/suricata
kali@kali:~/suricata-5.0.0/etc$ sudo cp suricata.yaml /etc/suricata
```

```
kali@kali:~/suricata-5.0.0/etc$ sudo cp suricata.yaml /etc/suricata
cp: cannot stat 'suricata.yaml': No such file or directory
```

```
kali@kali:~$ cd suricata-5.0.0
kali@kali:~/suricata-5.0.0$ sudo cp suricata.yaml /etc/suricata
```

```
kali@kali:~$ sudo suricata-update
[sudo] password for kali:
5/8/2020 -- 09:57:24 - <Info> -- Using data-directory /var/lib/suricata.
5/8/2020 -- 09:57:24 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
5/8/2020 -- 09:57:24 - <Info> -- Found Suricata version 5.0.0 at /usr/bin/suricata.
5/8/2020 -- 09:57:24 - <Info> -- No sources configured, will use Emerging Threats Open
5/8/2020 -- 09:57:24 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-5.0.0/emerging.rules.tar.gz.
100% - 2676155/2676155
```

```
5/8/2020 -- 09:57:40 - <Error> -- [ERRCODE: SC_ERR_FATAL(171)] - failed to open file: /etc/suricata
//suricata.yaml: No such file or directory
```

File not found, we created the file.

```
kali㉿kali:~$ sudo vim /etc/suricata/suricata.yaml
```

Step 6 : Configuration

suricata.yaml file:

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"45
    #HOME_NET: "[172.16.0.0/12]"45
    #HOME_NET: "any"

    #EXTERNAL_NET: "!"45
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"45
    SQL_SERVERS: "$HOME_NET"45
    DNS_SERVERS: "$HOME_NET"45
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

    FILE_LIST_PORTS: "[${HTTP_PORTS},110,143]"
```

```
# EXTERNAL_NET: "!$HOME_NET"
EXTERNAL_NET: "any"
HTTP_SERVERS: "$85.153.224.45"
SMTP_SERVERS: "$85.153.224.45"
SQL_SERVERS: "$85.153.224.45"
DNS_SERVERS: "$85.153.224.45"
TELNET_SERVERS: "$85.153.224.45"
AIM_SERVERS: any
```

port group should be like this.

```
port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNS_PORTS: 53, 108, 135, 389, 43, 45, 5353, 20000
```

```
host-os-policy:
    # Make the default policy windows.
    windows: [0.0.0.0/0]
    bsd: []
    bsd-right: []
    old-linux: []
    linux: []
    old-solaris: []
    solaris: []
    hpx10: []
    hpx11: []
    irix: []
    macos: []
    vista: []
    windows2k3: []
```

```
host-os-policy:
    # Make the default policy windows.
    windows: [0.0.0.0/0]
    bsd: []
    bsd-right: []
    old-linux: []
    linux: [10.0.0.0/8, 192.168.1.100, "8762:2352:6241:7245:E000:0000:0000:0000"]
    old-solaris: []
    solaris: ["::1"]
    hpx10: []
    hpx11: []
    irix: []
    macos: []
    vista: []
    windows2k3: []
```

Step 7 : Rule set management and download

Rule management with oinkmaster

```
kali㉿kali:~$ sudo apt-get install oinkmaster
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following NEW packages will be installed:
  oinkmaster
0 upgraded, 1 newly installed, 0 to remove and 764 not upgraded.
Need to get 90.6 kB of archives.
After this operation, 287 kB of additional disk space will be used.
0% [Working]
```

```
kali㉿kali:~$ sudo nano /etc/oinkmaster.conf
```

```
url = http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
```

```
kali㉿kali:~$ sudo mkdir /etc/suricata/rules
kali㉿kali:~$ cd /etc
kali㉿kali:/etc$
```

```
kali㉿kali:/etc$ sudo oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules
Loading /etc/oinkmaster.conf
Downloading file from http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz ...
```

The suricata.yaml file should be like this:

```
rule-files:
  - suricata.rules

##
## Auxiliary configuration files.
##

classification-file: /usr/local/etc/suricata/classification.config
reference-config-file: /usr/local/etc/suricata/reference.config
# threshold-file: /usr/local/etc/suricata/threshold.config

##
## Include other configs
##
```

Disabling some of the Rules files

```
emerging-exploit.rules      emerging-sniffcode.rules  
kali@kali:/etc/suricata/rules$ sudo nano /etc/oinkmaster.conf  
kali@kali:/etc/suricata/rules$
```

```
disablesid 2010495
```

Activation:

```
enablesid: 2010495
```

Update Rules

Should do it often.

It is recommended to update your rules frequently. Emerging Threats is modified daily, VRT is updated weekly or multiple times a week.

```
kali@kali:/etc/suricata/rules$ sudo oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules  
Loading /etc/oinkmaster.conf
```

Error:

suricata.service could not be found error.

Download suricata.service file from github.

And you put /etc/systemd/system/ OR /usr/lib/systemd/system/

Problem is solved.

```
kali㉿kali:/etc/systemd/system$ nano suricata.service
kali㉿kali:/etc/systemd/system$ sudo nano suricata.service
kali㉿kali:/etc/systemd/system$ ls
dbus-org.freedesktop.ModemManager1.service    samba-ad-dc.service
dbus-org.freedesktop.nm-dispatcher.service    smartd.service
default.target.wants                          sockets.target.wants
display-manager.service                      suricata.service
getty.target.wants                           sysinit.target.wants
iodined.service                            syslog.service
multi-user.target.wants                     timers.target.wants
network-online.target.wants                 vmtoolsd.service
remote-fs.target.wants
kali㉿kali:/etc/systemd/system$ sudo systemctl daemon-reload
kali㉿kali:/etc/systemd/system$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
  Loaded: loaded (/etc/systemd/system/suricata.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:suricata(8)
          man:suricatasc(8)
          https://redmine.openinfosecfoundation.org/projects/suricata/wiki
Aug 08 08:15:07 kali systemd[1]: /etc/systemd/system/suricata.service:13: PIDFile= reference
[lines 1-8/8 (END)]
```

```
kali㉿kali:~$ sudo nano /etc/suricata/suricata.yaml
```

```

af-packet:
- interface: eth0
# Number of receive threads. "auto" uses the number of cores
#threads: auto
# Default clusterid. AF_PACKET will load balance packets based on flow.
cluster-id: 99
# Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
# This is only supported for Linux kernel > 3.1
# possible value are:
# * cluster_flow: all packets of a given flow are send to the same socket
# * cluster_cpu: all packets treated in kernel by a CPU are send to the same socket
# * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
#   socket. Requires at least Linux 3.14.
# * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.
rst for
# more info.
# Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on syste
m
# with capture card using RSS (require cpu affinity tuning and system irq tuning)
cluster-type: cluster_flow
# In some fragmentation case, the hash can not be computed. If "defrag" is set
# to yes, the kernel will do the needed defragmentation before sending the packets.
defrag: yes
# To use the ring feature of AF_PACKET, set 'use-mmap' to yes
use-mmap: yes
# Lock memory map to avoid it goes to swap. Be careful that over subscribing could lock
# your system
#mmap-locked: yes
# Use tpacket_v3 capture mode, only active if use-mmap is true
# Don't use it in IPS or TAP mode as it causes severe latency
tpacket-v3: yes
# Ring size will be computed with respect to max_pending_packets and number
# of threads. You can set manually the ring size in number of packets by setting

```

```

af-packet:
- interface: enpls0
# Number of receive threads. "auto" uses the number of cores
#threads: auto
# Default clusterid. AF_PACKET will load balance packets based on flow.
cluster-id: 99
# Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
# This is only supported for Linux kernel > 3.1
# possible value are:
# * cluster_flow: all packets of a given flow are send to the same socket
# * cluster_cpu: all packets treated in kernel by a CPU are send to the same socket
# * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
#   socket. Requires at least Linux 3.14.
# * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.
rst for
# more info.
# Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on syste
m
# with capture card using RSS (require cpu affinity tuning and system irq tuning)
cluster-type: cluster_flow
# In some fragmentation case, the hash can not be computed. If "defrag" is set
# to yes, the kernel will do the needed defragmentation before sending the packets.
defrag: yes
# To use the ring feature of AF_PACKET, set 'use-mmap' to yes
use-mmap: yes
# Lock memory map to avoid it goes to swap. Be careful that over subscribing could lock
# your system
#mmap-locked: yes
# Use tpacket_v3 capture mode, only active if use-mmap is true
# Don't use it in IPS or TAP mode as it causes severe latency
tpacket-v3: yes
# Ring size will be computed with respect to max_pending_packets and number
# of threads. You can set manually the ring size in number of packets by setting

```

this will be changed.

```
root@kali:~# systemctl restart suricata
```

Suricata can run properly and thus we restart it:

To make sure Suricata is running check the Suricata log:

```
root@kali:~# tail /var/log/suricata/suricata.log
8/8/2020 -- 08:50:42 - <Info> - Threshold config parsed: 0 rule(s) found
8/8/2020 -- 08:50:42 - <Info> - 0 signatures processed. 0 are IP-only rules, 0 are inspecting
  packet payload, 0 inspect application layer, 0 are decoder event only
8/8/2020 -- 08:50:42 - <Info> - binding this thread 0 to queue '0'
8/8/2020 -- 08:50:42 - <Info> - setting queue length to 4096
8/8/2020 -- 08:50:42 - <Info> - setting nfnl bufsize to 6144000
8/8/2020 -- 08:50:42 - <Info> - binding this thread 1 to queue '1'
8/8/2020 -- 08:50:42 - <Info> - setting queue length to 4096
8/8/2020 -- 08:50:42 - <Info> - setting nfnl bufsize to 6144000
8/8/2020 -- 08:50:42 - <Info> - Using unix socket file '/var/run/suricata-command.socket'
8/8/2020 -- 08:50:42 - <Notice> - all 8 packet processing threads, 4 management threads initialized, engine started.
```

The amount of threads depends on the system and the configuration. To see statistics the stats.log can be checked: Every 20 seconds by default it will show updated informations about the current state, like how many packets have been processed and what type of traffic was decoded.

```

root@kali:~# tail -f /var/log/suricata/stats.log
Date: 8/8/2020 -- 08:54:50 (uptime: 0d, 00h 04m 08s)
-----
Counter | TM Name | Value
-----
flow.spare | Total | 10000
flow_mgr.rows_checked | Total | 65536
flow_mgr.rows_skipped | Total | 65536
tcp.memuse | Total | 2293760
tcp.reassembly_memuse | Total | 393216
flow.memuse | Total | 7554304
-----
Date: 8/8/2020 -- 08:54:58 (uptime: 0d, 00h 04m 16s)
-----
Counter | TM Name | Value
-----
flow.spare | Total | 10000
flow_mgr.rows_checked | Total | 65536
flow_mgr.rows_skipped | Total | 65536
tcp.memuse | Total | 2293760
tcp.reassembly_memuse | Total | 393216
flow.memuse | Total | 7554304
-----
Date: 8/8/2020 -- 08:55:06 (uptime: 0d, 00h 04m 24s)
-----
Counter | TM Name | Value
-----
flow.spare | Total | 10000
flow_mgr.rows_checked | Total | 65536
flow_mgr.rows_skipped | Total | 65536
tcp.memuse | Total | 2293760
tcp.reassembly_memuse | Total | 393216
flow.memuse | Total | 7554304

```

```
kali㉿kali:~$ sudo suricata --help
```

```
Suricata 5.0.3
USAGE: suricata [OPTIONS] [BPF FILTER]

  -c <path>                      : path to configuration file
  -T                                : test configuration file (use with -c)
  -i <dev or ip>                   : run in pcap live mode
  -F <bpf filter file>             : bpf filter file
  -r <path>                        : run in pcap file/offline mode
  -q <qid[:qid]>                  : run in inline nfqueue mode (use colon to specify a range of queues)
  -s <path>                        : path to signature file loaded in addition to suricata.yaml settings
(optional)
  -S <path>                        : path to signature file loaded exclusively (optional)
  -l <dir>                          : default log directory
  -D                                : run as daemon
  -k [all|none]                    : force checksum check (all) or disabled it (none)
  -V                                : display Suricata version
  -v                                : be more verbose (use multiple times to increase verbosity)
  --list-app-layer-protos          : list supported app layer protocols
  --list-keywords[=all|csv|<kword>] : list keywords implemented by the engine
  --list-runmodes                  : list supported runmodes
  --runmode <runmode_id>           : specific runmode modification the engine should run. The argument supplied should be the id for the runmode obtained by running --list-runmodes
  --engine-analysis                : print reports on analysis of different sections in the engine and ex
it.
Please have a look at the conf parameter engine-analysis on what rep
orts
  --pidfile <file>                : write pid to this file
  --init-errors-fatal              : enable fatal failure on signature init error
  --disable-detection              : disable detection engine
  --dump-config                    : show the running configuration
  --build-info                     : display build information
  --pcap[=<dev>]                  : run in pcap mode, no value select interfaces from suricata.yaml
  --pcap-file-continuous           : when running in pcap mode with a directory, continue checking direct
ory for pcaps until interrupted
  --pcap-file-delete               : when running in replay mode (-r with directory or file), will delete
pcap files that have been processed when done
  --pcap-buffer-size               : size of the pcap buffer value from 0 - 2147483647
  --af-packet[=<dev>]              : run in af-packet mode, no value select interfaces from suricata.yaml
  --simulate-ips                  : force engine into IPS mode. Useful for QA
  --user <user>                   : run suricata as this user after init
  --group <group>                 : run suricata as this group after init
  --erf-in <path>                 : process an ERF file
  --unix-socket[=<file>]           : use unix socket to control suricata work
  --set name=value                 : set a configuration value

To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the comm
and as:
suricata -c suricata.yaml -s signatures.rules -i eth0
```

Suricata Rules

9.1 Rules Format

Signatures are very important in Suricata.

Usually ready-made rulesets are used.

A rule/signature consists of these:

- Action: Decides what happens when the signature matches.
- Header: Defining the protocol, IP addresses, port and direction of the rule.
- Rule options: Defining the specifics of the rule.

Example of rule in suricata:

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2);
```

Snort Rule Actions

Action	Protocol	Source IP Address	Source Port	Action	Dest IP address	Dest Port
--------	----------	-------------------	-------------	--------	-----------------	-----------

(a) Rule Header

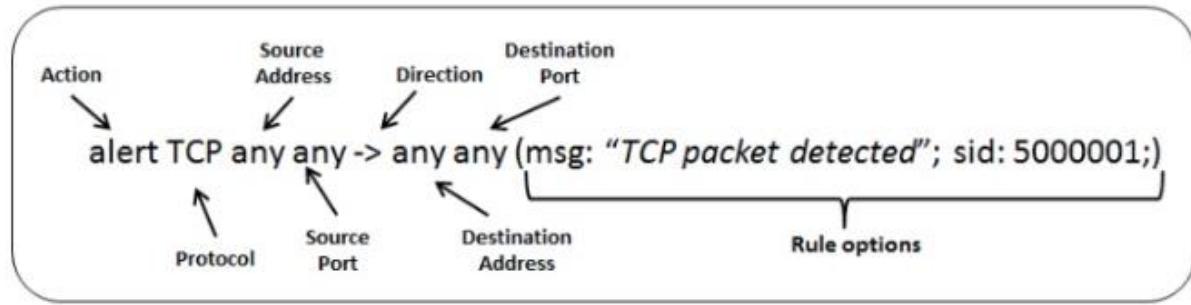
Option Keyword	Protocol Arguments	...
----------------	--------------------	-----

(b) Options

9.1.1 Action

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-
```

9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)



9.1.1.1 Action-order

All signatures have different features. One of those is the Action features. This one determines what will happen when a signature matches.

There are four types of Action.

What happens when a signature matches?

- 1) Pass

If a signature matches and contains pass, Suricata stops scanning the packets. Skips to the end of all rules but only for the current packet.

- 2) Drop

This only concerns the IPS/inline mode. If the program finds a signature that matches, containing drop. It stops immediately. The packet will no longer be sent.

Drawback: The receiver does not receive a message of what is going on, resulting in a time-out (certainly with TCP). Suricata generates an alert for this packet.

3) Reject

This is an active rejection of the packet. Both receiver and sender receive a reject packet.

There are two types of reject packets that will be automatically selected. If the offending packet concerns TCP, it will be a Reset-packet. For all other protocols it will be an ICMP-error packet. Suricata also generates an alert. When in Inline / IPS mode, the offending packet will also be dropped like with the 'drop' action.

4) Alert

If a signature matches and contains alert, the packet will be treated like any other non-threatening packet, except for this one an alert will be generated by Suricata. Only the system administrator can notice this alert. Inline / IPS can block network traffic in two ways.

One way is by drop and the other by reject.

Rules will be loaded in the order of which they appear in files. But they will be processed in a different order.

Signatures have different priorities. The most important signatures will be scanned first. There is a possibility to change the order of priority.

The default order is: pass, drop, reject, alert.

```
action-order:  
- pass  
- drop  
- reject  
- alert
```

This means a pass rule is considered before a drop rule, a drop rule before a reject rule and so on.

9.1.2 Protocol

What is Protocol?

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```

This keyword in a signature shows Suricata which protocol it is related to.

- tcp**(for tcp-traffic)
- udp**
- icmp**
- ip**(ip stands for 'all' or 'any')

There are also a few so-called application layer protocols, or layer 7 protocols. These are:

- http**
- ftp**
- tls** (this includes ssl)
- smb**
- dns**
- dcerpc**
- ssh**
- smtp**
- imap**
- modbus** (disabled by default)
- dnp3** (disabled by default)
- enip** (disabled by default)
- nfs** (depends on rust availability)
- ikev2** (depends on rust availability)
- krb5** (depends on rust availability)
- ntp** (depends on rust availability)
- dhcp** (depends on rust availability)

The availability of these protocols depends on whether the protocol is enabled in the configuration file `suricata.yaml`.

If you have a signature with for instance a `http` protocol, Suricata makes sure the signature can only match if it concerns http-traffic.

9.1.3 Source and Destination

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```

The first emphasized part is the source, the second is the destination (note the direction of the directional arrow).

With source and destination, you specify the source of the traffic and the destination of the traffic, respectively. You can assign IP addresses, (both IPv4 and IPv6 are supported) and IP ranges. These can be combined with operators:

Operator	Description
.../..	IP ranges (CIDR notation)
!	exception/negation
[..., ...]	grouping

Warning: If you set your configuration to something like this:

```
HOME_NET: any  
EXTERNAL_NET: ! $HOME_NET
```

You can not write a signature using \$EXTERNAL_NET because it stands for 'not any'. This is an invalid setting.

9.1.4 Ports(source and destination)

The first emphasized part is the source, the second is the destination (the direction of the directional arrow).

Traffic comes in and goes out through ports. Different ports have different port numbers. For example, the default port for HTTP is 80 while 443 is typically the port for HTTPS.

Operator	Description
:	port ranges
!	exception/negation
[..., ...]	grouping

Example	Meaning
[80, 81, 82]	port 80, 81 and 82
[80: 82]	Range from 80 till 82
[1024:]	From 1024 till the highest port-number
!80	Every port but 80
[80:100,!99]	Range from 80 till 100 but 99 excluded
[1:80,!{2,4}]	Range from 1-80, except ports 2 and 4
[..., ...]	

9.1.5 Direction

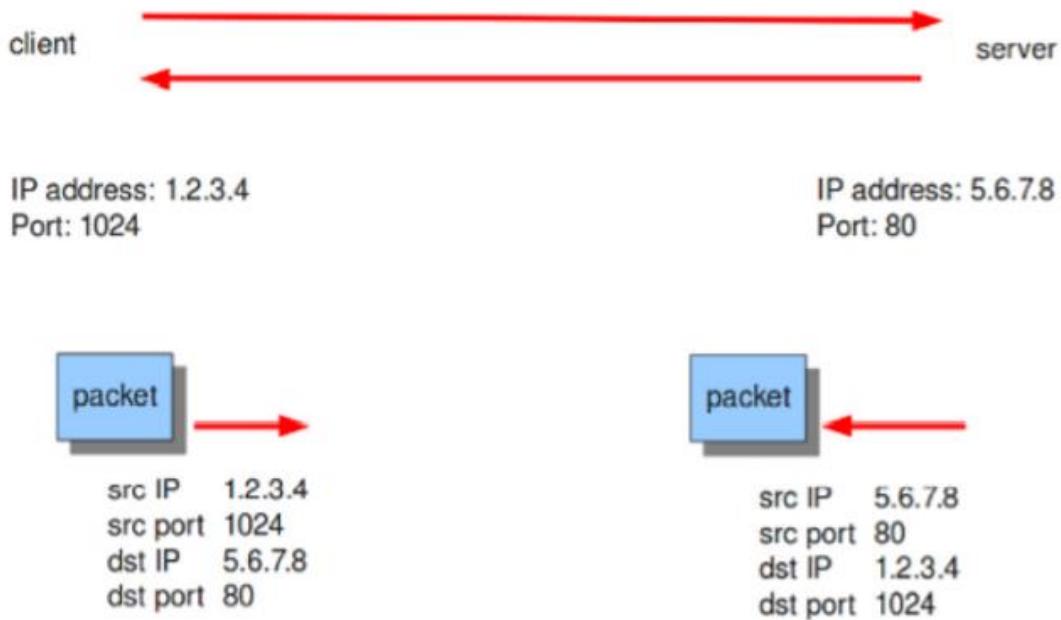
```
drop tcp $HOME_NET any ->$EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)
```

The direction tells in which way the signature has to match. Nearly every signature has an arrow to the right (->). This means that only packets with the same direction can match. However, it is also possible to have a rule match both ways (<>):

source -> destination
source <> destination (both directions)

Warning: There is no ‘reverse’ style direction, i.e. there is no <-.

The client sends a message to the server, and the server replies with its answer.



9.1.6 Rule options

The rest of the rule consists of options. These are enclosed by parenthesis and separated by semicolons. Some options have settings (such as msg), which are specified by the keyword of the option, followed by a colon, followed by the settings. Others have no settings, and are simply the keyword.

```
<keyword>: <settings>;
<keyword>;
```

Modifier Keywords

Some keywords function act as modifiers. There are two types of modifiers.

Content modifiers:

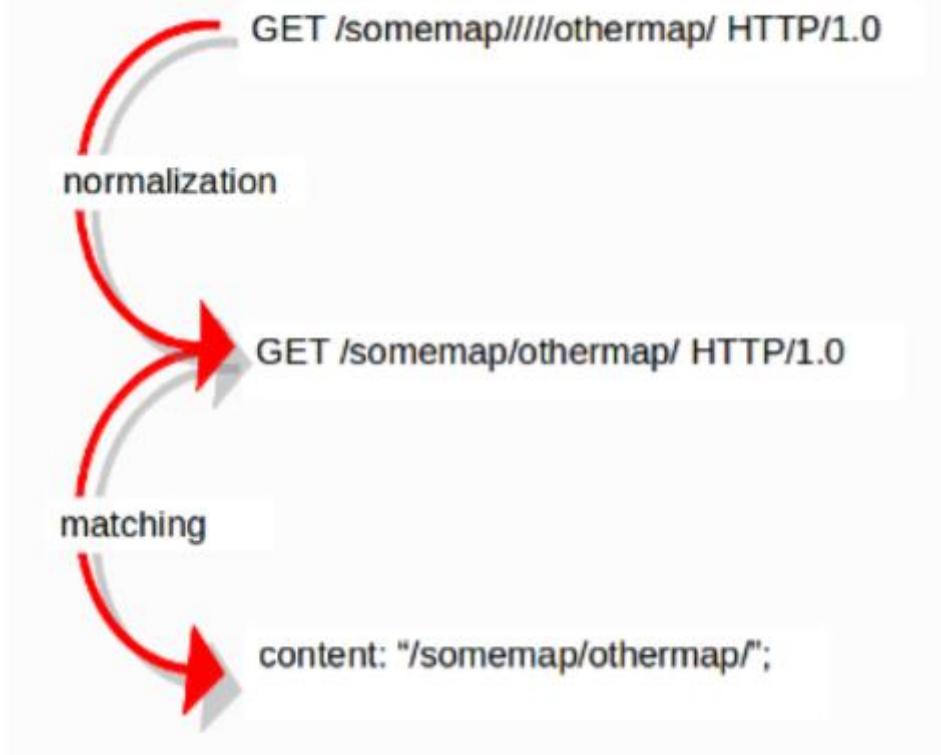
```
alert http any any -> any any (content:"index.php"; http_uri; sid:1;)
```

Sticky buffer:

```
alert http any any -> any any (http_response_line; content:"403 Forbidden"; sid:1;  
→)
```

Normalized Buffers

A packet consists of raw data. HTTP and reassembly make a copy of those kinds of packets data. They erase anomalous content, combine packets etcetera. What remains is a called the ‘normalized buffer’:



9.2 Meta Keywords

9.2.1 msg (message)

The keyword msg gives textual information about the signature and the possible alert.

```
msg : "some description";
```

```
msg:"ATTACK-RESPONSES 403 Forbidden";
```

```
msg:"ET EXPLOIT SMB-DS DCERPC PnP bind attempt";
```

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```

9.2.2 sid (signature ID)

The keyword sid gives every signature its own id. This id is stated with a number.

```
sid:123;
```

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```

9.2.3 rev (revision)

Usually the rev keyword is used together with the sid keyword. Rev represents the version of the signature. When the signature changes, the number of revs should also change.

```
rev:123;
```

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +..)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```

rev and sid are usually used after all keywords.

9.2.4 gid (group ID)

The gid keyword can be used to give different groups of signatures another id value (like in sid). Suricata uses by default gid 1.

9.2.5 classtype

The classtype keyword gives information about the classification of rules and alerts.

It can tell for example whether a rule is just informational or is about a hack etc.

```
config classification: web-application-attack,Web Application Attack,1
```

```
config classification: not-suspicious,Not Suspicious Traffic,3
```

classtype	Alert	Priority
web-application-attack	Web Application Attack	1
not-suspicious	Not Suspicious Traffic	3

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +.)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```

9.2.6 reference

This keyword is meant for signature-writers and analysts who investigate why a signature has matched.

```
reference: type, reference
```

```
reference: url, www.info.com
```

```
reference: cve, CVE-2014-1234
```

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +.)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```

9.2.7 priority

The priority keyword comes with a mandatory numeric value which can range from 1 till 255. The numbers 1 to 4 are most often used. Signatures with a higher priority will be examined first. The highest priority is 1.

```
priority:1;
```

9.2.8 metadata

The metadata keyword allows additional, non-functional information to be added to the signature.

```
metadata: key value;
```

```
metadata: key value, key value;
```

9.2.9 target

The target keyword allows the rules writer to specify which side of the alert is the target of the attack. If specified, the alert event is enhanced to contain information about source and target.

```
target:[src_ip|dest_ip]
```

9.3 IP Keywords

9.3.1 ttl

The ttl keyword is used to check for a specific IP time-to-live value in the header of a packet.

```
ttl:10;
```

```
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL MISC 0 ttl"; ttl:0;  
reference:url,support.microsoft.com/default.aspx?scid=kb#-#-EN-US#-#-q138268;  
reference:url,www.isi.edu/innotes/rfc1122.txt; classtype:misc-activity; sid:2101321; rev:9;)
```

9.3.2 ipopts

With the ipopts keyword you can check if a specific IP option is set.

IP Option	Description
rr	Record Route
eol	End of List
nop	No Op
ts	Time Stamp
sec	IP Security
esec	IP Extended Security
lsrr	Loose Source Routing
ssrr	Strict Source Routing
satid	Stream Identifier
any	any IP options are set

```
ipopts: lsrr;
```

```
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL MISC source route ssrr"; ipopts:ssrr;
reference:arachnids,422; classtype:bad-unknown; sid:2100502; rev:3;)
```

9.3.3 sameip

With the `sameip` keyword you can check if the IP address of the source is the same as the IP address of the destination.

```
sameip;
```

```
alert ip any any -> any any (msg:"GPL SCAN same SRC/DST"; sameip; reference:bugtraq,2666;
reference:cve,1999- 0016; reference:url,www.cert.org/advisories/CA-1997-28.html; classtype:bad-
unknown; sid:2100527; rev:9;)
```

9.3.4 ip_proto

With the `ip_proto` keyword you can match on the IP protocol in the packet-header. You can use the name or the number of the protocol.

```
1 ICMP Internet Control Message  
6 TCP Transmission Control Protocol  
17 UDP User Datagram  
47 GRE General Routing Encapsulation  
50 ESP Encap Security Payload for IPv6  
51 AH Authentication Header for Ipv6  
58 IPv6-ICMP ICMP for Ipv6
```

```
ip_proto:PIM
```

```
alert ip any any -> any any (msg:"GPL MISC IP Proto 103 PIM"; ip_proto:103; reference:bugtraq,8211; reference:cve,2003-0567; classtype:non-standard-protocol; sid:2102189; rev:4;)
```

9.3.5 ipv4.hdr

Sticky buffer to match on the whole IPv4 header.

```
alert ip any any -> any any (ipv4.hdr; content:"|3A|"; offset:9; depth:1; sid:1234; rev:5;)
```

9.3.6 ipv6.hdr

Sticky buffer to match on the whole Ipv6 header.

```
alert ip any any -> any any (ipv6.hdr; content:"|3A|"; offset:9; depth:1; sid:1234; rev:5;)
```

9.3.7 id

With the id keyword, you can match on a specific IP ID value.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET DELETED F5 BIG-IP 3DNS TCP Probe 1";  
id: 1; dsize: 24; flags: S,12; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; window: 2048; reference:url,www.f5.com/f5products/v9intro/index.html;  
reference:url,doc.emergingthreats.net/2001609; classtype:misc-activity; sid:2001609; rev:13;)
```

9.3.8 *geoip*

The geoip keyword enables (you) to match on the source, destination or source and destination IPv4 addresses of network traffic, and to see to which country it belongs.

```
geoip: src,RU;  
geoip: both,CN,RU;  
geoip: dst,CN,RU,IR;  
geoip: both,US,CA,UK;  
geoip: any,CN,IR;
```

Option	Description
both	Both directions have to match with the given geoip(s)
any	One of the directions has to match with the given geoip(s).
dest	If the destination matches with the given geoip.
src	The source matches with the given geoip.

9.3.9 *fragbits* (IP fragmentation)

With the fragbits keyword, you can check if the fragmentation and reserved bits are set in the IP header.

M - More Fragments

D - Do not Fragment

R - Reserved Bit

- + match on the specified bits, plus any others
- * match if any of the specified bits are set
- ! match if the specified bits are not set

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Invalid non-fragmented packet
with fragment offset>0"; fragbits: M; fragoffset: >0;
reference:url,doc.emergingthreats.net/bin/view/Main/2001022; classtype:bad-unknown;
sid:2001022; rev:5; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

9.3.10 fragoffset

With the fragoffset keyword you can match on specific decimal values of the IP fragment offset field.

- < match if the value is smaller than the specified value
- > match if the value is greater than the specified value
- ! match if the specified value is not present

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Invalid non-fragmented packet
with fragment offset>0"; fragbits: M; fragoffset: >0;
reference:url,doc.emergingthreats.net/bin/view/Main/2001022; classtype:bad-unknown;
sid:2001022; rev:5; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

9.3.11 tos

The tos keyword can match on specific decimal values of the IP header TOS field. The tos keyword can be have a value from 0 - 255.

```
alert ip any any -> any any (msg:"Differentiated Services Codepoint: Class Selector 1 (8)";
flow:established; tos:8; classtype:not-suspicious; sid:2600115; rev:1;)
```

```
alert ip any any -> any any (msg:"TGI HUNT non-DiffServ aware TOS setting";
flow:established,to_server; tos:!0; tos:!8; tos:!16; tos:!24; tos:!32; tos:!40; tos:!48; tos:!56;
threshold:type limit, track by_src, seconds 60, count 1; classtype:bad-unknown; sid:2600124; rev:1;)
```

9.4 TCP keywords

9.4.1 seq

The seq keyword can be used in a signature to check for a specific TCP sequence number.

```
seq:0;
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL SCAN NULL"; flow:stateless; ack:0;  
flags:0; seq:0; reference:arachnids,4; classtype:attempted-recon; sid:2100623; rev:7;)
```

9.4.2 ack

The ack is the acknowledgement of the receipt of all previous (data)-bytes send by the other side of the TCP connection.

```
ack:1;
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL SCAN NULL"; flow:stateless; ack:0;  
flags:0; seq:0; reference:arachnids,4; classtype:attempted-recon; sid:2100623; rev:7;)
```

9.4.3 window

The window keyword is used to check for a specific TCP window size. The TCP window size is a mechanism that has control of the data-flow.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL DELETED typot trojan traffic";  
flow:stateless; flags:S,12; window:55808; reference:mcafee,100406; classtype:trojan-activity;  
sid:2182; rev:8;)
```

9.4.4 tcp.mss

Match on the TCP MSS option value. Will not match if the option is not present.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (flow:stateless; flags:S,12; tcp.mss<536;sid:1234; rev:5;)
```

9.4.5 tcp.hdr

Sticky buffer to match on the whole TCP header.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (flags:S,12; tcp.hdr; content:"|02 04|"; offset:20; byte_test:2,
```

9.5 UDP keywords

9.5.1 udp.hdr

Sticky buffer to match on the whole UDP header.

```
alert udp any any -> any any (udp.hdr; content:"|00 08|"; offset:4; depth:2; sid:1234; rev:5;),
```

9.6 ICMP keywords

ICMP (Internet Control Message Protocol) is a part of IP. IP at itself is not reliable when it comes to delivering data (datagram). ICMP gives feedback in case problems occur. It does not prevent problems from happening, but helps in understanding what went wrong and where.

9.6.1 *itype*

The *itype* keyword is for matching on a specific ICMP type (number).

```
itype:>10;
```

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL SCAN Broadscan Smurf Scanner";  
dsize:4; icmp_id:0; icmp_seq:0; itype:8; classtype:attempted-recon; sid:2100478; rev:4;)
```

ICMP types:

ICMP Type	Name
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41	Experimental mobility protocols such as Seamoby

9.6.2 icode

With the icode keyword you can match on a specific ICMP code.

```
icode:>5;
```

```
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"GPL MISC Time-To-Live Exceeded in  
Transit"; icode:0; itype:11; classtype:misc-activity; sid:2100449; rev:7;)
```

ICMP Types:

ICMP Code	ICMP Type	Description
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Fragmentation Needed and Don't Fragment was Set
	5	Source Route Failed
	6	Destination Network Unknown
	7	Destination Host Unknown
	8	Source Host Isolated
	9	Communication with Destination Network is Administratively Prohibited
	10	Communication with Destination Host is Administratively Prohibited
	11	Destination Network Unreachable for Type of Service
	12	Destination Host Unreachable for Type of Service
	13	Communication Administratively Prohibited
	14	Host Precedence Violation
	15	Precedence cutoff in effect

5	0	Redirect Datagram for the Network (or subnet)
	1	Redirect Datagram for the Host
	2	Redirect Datagram for the Type of Service and Network
	3	Redirect Datagram for the Type of Service and Host
9	0	Normal router advertisement
	16	Doesn't route common traffic
11	0	Time to Live exceeded in Transit
	1	Fragment Reassembly Time Exceeded
12	0	Pointer indicates the error
	1	Missing a Required Option
	2	Bad Length
40	0	Bad SPI
	1	Authentication Failed
	2	Decompression Failed
	3	Decryption Failed
	4	Need Authentication
	5	Need Authorization

9.6.3 icmp_id

With the icmp_id keyword you can match on specific ICMP id-values.

```
icmp_id:0;
```

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL SCAN Broadscan Smurf Scanner";
dsize:4; icmp_id:0; icmp_seq:0; itype:8; classtype:attempted-recon; sid:2100478; rev:4;)
```

9.6.4 icmp_seq

You can use the icmp_seq keyword to check for a ICMP sequence number. ICMP messages all have sequence numbers.

```
icmp_seq:0;
```

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL SCAN Broadscan Smurf Scanner";
dsize:4; icmp_id:0; icmp_seq:0; itype:8; classtype:attempted-recon; sid:2100478; rev:4;)
```

9.7 Payload Keywords

Payload keywords inspect the content of the payload of a packet or stream.

What is Payload?

Payload is the part of [transmitted data](#) that is the actual intended message.

9.7.1 content

What to do can be written in quotation marks like a signature match.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +.)";  
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-  
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;  
rev:2;)
```



content:"abc";	X
content:"aBc";	X
content:"abC";	✓

✓ match

X no match

match in the payload

no match in the payload

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Outdated Firefox on Windows";
content:"User-Agent|3A| Mozilla/5.0 |28|Windows|3B| "; content:"Firefox/3."; distance:0;
content:!"Firefox/3.6.13"; distance:-10; sid:9000000; rev:1;)
```

content:"Firefox/3.6.13";

This means an alert will be generated if the used version of Firefox is not 3.6.13.

9.7.2 *nocase*

It eliminates the distinction between uppercase and lowercase letters.

```
nocase;
```

```
content: "abc"; nocase;
```



```
content:"abc"; nocase;
```



```
content:"aBc"; nocase;
```



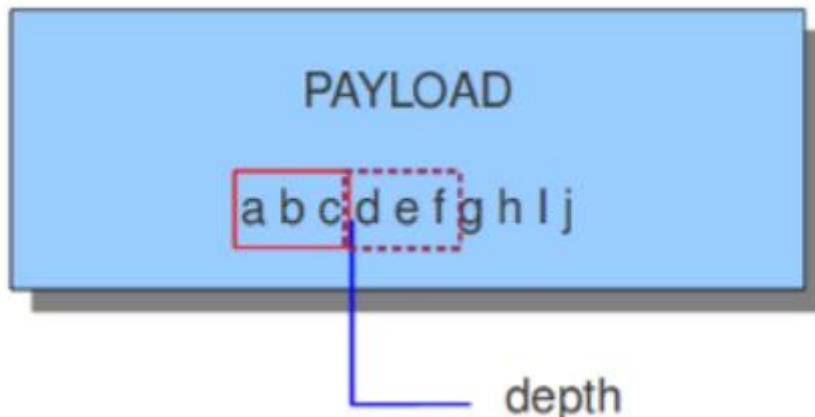
```
content:"abC"; nocase;
```



9.7.3 *depth*

The depth keyword is a absolute content modifier.

```
depth:12;
```



content:"**def**"; depth:3;



content:"**abc**"; depth:3;



9.7.4 *startswith*

It modifies the content to match exactly at the start of a buffer. This keyword is similar to depth.

```
content:"GET|20|"; startswith;
```

startswith is a short hand notation for:

```
content:"GET|20|"; depth:4; offset:0;
```

NOTE: *startswith* cannot be mixed with *depth*, *offset*, *within* or *distance* for the same pattern.

9.7.5 endswith

The `endswith` keyword is similar to `isdataat:!1,relative;`. It takes no arguments and must follow a content keyword. It modifies the content to match exactly at the end of a buffer.

```
content:".php"; endswith;
```

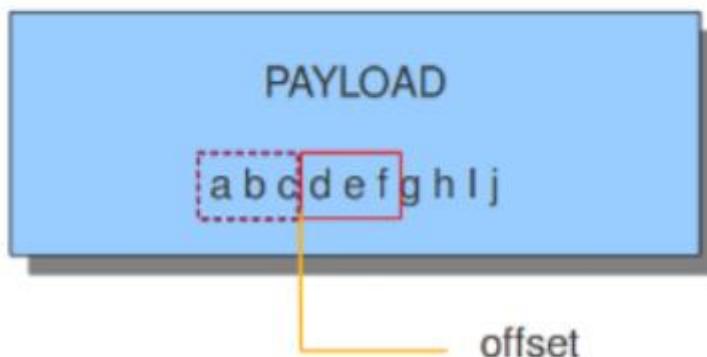
endswith is a short hand notation for:

```
content:".php"; isdatat:!1,relative;
```

NOTE: `endswith` cannot be mixed with offset, within or distance for the same pattern.

9.7.6 offset

The `offset` keyword designates from which byte in the payload will be checked to find a match.



`content:"abc"; offset:3;`



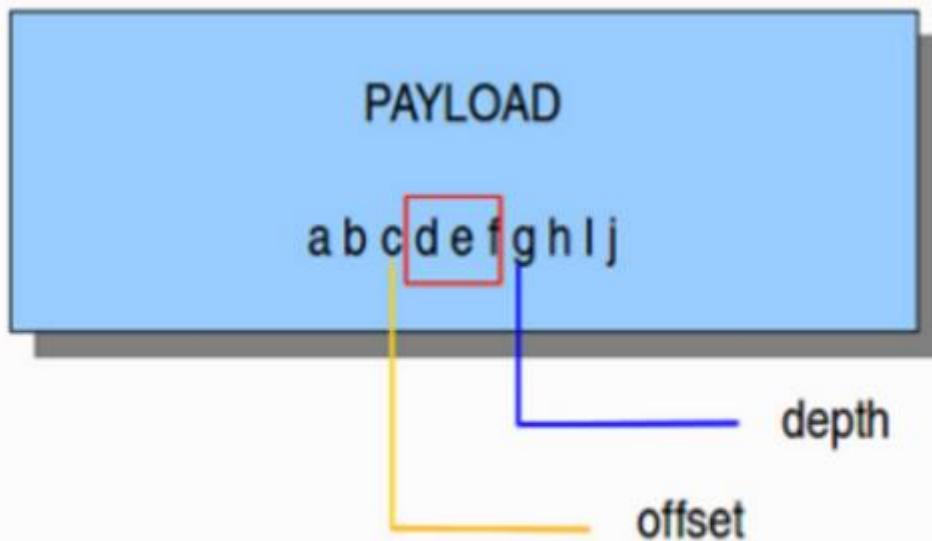
`content:"def"; offset:3;`



The keywords offset and depth can be combined and are often used together.

For example:

```
content:"def"; offset:3; depth:3;
```



```
content:"def"; offset:3; depth:3;
```

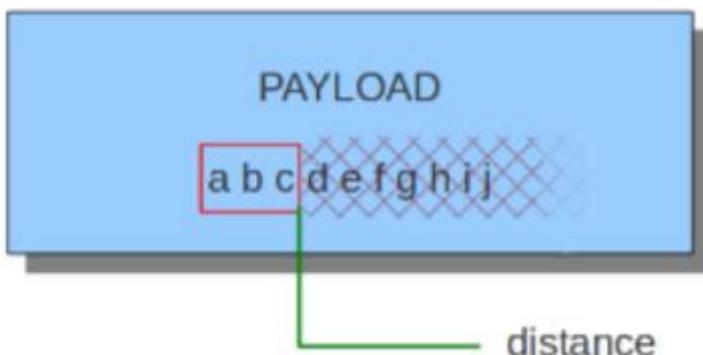


9.7.7 *distance*

The keyword distance is a relative content modifier. This means it indicates a relation between this content keyword and the content preceding it. Distance has its influence after the preceding match. The keyword distance comes with a mandatory numeric value.

content:"abc"; content:"klm"; distance: 0;
1 2 3

The distance (3), tells how the second (2) content relates to the first (1) content.

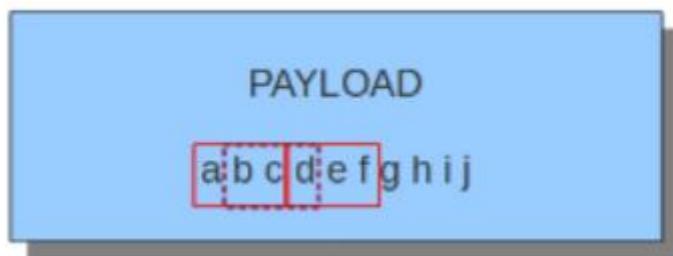


content:"abc"; content:"klm"; distance: 0;

X



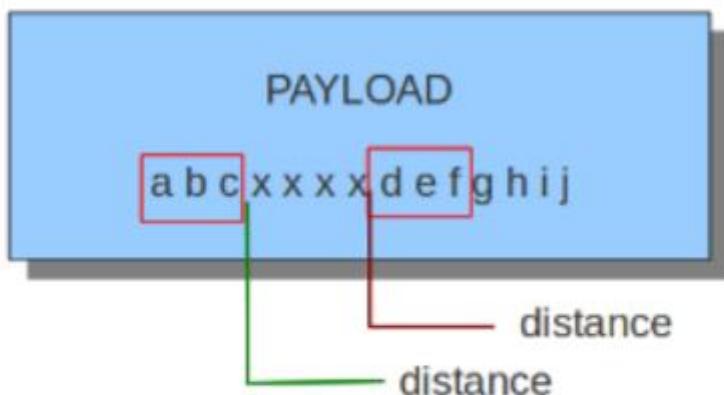
checked area using 'distance'



content:"abc"; content:"def"; distance:0;



content:"abc"; content:"bcd"; distance:0;



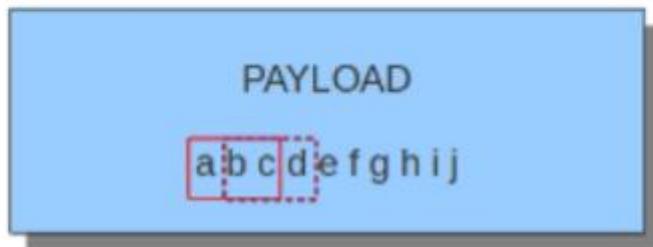
content:"abc"; content:"def"; distance:0;



content:"abc"; content:"def"; distance:4;



Distance can also be a negative number.



content:"abc"; content:"bcd"; distance:-2;



9.7.8 *within*

The keyword *within* is relative to the preceding match. The keyword *within* comes with a mandatory numeric value. Using *within* makes sure there will only be a match if the content matches with the payload *within* the set amount of bytes. *Within* can not be 0 (zero).

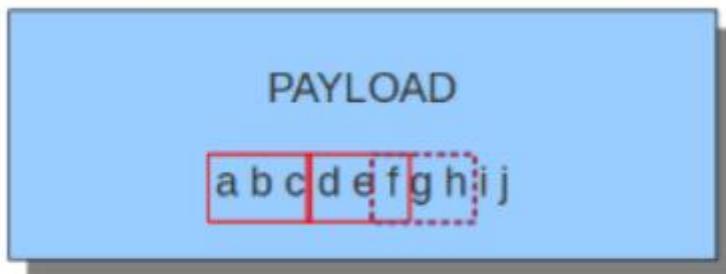
content:"abc"; content:"klm"; within:3;

1



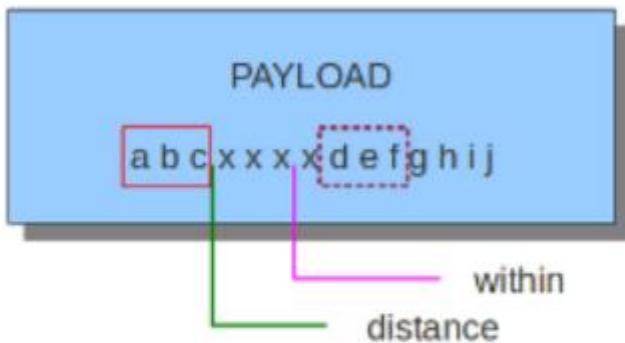
3

The keyword *within* (3), tells how the second (2) content relates to the first (1) content.

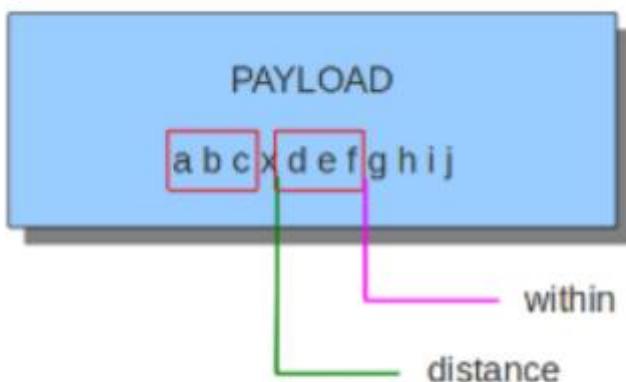


content:"abc"; content:"def"; within:3; ✓
 content:"abc"; content:"fgh"; within:3; ✗

The second content has to fall/come 'within 3' from the first content.



content:"abc"; content:"def"; distance:0; within:3; ✗



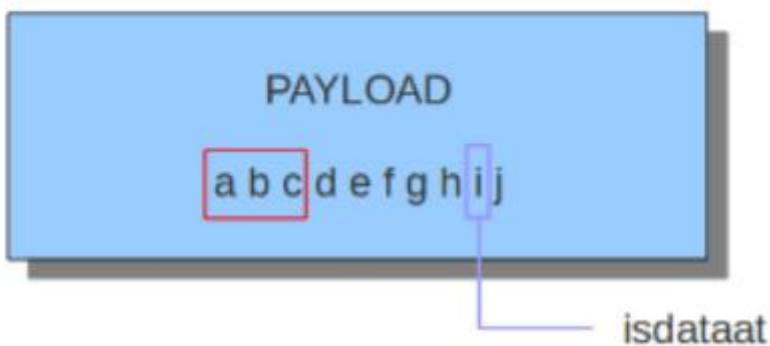
content:"abc"; content:"def"; distance:1; within:4; ✓

9.7.9 isdataat

The purpose of the isdataat keyword is to look if there is still data at a specific part of the payload.

```
isdataat:512;
```

```
isdataat:50, relative;
```



content:"abc"; isdataat:6, relative; ✓

content:"abc"; isdataat:8, relative; ✗

9.7.10 bsize

With the bsize keyword, you can match on the length of the buffer.

```
alert dns any any -> any any (msg:"test bsize rule"; dns.query; content:"google.com"; bsize:10;
sid:123; rev:1;)
```

9.7.11 dsize

With the dsize keyword, you can match on the size of the packet payload.

```
alert udp $EXTERNAL_NET any -> $HOME_NET 65535 (msg:"GPL DELETED EXPLOIT LANDesk
Management Suite Alerting Service buffer overflow"; dsize:>268; reference: bugtraq,23483;
reference: cve,2007-1674; classtype: attempted-admin; sid:100000928; rev:1;)
```

9.7.12 byte_test

The byte_test keyword extracts <num of bytes> and performs an operation selected with <operator> against the value in <test value> at a particular <offset>.

<num of bytes>	The number of bytes selected from the packet to be converted
<operator>	<ul style="list-style-type: none"> • [!] Negation can prefix other operators • < less than • > greater than • = equal • <= less than or equal • >= greater than or equal • & bitwise AND • ^ bitwise OR
<value>	Value to test the converted value against [hex or decimal accepted]
<offset>	Number of bytes into the payload
[relative]	Offset relative to last content match
[endian]	Type of number being read: - big (Most significant byte at lowest address) - little (Most significant byte at the highest address)
[string] <num>	<ul style="list-style-type: none"> • hex - Converted string represented in hex • dec - Converted string represented in decimal • oct - Converted string represented in octal
[dce]	Allow the DCE module determine the byte order

```
alert tcp any any -> any any \
```

```
(msg:"Byte_Test Example - Num = Value"; \
content:"|00 01 00 02|"; byte_test:2,=,0x01;)
```

```
alert tcp any any -> any any \
```

```
(msg:"Byte_Test Example - Num = Value relative to content"; \
content:"|00 01 00 02|"; byte_test:2,=,0x03,relative;)
```

```
alert tcp any any -> any any \
```

```
(msg:"Byte_Test Example - Num != Value"; content:"|00 01 00 02|"; \
byte_test:2,!!=,0x06;)
```

```

alert tcp any any -> any any \
(msg:"Byte_Test Example - Detect Large Values"; content:"|00 01 00 02|"; \
byte_test:2,>,1000,relatvive;)

```

```

alert tcp any any -> any any \
(msg:"Byte_Test Example - Lowest bit is set"; \
content:"|00 01 00 02|"; byte_test:2,&,0x01,relative;)

```

```

alert tcp any any -> any any (msg:"Byte_Test Example - Compare to String"; \
content:"foobar"; byte_test:4,=,1337,1,relative,string,dec;)

```

9.7.13 byte_jump

The byte_jump keyword allows for the ability to select a <num of bytes> from an <offset> and moves the detection pointer to that position.

<num of bytes>	The number of bytes selected from the packet to be converted
<offset>	Number of bytes into the payload
[relative]	Offset relative to last content match
[multiplier] <value>	Multiple the converted byte by the <value>
[Endian]	<ul style="list-style-type: none"> • big (Most significant byte at lowest address) • little (Most significant byte at the highest address)
[string] <num_type>	<ul style="list-style-type: none"> • hex Converted data is represented in hex • dec Converted data is represented in decimal • oct Converted data is represented as octal
[align]	Rounds the number up to the next 32bit boundary
[from_beginning]	Jumps forward from the beginning of the packet, instead of where the detection pointer is set
[from_end]	Jump will begin at the end of the payload, instead of where the detection point is set
[post_offset] <value>	After the jump operation has been performed, it will jump an additional number of bytes specified by <value>
[dce]	Allow the DCE module determine the byte order

```

alert tcp any any -> any any \
  (msg:"Byte_Jump Example"; \
  content:"Alice"; byte_jump:2,0; content:"Bob");

alert tcp any any -> any any \
  (msg:"Byte_Jump Multiple Jumps"; \
  byte_jump:2,0; byte_jump:2,0,relative; content:"foobar"; distance:0; within:6);

alert tcp any any -> any any \
  (msg:"Byte_Jump From the End -8 Bytes"; \
  byte_jump:0,0, from_end, post_offset -8; \
  content:"|6c 33 33 74|"; distance:0 within:4);

```

9.7.14 byte_extract

The byte_extract keyword extracts <num of bytes> at a particular <offset> and stores it in <var_name>. The value in <var_name> can be used in any modifier that takes a number as an option and in the case of byte_test it can be used as a value.

Keyword	Modifier
content	offset,depth,distance,within
byte_test	offset,value
byte_jump	offset
isdataat	offset

```

alert tcp any any -> any any \
  (msg:"Byte_Extract Example Using distance"; \
  content:"Alice"; byte_extract:2,0,size; content:"Bob"; distance:size; within:3; sid:1);

```

```
alert tcp any any -> any any \
  (msg:"Byte_Extract Example Using within"; \
  flow:established,to_server; content:"|00 FF|"; \
  byte_extract:1,0,len,relative; content:"|5c 00|"; distance:2; within:len;sid:2;)
```

```
alert tcp any any -> any any \
  (msg:"Byte_Extract Example Comparing Bytes"; \
  flow:established,to_server; content:"|00 FF|"; \
  byte_extract:2,0,cmp_ver,relative; content:"FooBar"; distance:0; byte_test:2,=,cmp_ver,0;
  sid:3;)
```

9.7.15 rpc

The rpc keyword used to match in the SUNRPC CALL on the RPC procedure numbers and the RPC version.

```
alert udp $EXTERNAL_NET any -> $HOME_NET 111 (msg:"RPC portmap request yppasswdd";
  rpc:100009,*,*; reference:bugtraq,2763; classtype:rpc-portmap-decode; sid:1296; rev:4;)
```

9.7.16 replace

The replace content modifier can only be used in ips. It adjusts network traffic.

content: "abc"; replace: "def";



9.7.17 byte_math

The byte_math keyword adds the capability to perform mathematical operations on extracted values with an existing variable or a specified value.

Keyword	Modifier
content	offset,depth,distance,within
byte_test	offset,value
byte_jump	offset
isdataat	offset

<num of bytes>	The number of bytes selected from the packet
<offset>	Number of bytes into the payload
oper <operator>	Mathematical operation to perform: +, -, *, /, <<, >>
rvalue <rvalue>	Value to perform the math operation with
result <result-var>	Where to store the computed value
[relative]	Offset relative to last content match
[endianness <type>]	<ul style="list-style-type: none">big (Most significant byte at lowest address)little (Most significant byte at the highest address)
[string <num_type>]	<ul style="list-style-type: none">hex Converted data is represented in hexdec Converted data is represented in decimaloct Converted data is represented as octal
[dce]	Allow the DCE module determine the byte order
[bitmask] <value>	The AND operator will be applied to the extracted value The result will be right shifted by the number of bits equal to the number of trailing zeros in the mask

```
alert tcp any any -> any any \
(msg:"Testing bytemath_body"; \
content:"|00 04 93 F3|"; \
content:"|00 00 00 07|"; distance:4; within:4; \
byte_math:bytes 4, offset 0, oper +, rvalue; \
248, result var, relative;)
```

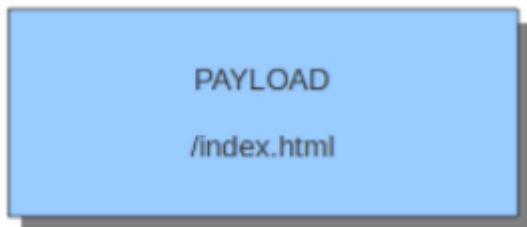
```
alert udp any any -> any any \
(byte_extract: 1, 0, extracted_val, relative; \
byte_math: bytes 1, offset 1, oper +, rvalue extracted_val, result var; \
byte_test: 2, =, var, 13; \
msg:"Byte extract and byte math with byte test verification";)
```

9.7.18 pcre (Perl Compatible Regular Expressions)

The keyword pcre matches specific on regular expressions.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA +.)";
flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK .*USA.*[0-
9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124;
rev:2;)
```

Suricata's modifiers



content:"/index."; http_uri; content:"htm"; http_uri; distance:0; ✓

content:"index."; http_uri; pcre:"/html?\$/UR"; ✓

content:"index."; http_uri; pcre:"/^index\.html?/\$/U"; ✓



content:"/index."; http_uri; content:"htm"; http_uri; distance:0; ✓

content:"index."; http_uri; pcre:"/html?\$/UR"; ✓

content:"index."; http_uri; pcre:"/^index\.html?/\$/U"; ✓



content:"/index."; http_uri; content:"htm"; http_uri; distance:0;	✓
content:"index."; http_uri; pcre:"/html?\$/UR";	✓
content:"index."; http_uri; pcre:"/^index\\.html?/\$/U";	✓



content:"/index."; http_uri; content:"htm"; http_uri; distance:0;	✓
content:"index."; http_uri; pcre:"/html?\$/UR";	✗
content:"index."; http_uri; pcre:"/^index\\.html?/\$/U";	✗



content:"/index."; http_uri; content:"htm"; http_uri; distance:0;	X
content:"index."; http_uri; pcre:"/html?\$/UR";	✓
content:"index."; http_uri; pcre:"^/index\.html?/\$U";	X

9.8 Transformations

Transformation keywords turn the data at a sticky buffer into something else.

```
alert http any any -> any any (file_data; strip_whitespace; \
    content:"window.navigate(); sid:1;")
```

Each transform's output acts as input for the next one.

```
alert http any any -> any any (http_request_line; compress_whitespace; to_sha256; \
    content:"|54A9 7A8A B09C 1B81 3725 2214 51D3 F997 F015 9DD7 049E E5AD CED3 945A
    FC79 7401|"; sid:1;)
```

9.8.1 dotprefix

Takes the buffer, and prepends a . character to help facilitate concise domain checks.

```
alert dns any any -> any any (dns.query; dotprefix; \
    content:".microsoft.com"; sid:1;)
```

This rule can be used to match on the domain only:

```
alert dns any any -> any any (dns.query; dotprefix; \
    content:".microsoft.com"; endswith; sid:1;)
```

this rule can be used to match on the TLD only;

```
alert dns any any -> any any (dns.query; dotprefix; \
    content:".co.uk"; endswith; sid:1;)
```

9.8.2 strip_whitespace

This rule is like isspace() in C.

```
alert http any any -> any any (file_data; strip_whitespace; \
    content:"window.navigate("; sid:1;)
```

9.8.3 compress_whitespace

Compresses all consecutive whitespace into a single space.

9.8.4 to_md5

Takes the buffer, calculates the MD5 hash and passes the raw hash value on.

```
alert http any any -> any any (http_request_line; to_md5; \
content:"|54 A9 7A 8A B0 9C 1B 81 37 25 22 14 51 D3 F9 97| "; sid:1;)
```

9.8.5 to_sha1

Takes the buffer, calculates the SHA-1 hash and passes the raw hash value on.

```
alert http any any -> any any (http_request_line; to_sha1; \
content:"|54A9 7A8A B09C 1B81 3725 2214 51D3 F997 F015 9DD7| "; sid:1;)
```

9.8.6 to_sha256

Takes the buffer, calculates the SHA-256 hash and passes the raw hash value on.

```
alert http any any -> any any (http_request_line; to_sha256; \
content:"|54A9 7A8A B09C 1B81 3725 2214 51D3 F997 F015 9DD7 049E E5AD CED3 945A
FC79 7401| "; sid:1;)
```

9.9 Prefiltering Keywords

9.9.1 fast_pattern

list_id	Content Modifier Keyword	Buffer Name	Registration Order
1	<none> (regular content match)	DETECT_SM_LIST_PMATCH	1 (first)
2	http_uri	DETECT_SM_LIST_UMATCH	2
6	http_client_body	DETECT_SM_LIST_HCBDMATCH	3
7	http_server_body	DETECT_SM_LIST_HSBDMATCH	4
8	http_header	DETECT_SM_LIST_HHDMATCH	5
9	http_raw_header	DETECT_SM_LIST_HRHDMATCH	6
10	http_method	DETECT_SM_LIST_HMDMATCH	7
11	http_cookie	DETECT_SM_LIST_HCDMATCH	8
12	http_raw_uri	DETECT_SM_LIST_HRUDMATCH	9
13	http_stat_msg	DETECT_SM_LIST_HSMDMATCH	10
14	http_stat_code	DETECT_SM_LIST_HSCDMATCH	11
15	http_user_agent	DETECT_SM_LIST_HUADMATCH	12 (last)

Priority (lower number is higher priority)	Registration Order	Content Modifier Keyword	Buffer Name	list_id
3	11	<none> (regular content match)	DETECT_SM_LIST_PMATCH	1
3	12	http_method	DETECT_SM_LIST_HMDMATCH	12
3	13	http_stat_code	DETECT_SM_LIST_HSCDMATCH	9
3	14	http_stat_msg	DETECT_SM_LIST_HSMDMATCH	8
2	1 (first)	http_client_body	DETECT_SM_LIST_HCBDMATCH	4
2	2	http_server_body	DETECT_SM_LIST_HSBDMATCH	5
2	3	http_header	DETECT_SM_LIST_HHDMATCH	6
2	4	http_raw_header	DETECT_SM_LIST_HRHDMATCH	7
2	5	http_uri	DETECT_SM_LIST_UMATCH	2
2	6	http_raw_uri	DETECT_SM_LIST_HRUDMATCH	3
2	7	http_host	DETECT_SM_LIST_HHHDMATCH	10
2	8	http_raw_host	DETECT_SM_LIST_HRHDMATCH	11
2	9	http_cookie	DETECT_SM_LIST_HCDMATCH	13
2	10	http_user_agent	DETECT_SM_LIST_HUADMATCH	14
2	15 (last)	dns_query	DETECT_SM_LIST_DNSQUERY_MATCH	20

9.9.2 prefILTER

TTL test will be used in prefILTERing instead of the single byte pattern.

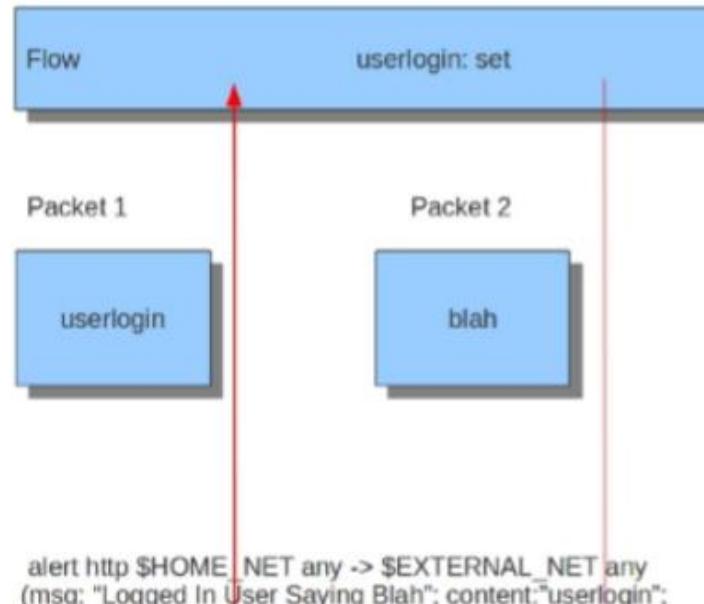
```
alert ip any any any -> any any (ttl:123; prefilter; content:"a"; sid:1;)
```

9.10 Flow Keywords

9.10.1 flowbits

Flowbits have different actions.

1. **flowbits: set, name** Will set the condition/'name', if present, in the flow.
2. **flowbits: isset, name** Can be used in the rule to make sure it generates an alert when the rule matches and the condition is set in the flow.
3. **flowbits: toggle, name** Reverses the present setting. So for example if a condition is set, it will be unset and viceversa.
4. **flowbits: unset, name** Can be used to unset the condition in the flow.
5. **flowbits: isnotset, name** Can be used in the rule to make sure it generates an alert when it matches and the condition is not set in the flow.
6. **flowbits: noalert** No alert will be generated by this rule.



```

alert http $HOME_NET any -> $EXTERNAL_NET any
(msg: "Logged In User Saying Blah"; content:"userlogin";
flowbits:set, userlogin; flowbits:noalert;)

alert http $HOME_NET any -> $EXTERNAL_NET any
(msg: "Logged In User Saying Blah"; flowbits:isset,
userlogin; content:"blah"; ;)

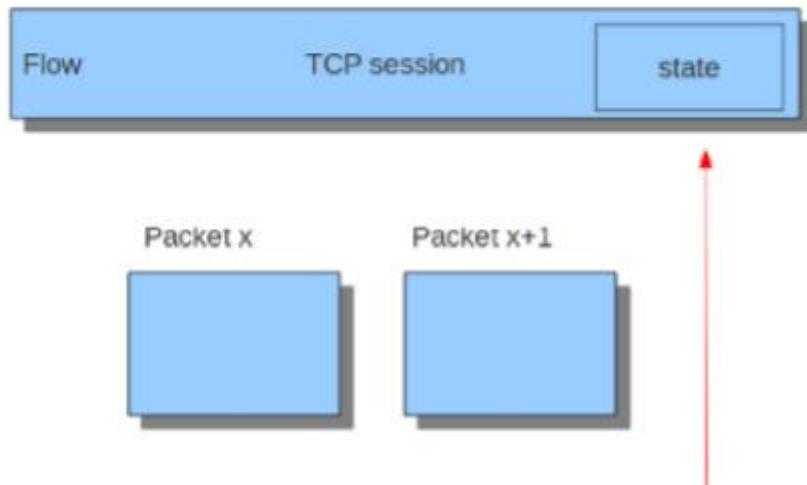
```

9.10.2 flow

This keyword can be used to match on direction of the flow, so to/from client or to/from server.

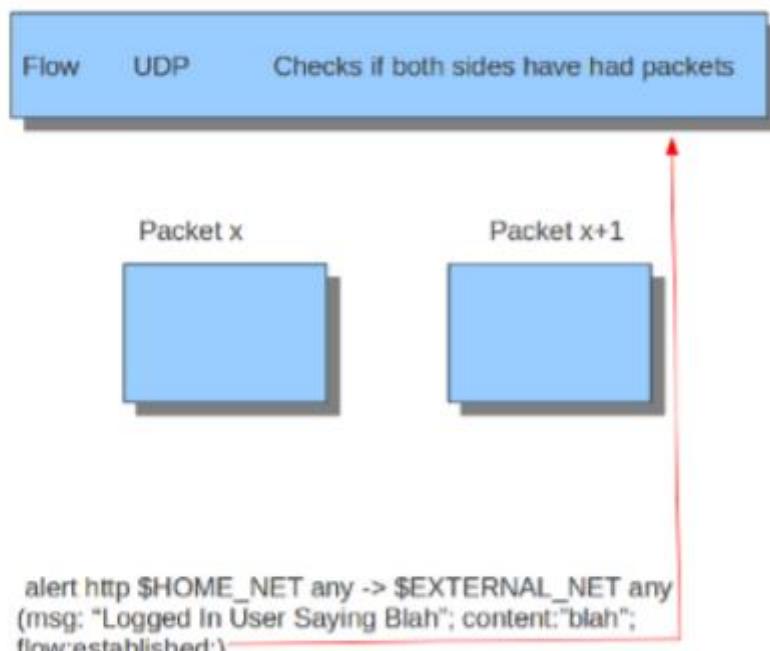
Those that can match the flow keyword:

- **to_server** Match on packets from client to server.
- **from_client** Match on packets from client to server (same as to_server).
- **from_server** Match on packets from server to client (same as to_client).
- **established** Match on established connections.
- **not_established** Match on packets that are not part of an established connection
- **stateless** Match on packets that are and are not part of an established connection.
- **only_stream** Match on packets that have been reassembled by the stream engine.
- **no_stream** Match on packets that have not been reassembled by the stream engine.
- **only_frag** Match packets that have been reassembled from fragments.
- **no_frag** Match packets that have not been reassembled from fragments.



```
alert http $HOME_NET any -> $EXTERNAL_NET any  
(msg: "Logged In User Saying Blah"; content:"blah";  
flow:established;)
```

for UDP:



9.10.3 flowint

Flowint allows storage and mathematical operations using variables.

```
flowint: name, modifier[, value];
```

```
alert tcp any any -> any any (msg:"Counting Usernames"; content:"jonkman"; \
flowint: usernamecount, +, 1; noalert;)
```

9.10.4 stream_size

The stream size option matches on traffic according to the registered amount of bytes by the sequence numbers.

```
alert tcp any any -> any any (stream_size:both,>,5000; sid:1;)
```

9.11 Bypass Keyword

This keyword can be used in signatures to exclude traffic from further evaluation.

9.11.1 bypass

Bypass a flow on matching http traffic.

```
alert http any any -> any any (content:"suricata-ids.org"; \
http_host; bypass; sid:10001; rev:1;)
```

9.12 HTTP Keywords

These keywords are an additional content modifier that can provide protocol specific capabilities at the application layer.

```
alert http any any -> any any (content:"index.php"; http_uri; sid:1;)
```

```
alert http any any -> any any (http.response_line; content:"403 Forbidden"; sid:1; )
```

request keywords:

Keyword	Sticky or Modifier	Direction
http.uri	Sticky Buffer	Request
http.uri.raw	Sticky Buffer	Request
http.method	Sticky Buffer	Request
http.request_line	Sticky Buffer	Request
http.request_body	Sticky Buffer	Request
http.header	Sticky Buffer	Both
http.header.raw	Sticky Buffer	Both
http.cookie	Sticky Buffer	Both
http.user_agent	Sticky Buffer	Request
http.host	Sticky Buffer	Request
http.host.raw	Sticky Buffer	Request
http.accept	Sticky Buffer	Request
http.accept_lang	Sticky Buffer	Request
http.accept_enc	Sticky Buffer	Request
http.referer	Sticky Buffer	Request
http.connection	Sticky Buffer	Request
http.content_type	Sticky Buffer	Both
http.content_len	Sticky Buffer	Both
http.start	Sticky Buffer	Both
http.protocol	Sticky Buffer	Both
http.header_names	Sticky Buffer	Both

response keywords:

Keyword	Sticky or Modifier	Direction
http.stat_msg	Sticky Buffer	Response
http.stat_code	Sticky Buffer	Response
http.response_line	Sticky Buffer	Response
http.header	Sticky Buffer	Both
http.header.raw	Sticky Buffer	Both
http.cookie	Sticky Buffer	Both
http.response_body	Sticky Buffer	Response
http.server	Sticky Buffer	Response
http.location	Sticky Buffer	Response
file_data	Sticky Buffer	Response
http.content_type	Sticky Buffer	Both
http.content_len	Sticky Buffer	Both
http.start	Sticky Buffer	Both
http.protocol	Sticky Buffer	Both
http.header_names	Sticky Buffer	Both

9.12.1 HTTP Primer

Each part of the table belongs to a so-called buffer. The HTTP method belongs to the method buffer, HTTP headers to the header buffer etc. A buffer is a specific portion of the request or response that Suricata extracts in memory for inspection.

Request:

GET / HTTP/1.1	HTTP-method, keyword: http_method HTTP-uri, keywords: http_uri or http_raw_uri HTTP-version
Host: www.google.com Connection: keep-alive User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US) AppleWebKit/534.16 (KHTML, like Gecko) Ubuntu/10.10 Chromium/10.0.618.0 Chrome/10.0.618.0 Safari/534.16 Accept-Encoding: gzip,deflate,sdch Accept-Language: en-US,en;q=0.8 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3	HTTP-header, keywords: http_header, http_raw_header User-Agent (part of HTTP-header), keyword: http_user_agent
Cookie: PREF=ID=efe36c63a3bfa6a4;U=aa0cf39996084d7e;TM=1252314621;LM=1292956821;GM=1:S=dYtecyNBioerA47b	HTTP-cookie, keyword: http_cookie

Response:

HTTP/1.1 302 Found	HTTP-version HTTP-response code, keyword: http_stat_code HTTP-response message, keyword: http_stat_msg
Location: http://www.google.nl/ Cache-Control: private Content-Type: text/html; charset=UTF-8 Set-Cookie: PREF=ID=efe36c63a3bfa6a4:FF =0:TM=1252314621:LM=129310 4406:GM=1:S=xeKylabZkPrZEk N; expires=Sat, 22-Dec-2012 11:40:06 GMT; path=/; domain=.google.com Date: Thu, 23 Dec 2010 11:40:06 GMT Server: gws Content-Length: 218 X-XSS-Protection: 1; mode=block	HTTP-header, keywords: http_header, http_raw_header
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8"> <TITLE>302 Moved</TITLE></HEAD><BODY> <H1>302 Moved</H1> The document has moved here. </BODY></HTML>	HTTP-response body, keywords: file_data, http_server_body

Request:

POST / HTTP/1.0	HTTP-method, keyword: http_method HTTP-uri, keywords: http_uri or http_raw_uri HTTP-version
Accept: */* Accept-Language: en-US x-flash-version: 9,0,115,0 Content-Type: application/x-www-form-urlencoded Content-Length: 31 Accept-Encoding: bbbbbbbbbblate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Host: nowhereasdfasdf.com Connection: Keep-Alive Cache-Control: no-cache	HTTP-header, keywords: http_header, http_raw_header
type=playerStart&position=tidal	HTTP-client body, keyword: http_client_body

9.12.2 *http.method*

With the `http.method` content modifier, it is possible to match specifically and only on the HTTP method buffer.

PAYLOAD

/index.html HTTP/1.0\r\n

content:"**GET**";



content:"**GET**"; http_method



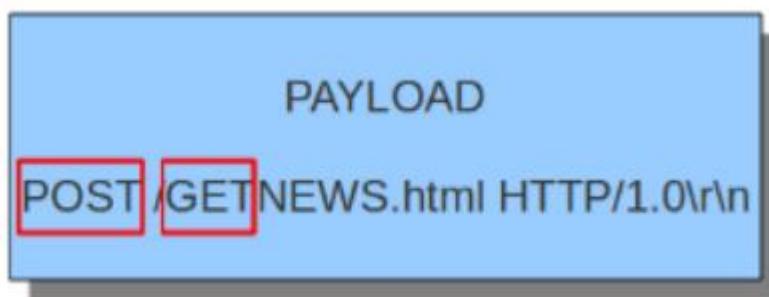
GET / HTTP/1.1

Host: www.google.com

Connection: keep-alive

Accept:

application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5



content:"**GET**"; ✓

content:"GET"; http_method ✗

content:"**POST**"; http_method ✓

9.12.3 *http.uri* and *http.uri.raw*

With the *http.uri* and the *http.uri.raw* content modifiers, it is possible to match specifically and only on the request URI buffer.

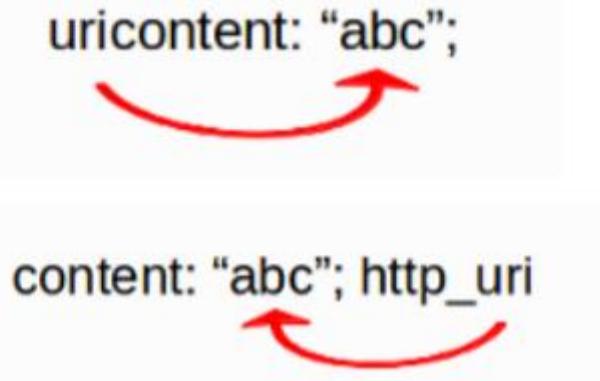
GET /**index.html** HTTP/1.0\r\n



content: "/index.html"; http_uri;	✓
content: "GET"; http_uri;	✗
content: "/index"; http_uri; content: ".html"; http_uri; within:5;	✓
content: "/index"; http_uri; depth:6;	✓

9.12.4 uricontent

This keyword is like http.uri.



```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Vundo Trojan  
Variant reporting to Controller"; flow:established,to_server; content:"POST "; depth:5;  
uricontent:"/frame.html?"; urilen:>80; classtype:trojan-activity;  
reference:url,doc.emergingthreats.net/2009173; reference:url,www.emergingthreats.net/cgi-  
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2009173; rev:2;)
```

9.12.5 urilen

The urilen keyword is used to match on the length of the request URI.

```
urilen:3;
```

```
urilen:1;
```

```
urilen:>1;
```

```
urilen:<>20; (bigger than 10, smaller than 20)
```



urilen:10;	✓
urilen:<10;	✗
urilen:5<>20;	✓
urilen:20;	✗
urilen:>4;	✓

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Possible Vundo Trojan Variant reporting to Controller"; flow:established,to_server; content:"POST "; depth:5; uricontent:"/frame.html?"; urilen:>80; classtype:trojan-activity; reference:url,doc.emergingthreats.net/2009173; reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Vundo; sid:2009173; rev:2;)
```

9.12.6 http.protocol

The http.protocol inspects the protocol field from the HTTP request or response line.

```
alert http any any -> any any (flow:to_server; http.protocol; content:"HTTP/1.0";sid:1;)
```

9.12.7 http.request_line

The http.request_line forces the whole HTTP request line to be inspected.

```
alert http any any -> any any (http.request_line; content:"GET / HTTP/1.0"; sid:1;)
```

9.12.8 http.header and http.header.raw

With the http.header content modifier, it is possible to match specifically and only on the HTTP header buffer.

header in a HTTP request:

```
GET / HTTP/1.1
Host: www.google.com
Connection: keep-alive
Accept:
application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
```

Purpose of http.header:



content:"www.google.com"; http_header ; ✓

content:"GET"; http_header; X



9.12.9 http.cookie

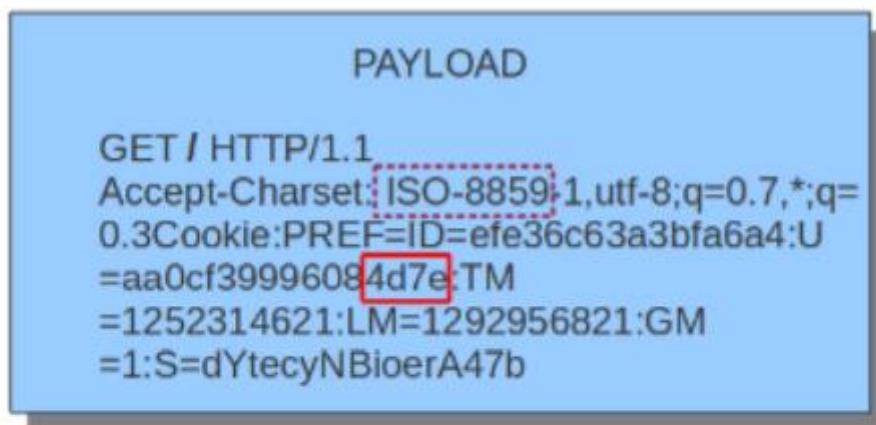
With the http.cookie content modifier, it is possible to match specifically and only on the cookie buffer.

Cookie in a http request:

```

User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US)
AppleWebKit/534.16
(KHTML, like Gecko) Ubuntu/10.10 Chromium/10.0.618.0
Chrome/10.0.618.0
Safari/534.16
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie:
PREF=ID=efe36c63a3bfa6a4:U=aa0cf39996084d7e:TM
=1252314621:L.M=1292956821:GM=1:S=dYtecyNBioer
A47b
  
```

Purpose of http.cookie:



content:"4d7e"; http_uri; ✓

content:"ISO-8859"; http_uri; ✗

content:"4d7e"; http_cookie; depth: 13; ✗

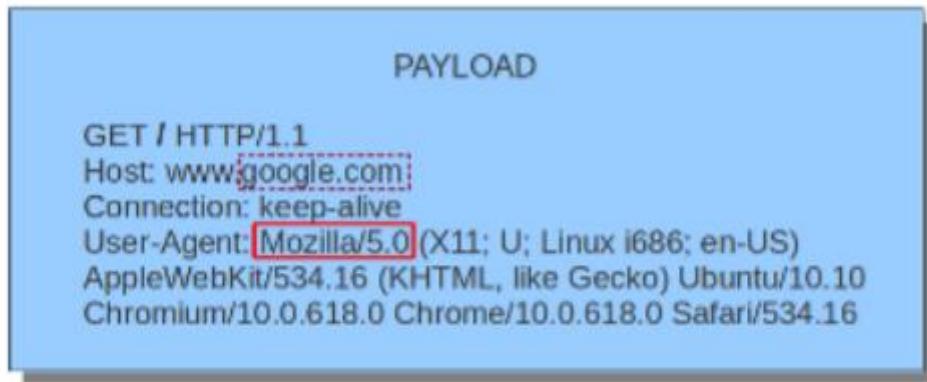
9.12.10 http.user_agent

The http.user_agent content modifier is part of the HTTP request header. It makes it possible to match specifically on the value of the User-Agent header.

User-Agent header in a http request:

```
GET / HTTP/1.1
Host: www.google.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US)
AppleWebKit/534.16
(KHTML, like Gecko) Ubuntu/10.10
Chromium/10.0.618.0 Chrome/10.0.618.0
Safari/534.16
```

Purpose of http.user_agent:



content:"Mozilla/5.0"; http_user_agent; ✓

content:"google.com"; http_user_agent; ✗

9.12.11 http.accept

Sticky buffer to match on the HTTP Accept header.

```
alert http any any -> any any (http.accept; content:"image/gif"; sid:1;)
```

9.12.12 http.accept_enc

Sticky buffer to match on the HTTP Accept-Encoding header

```
alert http any any -> any any (http.accept_enc; content:"gzip"; sid:1;)
```

9.12.13 http.accept_lang

Sticky buffer to match on the HTTP Accept-Language header.

```
alert http any any -> any any (http.accept_lang; content:"en-us"; sid:1;)
```

9.12.14 http.connection

```
alert http any any -> any any (http.connection; content:"keep-alive"; sid:1;)
```

9.12.15 http.content_type

Sticky buffer to match on the HTTP Content-Type headers.

```
alert http any any -> any any (flow:to_server; \
    http.content_type; content:"x-www-form-urlencoded"; sid:1;)
```

```
alert http any any -> any any (flow:to_client; \
    http.content_type; content:"text/javascript"; sid:2;)
```

9.12.16 http.content_len

Sticky buffer to match on the HTTP Content-Length headers.

```
alert http any any -> any any (flow:to_server; \
    http.content_len; content:"666"; sid:1;)
```

```
alert http any any -> any any (flow:to_client; \
    http.content_len; content:"555"; sid:2;)
```

```
alert http any any -> any any (flow:to_client; \
    http.content_len; byte_test:0,>=,8079,0,string,dec; sid:3;)
```

9.12.17 http.referer

Sticky buffer to match on the HTTP Referer header.

```
alert http any any -> any any (http.referer; content:".php"; sid:1;)
```

9.12.18 http.start

```
alert http any any -> any any (http.start; content:"HTTP/1.1|0d 0a|User-Agent"; sid:1; )
```

9.12.19 http.header_names

Inspect a buffer only containing the names of the HTTP headers.

```
alert http any any -> any any (http.header_names; content:"|0d 0a|Host|0d 0a|"; sid:1; )
```

make sure only Host is present:

```
alert http any any -> any any (http.header_names; \  
content:"|0d 0a|Host|0d 0a 0d 0a|"; sid:1;)
```

make sure User-Agent is directly after Host:

```
alert http any any -> any any (http.header_names; \  
content:"|0d 0a|Host|0d 0a|User-Agent|0d 0a|"; sid:1;)
```

9.12.20 http.request_body

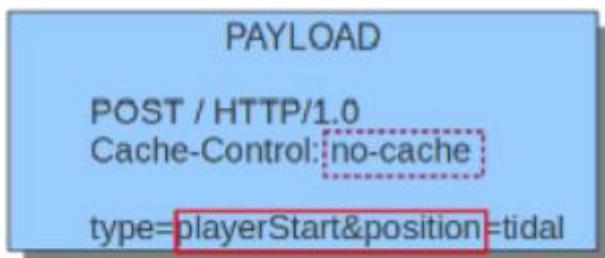
With the `http.request_body` content modifier, it is possible to match specifically and only on the HTTP request body.

http.request_body in a HTTP request:

```
Host: nowhereasdfasdf.com  
Connection: Keep-Alive  
Cache-Control: no-cache
```

type=playerStart&position=tidal

purpose of http.client_body:



- | | |
|---|---|
| content:"playerStart&position"; http_client_body; | ✓ |
| content:"no-cache"; http_client_body; | ✗ |
| content:"playerStart"; depth: 16; http_client_body; | ✓ |
| content:"playerStart"; http_client_body;
content:"&position"; distance:0; within:9 | ✓ |

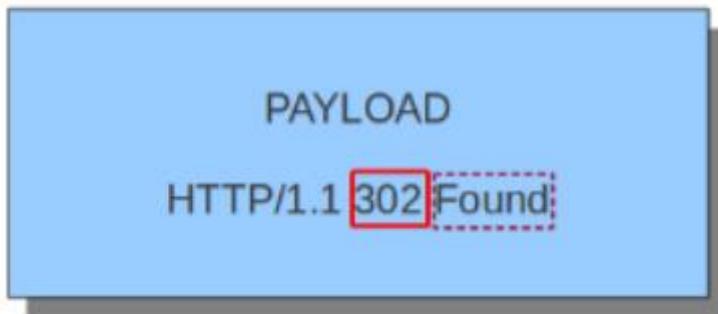
9.12.21 http.stat_code

With the http.stat_code content modifier, it is possible to match specifically and only on the HTTP status code buffer.

http.stat_code in a HTTP response:

HTTP/1.1 302 Found

purpose of http.stat_code:



- | | |
|---|---|
| content:"302"; http_stat_code; | ✓ |
| content:"found"; http_stat_code; | ✗ |
| content:"302"; http_stat_code; depth:5; | ✓ |

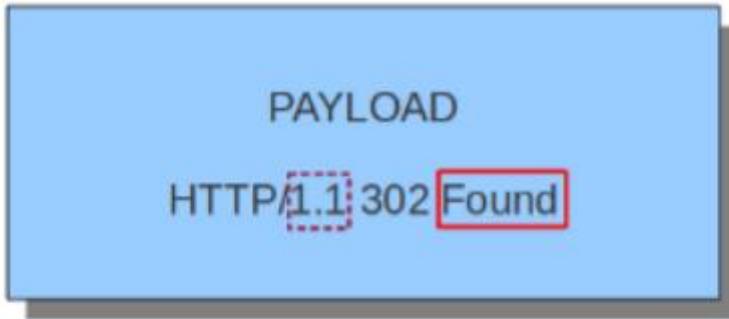
9.12.22 http.stat_msg

With the http.stat_msg content modifier, it is possible to match specifically and only on the HTTP status message buffer.

http.stat_msg in a HTTP response:

HTTP/1.1 302 **Found**

purpose of http.stat_msg:



content:"**Found**"; http_stat_msg;

content:"**1.1**"; http_stat_msg;

content:"**found**"; http_stat_msg; nocase;

9.12.23 http.response_line

The http.response_line forces the whole HTTP response line to be inspected.

```
alert http any any -> any any (http.response_line; content:"HTTP/1.0 200 OK"; sid:1;)
```

9.12.24 http.response_body

With the http.response_body content modifier, it is possible to match specifically and only on the HTTP response body.

9.12.25 http.server

Sticky buffer to match on the HTTP Server headers

```
alert http any any -> any any (flow:to_client; \
    http.server; content:"Microsoft-IIS/6.0"; sid:1;)
```

9.12.26 http.location

Sticky buffer to match on the HTTP Location headers.

```
alert http any any -> any any (flow:to_client; \
    http.location; content: "http://www.google.com"; sid:1;)
```

9.12.27 http.host and http.host.raw

With the http.host content modifier, it is possible to match specifically and only the normalized hostname. The http.host.raw inspects the raw hostname

Example request:

GET /test.html

HTTP/1.1

Host: ABC.com

Accept: */* Host: efg.net

http.host buffer contents:

abc.com, efg.net

http.host.raw buffer contents:

ABC.com, efg.net

9.12.28 file_data

With file_data, the HTTP response body is inspected, just like with http.response_body.

```
alert http any any -> any any (file_data; content:"abc"; content:"xyz");
```

9.13 File Keywords

9.13.1 filename

Matches on the file name.

```
filename:<string>;
```

```
filename:"secret";
```

9.13.2 fileext

Matches on the extension of a file name.

```
fileext:<string>;
```

```
fileext:"jpg";
```

9.13.3 *filemagic*

Matches on the information libmagic returns about a file.

```
filemagic:<string>;
```

```
filemagic:"executable for MS Windows";
```

9.13.4 *filestore*

Stores files to disk if the signature matched.

```
filestore:<direction>,<scope>;
```

direction can be:

- **request/to_server:** store a file in the request / to_server direction
- **response/to_client:** store a file in the response / to_client direction
- **both:** store both directions

scope can be:

- **file:** only store the matching file (for filename,fileext,filemagic matches)
- **tx:** store all files from the matching HTTP transaction
- **ssn/flow:** store all files from the TCP session/flow.

9.13.5 *filesize*

Match on the size of the file as it is being transferred.

```
filesize:<value>;
```

```
filesize:100; # exactly 100 bytes
```

```
filesize:100<>200; # greater than 100 and smaller than 200
```

```
filesize:>100MB; # greater than 100 megabytes
```

```
filesize: <100MB; # smaller than 100 megabytes
```

9.14 DNS Keywords

These ones make sure the signature checks a specific part of the network-traffic.

9.14.1 dns.opcode

This keyword matches on the opcode found in the DNS header flags.

```
dns.opcode:[!]<number>
```

```
dns.opcode:4;
```

```
dns.opcode:!0;
```

9.14.2 dns.query

With dns.query the DNS request queries are inspected.

```
alert dns any any any -> any any (msg:"Test dns.query option"; dns.query; content:"google"; nocase; sid:1;)
```

9.15 SSL/TLS Keywords

9.15.1 *tls.cert_subject*

Match TLS/SSL certificate Subject field.

```
tls.cert_subject; content:"CN=*.googleusercontent.com"; isdataat:!1,relative;
```

```
tls.cert_subject; content:"google.com"; nocase; pcre:"/google.com$/";
```

- *tls.cert_subject* is a ‘sticky buffer’.
- *tls.cert_subject* can be used as *fast_pattern*.

9.15.2 *tls.cert_issuer*

Match TLS/SSL certificate Issuer field.

```
tls.cert_issuer; content:"WoSign"; nocase; isdataat:!1,relative;
```

```
tls.cert_issuer; content:"StartCom"; nocase; pcre:"/StartCom$/";
```

- *tls.cert_issuer* is a ‘sticky buffer’.
- *tls.cert_issuer* can be used as *fast_pattern*

9.15.3 `tls.cert_serial`

Match on the serial number in a certificate.

```
alert tls any any -> any any (msg:"match cert serial"; \
    tls.cert_serial; content:"5C:19:B7:B1:32:3B:1C:A1"; sid:200012;)
```

- `tls.cert_serial` is a ‘sticky buffer’.
- `tls.cert_serial` can be used as `fast_pattern`.

9.15.4 `tls.cert_fingerprint`

Match on the SHA-1 fingerprint of the certificate.

```
alert tls any any -> any any (msg:"match cert fingerprint"; \
    tls.cert_fingerprint; \
    content:"4a:a3:66:76:82:cb:6b:23:bb:c3:58:47:23:a4:63:a7:78:a4:a1:18"; \
    sid:200023;)
```

- `tls.cert_fingerprint` is a ‘sticky buffer’.
- `tls.cert_fingerprint` can be used as `fast_pattern`.

9.15.5 `tls.sni`

Match TLS/SSL Server Name Indication field.

```
tls.sni; content:"oisf.net"; nocase; isdataat:!1,relative;
```

```
tls.sni; content:"oisf.net"; nocase; pcre:"/oisf.net$/";
```

- `tls.sni` is a ‘sticky buffer’.
- `tls.sni` can be used as `fast_pattern`.

9.15.6 `tls_cert_notbefore`

Match on the `NotBefore` field in a certificate.

```
alert tls any any -> any any (msg:"match cert NotBefore"; \
    tls_cert_notbefore:1998-05-01<>2008-05-01; sid:200005;)
```

9.15.7 `tls_cert_notafter`

Match on the `NotAfter` field in a certificate.

```
alert tls any any -> any any (msg:"match cert NotAfter"; \
    tls_cert_notafter:>2015; sid:200006;)
```

9.15.8 `tls_cert_expired`

Match returns true if certificate is expired.

```
tls_cert_expired;
```

9.15.9 `tls_cert_valid`

Match returns true if certificate is not expired.

```
tls_cert_valid;
```

9.15.10 *tls.certs*

Do a “raw” match on each of the certificates in the TLS certificate chain.

```
alert tls any any -> any any (msg:"match bytes in TLS cert"; tls.certs; \
content:"|06 09 2a 86|"; sid:200070;)
```

- *tls.certs* is a ‘sticky buffer’.
- *tls.certs* can be used as *fast_pattern*.

9.15.11 *tls.version*

Match on negotiated TLS/SSL version.

```
tls.version:1.2;
```

```
tls.version:0x7f12;
```

9.15.12 *ssl_version*

Match version of SSL/TLS record.

```
alert tls any any -> any any (msg:"match TLSv1.2"; \
ssl_version:tls1.2; sid:200030;)
```

```
alert tls any any -> any any (msg:"match SSLv2 and SSLv3"; \
ssl_version:sslv2,sslv3; sid:200031;)
```

*9.15.13 **tls.subject***

Match TLS/SSL certificate Subject field.

```
tls.subject:"CN=*.googleusercontent.com"
```

*9.15.14 **tls.issuerdn***

match TLS/SSL certificate IssuerDN field.

```
tls.issuerdn:!"CN=Google-Internet-Authority"
```

*9.15.15 **tls.fingerprint***

match TLS/SSL certificate SHA1 fingerprint.

```
tls.fingerprint:!"f3:40:21:48:70:2c:31:bc:b5:aa:22:ad:63:d6:bc:2e:b3:46:e2:5a"
```

*9.15.16 **tls.store store***

TLS/SSL certificate on disk

9.15.17 *ssl_state*

The *ssl_state* keyword matches the state of the SSL connection.

9.16 SSH Keywords

9.16.1 *ssh.proto*

Match on the version of the SSH protocol used.

```
alert ssh any any -> any any (msg:"match SSH protocol version"; ssh.proto; content:"2.0"; sid:1000010;)
```

9.16.2 *ssh.software*

Match on the software string from the SSH banner

```
alert ssh any any -> any any (msg:"match SSH software string"; ssh.software; content:"openssh"; nocase; sid:1000020;)
```

9.16.3 *ssh.protoversion*

Matches on the version of the SSH protocol used

```
alert ssh any any -> any any (msg:"SSH v2 compatible"; ssh.protoversion:2_compat; sid:1;)
```

```
alert ssh any any -> any any (msg:"SSH v1.10"; ssh.protoversion:1.10; sid:1;)
```

9.16.4 ssh.softwareversion

Matches on the software string from the SSH banner.

```
alert ssh any any -> any any (msg:"match SSH software string"; ssh.softwareversion:"OpenSSH"; sid:10000040);
```

9.16.5 ssh.hassh

Match on hassh(client)

```
alert ssh any any -> any any (msg:"match hassh"; \  
    ssh.hassh; content:"ec7378c1a92f5a8dde7e8b7a1ddf33d1"; \  
    sid:1000010);
```

- ssh.hassh is a ‘sticky buffer’.
- ssh.hassh can be used as fast_pattern.

9.16.6 ssh.hassh.string

Match on Hassh string

```
alert ssh any any -> any any (msg:"match hassh-string"; \  
    ssh.hassh.string; content:"none,zlib@openssh.com,zlib"; \  
    sid:1000030);
```

- ssh.hassh.string is a ‘sticky buffer’.
- ssh.hassh.string can be used as fast_pattern.

9.16.7 ssh.hassh.server

Match on hassh(server)

```
alert ssh any any -> any any (msg:"match SSH hash-server"; \
ssh.hassh.server; content:"b12d2871a1189eff20364cf5333619ee"; \
sid:1000020);
```

- ssh.hassh.server is a ‘sticky buffer’.
- ssh.hassh.server can be used as fast_pattern.

9.16.8 ssh.hassh.server.string

Match on hassh string

```
alert ssh any any -> any any (msg:"match SSH hash-server-string"; ssh.hassh.server.string;
content:"umac-64-etm@openssh.com,umac-128-etm@openssh.com"; sid:1000040);
```

- ssh.hassh.server.string is a ‘sticky buffer’.
- ssh.hassh.server.string can be used as fast_pattern.

9.17 SIP Keywords

The SIP keywords are implemented as sticky buffers and can be used to match on fields in SIP messages.

Keyword	Direction
sip.method	Request
sip.uri	Request
sip.request_line	Request
sip.stat_code	Response
sip.stat_msg	Response
sip.response_line	Response
sip.protocol	Both

9.17.1 sip.method

This keyword matches on the method found in a SIP request.

```
sip.method; content:<method>;
```

Examples of methods are:

- INVITE
- BYE
- REGISTER
- CANCEL
- ACK
- OPTIONS

```
sip.method; content:"INVITE";
```

9.17.2 sip.uri

This keyword matches on the uri found in a SIP request

```
sip.uri; content:<uri>;
```

```
sip.uri; content:"sip:sip.url.org";
```

9.17.3 sip.request_line

This keyword forces the whole SIP request line to be inspected.

```
sip.request_line; content:<request_line>;
```

```
sip.request_line; content:"REGISTER sip:sip.url.org SIP/2.0"
```

9.17.4 sip.stat_code

This keyword matches on the status code found in a SIP response.

```
sip.stat_code; content<stat_msg>
```

```
sip.stat_msg; content:"Trying";
```

9.17.5 sip.response_line

This keyword forces the whole SIP response line to be inspected.

```
sip.response_line; content:<response_line>;
```

```
sip.response_line; content:"SIP/2.0 100 OK"
```

9.17.6 *sip.protocol*

This keyword matches the protocol field from a SIP request or response line.

```
sip.protocol; content:<protocol>
```

```
sip.protocol; content:"SIP/2.0"
```

9.18 RFB Keywords

The rfb.name and rfb.sectype keywords can be used for matching on various properties of RFB (Remote Framebuffer, i.e. VNC) handshakes.

9.18.1 *rfb.name*

Match on the value of the RFB desktop name field.

```
rfb.name; content:"Alice's desktop";
```

```
rfb.name; pcre:"/. * \screen [0-9]\$/";
```

- rfb.name is a ‘sticky buffer’.
- rfb.name can be used as fast_pattern

9.18.2 *rfb.secresult*

Match on the value of the RFB security result,

```
rfb.secresult: ok;
```

```
rfb.secresult: unknown;
```

9.18.3 *rfb.sectype*

Match on the value of the RFB security type field

```
rfb.sectype:2;
```

```
rfb.sectype:>=3;
```

9.19 MQTT Keywords

Various keywords can be used for matching on fields in fixed and variable headers of MQTT messages as well as payload values.

9.19.1 *mqtt.protocol_version*

Match on the value of the MQTT protocol version field in the fixed header.

```
mqtt.protocol_version:5;
```

9.19.2 *mqtt.type*

Match on the MQTT message type.

Valid values are :

- CONNECT
- CONNACK
- PUBLISH
- PUBACK
- PUBREC
- PUBREL
- PUBCOMP
- SUBSCRIBE
- SUBACK
- UNSUBSCRIBE
- UNSUBACK
- PINGREQ
- PINGRESP
- DISCONNECT
- AUTH
- UNASSIGNED

mqtt.type:CONNECT;

mqtt.type:PUBLISH;

9.19.3 mqtt.flags

Match on a combination of MQTT header flags,

- **dup** (duplicate message)
- **retain** (message should be retained on the broker)

mqtt.flags:dup,!retain;

mqtt.flags:retain;

9.19.4 mqtt.qos

Match on the Quality of Service request code in the MQTT fixed header.

Valid values are:

- 0 (fire and forget)
- 1 (at least one delivery)
- 2 (exactly one delivery)

```
mqtt.qos:0;
```

```
mqtt.qos:2;
```

9.19.5 mqtt.connack.session_present

Match on the MQTT CONNACK session_present flag.

```
mqtt.CONNACK; mqtt.connack.session_present:true;
```

9.20 HTTP2 Keywords

9.20.1 http2.frametype

Match on the frame type present in a transaction.

```
http2.frametype:GOAWAY;
```

9.20.2 http2.errorcode

Match on the error code in a GOWAY or RST_STREAM frame

```
http2.errorcode: NO_ERROR;
```

```
http2.errorcode: INADEQUATE_SECURITY;
```

9.20.3 http2.priority

Match on the value of the HTTP2 priority field present in a PRIORITY or HEADERS frame

```
http2.priority:2;
```

```
http2.priority:>100;
```

```
http2.priority:32-64;
```

9.20.4 http2.window

Match on the value of the HTTP2 value field present in a WINDOWUPDATE frame.

```
http2.window:1;
```

```
http2.window:<100000;
```

9.20.5 http2.size_update

Match on the size of the HTTP2 Dynamic Headers Table

```
http2.size_update:1234;
```

```
http2.size_update:>4096;
```

9.20.6 http2.settings

Match on the name and value of a HTTP2 setting from a SETTINGS frame

```
http2.settings:SETTINGS_ENABLE_PUSH=0;
```

```
http2.settings:SETTINGS_HEADER_TABLE_SIZE>4096;
```

9.20.7 http2.header_name

Match on the name of a HTTP2 header from a HEADER frame

```
http2.header_name; content:"agent";
```

- http2.header_name is a ‘sticky buffer’.
- http2.header_name can be used as fast_pattern.

9.20.8 http2.header

Match on the name and value of a HTTP2 header from a HEADER frame

```
http2.header; content:"agent: nghttp2";
```

```
http2.header; content:"custom-header: I love::colons";
```

- http2.header is a ‘sticky buffer’.
- http2.header can be used as fast_pattern.

9.21 Generic App Layer Keywords

9.21.1 *app-layer-protocol*

Match on the detected app-layer protocol.

```
app-layer-protocol:ssh;
```

```
app-layer-protocol:!tls;
```

```
app-layer-protocol:failed;
```

9.21.2 *app-layer-event*

Match on events generated by the App Layer Parsers and the protocol detection engine.

```
app-layer-event:applayer_mismatch_protocol_both_directions;
```

```
app-layer-event:http.gzip_decompression_failed;
```

9.22 IP Reputation Keyword

9.22.1 iprep

The iprep directive matches on the IP reputation information for a host.

```
alert ip $HOME_NET any -> any any (msg:"IPREP internal host talking to CnC server"; flow:to_server;  
iprep:dst,CnC,>,30; sid:1; rev:1;)
```

Testing Suricata with Basic Rules

Example 1:

```
kali@kali:~$ cd /etc/suricata
kali@kali:/etc/suricata$ ls -lh
total 164K
-rw-r--r-- 1 root root 4.2K Aug  5 14:25 classification.config
-rw-r--r-- 1 root root 1.4K Aug  5 14:25 reference.config
drwxr-xr-x 2 root root 4.0K Aug 10 16:26 rules
-rw-r--r-- 1 root root 69K Apr 29 03:34 suricata.yaml
-rw-r--r-- 1 root root 69K Aug  8 08:34 suricata.yaml.dpkg-old
-rw-r--r-- 1 root root 1.7K Apr 28 06:06 threshold.config
kali@kali:/etc/suricata$ cd rules
kali@kali:/etc/suricata/rules$ ls
3coresec.rules           emerging-ftp.rules          emerging-tftp.rules
app-layer-events.rules   emerging-games.rules       emerging-trojan.rules
botcc.portgrouped.rules  emerging-icmp_info.rules  emerging-user_agents.rules
botcc.rules               emerging-icmp.rules        emerging-voip.rules
BSD-License.txt           emerging-imap.rules       emerging-web_client.rules
ciarmy.rules              emerging-inappropriate.rules emerging-web_server.rules
classification.config     emerging-info.rules       emerging-web_specific_apps.rules
compromised-ips.txt      emerging-malware.rules    emerging-worm.rules
compromised.rules         emerging-misc.rules       files.rules
decoder-events.rules     emerging-mobile_malware.rules gpl-2.0.txt
dhcp-events.rules         emerging-netbios.rules    http-events.rules
dnp3-events.rules         emerging-p2p.rules        ipsec-events.rules
dns-events.rules          emerging-policy.rules    kerberos-events.rules
drop.rules                emerging-pop3.rules      modbus-events.rules
dshield.rules              emerging-rpc.rules       nfs-events.rules
emerging-activex.rules   emerging-scada.rules     ntp-events.rules
emerging-attack_response.rules emerging-scan.rules     sid-msg.map
emerging-chat.rules        emerging-scan.rules.save smb-events.rules
emerging-current_events.rules emerging-shellcode.rules smtp-events.rules
emerging-deleted.rules    emerging-smtp.rules      stream-events.rules
emerging-dns.rules         emerging-snmp.rules      suricata-4.0-enhanced-open.txt
emerging-dos.rules         emerging-sql.rules       tls-events.rules
emerging-exploit.rules    emerging-telnet.rules    tor.rules
```

```
kali@kali:/etc/suricata/rules$ sudo nano emerging-activex.rules
```

```
cat *.rules | grep alert | wc -l
```

How many rules are available in default install.

```
kali@kali:/etc/suricata/rules$ cat *.rules | grep alert | wc -l
30040
```

```
kali㉿kali:/etc/suricata/rules$ cd ..
kali㉿kali:/etc/suricata$ ls
classification.config reference.config rules suricata.yaml suricata.yaml.pkg-old threshold.config
kali㉿kali:/etc/suricata$ sudo nano suricata.yaml
```

```
address-groups:
  HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
  #HOME_NET: "[192.168.0.0/16]"
```

```
rule-files:
  - suricata.rules
  - test.rules
```

add test.rules to suricata.yaml to apply when new rules are added

```
kali㉿kali:~$ sudo ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            ENI valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                ENI valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:ac:84:38 brd ff:ff:ff:ff:ff:ff
        inet 192.168.40.135/24 brd 192.168.40.255 scope global dynamic eth0
            ENI valid_lft 1120sec preferred_lft 1120sec
            inet6 fe80::20c:29ff:feac:8438/64 scope link
                ENI valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:ac:84:42 brd ff:ff:ff:ff:ff:ff
```

Here must be its own internal network (private).

```
address-groups:
  HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12,192.168.40.135/24]"
  #HOME_NET: "[192.168.0.0/16]"
```

It shows in which modes the suricata is operating.

```
kali㉿kali:/etc/suricata$ suricata --list-runmodes
```

RunMode Type	Custom Mode	Runmodes
PCAP_DEV	single	Single threaded pcap live mode
	autofp	Multi threaded pcap live mode. Packets from each flow are assigned to a single detect thread, unlike "pcap_live_auto" where packets from the same flow can be processed by any detect thread
	workers	Workers pcap live mode, each thread does all tasks from acquisition to logging
PCAP_FILE	single	Single threaded pcap file mode
	autofp	Multi threaded pcap file mode. Packets from each flow are assigned to a single detect thread, unlike "pcap-file-auto" where packets from the same flow can be processed by any detect thread
PFRING(DISABLED)	autofp	Multi threaded pfring mode. Packets from each flow are assigned to a single detect thread, unlike "pfring-auto" where packets from the same flow can be processed by any detect thread
	single	Single threaded pfring mode
	workers	Workers pfring mode, each thread does all tasks from acquisition to logging
NFQ	autofp	Multi threaded NFQ IPS mode with respect to flow
	single	Multi queue NFQ IPS mode with one thread per queue
	workers	Multi queue NFQ IPS mode with one thread per queue
NFLOG	autofp	Multi threaded nflog mode
	single	Single threaded nflog mode
	workers	Workers nflog mode
IPFW	autofp	Multi threaded IPFW IPS mode with respect to flow
	single	Multi queue IPFW IPS mode with one thread per queue
	workers	Multi queue IPFW IPS mode with one thread per queue
ERF_FILE	single	Single threaded ERF file mode
	autofp	Multi threaded ERF file mode. Packets from each flow are assigned to a single detect thread
ERF_DAG	autofp	Multi threaded DAG mode. Packets from each flow are assigned to a single detect thread, unlike "dag_auto" where packets from the same flow can be processed by any detect thread
	single	Singled threaded DAG mode
	workers	Workers DAG mode, each thread does all tasks from acquisition to logging
AF_PACKET_DEV	single	Single threaded af-packet mode
	workers	Workers af-packet mode, each thread does all tasks from acquisition to logging
	autofp	Multi socket AF_PACKET mode. Packets from each flow are assigned to a single detect thread.
NETMAP(DISABLED)	single	Single threaded netmap mode
	workers	Workers netmap mode, each thread does all tasks from acquisition to logging

Adding rules to test.rules

```
kali㉿kali:/etc/suricata/rules$ sudo nano test.rules
```

```
alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
```

```
GNU nano 4.9.2                                         test.rules                         Modified
alert icmp any any → $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
```

```
ethtool -K eth0 gro off lro off
```

```
kali@kali:/etc/suricata/rules$ sudo ethtool -K eth0 gro off lro off
Cannot change large-receive-offload
```

```
suricata -i eth0 --init-errors-fatal
```

```
kali@kali:/etc/suricata/rules$ sudo suricata -i eth0 --init-errors-fatal
```

(suricata.yaml)

```
23/8/2020 -- 10:22:21 - <Notice> - This is Suricata version 5.0.3 RELEASE running in SYSTEM mode
23/8/2020 -- 10:22:22 - <Warning> - [ERRCODE: SC_ERR_NO_RULES(42)] - No rule files match the pattern /etc/suricata/rules/suricata.rules
```

```
rule-files:
# - suricata.rules
- test.rules
```

Fix the error and continue.

```
23/8/2020 -- 13:38:44 - <Notice> - This is Suricata version 5.0.3 RELEASE running in SYSTEM mode
23/8/2020 -- 13:38:45 - <Notice> - all 4 packet processing threads, 4 management threads initialized, engine started.
^C23/8/2020 -- 13:39:43 - <Notice> - Signal Received. Stopping engine.
23/8/2020 -- 13:39:44 - <Notice> - Stats for 'eth0': pkts: 0, drop: 0 (-nan%), invalid checksum: 0
```

To see what is happening:

```
ps aux | grep ssh
```

```
kali@kali:/etc/suricata/rules$ sudo ps aux | grep ssh
kali    ine 1665  0.0  0.0  5892 5432 ? 09:56 Ss   0:00 /usr/bin/ssh-agent x-session-manager
kali    eth12470 0.0  0.0  6080 832 pts/0 13:40  0:00 grep ssh
```

We are also looking at effects by sending a ping from another device.

```
kali@kali:~$ sudo ping 10.20.15
[sudo] password for kali:
PING 10.20.15 (10.20.0.15) 56(84) bytes of data.
^C
--- 10.20.15 ping statistics ---
36 packets transmitted, 0 received, 100% packet loss, time 35834ms
```

```
kali@kali:/var/log$ cd /var/log/suricata
kali@kali:/var/log/suricata$
```

```
ping google.com
```

```
kali@kali:/var/log/suricata$ ping google.com 255.0 broadcast 192.168.40.255
PING google.com (172.217.169.174) 56(84) bytes of data.
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=1 ttl=128 time=38.2 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=2 ttl=128 time=38.9 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=3 ttl=128 time=41.4 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=4 ttl=128 time=39.2 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=5 ttl=128 time=38.2 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=6 ttl=128 time=40.4 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=7 ttl=128 time=39.5 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=8 ttl=128 time=39.5 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=9 ttl=128 time=42.1 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=10 ttl=128 time=39.8 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=11 ttl=128 time=39.3 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=12 ttl=128 time=38.5 ms
64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=13 ttl=128 time=83.3 ms
^X64 bytes from sof02s33-in-f14.1e100.net (172.217.169.174): icmp_seq=14 ttl=128 time=40.6 ms
Flags=73<UP,LOOPBACK,RUNNING> mtu 65536
^C      inet 127.0.0.1 netmask 255.0.0.0
--- google.com ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13051ms
rtt min/avg/max/mdev = 38.172/42.769/83.251/11.280 ms
```

Examining the logs:

```
kali㉿kali:/var/log/suricata$ cat suricata.log
```

```
23/8/2020 -- 13:37:52 - <Warning> - [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - 1 rule files specified, but no rule was loaded at all!
23/8/2020 -- 13:37:52 - <Error> - [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - Loading signatures failed.
23/8/2020 -- 13:38:44 - <Notice> - This is Suricata version 5.0.3 RELEASE running in SYSTEM mode
23/8/2020 -- 13:38:44 - <Info> - CPUs/cores online: 4
23/8/2020 -- 13:38:45 - <Info> - Found an MTU of 1500 for 'eth0'
23/8/2020 -- 13:38:45 - <Info> - Found an MTU of 1500 for 'eth0'
23/8/2020 -- 13:38:45 - <Info> - fast output device (regular) initialized: fast.log
23/8/2020 -- 13:38:45 - <Info> - eve-log output device (regular) initialized: eve.json
23/8/2020 -- 13:38:45 - <Info> - stats output device (regular) initialized: stats.log
23/8/2020 -- 13:38:45 - <Info> - 1 rule files processed. 1 rules successfully loaded, 0 rules failed
23/8/2020 -- 13:38:45 - <Info> - Threshold config parsed: 0 rule(s) found
23/8/2020 -- 13:38:45 - <Info> - 1 signatures processed. 1 are IP-only rules, 0 are inspecting packet payload, 0 inspect application layer, 0 are decoder event only
23/8/2020 -- 13:38:45 - <Info> - Going to use 4 thread(s)
23/8/2020 -- 13:38:45 - <Info> - Using unix socket file '/var/run/suricata-command.socket'
23/8/2020 -- 13:38:45 - <Notice> - All 4 packet processing threads, 4 management threads initialized, engine started.
23/8/2020 -- 13:39:43 - <Notice> - Signal Received. Stopping engine.
23/8/2020 -- 13:39:43 - <Info> - time elapsed 58.525s
23/8/2020 -- 13:39:44 - <Info> - Alerts: 0
23/8/2020 -- 13:39:44 - <Info> - cleaning up signature grouping structure ... complete
23/8/2020 -- 13:39:44 - <Notice> - Stats for 'eth0': pkts: 0, drop: 0 (-nan%), invalid checksum: 0 000
23/8/2020 -- 13:47:36 - <Notice> - This is Suricata version 5.0.3 RELEASE running in SYSTEM mode
23/8/2020 -- 13:47:36 - <Info> - CPUs/cores online: 4
23/8/2020 -- 13:47:36 - <Info> - Found an MTU of 1500 for 'eth0'
23/8/2020 -- 13:47:36 - <Info> - Found an MTU of 1500 for 'eth0'
23/8/2020 -- 13:47:36 - <Info> - fast output device (regular) initialized: fast.log
23/8/2020 -- 13:47:36 - <Info> - eve-log output device (regular) initialized: eve.json null qm 1000
23/8/2020 -- 13:47:36 - <Info> - stats output device (regular) initialized: stats.log
23/8/2020 -- 13:47:36 - <Info> - 1 rule files processed. 1 rules successfully loaded, 0 rules failed
23/8/2020 -- 13:47:36 - <Info> - Threshold config parsed: 0 rule(s) found
23/8/2020 -- 13:47:36 - <Info> - 1 signatures processed. 1 are IP-only rules, 0 are inspecting packet payload, 0 inspect application layer, 0 are decoder event only
23/8/2020 -- 13:47:36 - <Info> - Going to use 4 thread(s)
23/8/2020 -- 13:47:36 - <Info> - Using unix socket file '/var/run/suricata-command.socket'
23/8/2020 -- 13:47:36 - <Notice> - All 4 packet processing threads, 4 management threads initialized, engine started.
23/8/2020 -- 13:47:39 - <Notice> - All AFP capture threads are running.
23/8/2020 -- 13:47:39 - <Notice> - Signal Received. Stopping engine.
23/8/2020 -- 13:47:39 - <Info> - time elapsed 3.476s
23/8/2020 -- 13:47:40 - <Info> - Alerts: 0
23/8/2020 -- 13:47:40 - <Info> - cleaning up signature grouping structure... complete
23/8/2020 -- 13:47:40 - <Notice> - Stats for 'eth0': pkts: 0, drop: 0 (-nan%), invalid checksum: 0
```

```
eve.json eve.json.1 fast.log fast.log.1
kali㉿kali:/var/log/suricata$ cat stats.log
```

Counter	TM Name	Value
flow.spare_d_lft	Total	10000
flow_mgr.rows_checked	Total	65536
flow_mgr.rows_skipped	Total	65536
tcp.memuse	Total	2293760
tcp.reassembly_memuse	Total	393216
flow.memuse	Total	7554304

Counter	TM Name	Value
flow.spare	Total	10000
flow_mgr.rows_checked	Total	65536
flow_mgr.rows_skipped	Total	65536
tcp.memuse	Total	2293760
tcp.reassembly_memuse	Total	393216
flow.memuse	Total	7554304

Example 2:

```
root@kali:~# cd /etc/suricata
root@kali:/etc/suricata# ls
classification.config reference.config rules suricata.yaml threshold.config
root@kali:/etc/suricata# cd rules
root@kali:/etc/suricata/rules# ls
app-layer-events.rules dns-events.rules kerberos-events.rules smb-events.rules
decoder-events.rules files.rules modbus-events.rules smtp-events.rules
dhcp-events.rules http-events.rules nfs-events.rules stream-events.rules
dnp3-events.rules ipsec-events.rules ntp-events.rules tls-events.rules
root@kali:/etc/suricata/rules# sudo nano local.rules
root@kali:/etc/suricata/rules#
```

```
alert http any any -> any any (msg:"Do not read gossip during work";
content:"Scarlett"; nocase; classtype:policy-violation; sid:1; rev:1;)
```

```
GNU nano 4.9.2                               local.rules
alert http any any → any any (msg:"Do not read gossip during work";
content:"Scarlett"; nocase; classtype:policy-violation; sid:1; rev:1;)
```

```
root@kali:/etc/suricata/rules# sudo nano /etc/suricata/suricata.yaml
```

```
default-rule-path: /etc/suricata/rules
rule-files:
  - local.rules
```

```
2020-08-29T15:27:56+00:00 [Notice] - all 2 packet processing threads, 4 management threads initialized, engine started.
^C2020-08-29T15:29:25+00:00 [Notice] - Signal Received. Stopping engine.
2020-08-29T15:29:26+00:00 [Notice] - Stats for 'eth2': pkts: 22, drop: 0 (0.00%), invalid checksum: 0
root@kali:/etc/suricata#
```

```
.v
29/8/2020 -- 15:32:45 - <Notice> - This is Suricata version 5.0.3 RELEASE running in SYSTEM mode
29/8/2020 -- 15:32:45 - <Info> - CPUs/cores online: 2
29/8/2020 -- 15:32:45 - <Info> - Found an MTU of 1500 for 'eth0'
29/8/2020 -- 15:32:45 - <Info> - Found an MTU of 1500 for 'eth0'
29/8/2020 -- 15:32:45 - <Info> - fast output device (regular) initialized: fast.log
29/8/2020 -- 15:32:45 - <Info> - eve-log output device (regular) initialized: eve.json
29/8/2020 -- 15:32:45 - <Info> - stats output device (regular) initialized: stats.log
29/8/2020 -- 15:32:45 - <Warning> - [ERRCODE: SC_ERR_INVALID_ARGUMENT(13)] - Invalid rule-files configuration section: expected a list of filenames.
29/8/2020 -- 15:32:45 - <Info> - No signatures supplied.
29/8/2020 -- 15:32:45 - <Info> - Going to use 2 thread(s)
29/8/2020 -- 15:32:45 - <Info> - Using unix socket file '/var/run/suricata-command.socket'
29/8/2020 -- 15:32:45 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
29/8/2020 -- 15:32:45 - <Info> - All AFP capture threads are running.
29/8/2020 -- 15:32:59 - <Notice> - Signal Received. Stopping engine.
29/8/2020 -- 15:32:59 - <Info> - time elapsed 13.837s
29/8/2020 -- 15:33:00 - <Info> - Alerts: 0
29/8/2020 -- 15:33:00 - <Info> - cleaning up signature grouping structure... complete
29/8/2020 -- 15:33:00 - <Notice> - Stats for 'eth0': pkts: 0, drop: 0 (-nan%), invalid checksum: 0
```

drop tcp \$HOME_NET any -> \$EXTERNAL_NET any (msg:"ET TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)



Action



Header



Rule options

CHAPTER 11

Suricata's Command Line Options

→ suricata -h

Display a brief usage overview.

root@kali:~# suricata -h

```
Suricata 5.0.3
USAGE: suricata [OPTIONS] [BPF FILTER]

-c <path>          : path to configuration file
-T                 : test configuration file (use with -c)
-i <dev or ip>     : run in pcap live mode
-f <bpf filter file> : bpf filter file
-r <path>          : run in pcap file/offline mode
-q <qid:qid>       : run in inline nfqueue mode (use colon to specify a range of queues)
-s <path>          : path to signature file loaded in addition to suricata.yaml settings (optional)
-e <path>          : path to signature file loaded exclusively (optional)
-l <dir>           : default log directory
-D                 : run as daemon
-k [all|none]      : force checksum check (all) or disabled it (none)
-V                 : display Suricata version
-v                 : be more verbose (use multiple times to increase verbosity)
--list-app-layer-protos   : list supported app layer protocols
--list-keywords[=all|csv|<keyword>] : list keywords implemented by the engine
--list-rummodes      : list supported rummodes
--runmode <runmode_id>    : specific rummode modification the engine should run. The argument supplied should be the id for the rummode obtained by running --list-rummodes
--engine-analysis     : print reports on analysis of different sections in the engine and exit.
                       Please have a look at the conf parameter engine-analysis on what reports can be printed
--pidfile <file>      : write pid to this file
--init-errors-fatal    : enable fatal failure on signature init error
--disable-detection    : disable detection engine
--dump-config         : show the running configuration
--build-info          : display build information
--pcap[=<dev>]         : run in pcap mode, no value select interfaces from suricata.yaml
                       when running in pcap mode with a directory, continue checking directory for pcaps until interrupted
--pcap-file-continuous : when running in replay mode (-r with directory or file), will delete pcap files that have been processed when done
--pcap-file-delete     : size of the pcap buffer value from 0 - 2147483647
--pcap-buffer-size     : run in af-packet mode, no value select interfaces from suricata.yaml
--af-packet[=<dev>]     : force engine into IPS mode. Useful for QA
--simulate-ips        : run suricata as this user after init
--user <user>          : run suricata as this user after init
--group <group>        : group suricata as this group after init
--erf-in <path>        : process an ERF file
--unix-socket[=<file>]  : use unix socket to control suricata work
--set name=value        : set a configuration value

To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:
suricata -c suricata.yaml -s signatures.rules -i eth0
```

→ suricata -V

Display the version of Suricata.

root@kali:~# suricata -V

```
root@kali:~# suricata -v  
This is Suricata version 5.0.3 RELEASE
```

→ suricata -c <path>

Path to configuration file.

```
root@kali:/etc/suricata# suricata -c /etc/suricata  
Suricata 5.0.3
```

→ suricata -T

Test configuration.

```
root@kali:~# suricata -T
```

```
24/8/2020 -- 08:48:48 - <Info> - Running suricata under test mode  
24/8/2020 -- 08:48:48 - <Notice> - This is Suricata version 5.0.3 RELEASE running in SYSTEM mode  
24/8/2020 -- 08:48:48 - <Notice> - Configuration provided was successfully loaded. Exiting.
```

→ suricata -v

Increase the verbosity of the Suricata application logging by increasing the log level from the default. This option can be passed multiple times to further increase the verbosity.

- -v: INFO

```
root@kali:~# suricata -v
```

```

Suricata 5.0.3
USAGE: suricata [OPTIONS] [BPF FILTER]

-c <path> : path to configuration file
-i <dev or ip> : test configuration file (use with -c)
-f <bpf filter file> : run in pcap live mode
-r <path> : bpf filter file
-q <qid:qid> : run in pcap file/offline mode
-s <path> : run in inline nqueue mode (use colon to specify a range of queues)
-S <path> : path to signature file loaded in addition to suricata.yaml settings (optional)
-l <dir> : path to signature file loaded exclusively (optional)
-d : default log directory
-k [all|none] : run as daemon
-V : force checksum check (all) or disabled it (none)
-v : display Suricata version
--list-app-layer-protocols : be more verbose (use multiple times to increase verbosity)
--list-keywords[=all|csv|<keyword>] : list supported app layer protocols
--list-rummodes : list keywords implemented by the engine
--rummode <rummode_id> : list supported rummodes
--rummode <runmode_id> : specific rummode modification the engine should run. The argument supplied should be the id for the rummode obtained by running --list-rummodes
--engine-analysis : print reports on analysis of different sections in the engine and exit.
--pidfile <file> : Please have a look at the conf parameter engine-analysis on what reports can be printed
--init-errors-fatal : write pid to this file
--disable-detection : enable fatal failure on signature init error
--dump-config : disable detection engine
--build-info : show the running configuration
--pcap[=<dev>] : display build information
--pcap-file-continuous : run in pcap mode, no value select interfaces from suricata.yaml
--pcap-file-delete : when running in pcap mode with a directory, continue checking directory for pcaps until interrupted
--pcap-buffer-size : when running in replay mode (-r with directory or file), will delete pcap files that have been processed when done
--af-packet[=<dev>] : size of the pcap buffer value from 0 - 2147483647
--simulate-ips : run in af-packet mode, no value select interfaces from suricata.yaml
--user <user> : force engine into IPS mode. Useful for QA
--group <group> : run suricata as this user after init
--erf-in <path> : run suricata as this group after init
--unix-socket[=<file>] : process an ERF file
--set name=value : use unix socket to control suricata work
--set name=value : set a configuration value

To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:
suricata -c suricata.yaml -s signatures.rules -i eth0

```

- -vv: PERFORMANCE
- -vvv: CONFIGURATION
- -vvvv: DEBUG

This option will not decrease the log level set in the configuration file if it is already more verbose than the level requested with this option

→ `suricata -r <path>`

Run in pcap offline mode (replay mode) reading files from pcap file. If specifies a directory, all files in that directory will be processed in order of modified time maintaining flow state between files.

11.1 What is pcap?

Pcap is an application programming interface (API) for capturing network traffic.

`suricata --pcap-file-continuous`

Used with the -r option to indicate that the mode should stay alive until interrupted. This is useful with directories to add new files and not reset flow state between files.

```
suricata --pcap-file-delete
```

Used with the -r option to indicate that the mode should delete pcap files after they have been processed. This is useful with pcap-file-continuous to continuously feed files to a directory and have them cleaned up when done. If this option is not set, pcap files will not be deleted after processing.

```
➔ suricata -i <interface>
```

After the -i option you can enter the interface card you would like to use to sniff packets from. This option will try to use the best capture method available. Can be used several times to sniff packets from several interfaces.

```
➔ suricata --init-errors-fatal
```

Exit with a failure when errors are encountered loading signatures.

```
➔ suricata --disable-detection
```

Disable the detection engine.

```
➔ suricata --dump-config
```

Dump the configuration loaded from the configuration file to the terminal and exit.

```
root@kali:/etc/suricata# suricata --dump-config
```

```
profiling.packets = (null)
profiling.packets.enabled = yes
profiling.packets.filename = packet_stats.log
profiling.packets.append = yes
profiling.packets.csv = (null)
profiling.packets.csv.enabled = no
profiling.packets.csv.filename = packet_stats.csv
profiling.locks = (null)
profiling.locks.enabled = no
profiling.locks.filename = lock_stats.log
profiling.locks.append = yes
profiling.pcap-log = (null)
profiling.pcap-log.enabled = no
profiling.pcap-log.filename = pcaplog_stats.log
profiling.pcap-log.append = yes
nfq = Home
nflog = (null)
nflog.0 = group
nflog.0.group = 2
nflog.0.buffer-size = 18432
nflog.1 = group
nflog.1.group = default
nflog.1.qthreshold = 1
nflog.1.qtimeout = 100
nflog.1.max-size = 20000
capture =
netmap = (null)
netmap.0 = interface
netmap.0.interface = eth2
netmap.1 = interface
netmap.1.interface = default
pfring = (null)
pfring.0 = interface
pfring.0.interface = eth0
pfring.0.threads = auto
pfring.0.cluster-id = 99
pfring.0.cluster-type = cluster_flow
pfring.1 = interface
pfring.1.interface = default
ipfw =
napatech = (null)
napatech.streams = (null)
napatech.streams.0 = 0-3
napatech.auto-config = yes
napatech.ports = (null)
napatech.ports.0 = all
napatech.hashmode = hash5tuplesorted
default-rule-path = /etc/suricata/rules
rule-files = (null)
rule-files.0 = test.rules
classification-file = /etc/suricata/classification.config
reference-config-file = /etc/suricata/reference.config
```

```
host os-policies/windows2008 (none)
defrag = (null)
defrag.memcap = 32mb
defrag.hash-size = 65536
defrag.trackers = 65535
defrag.max-frags = 65535
defrag.prealloc = yes
defrag.timeout = 60
flow = (null)
flow.memcap = 128mb
flow.hash-size = 65536
flow.prealloc = 10000
flow.emergency-recovery = 30
vlan = (null)
vlan.use-for-tracking = true
flow-timeouts = (null)
flow-timeouts.default = (null)
flow-timeouts.default.new = 30
flow-timeouts.default.established = 300
flow-timeouts.default.closed = 0
flow-timeouts.default.bypassed = 100
flow-timeouts.default.emergency-new = 10
flow-timeouts.default.emergency-established = 100
flow-timeouts.default.emergency-closed = 0
flow-timeouts.default.emergency-bypassed = 50
flow-timeouts.tcp = (null)
flow-timeouts.tcp.new = 60
flow-timeouts.tcp.established = 600
flow-timeouts.tcp.closed = 60
flow-timeouts.tcp.bypassed = 100
flow-timeouts.tcp.emergency-new = 5
flow-timeouts.tcp.emergency-established = 100
flow-timeouts.tcp.emergency-closed = 10
flow-timeouts.tcp.emergency-bypassed = 50
flow-timeouts.udp = (null)
flow-timeouts.udp.new = 30
flow-timeouts.udp.established = 300
flow-timeouts.udp.bypassed = 100
flow-timeouts.udp.emergency-new = 10
flow-timeouts.udp.emergency-established = 100
flow-timeouts.udp.emergency-bypassed = 50
flow-timeouts.icmp = (null)
flow-timeouts.icmp.new = 30
flow-timeouts.icmp.established = 300
flow-timeouts.icmp.bypassed = 100
flow-timeouts.icmp.emergency-new = 10
flow-timeouts.icmp.emergency-established = 100
flow-timeouts.icmp.emergency-bypassed = 50
stream = (null)
```

Output like this.

```
➔ suricata --build-info
```

Display the build information the Suricata was built with.

```
root@kali:/etc/suricata# suricata --build-info
```

```
This is Suricata version 5.0.3 RELEASE
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTPP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT HAVE_LIBJANSSON TLS MAGIC RUST
SIMD support: none
Atomics support: i 2 4 8 byte(s)
64bits, Little-endian architecture
GCC version 9.3.0, C version 199901
compiled with _FORTIFY_SOURCE=2
L1 Cache line size (CLS)=64
thread local storage method: _thread
compiled with LibHTTP v0.5.33, linked against LibHTTP v0.5.33

Suricata Configuration:
AF_PACKET support: yes
eBPF support: yes
XDP support: yes
PF_RING support: no
NFQueue support: yes
NFLOG support: yes
IPFW support: no
Netmap support: no
DAG enabled: no
Napatch enabled: no
WinDivert enabled: no

Unix socket enabled: yes
Detection enabled: yes

Libmagic support: yes
libnss support: yes
libnspr support: yes
libjansson support: yes
hiredis support: yes
hiredis async with libevent: yes
Prelude support: yes
PCRE jit: yes
LUA support: yes, through luajit
libluajit: yes
GeoIP2 support: yes
Non-bundled http: yes
Old barnyard2 support: no
Hyperscan support: yes
Libnet support: yes
liblz4 support: yes

Rust support: yes
Rust strict mode: no
Rust compiler path: /usr/bin/rustc
Rust compiler version: rustc 1.42.0
Cargo path: /usr/bin/cargo
Cargo version: cargo 1.42.1
Cargo vendor: yes
```

```
Python support: yes
Python path: /usr/bin/python3
Python distutils: yes
Python yaml: no
Install suricatactl: yes
Install suricatasc: yes
Install suricata-update: no, requires pyyaml

Profiling enabled: no
Profiling locks enabled: no

Development settings:
Coccinelle / spatch: no
Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no

Generic build parameters:
Installation prefix: /usr
Configuration directory: /etc/suricata/
Log directory: /var/log/suricata/

--prefix: /usr
--sysconfdir: /etc
--localstatedir: /var
--datarootdir: /usr/share

Host: x86_64-pc-linux-gnu
Compiler: gcc (exec name) / gcc (real)
GCC Protect enabled: yes
GCC march native enabled: no
GCC Profile enabled: no
Position Independent Executable enabled: no
CFLAGS: -g -O2 -fstack-protector-strong -Wformat -Werror=format-security -I${srcdir}/../rust/gen/c-headers
PCAP_CFLAGS: -I/usr/include
SECCFLAGS: -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security
```

```
➔ suricata --list-app-layer-protos
```

List all supported application layer protocols.

```
root@kali:~# suricata --list-app-layer-protos
```

```
=====Supported App Layer Protocols=====  
http  
ftp  
smtp  
tls  
ssh  
imap  
smb  
dcerpc  
dns  
nfs  
ntp  
ftp-data  
tftp  
ikev2  
krb5  
dhcp  
snmp
```

```
suricata --list-keywords=[all|csv|]
```

List all supported rule keywords.

```
suricata --list-runmodes
```

List all supported run modes

```
root@kali:~# suricata --list-runmodes
```

NFQ	autofp	Multi threaded NFQ IPS mode with respect to flow
	workers	Multi queue NFQ IPS mode with one thread per queue
NFLOG	autofp	Multi threaded nflog mode
	single	Single threaded nflog mode
	workers	Workers nflog mode
IPFW	autofp	Multi threaded IPFW IPS mode with respect to flow
	workers	Multi queue IPFW IPS mode with one thread per queue
ERF_FILE	single	Single threaded ERF file mode
	autofp	Multi threaded ERF file mode. Packets from each flow are assigned to a single detect thread
ERF_DAG	autofp	Multi threaded DAG mode. Packets from each Flow are assigned to a single detect thread, unlike "dag_auto" where packets from the same flow can be processed by any detect thread
	single	Singled threaded DAG mode
	workers	Workers DAG mode, each thread does all tasks from acquisition to logging
AF_PACKET_DEV	single	Single threaded af-packet mode
	workers	Workers af-packet mode, each thread does all tasks from acquisition to logging
	autofp	Multi socket AF_PACKET mode. Packets from each flow are assigned to a single detect thread.
NETMAP(DISABLED)	single	Single threaded netmap mode
	workers	Workers netmap mode, each thread does all tasks from acquisition to logging
	autofp	Multi threaded netmap mode. Packets from each flow are assigned to a single detect thread.
UNIX_SOCKET	single	Unix socket mode
	autofp	Unix socket mode
WINDIVERT(DISABLED)	autofp	Multi-threaded WinDivert IPS mode load-balanced by flow

→ suricata --engine-analysis

Print reports on analysis of different sections in the engine and exit. Please have a look at the conf parameter engine-analysis on what reports can be printed.

root@kali:~# suricata --engine-analysis

24/8/2020 -- 09:38:59 - <Notice> - This is Suricata version 5.0.3 RELEASE running in USER mode

→ suricata --napatech

Enable packet capture using the Napatech Streams API.

→ suricata --simulate-ips

Simulate IPS mode when running in a non-IPS mode.

root@kali:~# suricata --simulate-ips

24/8/2020 -- 09:40:38 - <Info> - Setting IPS mode

11.2 Unit Tests

Builtin unittests are only available if Suricata has been built with

```
➔ suricata --enable-unittests
```

```
root@kali:~# suricata --enable-unittests
```

Running unit tests does not take a configuration file. Use **-I** to supply an output directory.

```
➔ -u
```

Run the unit tests and exit. Requires that Suricata be compiled with **--enable-unittests**.

```
➔ U, --unittest-filter=REGEX
```

With the **-U** option you can select which of the unit tests you want to run. This option uses REGEX.

Example of use: `suricata -u -U http`

```
➔ --list-unittests
```

List all unit tests.

```
➔ --fatal-unittests
```

Enables fatal failure on a unit test error. Suricata will exit instead of continuing more tests.

```
➔ --unittests-coverage
```

Display unit test coverage report.

Packet Profiling

Packet profiling is useful if you want to know how long it takes to process packets. It is a way of understanding why certain packets are processed faster than others. Suricata is a good tool for developing.

12.1 Update Suricata from GIT repository

Step 1: Pre-installation requirements

```
sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev \
build-essential autoconf automake libtool libpcap-dev libnet1-dev \
libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 \
make libmagic-dev libjansson-dev
```

```
root@kali:~# sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev \
> build-essential autoconf automake libtool libpcap-dev libnet1-dev \
> libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 \
> make libmagic-dev libjansson-dev
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
autoconf is already the newest version (2.69-11.1).
automake is already the newest version (1:1.16.2-3).
build-essential is already the newest version (12.8).
libcap-ng-dev is already the newest version (0.7.9-2.2).
libcap-ng0 is already the newest version (0.7.9-2.2).
libjansson-dev is already the newest version (2.13.1-1).
libmagic-dev is already the newest version (1:5.38-5).
libnet1-dev is already the newest version (1.1.6+dfsg-3.1).
libpcap-dev is already the newest version (1.9.1-4).
libpcre3 is already the newest version (2:8.39-13).
libpcre3-dbg is already the newest version (2:8.39-13).
libpcre3-dev is already the newest version (2:8.39-13).
libtool is already the newest version (2.4.6-14).
libyaml-0-2 is already the newest version (0.2.2-1).
libyaml-dev is already the newest version (0.2.2-1).
make is already the newest version (4.3-4).
pkg-config is already the newest version (0.29.2-1).
zlib1g is already the newest version (1:1.2.11.dfsg-2).
zlib1g-dev is already the newest version (1:1.2.11.dfsg-2).
0 upgraded, 0 newly installed, 0 to remove and 831 not upgraded.
1 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Setting up camchain (/etc/camchain)
```

```
sudo apt-get install git-core
```

```
root@kali:~# sudo apt-get install git-core
```



```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  git-core
0 upgraded, 1 newly installed, 0 to remove and 831 not upgraded.
Need to get 1,506 B of archives.
After this operation, 21.5 kB of additional disk space will be used.
Get:1 http://httpredir.debian.org/debian jessie/main amd64 git-core all 1:2.1.4-2.1+deb8u6 [1,506 B]
Fetched 1,506 B in 10s (143 B/s)
Selecting previously unselected package git-core.
(Reading database ... 302233 files and directories currently installed.)
Preparing to unpack .../git-core_1%3a2.1.4-2.1+deb8u6_all.deb ...
Unpacking git-core (1:2.1.4-2.1+deb8u6) ...
Setting up git-core (1:2.1.4-2.1+deb8u6) ...
```

Step 2 : IPS

```
sudo apt-get -y install libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0
```

```
root@kali:~# sudo apt-get -y install libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0
Trash
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
libnetfilter-queue-dev is already the newest version (1.0.3-1).
libnetfilter-queue1 is already the newest version (1.0.3-1).
libnetfilter-queue1 set to manually installed.
libnfnetlink-dev is already the newest version (1.0.1-3+b1).
libnfnetlink-dev set to manually installed.
libnfnetlink0 is already the newest version (1.0.1-3+b1).
0 upgraded, 0 newly installed, 0 to remove and 831 not upgraded.
```

Step 3 : Configure, compile, install

```
root@kali:~# mkdir suricata
```

```
git clone https://github.com/OISF/libhttp.git -b 0.5.x
```

```
root@kali:~# cd suricata
root@kali:~/suricata# git clone git://phalanx.openinfosecfoundation.org/oisf.git
```

```
Cloning into 'oisf'...
remote: Counting objects: 80047, done.
remote: Compressing objects: 100% (16539/16539), done.
remote: Total 80047 (delta 65413), reused 77469 (delta 63370)
Receiving objects: 100% (80047/80047), 23.83 MiB | 1.05 MiB/s, done.
Resolving deltas: 100% (65413/65413), done.
```

```
root@kali:~/suricata# cd oisf
root@kali:~/suricata/oisf# git clone https://github.com/OISF/libhttp.git -b 0.5.x
Cloning into 'libhttp'...
```

```
Cloning into 'libhttp' ...
remote: Enumerating objects: 38, done.
remote: Counting objects: 100% (38/38), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 10615 (delta 18), reused 27 (delta 14), pack-reused 10577
Receiving objects: 100% (10615/10615), 10.21 MiB | 1.27 MiB/s, done.
Resolving deltas: 100% (6498/6498), done.
```

```
./autogen.sh
```

```
root@kali:~/suricata/oisf# ./autogen.sh
```

```
configure.ac:9: installing './compile'
configure.ac:9: installing './config.guess'
configure.ac:9: installing './config.sub'
configure.ac:6: installing './install-sh'
configure.ac:6: installing './missing'
src/Makefile.am: installing './depcomp'
autoreconf: Leaving directory `.'
You can now run "./configure" and then "make".
```

```
Found libtoolize
libtoolize: putting auxiliary files in '..'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
libtoolize: 'AC_PROG_RANLIB' is rendered obsolete by 'LT_INIT'
autoreconf: Entering directory `.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force -I m4
autoreconf: configure.ac: tracing
autoreconf: configure.ac: adding subdirectory libhttp to autoreconf
autoreconf: Entering directory `libhttp'
autoreconf: running: libtoolize --copy --force
libtoolize: putting auxiliary files in '..'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
autoreconf: running: /usr/bin/autoconf --force
autoreconf: running: /usr/bin/autoheader --force
autoreconf: running: automake --add-missing --copy --force-missing
configure.ac:86: installing './compile'
configure.ac:89: installing './config.guess'
configure.ac:89: installing './config.sub'
configure.ac:7: installing './install-sh'
configure.ac:7: installing './missing'
Makefile.am: installing './INSTALL'
http/Makefile.am: installing './depcomp'
parallel-tests: installing './test-driver'
autoreconf: Leaving directory `libhttp'
libtoolize: putting auxiliary files in '..'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
libtoolize: 'AC_PROG_RANLIB' is rendered obsolete by 'LT_INIT'
```

```
./configure
```

```
root@kali:~/suricata/oisf# ./configure
      Trash
```

```
checking for gawk ... gawk
checking whether make sets $(MAKE) ... yes
checking whether UID '0' is supported by ustar format... yes
checking whether GID '0' is supported by ustar format... yes
checking how to create a ustar tar archive... gnutar
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-pc-linux-gnu file names to x86_64-pc-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-pc-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
checking how to recognize dependent libraries... pass_all
checking for dlltool... no
checking how to associate runtime and link libraries... printf %s\n
checking for ar... ar
checking for archiver @FILE support... @
checking for strip... strip
checking for ranlib... ranlib
checking command to parse /usr/bin/nm -B output from gcc object... ok
checking for sysroot... no
checking for a working dd... /usr/bin/dd
checking how to truncate binary pipes... /usr/bin/dd bs=4096 count=1
checking for mt... mt
checking if mt is a manifest tool... no
checking how to run the C preprocessor... gcc -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
```

```
checking for _FILE_OFFSET_BITS value needed for large files ... no
checking host os ... installation for x86_64-pc-linux-gnu OS ... ok
checking for c11 support ... yes
checking for thread local storage gnu __thread support ... yes
checking for dlfcn.h ... (cached) yes
checking for plugin support ... yes
checking checking if gcc supports -march=native ... yes
checking for g++ ... g++
checking whether we are using the GNU C++ compiler ... yes
checking whether g++ accepts -g ... yes
checking dependency style of g++ ... gcc3
checking how to run the C++ preprocessor ... g++ -E
checking for ld used by g++ ... /usr/bin/ld -m elf_x86_64
checking if the linker (/usr/bin/ld -m elf_x86_64) is GNU ld ... yes
checking whether the g++ linker (/usr/bin/ld -m elf_x86_64) supports shared libraries ... yes
checking for g++ option to produce PIC ... -fPIC -DPIC
checking if g++ PIC flag -fPIC -DPIC works ... yes
checking if g++ static flag -static works ... yes
checking if g++ supports -c -o file.o ... yes
checking if g++ supports -c -o file.o ... (cached) yes
checking whether the g++ linker (/usr/bin/ld -m elf_x86_64) supports shared libraries ... yes
checking dynamic linker characteristics ... (cached) GNU/Linux ld.so
checking how to hardcode library paths into programs ... immediate
checking for spatch ... no
checking zlib.h usability ... yes
checking zlib.h presence ... yes
checking for zlib.h ... yes
checking for inflate in -lz ... yes
checking pcre.h usability ... yes
checking pcre.h presence ... yes
checking for pcre.h ... yes
checking for pcre_get_substring in -lpcre ... yes
checking for libpcre = 8.35 ... no
checking for pcre_dfa_exec in -lpcre ... yes
checking for PCRE JIT support ... yes
checking for PCRE JIT support usability ... yes
checking for PCRE JIT EXEC support usability ... yes
checking for libhs ... no
checking hs.h usability ... no
checking hs.h presence ... no
checking for hs.h ... no
checking yaml.h usability ... yes
checking yaml.h presence ... yes
checking for yaml.h ... yes
checking for yaml_parser_initialize in -lyaml ... yes
checking for pthread_create in -lpthread ... yes
checking for pthread_spin_unlock ... yes
checking jansson.h usability ... yes
checking jansson.h presence ... yes
checking for jansson.h ... yes
checking for jansson.h ... yes
```

```
libnss library not found, go get it
from Mozilla or your distribution:

Ubuntu: apt-get install libnss3-dev
Fedora: dnf install nss-devel
CentOS/RHEL: yum install nss-devel

checking magic.h usability... yes
checking magic.h presence... yes
checking for magic.h... yes
checking for magic_open in -lmagic... yes
checking for LZ4F_createCompressionContext in -llz4... yes
checking for getconf... /usr/bin/getconf
checking for sphinx-build... no
checking for pdflatex... no
checking for rustc... /usr/bin/rustc
checking for cargo... /usr/bin/cargo
checking for Rust version 1.34.2 or newer... yes
checking for rustup... no
checking for cargo vendor support... yes
checking for ./rust/dist... no
checking for ./rust/gen... no
checking for cbindgen... no
  Warning: cbindgen too old or not found, it is required to
          generate header files.
  To install: cargo install --force cbindgen
configure: error: cbindgen required
```

```
apt-get install libnss3-dev
```

```
root@kali:~/suricata/oisf# apt-get install libnss3-dev
```

```
root@kali:~/. Suricata-0.10.0 apt-get install libnss3-dev  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  libnsspr4 libnsspr4-dev libnss3  
The following NEW packages will be installed:  
  libnsspr4-dev libnss3-dev  
The following packages will be upgraded:  
  libnsspr4 libnss3  
2 upgraded, 2 newly installed, 0 to remove and 829 not upgraded.  
Need to get 461 kB/1,870 kB of archives.  
After this operation, 2,861 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://kali.download/kali kali-rolling/main amd64 libnsspr4-dev amd64 2:4.27-1 [211 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 libnss3-dev amd64 2:3.55-1 [251 kB]  
Fetched 461 kB in 24s (19.6 kB/s)  
Reading changelogs... Done  
(Reading database... 302234 files and directories currently installed.)  
Preparing to unpack... /libnsspr4_2%3a4.27-1_amd64.deb ...  
Unpacking libnsspr4:amd64 (2:4.27-1) over (2:4.25-1) ...  
Selecting previously unselected package libnsspr4-dev.  
Preparing to unpack... /libnsspr4-dev_2%3a4.27-1_amd64.deb ...  
Unpacking libnsspr4-dev (2:4.27-1) ...  
Preparing to unpack... /libnss3_2%3a3.55-1_amd64.deb ...  
Unpacking libnss3:amd64 (2:3.55-1) over (2:3.49.1-1) ...  
Selecting previously unselected package libnss3-dev:amd64.  
Preparing to unpack... /libnss3-dev_2%3a3.55-1_amd64.deb ...  
Unpacking libnss3-dev:amd64 (2:3.55-1) ...  
Setting up libnsspr4:amd64 (2:4.27-1) ...  
Setting up libnsspr4-dev (2:4.27-1) ...  
Setting up libnss3:amd64 (2:3.55-1) ...  
Setting up libnss3-dev:amd64 (2:3.55-1) ...  
Processing triggers for libc-bin (2.30-4) ...  
Processing triggers for kali-menu (2020.2.2) ...
```

```
cargo install --force cbindgen
```

```
root@kali:~/suricata/oisf# cargo install --force cbindgen
```

```
Updating crates.io index
Downloaded cbindgen v0.14.4
Downloaded 1 crate (172.1 KB) in 2.08s
Installing cbindgen v0.14.4
Downloaded tempfile v3.1.0
Downloaded toml v0.5.6
Downloaded heck v0.3.1
Downloaded proc-macro2 v1.0.19
Downloaded serde_json v1.0.57
Downloaded serde v1.0.115
Downloaded clap v2.33.3
Downloaded log v0.4.11
Downloaded quote v1.0.7
Downloaded syn v1.0.39
Downloaded unicode-segmentation v1.6.0
Downloaded cfg-if v0.1.10
Downloaded itoa v0.4.6
Downloaded remove_dir_all v0.5.3
Downloaded libc v0.2.76
Downloaded ryu v1.0.5
Downloaded serde_derive v1.0.115
Downloaded rand v0.7.3
Downloaded unicode-xid v0.2.1
Downloaded ansi_term v0.11.0
Downloaded atty v0.2.14
Downloaded unicode-width v0.1.8
Downloaded vec_map v0.8.2
Downloaded textwrap v0.11.0
Downloaded bitflags v1.2.1
Downloaded strsim v0.8.0
Downloaded getrandom v0.1.14
Downloaded rand_chacha v0.2.2
Downloaded rand_core v0.5.1
Downloaded ppv-lite86 v0.2.9
```

```
Compiling libc v0.2.76
Compiling proc-macro2 v1.0.19
Compiling unicode-xid v0.2.1
Compiling getrandom v0.1.14
Compiling syn v1.0.39
Compiling cfg-if v0.1.10
Compiling serde_derive v1.0.115
Compiling serde v1.0.115
Compiling ppv-lite86 v0.2.9
Compiling bitflags v1.2.1
Compiling ryu v1.0.5
Compiling log v0.4.11
Compiling serde_json v1.0.57
Compiling unicode-width v0.1.8
Compiling ansi_term v0.11.0
Compiling itoa v0.4.6
Compiling strsim v0.8.0
Compiling vec_map v0.8.2
Compiling cbindgen v0.14.4
Compiling unicode-segmentation v1.6.0
Compiling remove_dir_all v0.5.3
Compiling textwrap v0.11.0
Compiling heck v0.3.1
Compiling quote v1.0.7
Compiling atty v0.2.14
Compiling clap v2.33.3
Compiling rand_core v0.5.1
Compiling rand_chacha v0.2.2
Compiling rand v0.7.3
Compiling tempfile v3.1.0
```

Gives an error.

```
Compiling toml v0.5.6
  Finished release [optimized] target(s) in 2m 15s
Installing /root/.cargo/bin/cbindgen
  Installed package `cbindgen v0.14.4` (executable `cbindgen`)
warning: be sure to add `/root/.cargo/bin` to your PATH to be able to run the installed binaries
```

```
warning: be sure to add `/root/.cargo/bin` to your PATH to be able to run the installed binaries
```

```
root@kali:~/suricata/oisf# cd /root/.cargo/bin
root@kali:~/.cargo/bin# cargo install --force cbindgen
```

```
Updating crates.io index
Installing cbindgen v0.14.4
Compiling libc v0.2.76
Compiling proc-macro2 v1.0.19
Compiling unicode-xid v0.2.1
Compiling getrandom v0.1.14
Compiling syn v1.0.39
Compiling cfg-if v0.1.10
Compiling serde_derive v1.0.115
Compiling serde v1.0.115
Compiling ppv-lite86 v0.2.9
Compiling ryu v1.0.5
Compiling bitflags v1.2.1
Compiling serde_json v1.0.57
Compiling log v0.4.11
Compiling unicode-width v0.1.8
Compiling ansi_term v0.11.0
Compiling unicode-segmentation v1.6.0
Compiling remove_dir_all v0.5.3
Compiling vec_map v0.8.2
Compiling itoa v0.4.6
Compiling strsim v0.8.0
Compiling cbindgen v0.14.4
Compiling textwrap v0.11.0
Compiling heck v0.3.1
Compiling quote v1.0.7
Compiling atty v0.2.14
Compiling clap v2.33.3
Compiling rand_core v0.5.1
Compiling rand_chacha v0.2.2
Compiling rand v0.7.3
Compiling tempfile v3.1.0
Compiling toml v0.5.6
Finished release [optimized] target(s) in 1m 31s
Replacing /root/.cargo/bin/cbindgen
Replaced package `cbindgen v0.14.4` with `cbindgen v0.14.4` (executable `cbindgen`)
warning: be sure to add `/root/.cargo/bin` to your PATH to be able to run the installed binaries
```

error was continuing.

```
root@kali:~/suricata/oisf# apt-get install cbindgen
```

```
Reading package lists... Done
Building dependency tree...
Reading state information... Done
The following NEW packages will be installed:
  cbindgen
0 upgraded, 1 newly installed, 0 to remove and 850 not upgraded.
Need to get 1,298 kB of archives.
After this operation, 5,046 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 cbindgen amd64 0.14.3-1 [1,298 kB]
Fetched 1,298 kB in 22s (59.3 kB/s)
Selecting previously unselected package cbindgen.
(Reading database ... 302434 files and directories currently installed.)
Preparing to unpack .../cbindgen_0.14.3-1_amd64.deb ...
Unpacking cbindgen (0.14.3-1) ...
Setting up cbindgen (0.14.3-1) ...
Processing triggers for kali-menu (2020.2.2) ...
Processing triggers for man-db (2.9.1-1) ...
```

Again ./configure

```
checking whether to build static libraries ... yes
checking how to run the C++ preprocessor... g++ -E
checking for ld used by g++ ... /usr/bin/ld -m elf_x86_64
checking if the linker (/usr/bin/ld -m elf_x86_64) is GNU ld... yes
checking whether the g++ linker (/usr/bin/ld -m elf_x86_64) supports shared libraries ... yes
checking for g++ option to produce PIC ... -fPIC -DPIC
checking if g++ PIC flag -fPIC -DPIC works ... yes
checking if g++ static flag -static works ... yes
checking if g++ supports -c -o file.o ... yes
checking if g++ supports -c -o file.o... (cached) yes
checking whether the g++ linker (/usr/bin/ld -m elf_x86_64) supports shared libraries ... yes
checking dynamic linker characteristics ... (cached) GNU/Linux ld.so
checking how to hardcode library paths into programs ... immediate
checking whether build environment is sane ... yes
checking for strlcpy ... no
checking for strlcat ... no
checking zlib.h usability ... yes
checking zlib.h presence ... yes
checking for zlib.h ... yes
checking for inflate in -lz ... yes
checking OS ... Linux
checking for ld used by GCC ... /usr/bin/ld -m elf_x86_64
checking if the linker (/usr/bin/ld -m elf_x86_64) is GNU ld... yes
checking for shared library run path origin... done
checking for iconv... yes
checking for working iconv ... yes
checking for iconv declaration...
    extern size_t iconv (iconv_t cd, char * *inbuf, size_t *inbytesleft, char * *outbuf, size_t *outbytesleft
);
checking for iconvctl ...
checking for gcc support of -Wstrict-overflow=1... yes
checking for gcc support of stack smashing protection ... yes
checking for gcc support of FORTIFY_SOURCE ... yes
checking for gcc support of -Wformat -Wformat-security ... yes
checking for gcc support of -fPIC ... yes
checking for doxygen ... no
checking for lcov ... no
checking that generated files are newer than configure ... done
checking that generated files are newer than configure ... done
configure: creating ./config.status
config.status: creating http/htp_version.h
config.status: creating Makefile
config.status: creating htp.pc
config.status: creating http/Makefile
config.status: creating http/lzma/Makefile
config.status: creating test/Makefile
config.status: creating docs/Makefile
config.status: creating http_config_auto_gen.h
config.status: executing depfiles commands
config.status: executing libtool commands
```

```

Non-bundled http: no
Old barnyard2 support: no
Hyperscan support: no
Libnet support: yes
liblz4 support: yes

Rust support: yes
Rust strict mode: no
Rust compiler path: /usr/bin/rustc
Rust compiler version: rustc 1.43.0
Cargo path: /usr/bin/cargo
Cargo version: cargo 1.42.1
Cargo vendor: yes

Python support: yes
Python path: /usr/bin/python3
Python distutils: yes
Python yaml: yes
Install suricatactl: yes
Install suricatasc: yes
Install suricata-update: not bundled

Profiling enabled: no
Profiling locks enabled: no

Plugin support (experimental): yes

Development settings:
Coccinelle / spatch: no
Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no

Generic build parameters:
Installation prefix: /usr/local
Configuration directory: /usr/local/etc/suricata/
Log directory: /usr/local/var/log/suricata/

--prefix /usr/local
--sysconfdir /usr/local/etc
--localstatedir /usr/local/var
--datarootdir /usr/local/share

Host: x86_64-pc-linux-gnu
Compiler: gcc (exec name) / g++ (real)
GCC Protect enabled: no
GCC march native enabled: yes
GCC Profile enabled: no
Position Independent Executable enabled: no
CFLAGS -g -O2 -std=c11 -march=native -I${srcdir}/../rust/gen -I${srcdir}/../rust/gen/include
st/dist -I/usr/include
PCAP_CFLAGS
SECCFLAGS

```

```

$ ./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/

```

make

```
root@kali:~/suricata/oisf# make
```

```
Making all in libhttp
make[1]: Entering directory '/root/suricata/oisf/libhttp'
make  all-recurse
make[2]: Entering directory '/root/suricata/oisf/libhttp'
Making all in htp
make[3]: Entering directory '/root/suricata/oisf/libhttp/htp'
Making all in lzma
make[4]: Entering directory '/root/suricata/oisf/libhttp/htp/lzma'
make[4]: Nothing to be done for 'all'.
make[4]: Leaving directory '/root/suricata/oisf/libhttp/htp/lzma'
make[4]: Entering directory '/root/suricata/oisf/libhttp/htp'
make[4]: Nothing to be done for 'all-am'.
make[4]: Leaving directory '/root/suricata/oisf/libhttp/htp'
make[3]: Leaving directory '/root/suricata/oisf/libhttp/htp'
Making all in test
make[3]: Entering directory '/root/suricata/oisf/libhttp/test'
make[3]: Nothing to be done for 'all'.
make[3]: Leaving directory '/root/suricata/oisf/libhttp/test'
Making all in docs
make[3]: Entering directory '/root/suricata/oisf/libhttp/docs'
make[3]: Nothing to be done for 'all'.
make[3]: Leaving directory '/root/suricata/oisf/libhttp/docs'
make[3]: Entering directory '/root/suricata/oisf/libhttp'
make[3]: Leaving directory '/root/suricata/oisf/libhttp'
make[2]: Leaving directory '/root/suricata/oisf/libhttp'
make[1]: Leaving directory '/root/suricata/oisf/libhttp'
Making all in rust
make[1]: Entering directory '/root/suricata/oisf/rust'
 \
  CARGO_HOME="/root/.cargo" \
  CARGO_TARGET_DIR="/root/suricata/oisf/rust/target" \
  /usr/bin/cargo build --release \
    --features "
Compiling num-bigint v0.3.0
Compiling num-bigint v0.2.6
Compiling num-iter v0.1.41
Compiling syn v0.15.44
Compiling lexical-core v0.6.7
Compiling rand_chacha v0.2.2
Compiling num-rational v0.2.4
Compiling nom v5.1.1
Building [=====>] 81/103: syn, num-rational, nom, num-bigint
```

```
Compiling Suricata v0.0.0-dev (/root/suricata/oisf/rust)
  Finished release [optimized + debuginfo] target(s) in 50.03s
make gen/rust-bindings.h
make[2]: Entering directory '/root/suricata/oisf/rust'
rm -f gen/rust-bindings.h
cbindgen --config /root/suricata/oisf/rust/cbindgen.toml \
    --quiet --output /root/suricata/oisf/rust/gen/rust-bindings.h
make[2]: Leaving directory '/root/suricata/oisf/rust'
make[1]: Leaving directory '/root/suricata/oisf/rust'
Making all in src
make[1]: Entering directory '/root/suricata/oisf/src'
make  all-am
make[2]: Entering directory '/root/suricata/oisf/src'
  CC      main.o
  CC      alert-debuglog.o
  CC      alert-fastlog.o
  CC      alert-prelude.o
  CC      alert-syslog.o
  CC      app-layer.o
  CC      app-layer-dcerpc.o
  CC      app-layer-dcerpc-udp.o
  CC      app-layer-detect-proto.o
  CC      app-layer-dnp3.o
  CC      app-layer-dnp3-objects.o
  CC      app-layer-enip.o
  CC      app-layer-enip-common.o
  CC      app-layer-events.o
  CC      app-layer-expectation.o
  CC      app-layer-ftp.o
  CC      app-layer-htp-body.o
  CC      app-layer-htp.o
  CC      app-layer-htp-file.o
  CC      app-layer-htp-libhtp.o
  CC      app-layer-htp-mem.o
  CC      app-layer-htp-xff.o
  CC      app-layer-http2.o
  CC      app-layer-modbus.o
  CC      app-layer-parser.o
  CC      app-layer-protos.o
  CC      app-layer-smb.o
  CC      app-layer-smtp.o
  CC      app-layer-snmp.o
  CC      app-layer-nfs-tcp.o
  CC      app-layer-nfs-udp.o
  CC      app-layer-ntp.o
```

```
make[1]: Leaving directory '/root/suricata/oisf/etc'
Making all in python
make[1]: Entering directory '/root/suricata/oisf/python'
cd . && \
/usr/bin/python3 setup.py build --build-base "/root/suricata/oisf/python"
running build
running build_py
creating /root/suricata/oisf/python/lib
creating /root/suricata/oisf/python/lib/suricata
copying suricata/__init__.py → /root/suricata/oisf/python/lib/suricata
creating /root/suricata/oisf/python/lib/suricata/config
copying suricata/config/__init__.py → /root/suricata/oisf/python/lib/suricata/config
copying suricata/config/defaults.py → /root/suricata/oisf/python/lib/suricata/config
creating /root/suricata/oisf/python/lib/suricata/ctl
copying suricata/ctl/__init__.py → /root/suricata/oisf/python/lib/suricata/ctl
copying suricata/ctl/main.py → /root/suricata/oisf/python/lib/suricata/ctl
copying suricata/ctl/filestore.py → /root/suricata/oisf/python/lib/suricata/ctl
copying suricata/ctl/test_filestore.py → /root/suricata/oisf/python/lib/suricata/ctl
copying suricata/ctl/loghandler.py → /root/suricata/oisf/python/lib/suricata/ctl
creating /root/suricata/oisf/python/lib/suricata/sc
copying suricata/sc/__init__.py → /root/suricata/oisf/python/lib/suricata/sc
copying suricata/sc/specs.py → /root/suricata/oisf/python/lib/suricata/sc
copying suricata/sc/suricatasc.py → /root/suricata/oisf/python/lib/suricata/sc
creating /root/suricata/oisf/python/lib/suricatasc
copying suricatasc/__init__.py → /root/suricata/oisf/python/lib/suricatasc
running build_scripts
creating /root/suricata/oisf/python/scripts-3.8
copying and adjusting bin/suricatactl → /root/suricata/oisf/python/scripts-3.8
copying and adjusting bin/suricatasc → /root/suricata/oisf/python/scripts-3.8
changing mode of /root/suricata/oisf/python/scripts-3.8/suricatactl from 644 to 755
changing mode of /root/suricata/oisf/python/scripts-3.8/suricatasc from 644 to 755
make[1]: Leaving directory '/root/suricata/oisf/python'
Making all in ebpf
make[1]: Entering directory '/root/suricata/oisf/ebpf'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/root/suricata/oisf/ebpf'
make[1]: Entering directory '/root/suricata/oisf'
make[1]: Nothing to be done for 'all-am'.
make[1]: Leaving directory '/root/suricata/oisf'
```

make install-full

```
root@kali:~/suricata/oisf# make install-full
```

```
make[3]: Entering directory '/root/suricata/oisf/python'
cd . && \
    /usr/bin/python3 setup.py build --build-base "/root/suricata/oisf/python" \
        install --prefix /usr/local
running build
running build_py
running build_scripts
running install
running install_lib
running install_scripts
changing mode of /usr/local/bin/suricatasc to 755
changing mode of /usr/local/bin/suricatactl to 755
running install_egg_info
Removing /usr/local/lib/python3.8/dist-packages/suricata-6.0.0_dev-py3.8.egg-info
Writing /usr/local/lib/python3.8/dist-packages/suricata-6.0.0_dev-py3.8.egg-info
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/root/suricata/oisf/python'
make[2]: Leaving directory '/root/suricata/oisf/python'
Making install in ebpf
make[2]: Entering directory '/root/suricata/oisf/ebpf'
make[3]: Entering directory '/root/suricata/oisf/ebpf'
make[3]: Nothing to be done for 'install-exec-am'.
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/root/suricata/oisf/ebpf'
make[2]: Leaving directory '/root/suricata/oisf/ebpf'
make[2]: Entering directory '/root/suricata/oisf'
make[3]: Entering directory '/root/suricata/oisf'
make[3]: Nothing to be done for 'install-exec-am'.
Run 'make install-conf' if you want to install initial configuration files. Or 'make install-full' to install configuration and rules
make[3]: Leaving directory '/root/suricata/oisf'
make[2]: Leaving directory '/root/suricata/oisf'
make[1]: Leaving directory '/root/suricata/oisf'
make install-conf
make[1]: Entering directory '/root/suricata/oisf'
install -d "/usr/local/etc/suricata/"
install -d "/usr/local/var/log/suricata/files"
install -d "/usr/local/var/log/suricata/certs"
install -d "/usr/local/var/run/"
install -m 770 -d "/usr/local/var/run/suricata"
make[1]: Leaving directory '/root/suricata/oisf'
make install-rules
make[1]: Entering directory '/root/suricata/oisf'
error: rules not installed as suricata-update not available
make[1]: *** [Makefile:937: install-rules] Error 1
make[1]: Leaving directory '/root/suricata/oisf'
make: *** [Makefile:918: install-full] Error 2
```

```
[root@kali:~/suricata/oisf# git pull
Already up to date.
```

12.2 Wireshark

Step 4: Download Wireshark

What is Wireshark?

- The most famous network protocol analyzer is Wireshark.
- Its purpose is a tool that allows you to see what is happening on the network.
- Can be used with suricata.

```
sudo apt-get install wireshark
```

```
kali@kali:~$ sudo apt-get install wireshark
```

```
kali@kali:~$ sudo apt-get install wireshark
Reading package lists... Done
Building dependency tree...
Reading state information... Done
The following additional packages will be installed:
  libmd4c0 libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5 libqt5help5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediasettings5
  libqt5multimedawidgets5 libqt5network5 libqt5opengl5 libqt5positioning5
  libqt5printsupport5 libqt5qml5 libqt5qmlmodels5 libqt5quick5 libqt5sensors5 libqt5sql5
  libqt5sql5-sqlite libqt5svg5 libqt5test5 libqt5webchannel5 libqt5webkit5 libqt5widgets5
  libqt5xml5 libwireshark-data libwireshark13 libwiretap10 libwsutil11 python3-pyqt5
  python3-pyqt5.qtopen gl qt5-gtk-platformtheme qt5-gtk2-platformtheme qt5ct tshark
  wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 qt5-qmltooling-plugins geoipupdate
  geoip-database-extra libjs-leaflet libjs-leaflet.markercluster snmp-mibs-downloader
  wireshark-doc python3-pyqt5-dbg qt5-style-plugins
The following NEW packages will be installed:
  libmd4c0 libqt5qmlmodels5
The following packages will be upgraded:
  libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5 libqt5help5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediasettings5 libqt5multimedawidgets5
  libqt5network5 libqt5opengl5 libqt5positioning5 libqt5printsupport5 libqt5qml5
  libqt5quick5 libqt5sensors5 libqt5sql5 libqt5sql5-sqlite libqt5svg5 libqt5test5
  libqt5webchannel5 libqt5webkit5 libqt5widgets5 libqt5xml5 libwireshark-data
  libwireshark13 libwiretap10 libwsutil11 python3-pyqt5 python3-pyqt5.qtopen gl
  qt5-gtk-platformtheme qt5-gtk2-platformtheme qt5ct tshark wireshark wireshark-common
  wireshark-qt
37 upgraded, 2 newly installed, 0 to remove and 732 not upgraded.
Need to get 53.4 MB of archives.
After this operation, 2,219 kB of additional disk space will be used.
Do you want to continue? [Y/n] 
```

```
Do you want to continue? [Y/n] y
0% [Working]
```

```
Preparing to unpack ... /25-libqt5multimeddiagsttools5_5.14.2-2_amd64.deb ...
Unpacking libqt5multimeddiagsttools5:amd64 (5.14.2-2) over (5.12.5-1+b1) ...
Preparing to unpack ... /26-libqt5multimedia5-plugins_5.14.2-2_amd64.deb ...
Unpacking libqt5multimedia5-plugins:amd64 (5.14.2-2) over (5.12.5-1+b1) ...
Preparing to unpack ... /27-libqt5multimedia5_5.14.2-2_amd64.deb ...
Unpacking libqt5multimedia5:amd64 (5.14.2-2) over (5.12.5-1+b1) ...
Preparing to unpack ... /28-libqt5multimediacore5_5.14.2-2_amd64.deb ...
Unpacking libqt5multimediacore5:amd64 (5.14.2-2) over (5.12.5-1+b1) ...
Preparing to unpack ... /29-libqt5svg5_5.14.2-2_amd64.deb ...
Unpacking libqt5svg5:amd64 (5.14.2-2) over (5.12.5-2) ...
Preparing to unpack ... /30-libqt5core5a_5.14.2+dfsg-4_amd64.deb ...
Unpacking libqt5core5a:amd64 (5.14.2+dfsg-4) over (5.12.5+dfsg-10) ...
Preparing to unpack ... /31-libwireshark-data_3.2.5-1_all.deb ...
Unpacking libwireshark-data (3.2.5-1) over (3.2.3-1) ...
Preparing to unpack ... /32-libwsutil11_3.2.5-1_amd64.deb ...
Unpacking libwsutil11:amd64 (3.2.5-1) over (3.2.3-1) ...
Preparing to unpack ... /33-libwiretap10_3.2.5-1_amd64.deb ...
Unpacking libwiretap10:amd64 (3.2.5-1) over (3.2.3-1) ...
Preparing to unpack ... /34-libwireshark13_3.2.5-1_amd64.deb ...
Unpacking libwireshark13:amd64 (3.2.5-1) over (3.2.3-1) ...
```

Type in following two commands to check the Wireshark utiliy in the system.

```
wireshark -h
```

```
tshark -h
```

What is Tshark?

It is a network analysis program that runs from the command line.

```
kali㉿kali:~$ wireshark -h
Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1)
Interactively dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: wireshark [options] ... [ <infile> ]

Capture interface:
-i <interface>, --interface <interface>
    name or idx of interface (def: first non-loopback)
-f <capture filter>      packet filter in libpcap filter syntax
-s <snaplen>, --snapshot-length <snaplen>
    packet snapshot length (def: appropriate maximum)
-p, --no-promiscuous-mode
    don't capture in promiscuous mode
-k Home
    start capturing immediately (def: do nothing)
-S
    update packet display when new packets are captured
-l
    turn on automatic scrolling while -S is in use
-I, --monitor-mode
    capture in monitor mode, if available
-B <buffer size>, --buffer-size <buffer size>
    size of kernel buffer (def: 2MB)
-y <link type>, --linktype <link type>
    link layer type (def: first appropriate)
--time-stamp-type <type> timestamp method for interface
-D, --list-interfaces  print list of interfaces and exit
-L, --list-data-link-types
    print list of link-layer types of iface and exit
--list-time-stamp-types print list of timestamp types for iface and exit

Capture stop conditions:
-c <packet count>      stop after n packets (def: infinite)
-a <autostop cond.> ... , --autostop <autostop cond.> ...
    duration:NUM - stop after NUM seconds
    filesize:NUM - stop this file after NUM KB
    files:NUM - stop after NUM files
    packets:NUM - stop after NUM packets

Capture output:
-b <ringbuffer opt.> ... , --ring-buffer <ringbuffer opt.>
    duration:NUM - switch to next file after NUM secs
    filesize:NUM - switch to next file after NUM KB
    files:NUM - ringbuffer: replace after NUM files
    packets:NUM - switch to next file after NUM packets
    interval:NUM - switch to next file when the time is
                    an exact multiple of NUM secs

Input file:
-r <infile>, --read-file <infile>
    set the filename to read from (no pipes or stdin!)
```

```
kali㉿kali:~$ tshark -h
TShark (Wireshark) 3.2.5 (Git v3.2.5 packaged as 3.2.5-1)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...
      File System
Capture interface:
  -i <interface>, --interface <interface>
                                name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>, --snapshot-length <snaplen>
                                packet snapshot length (def: appropriate maximum)
  -p, --no-promiscuous-mode
                                don't capture in promiscuous mode
  -I, --monitor-mode        capture in monitor mode, if available
  -B <buffer size>, --buffer-size <buffer size>
                                size of kernel buffer (def: 2MB)
  -y <link type>, --linktype <link type>
                                link layer type (def: first appropriate)
  --time-stamp-type <type> timestamp method for interface
  -D, --list-interfaces    print list of interfaces and exit
  -L, --list-data-link-types
                                print list of link-layer types of iface and exit
  --list-time-stamp-types  print list of timestamp types for iface and exit

Capture stop conditions:
  -c <packet count>       stop after n packets (def: infinite)
  -a <autostop cond.> ... , --autostop <autostop cond.> ...
                                duration:NUM - stop after NUM seconds
                                filesize:NUM - stop this file after NUM KB
                                files:NUM - stop after NUM files
                                packets:NUM - stop after NUM packets

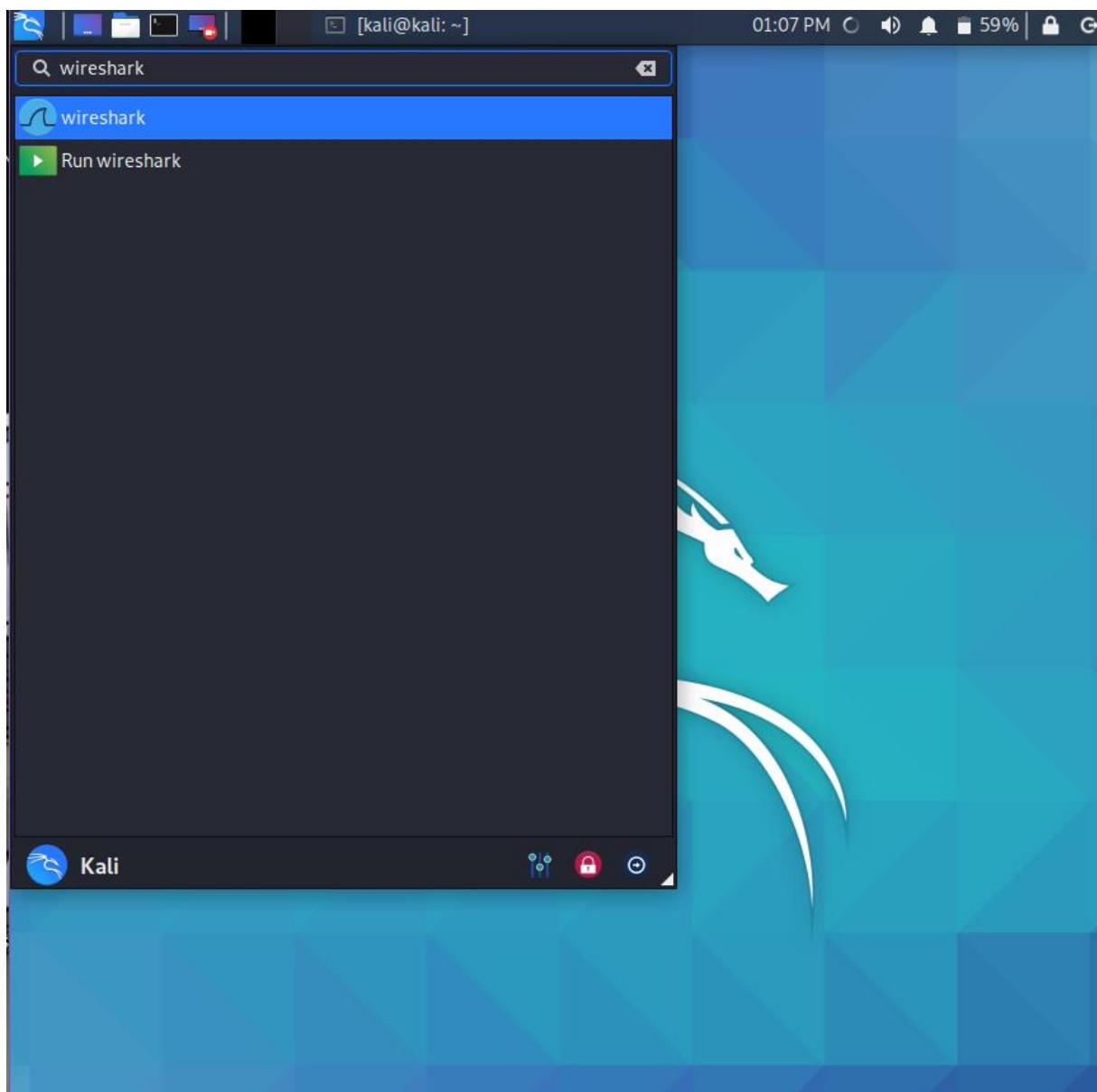
Capture output:
  -b <ringbuffer opt.> ... , --ring-buffer <ringbuffer opt.>
                                duration:NUM - switch to next file after NUM secs
                                filesize:NUM - switch to next file after NUM KB
                                files:NUM - ringbuffer: replace after NUM files
                                packets:NUM - switch to next file after NUM packets
                                interval:NUM - switch to next file when the time is
                                an exact multiple of NUM secs

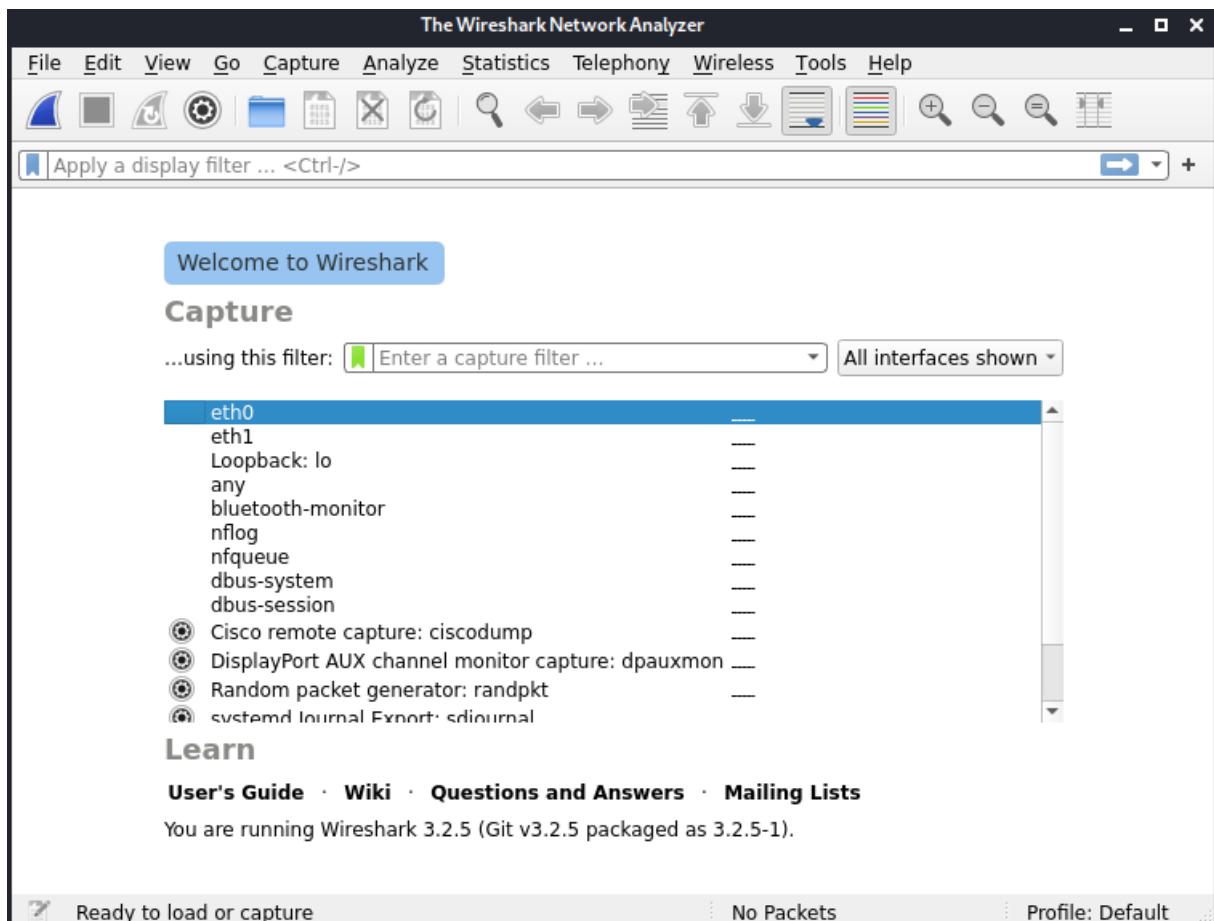
Input file:
  -r <infile>, --read-file <infile>
                                set the filename to read from (or '-' for stdin)

Processing:
  -2                         perform a two-pass analysis
  -M <packet count>        perform session auto reset
  -R <read filter>, --read-filter <read filter>
                                packet Read filter in Wireshark display filter syntax
```

12.3 Use of Wireshark

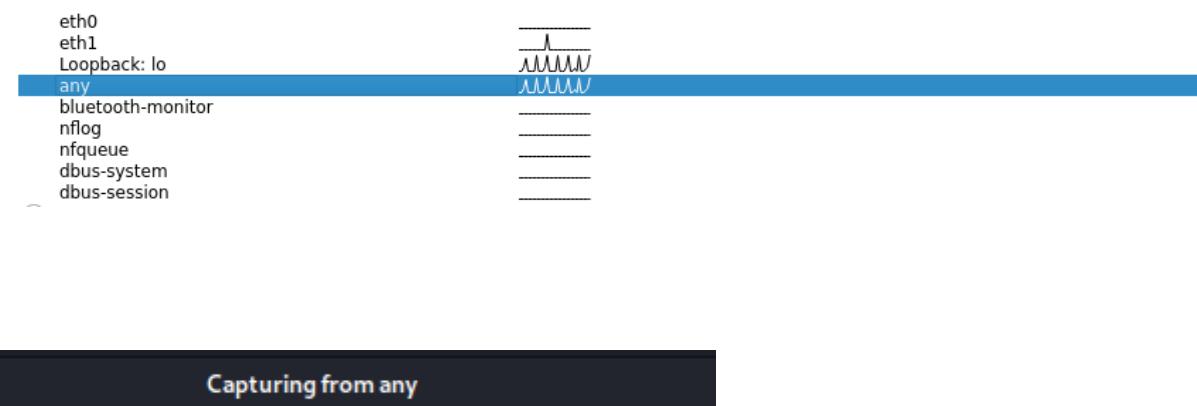
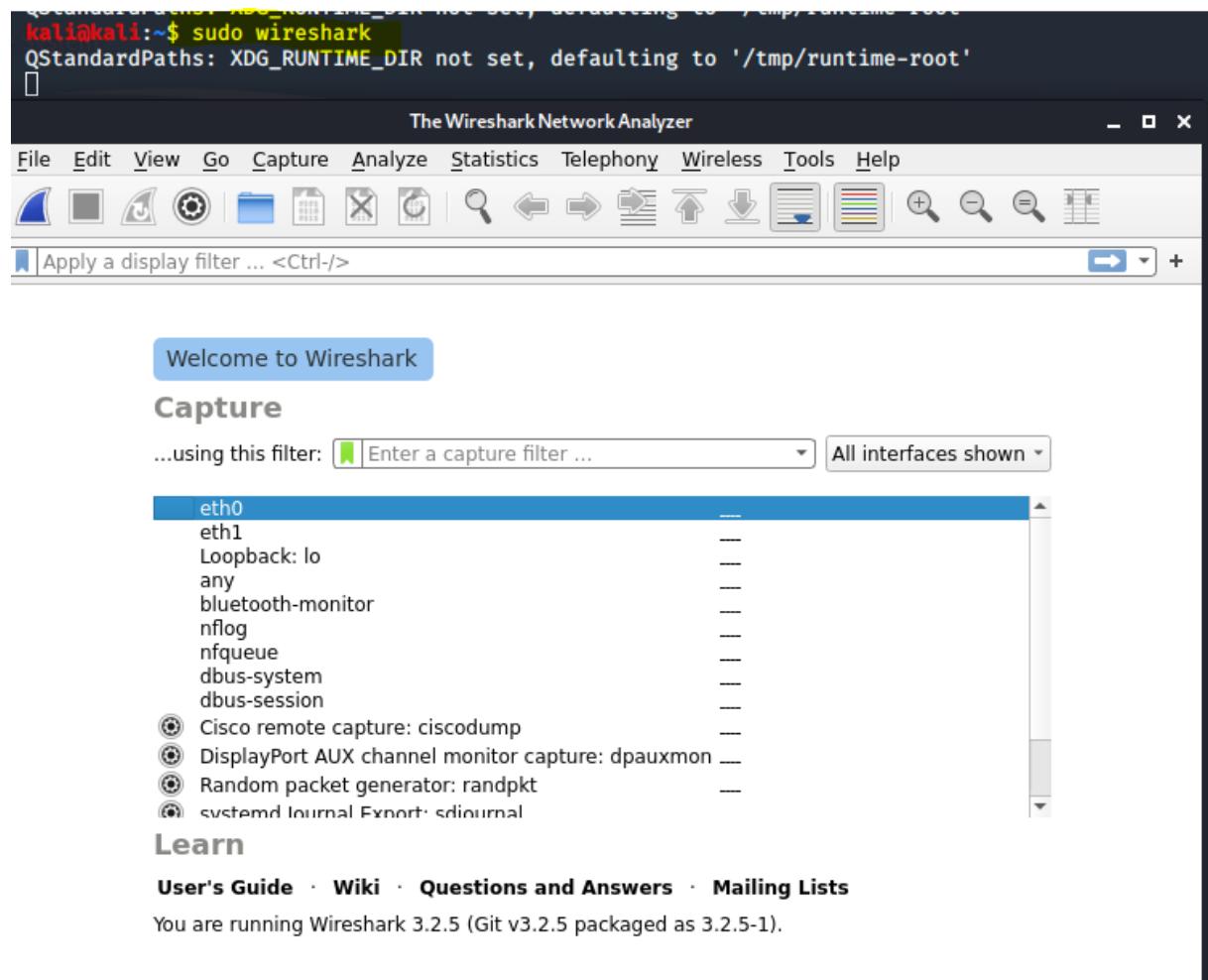
Wireshark gui:





Open wireshark:

```
sudo wireshark
```



*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
409	58.626364715	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=29847 Ack=95130 Win=512 Len=0 TSval=671096860 TSe...
410	58.626492533	127.0.0.1	127.0.0.1	TLSv1.2	337	Application Data
411	58.626688046	127.0.0.1	127.0.0.1	TLSv1.2	261	Application Data
412	58.626737292	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=30116 Ack=95322 Win=512 Len=0 TSval=671096860 TSe...
413	58.626913119	127.0.0.1	127.0.0.1	TLSv1.2	422	Application Data
414	58.627308235	127.0.0.1	127.0.0.1	TLSv1.2	912	Application Data
415	58.627374785	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=30470 Ack=96166 Win=512 Len=0 TSval=671096861 TSe...
416	58.627498493	127.0.0.1	127.0.0.1	TLSv1.2	349	Application Data
417	58.627757707	127.0.0.1	127.0.0.1	TLSv1.2	982	Application Data
418	58.627816518	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=30751 Ack=97080 Win=512 Len=0 TSval=671096861 TSe...
419	58.629273822	127.0.0.1	127.0.0.1	TLSv1.2	283	Application Data
420	58.629537005	127.0.0.1	127.0.0.1	TLSv1.2	133	Application Data
421	58.629600567	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=30966 Ack=97145 Win=512 Len=0 TSval=671096863 TSe...
422	58.629799171	127.0.0.1	127.0.0.1	TLSv1.2	283	Application Data
423	58.630022285	127.0.0.1	127.0.0.1	TLSv1.2	133	Application Data
424	58.630082499	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=31181 Ack=97210 Win=512 Len=0 TSval=671096864 TSe...
425	58.630267637	127.0.0.1	127.0.0.1	TLSv1.2	283	Application Data
426	58.630484846	127.0.0.1	127.0.0.1	TLSv1.2	133	Application Data
427	58.630543083	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=31396 Ack=97275 Win=512 Len=0 TSval=671096864 TSe...
428	58.630723331	127.0.0.1	127.0.0.1	TLSv1.2	283	Application Data
429	58.630930694	127.0.0.1	127.0.0.1	TLSv1.2	133	Application Data
430	58.630987538	127.0.0.1	127.0.0.1	TCP	68	54422 - 8191 [ACK] Seq=31611 Ack=97340 Win=512 Len=0 TSval=671096865 TSe...

Frame 1: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) on interface any, id 0

- Interface id: 0 (any)
- Encapsulation type: Linux cooked-mode capture (25)
- Arrival Time: Aug 25, 2020 18:52:34.951425438 EDT
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1598395954.951425438 seconds
- [Time delta from previous frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.000000000 seconds]
- Frame Number: 1
- Frame Length: 337 bytes (2696 bits)
- Capture Length: 337 bytes (2696 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: sll:ethertype:ip:tcp:tls]
- [Coloring Rule Name: TCP]
- [Coloring Rule String: tcp]

Linux cooked capture

▼ Linux cooked capture

- Packet type: Unicast to us (0)
- Link-layer address type: 772
- Link-layer address length: 6
- Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Unused: 0000
- Protocol: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 321
- Identification: 0xb114 (45332)
- Flags: 0x4000, Don't fragment
- Fragment offset: 0
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0x8aa0 [validation disabled]
- [Header checksum status: Unverified]
- Source: 127.0.0.1
- Destination: 127.0.0.1

```
▼ Transmission Control Protocol, Src Port: 54422, Dst Port: 8191, Seq: 1, Ack: 1, Len: 269
  Source Port: 54422
  Destination Port: 8191
  [Stream index: 0]
  [TCP Segment Len: 269]
  Sequence number: 1      (relative sequence number)
  Sequence number (raw): 2977703256
  [Next sequence number: 270      (relative sequence number)]
  Acknowledgment number: 1      (relative ack number)
  Acknowledgment number (raw): 3090581893
  1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x018 (PSH, ACK)
  Window size value: 512
  [Calculated window size: 512]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xff35 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
  TCP payload (269 bytes)
  ▶ Application Data
▼ Transport Layer Security
  ▶ TLSv1.2 Record Layer: Application Data Protocol: Application Data
```

Step 5: Enable Packet Profiling

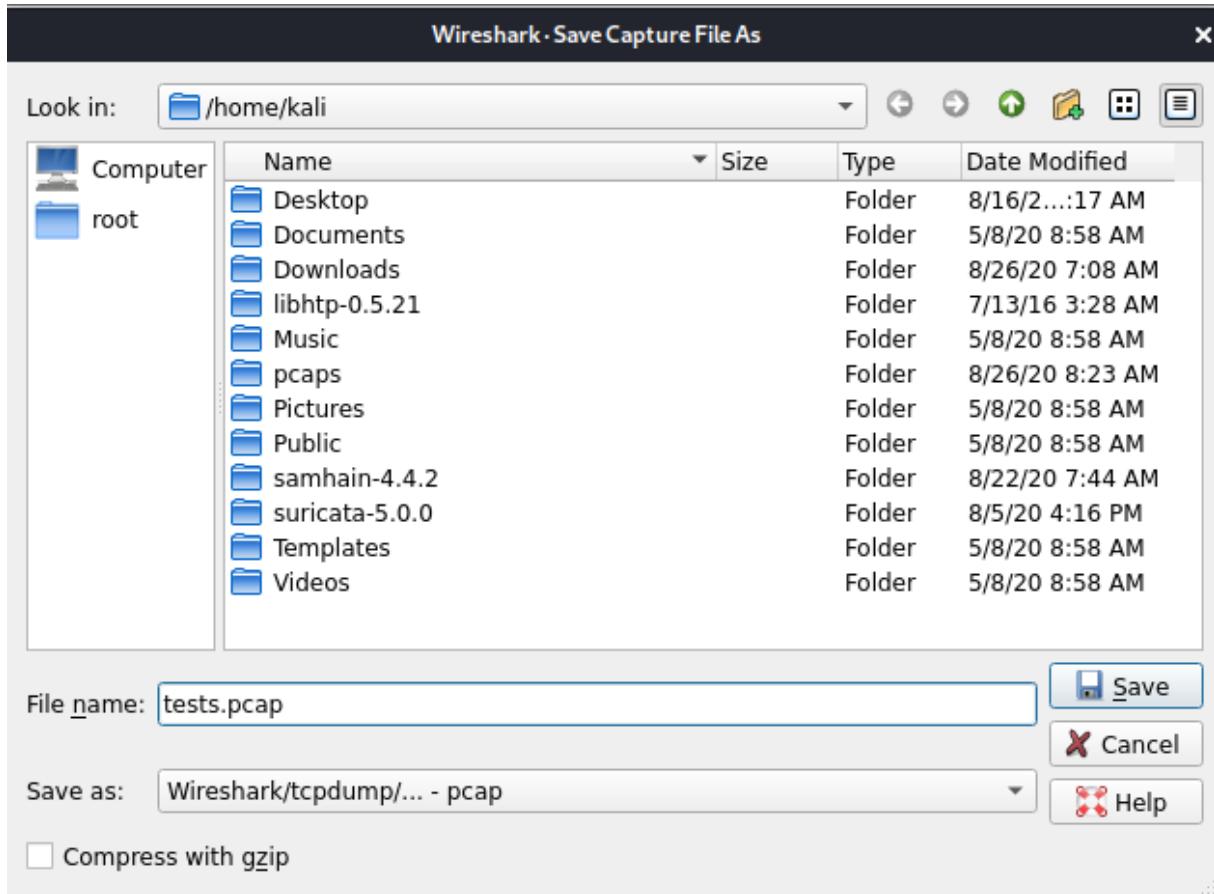
```
./configure --enable-profiling
```

```
root@kali:~/suricata/oisf# ./configure --enable-profiling
Trash
```

```
checking for pid_t ... yes
checking for mode_t ... yes
checking for size_t ... yes
checking for ssize_t ... yes
checking for int8_t ... yes
checking for int16_t ... yes
checking for int32_t ... yes
checking for int64_t ... yes
checking for uint8_t ... yes
checking for uint16_t ... yes
checking for uint32_t ... yes
checking for uint64_t ... yes
checking for u_int ... yes
checking for u_short ... yes
checking for u_long ... yes
checking for u_char ... yes
checking whether struct tm is in sys/time.h or time.h ... time.h
checking for struct tm.tm_zone ... yes
checking for ptrdiff_t ... yes
checking for stdbool.h that conforms to C99 ... (cached) yes
checking for _Bool ... yes
checking for stdlib.h ... (cached) yes
checking for GNU libc compatible malloc ... yes
checking for stdlib.h ... (cached) yes
checking for GNU libc compatible realloc ... yes
checking vfork.h usability ... no
checking vfork.h presence ... no
checking for vfork.h ... no
checking for fork ... yes
checking for vfork ... yes
checking for working fork ... yes
checking for working vfork ... (cached) yes
checking whether time.h and sys/time.h may both be included ... yes
checking for sys/time.h ... (cached) yes
checking for unistd.h ... (cached) yes
checking for stdlib.h ... (cached) yes
checking for sys/param.h ... (cached) yes
checking for alarm... yes
checking for working mktime ... yes
checking for getpagesize ... yes
checking for working mmap ... yes
checking for working strtod ... yes
checking for memmem ... yes
checking for memset ... yes
checking for memchr ... yes
checking for memrchr ... yes
```

Step 6 : Run Suricata with that pcap:

Create pcap file:



Welcome to Wireshark

Open

/home/kali/tests.pcap (43 KB)
/suricataW.pcap (219 KB)

```
suricata -c /etc/suricata/suricata.yaml -r tests.pcap
```

```
root@kali:/home/kali# suricata -c /etc/suricata/suricata.yaml -r tests.pcap
```

```
26/8/2020 -- 08:26:29 - <Notice> - This is Suricata version 5.0.3 RELEASE running in USER mode
26/8/2020 -- 08:26:29 - <Notice> - all 5 packet processing threads, 4 management threads initialized, engine started.
26/8/2020 -- 08:26:29 - <Notice> - Signal Received. Stopping engine.
26/8/2020 -- 08:26:29 - <Warning> - [ERRCODE: SC_ERR_INVALID_CHECKSUM(11)] - 1/1th of packets have an invalid checksum, consider setting pcap-file.checksum-checks variable to no or use '-k none' option on command line.
26/8/2020 -- 08:26:29 - <Notice> - Pcap-file module read 1 files, 84 packets, 42797 bytes
```

12.4 Suriwire

Suriwire is a plugin for wireshark that allow you to display suricata alert and protocol information as element of the protocol dissection.

Suriwire has parsing for the following events:

- Alerts
- HTTP
- fileinfo
- TLS
- SSH
- SMB

```
kali㉿kali:~/Downloads$ sudo tar -xvf suriwire-suriwire-0.2.tar.gz
suriwire-suriwire-0.2/
suriwire-suriwire-0.2/ChangeLog
suriwire-suriwire-0.2/INSTALL
suriwire-suriwire-0.2/LICENSE
suriwire-suriwire-0.2/README.rst
suriwire-suriwire-0.2/TODO
suriwire-suriwire-0.2/doc/
suriwire-suriwire-0.2/doc/suriwire.png
suriwire-suriwire-0.2/suriwire.lua
```

```
root@kali:/etc/wireshark# nano suriwire.lua
```

<https://github.com/regit/suriwire/blob/master/suriwire.lua>

NOTE : A search can be made on suricata.alert to view all packets that triggered a warning. suricata.alert.msg and suricata.alert.sid can be used to search for something more specific.

```

if (gui_enabled()) then
    local suri_proto = Proto("suricata", "Suricata Analysis")
    local suri_gid = ProtoField.string("suricata.alert.gid", "GID", FT_INTEGER)
    local suri_sid = ProtoField.string("suricata.alert.sid", "SID", FT_INTEGER)
    local suri_rev = ProtoField.string("suricata.alert.rev", "Rev", FT_INTEGER)
    local suri_msg = ProtoField.string("suricata.alert.msg", "Message", FT_STRING)
    local suri_tls_subject = ProtoField.string("suricata.tls.subject", "TLS subject", FT_STRING)
    local suri_tls_issuerdn = ProtoField.string("suricata.tls.issuerdn", "TLS issuer DN", FT_STRING)
    local suri_tls_fingerprint = ProtoField.string("suricata.tls.fingerprint", "TLS fingerprint", FT_STRING)
    local suri_tls_version = ProtoField.string("suricata.tls.version", "TLS version", FT_STRING)

    local suri_ssh_client_version = ProtoField.string("suricata.ssh.client.version", "SSH client version", FT_STRING)
    local suri_ssh_client_proto = ProtoField.string("suricata.ssh.client.proto", "SSH client protocol", FT_STRING)
    local suri_ssh_server_version = ProtoField.string("suricata.ssh.server.version", "SSH server version", FT_STRING)
    local suri_ssh_server_proto = ProtoField.string("suricata.ssh.server.proto", "SSH server protocol", FT_STRING)

    local suri_fileinfo_filename = ProtoField.string("suricata.fileinfo.filename", "Fileinfo filename", FT_STRING)
    local suri_fileinfo_magic = ProtoField.string("suricata.fileinfo.magic", "Fileinfo magic", FT_STRING)
    local suri_fileinfo_md5 = ProtoField.string("suricata.fileinfo.md5", "Fileinfo md5", FT_STRING)
    local suri_fileinfo_sha1 = ProtoField.string("suricata.fileinfo.sha1", "Fileinfo sha1", FT_STRING)
    local suri_fileinfo_sha256 = ProtoField.string("suricata.fileinfo.sha256", "Fileinfo sha256", FT_STRING)
    local suri_fileinfo_size = ProtoField.string("suricata.fileinfo.size", "Fileinfo size", FT_INTEGER)
    local suri_fileinfo_stored = ProtoField.string("suricata.fileinfo.stored", "Fileinfo stored", FT_STRING)

    local suri_http_url = ProtoField.string("suricata.http.url", "HTTP URL", FT_STRING)
    local suri_http_hostname = ProtoField.string("suricata.http.hostname", "HTTP hostname", FT_STRING)
    local suri_http_user_agent = ProtoField.string("suricata.http.user_agent", "HTTP user agent", FT_STRING)
    local suri_http_content_type = ProtoField.string("suricata.http.content_type", "HTTP Content Type", FT_STRING)
    local suri_http_method = ProtoField.string("suricata.http.method", "HTTP Method", FT_STRING)
    local suri_http_protocol = ProtoField.string("suricata.http.protocol", "HTTP Protocol", FT_STRING)
    local suri_http_status = ProtoField.string("suricata.http.status", "HTTP Status", FT_STRING)
    local suri_http_length = ProtoField.string("suricata.http.length", "HTTP Length", FT_STRING)
    local suri_http_referer = ProtoField.string("suricata.http.referer", "HTTP Referer", FT_STRING)

    local suri_smb_command = ProtoField.string("suricata.smb.command", "SMB Command", FT_STRING)
    local suri_smb_filename = ProtoField.string("suricata.smb.filename", "SMB Filename", FT_STRING)
    local suri_smb_share = ProtoField.string("suricata.smb.share", "SMB Share", FT_STRING)
    local suri_smb_status = ProtoField.string("suricata.smb.status", "SMB Status", FT_STRING)

local suri_prefs = suri_proto.prefs
local suri_running = false
local suri_alerts = {}

-- suri_prefs.suri_command = Pref.string("Suricata binary", "/usr/bin/suricata",
--                                         "Path to suricata binary")
-- suri_prefs.config_file = Pref.string("Suricata configuration", "/etc/suricata/suricata.yaml",
--                                         "Alert file containing information about pcap")

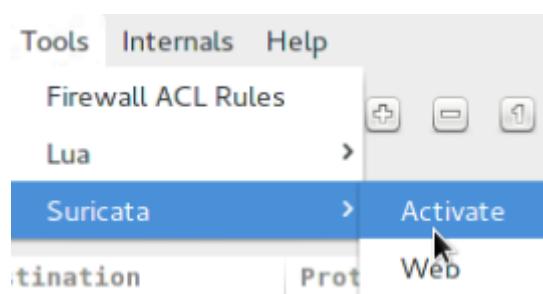
```

```

function suri_proto.dissector(buffer,pinfo,tree)
    if not(suri_alerts[pinfo.number] == nil) then
        for i, val in ipairs(suri_alerts[pinfo.number]) do
            if val['sid'] then
                subtree = tree:add(suri_proto,
                    "Suricata alert: "..val['sid'].." ("..val['msg'].."")")
                -- add protocol fields to subtree
                subtree:add(suri_gid, val['gid'])
                subtree:add(suri_sid, val['sid'])
                subtree:add(suri_rev, val['rev'])
                subtree:add(suri_msg, val['msg'])
                subtree:add_expert_info(PI_MALFORMED, PI_WARN, val['msg'])
            elseif val['tls_subject'] then
                subtree = tree:add(suri_proto, "Suricata TLS Info")
                -- add protocol fields to subtree
                subtree:add(suri_tls_subject, val['tls_subject'])
                subtree:add(suri_tls_issuerdn, val['tls_issuerdn'])
                subtree:add(suri_tls_fingerprint, val['tls_fingerprint'])
                subtree:add(suri_tls_version, val['tls_version'])
                subtree:add_expert_info(PI_REASSEMBLE, PI_NOTE, 'TLS Info')
            elseif val['ssh_client_version'] then
                subtree = tree:add(suri_proto, "Suricata SSH Info")
                -- add protocol fields to subtree
                subtree:add(suri_ssh_client_version, val['ssh_client_version'])
                subtree:add(suri_ssh_client_proto, val['ssh_client_proto'])
                subtree:add(suri_ssh_server_version, val['ssh_server_version'])
                subtree:add(suri_ssh_server_proto, val['ssh_server_proto'])
                subtree:add_expert_info(PI_REASSEMBLE, PI_NOTE, 'SSH Info')
            elseif val['fileinfo_filename'] then
                subtree = tree:add(suri_proto, "Suricata File Info")
                -- add protocol fields to subtree
                subtree:add(suri_fileinfo_filename, val['fileinfo_filename'])
                if val['fileinfo_magic'] then
                    subtree:add(suri_fileinfo_magic, val['fileinfo_magic'])
                end
                if val['fileinfo_md5'] then
                    subtree:add(suri_fileinfo_md5, val['fileinfo_md5'])
                end
                if val['fileinfo_sha1'] then
                    subtree:add(suri_fileinfo_sha1, val['fileinfo_sha1'])
                end
                if val['fileinfo_sha256'] then
                    subtree:add(suri_fileinfo_sha256, val['fileinfo_sha256'])
                end
                subtree:add(suri_fileinfo_size, val['fileinfo_size'])
                if val['fileinfo_stored'] then
                    subtree:add(suri_fileinfo_stored, val['fileinfo_stored'])
                end
            end
        end
    end
end

```

Wireshark with Suricata:



Using Capture Hardware

13.1 eBPF and XDP

(Berkeley Packet Filter)

eBPF is used for three things in Suricata:

- eBPF filter: any BPF like filter can be developed. A bypass implementation is also provided.
- eBPF load balancing: provide programmable load balancing.
- XDP programs: suricata can load XDP programs. A bypass program is provided.

Prerequisites

```
sudo apt install clang
```

```
root@kali:~# sudo apt-get install clang
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
clang is already the newest version (1:9.0-49.1).
clang set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 850 not upgraded.
```

```
git clone https://github.com/regit/linux.git
```

```
root@kali:~# git clone https://github.com/libbpf/libbpf.git
```

```
root@kali: ~ git clone https://github.com/tibopf/tibopf.git
Cloning into 'libbpf' ...
remote: Enumerating objects: 130, done.
remote: Counting objects: 100% (130/130), done.
remote: Compressing objects: 100% (49/49), done.
remote: Total 3773 (delta 73), reused 107 (delta 68), pack-reused 3643
Receiving objects: 100% (3773/3773), 2.18 MiB | 3.02 MiB/s, done.
Resolving deltas: 100% (2477/2477), done.
```

```
cd libbpf/src/
```

```
root@kali:~/libbpf/src#
```

```
root@kali:~/libbpf/src# make
```

```
Package libelf was not found in the pkg-config search path.
Perhaps you should add the directory containing `libelf.pc'
to the PKG_CONFIG_PATH environment variable
No package 'libelf' found
mkdir -p ./staticcobjs
cc -I.. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=64 -c bpf.c -o staticcobjs/bpf.o
cc -I.. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=64 -c btf.c -o staticcobjs/btf.o
btf.c:17:10: fatal error: gelf.h: No such file or directory
  17 | #include <gelf.h>
               ^
compilation terminated.
make: *** [Makefile:102: staticcobjs/btf.o] Error 1
root@kali:~/libbpf/src#
```

There was an error. Solution:

```
apt install libelf-dev
```

```
root@kali:~/libbpf/src# apt install libelf-dev
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdw1 libelf1
The following NEW packages will be installed:
  libelf-dev
The following packages will be upgraded:
  libdw1 libelf1
2 upgraded, 1 newly installed, 0 to remove and 848 not upgraded.
Need to get 74.5 kB/473 kB of archives.
After this operation, 232 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libelf-dev amd64 0.180-1+b1 [74.5 kB]
Fetched 74.5 kB in 22s (3,448 B/s)
Reading changelogs... Done
(Reading database ... 302440 files and directories currently installed.)
Preparing to unpack .../libdw1_0.180-1+b1_amd64.deb ...
Unpacking libdw1:amd64 (0.180-1+b1) over (0.176-1.1) ...
Preparing to unpack .../libelf1_0.180-1+b1_amd64.deb ...
Unpacking libelf1:amd64 (0.180-1+b1) over (0.176-1.1) ...
Selecting previously unselected package libelf-dev:amd64.
Preparing to unpack .../libelf-dev_0.180-1+b1_amd64.deb ...
Unpacking libelf-dev:amd64 (0.180-1+b1) ...
Setting up libelf1:amd64 (0.180-1+b1) ...
Setting up libdw1:amd64 (0.180-1+b1) ...
Setting up libelf-dev:amd64 (0.180-1+b1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.30-4) ...
```

Again:

```
root@kali:~/libbpf/src# make
```

```

64 -c libbpf.c -o staticobjs/libbpf.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c libbpf_errno.c -o staticobjs/libbpf_errno.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c netlink.c -o staticobjs/netlink.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c nlattr.c -o staticobjs/nlattr.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c str_error.c -o staticobjs/str_error.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c libbpf_probes.c -o staticobjs/libbpf_probes.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c bpf_prog_linfo.c -o staticobjs/bpf_prog_linfo.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c xsk.c -o staticobjs/xsk.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c btf_dump.c -o staticobjs/btf_dump.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c hashmap.c -o staticobjs/hashmap.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -c ringbuf.c -o staticobjs/ringbuf.o
ar rcs libbpf.a staticobjs/bpf.o staticobjs/btf.o staticobjs/libbpf.o staticobjs/libbpf_errno.o stati
cobjs/netlink.o staticobjs/nlattr.o staticobjs/str_error.o staticobjs/libbpf_probes.o staticobjs/bpf_
prog_linfo.o staticobjs/xsk.o staticobjs/btf_dump.o staticobjs/hashmap.o staticobjs/ringbuf.o
mkdir -p ./sharedobjs
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c bpf.c -o sharedobjs/bpf.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c btf.c -o sharedobjs/btf.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c libbpf.c -o sharedobjs/libbpf.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c libbpf_errno.c -o sharedobjs/libbpf_errno.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c netlink.c -o sharedobjs/netlink.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c nlattr.c -o sharedobjs/nlattr.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c str_error.c -o sharedobjs/str_error.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c libbpf_probes.c -o sharedobjs/libbpf_probes.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c bpf_prog_linfo.c -o sharedobjs/bpf_prog_linfo.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c xsk.c -o sharedobjs/xsk.o
cc -I. -I../include -I../include/uapi -g -O2 -Werror -Wall -D_LARGEFILE64_SOURCE -D_FILE_OFFSET_BITS=
64 -fPIC -fvisibility=hidden -DSHARED -c btf_dump.c -o sharedobjs/btf_dump.o

```

```

libbpf.so.0.2.0
ln -sf libbpf.so.0.2.0 libbpf.so.0
ln -sf libbpf.so.0 libbpf.so
sed -e "s|@PREFIX@|/usr|" \
      -e "s|@LIBDIR@|/usr/lib64|" \
      -e "s|@VERSION@|0.2.0|" \
      < libbpf.pc.template > libbpf.pc

```

Problem is solved.

```

root@kali:~/libbpf/src# make install

```

```
if [ ! -d '/usr/include/bpf' ]; then install -d -m 755 '/usr/include/bpf'; fi; install bpf.h libbpf.h  
btf.h xsk.h libbpf_util.h bpf_helpers.h bpf_helper_defs.h bpf_tracing.h bpf_endian.h bpf_core_read.h  
libbpf_common.h -m 644 '/usr/include/bpf'  
if [ ! -d '/usr/lib64/pkgconfig' ]; then install -d -m 755 '/usr/lib64/pkgconfig'; fi; install ./libb  
pf.pc -m 644 '/usr/lib64/pkgconfig'  
if [ ! -d '/usr/lib64' ]; then install -d -m 755 '/usr/lib64'; fi; cp -fpR ./libbpf.a ./libbpf.so ./l  
ibbpf.so.0 ./libbpf.so.0.2.0 '/usr/lib64'
```

sudo make install_headers

```
root@kali:~/libbpf/src# make install_headers
```

```
root@kali:~/libbpf/src# make install_headers  
if [ ! -d '/usr/include/bpf' ]; then install -d -m 755 '/usr/include/bpf'; fi; install bpf.h libbpf.h  
btf.h xsk.h libbpf_util.h bpf_helpers.h bpf_helper_defs.h bpf_tracing.h bpf_endian.h bpf_core_read.h  
libbpf_common.h -m 644 '/usr/include/bpf'
```

sudo ldconfig

```
root@kali:~/libbpf/src# sudo ldconfig  
root@kali:~/libbpf/src#
```

git clone <https://github.com/OISF/suricata.git>

```
root@kali:~/libbpf/src# git clone https://github.com/OISF/suricata.git  
  Trash
```

```
Cloning into 'suricata' ...  
remote: Enumerating objects: 67, done.  
remote: Counting objects: 100% (67/67), done.  
remote: Compressing objects: 100% (35/35), done.  
Receiving objects: 19% (15379/80098), 8.11 MiB | 623.00 KiB/s
```

```
  Remote: total 80098 (delta 67), reused 38 (delta 32), pack-reused 80051  
Receiving objects: 100% (80098/80098), 47.80 MiB | 871.00 KiB/s, done.  
Resolving deltas: 100% (63128/63128), done.  
root@kali:~/libbpf/src#
```

cd suricata && git clone https://github.com/OISF/libhtp.git -b 0.5.x

```
root@kali:~/libbpf/src# cd suricata && git clone https://github.com/OISF/libhttp.git -b 0.5.x
Cloning into 'libhttp'...
```

```
Cloning into 'libhttp' ...
remote: Enumerating objects: 38, done.
remote: Counting objects: 100% (38/38), done.
remote: Compressing objects: 100% (24/24), done.
Receiving objects: 21% (2329/10615), 3.79 MiB | 1.26 MiB/s
```

```
Receiving objects: 100% (10615/10615), 10.21 MiB | 800.00 KiB/s, done.
Resolving deltas: 100% (6498/6498), done.
```

```
./autogen.sh
```

```
root@kali:~/libbpf/src/suricata# ./autogen.sh
Trash
```

```
Found libtoolize
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
libtoolize: 'AC_PROG_RANLIB' is rendered obsolete by 'LT_INIT'
autoreconf: Entering directory `.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force -I m4
autoreconf: configure.ac: tracing
autoreconf: configure.ac: adding subdirectory libhttp to autoreconf
autoreconf: Entering directory `libhttp'
autoreconf: running: libtoolize --copy --force
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
```

```
configure.ac:9: installing './compile'
configure.ac:9: installing './config.guess'
configure.ac:9: installing './config.sub'
configure.ac:6: installing './install-sh'
configure.ac:6: installing './missing'
src/Makefile.am: installing './depcomp'
autoreconf: Leaving directory `.'
You can now run "./configure" and then "make".
```

```
CC=clang ./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/ \ --enable-ebpf --enable-ebpf-build
```

```
root@kali:~/libbpf/src/suricata# CC=clang ./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/ --enable-ebpf --enable-ebpf-build
```

```
checking for pcap.h ... yes
checking for pcap.h ... (cached) yes
checking for pcap/pcap.h ... yes
checking for pcap/bpf.h ... no
checking for libpcap ... yes
checking for pcap_open_live in -lpcap ... yes
checking for pcap_activate in -lpcap ... yes
checking for pcap-config ... /usr/bin/pcap-config
checking for pcap_set_buffer_size in -lpcap ... yes
```

```
checking whether GCC or Clang is our compiler... clang
checking for gawk ... (cached) gawk
checking for gcc ... (cached) clang
checking whether we are using the GNU C compiler ... (cached) yes
checking whether clang accepts -g ... (cached) yes
checking for clang option to accept ISO C89 ... (cached) none needed
checking whether clang understands -c and -o together... (cached) yes
checking dependency style of clang ... (cached) gcc3
checking how to run the C preprocessor ... clang -E
checking for ranlib ... (cached) ranlib
checking whether ln -s works ... yes
checking whether make sets $(MAKE) ... (cached) yes
checking for grep that handles long lines and -e ... (cached) /usr/bin/grep
checking for cygpath... no
checking for pkg-config ... /usr/bin/pkg-config
checking for python3 ... /usr/bin/python3
checking for python-distutils ... yes
checking for python-yaml ... yes
checking for wget ... /usr/bin/wget
checking stddef.h usability ... yes
checking stddef.h presence ... yes
checking for stddef.h ... yes
checking arpa/inet.h usability ... yes
checking arpa/inet.h presence ... yes
checking for arpa/inet.h ... yes
checking assert.h usability ... yes
checking assert.h presence ... yes
checking for assert.h... yes
checking ctype.h usability ... yes
checking ctype.h presence ... yes
checking for ctype.h ... yes
checking errno.h usability ... yes
checking errno.h presence ... yes
checking for errno.h... yes
checking fcntl.h usability ... yes
checking fcntl.h presence ... yes
checking for fcntl.h... yes
checking for inttypes.h ... (cached) yes
checking getopt.h usability ... yes
checking getopt.h presence ... yes
checking for getopt.h... yes
checking limits.h usability ... yes
checking limits.h presence ... yes
checking for limits.h... yes
checking netdb.h usability ... yes
checking netdb.h presence ... yes
checking for netdb.h... yes
checking netinet/in.h usability ...
```

```
checking for size_t ... yes
checking for ssize_t ... yes
checking for int8_t ... yes
checking for int16_t ... yes
checking for int32_t ... yes
checking for int64_t ... yes
checking for uint8_t ... yes
checking for uint16_t ... yes
checking for uint32_t ... yes
checking for uint64_t ... yes
checking for u_int ... yes
checking for u_short ... yes
checking for u_long ... yes
checking for u_char ... yes
checking whether struct tm is in sys/time.h or time.h ... time.h
checking for struct tm.tm_zone ... yes
checking for ptrdiff_t ... yes
checking for stdbool.h that conforms to C99 ... (cached) yes
checking for _Bool ... yes
checking for stdlib.h ... (cached) yes
checking for GNU libc compatible malloc ... yes
checking for stdlib.h ... (cached) yes
checking for GNU libc compatible realloc ... yes
checking vfork.h usability ... no
checking vfork.h presence ... no
checking for vfork.h ... no
checking for fork ... yes
checking for vfork
```

```

Python support: yes
Python path: /usr/bin/python3
Python distutils: yes
Python yaml: yes
Install suricatactl: yes
Install suricatasc: yes
Install suricata-update: not bundled
File System:
Profiling enabled: no
Profiling locks enabled: no

Plugin support (experimental): yes

Development settings:
Coccinelle / spatch: no
Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no

Generic build parameters:
Installation prefix: /usr
Configuration directory: /etc/suricata/
Log directory: /var/log/suricata/

--prefix /usr
--sysconfdir /etc
--localstatedir /var
--datarootdir /usr/share

Host: x86_64-pc-linux-gnu
Compiler: clang (exec name) / g++ (real)
GCC Protect enabled: no
GCC march native enabled: yes
GCC Profile enabled: no
Position Independent Executable enabled: no
CFLAGS -g -O2 -std=c11 -march=native -I${srcdir}/..//rust/gen -I${srcdir}/..//rust/dist
PCAP_CFLAGS -I/usr/include
SECCFLAGS

To build and install run 'make' and 'make install'.

You can run 'make install-conf' if you want to install initial configuration
files to /etc/suricata/. Running 'make install-full' will install configuration
and rules and provide you a ready-to-run suricata.

To install Suricata into /usr/bin/suricata, have the config in
/etc/suricata and use /var/log/suricata as log dir, use:
./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/

```

make clean && make

```

root@kali:~/libbpf/src/suricata# make clean && make

```

```
        built base - /root/libbpf/src/suricata/python
running clean
rm -rf scripts-* lib* build
find . -name \*.pyc -print0 | xargs -0 rm -f
rm -f *.lo
make[1]: Leaving directory '/root/libbpf/src/suricata/python'
Making clean in ebpf
make[1]: Entering directory '/root/libbpf/src/suricata/ebpf'
test -z ".*.bpf *.ll" || rm -f *.bpf *.ll
rm -rf .libs _libs
rm -f *.lo
make[1]: Leaving directory '/root/libbpf/src/suricata/ebpf'
make[1]: Entering directory '/root/libbpf/src/suricata'
test -z "stamp-h[0-9]*" || rm -f stamp-h[0-9]*
rm -rf .libs _libs
rm -f *.lo
make[1]: Leaving directory '/root/libbpf/src/suricata'
Making all in libhttp
make[1]: Entering directory '/root/libbpf/src/suricata/libhttp'
make all-recursive
make[2]: Entering directory '/root/libbpf/src/suricata/libhttp'
Making all in http
make[3]: Entering directory '/root/libbpf/src/suricata/libhttp/http'
Making all in lzma
make[4]: Entering directory '/root/libbpf/src/suricata/libhttp/http/lzma'
/bin/bash: /lib/modules/4.15.0-102-generic/build/include/uapi/linux/bpf.h: No such file or directory
make[4]: *** [Makefile:104: headers] Error 1
make[4]: Leaving directory '/root/libbpf/src/suricata/libhttp/http/lzma'
make[3]: *** [Makefile:104: headers] Error 1
make[3]: Leaving directory '/root/libbpf/src/suricata/libhttp/http'
make[2]: *** [Makefile:104: headers] Error 1
make[2]: Leaving directory '/root/libbpf/src/suricata/libhttp'
make[1]: *** [Makefile:104: headers] Error 1
make[1]: Leaving directory '/root/libbpf/src/suricata'
make: *** [Makefile:104: headers] Error 1
```

```
Making all in rust
make[1]: Entering directory '/root/libbpf/src/suricata/rust'
\
  CARGO_HOME="/root/.cargo" \
  CARGO_TARGET_DIR="/root/libbpf/src/suricata/rust/target" \
  /usr/bin/cargo build --release \
    --features "
  Updating crates.io index
  Downloaded time v0.1.44
  Compiling autocfg v1.0.1
  Compiling cfg-if v0.1.9
  Compiling semver-parser v0.7.0
  Compiling ryu v1.0.5
  Compiling arrayvec v0.4.12
  Compiling libc v0.2.76
  Compiling bitflags v1.2.1
  Building [> ] 3/103: bitflags(build.r...
```

```
  Finished release [optimized + debuginfo] target(s) in 4m 19s
make gen/rust-bindings.h
make[2]: Entering directory '/root/libbpf/src/suricata/rust'
rm -f gen/rust-bindings.h
cbindgen --config /root/libbpf/src/suricata/rust/cbindgen.toml \
    --quiet --output /root/libbpf/src/suricata/rust/gen/rust-bindings.h
make[2]: Leaving directory '/root/libbpf/src/suricata/rust'
make[1]: Leaving directory '/root/libbpf/src/suricata/rust'
Making all in src
make[1]: Entering directory '/root/libbpf/src/suricata/src'
make  all-am
make[2]: Entering directory '/root/libbpf/src/suricata/src'
  CC      main.o
  CC      alert-debuglog.o
  CC      alert-fastlog.o
  CC      alert-prelude.o
  CC      alert-syslog.o
  CC      app-layer.o
  CC      app-layer-dcerpc.o
  CC      app-layer-dcerpc-udp.o
  CC      app-layer-detect-proto.o
  CC      app-layer-dnp3.o
  CC      app-layer-dnp3-objects.o
```

```
/usr/include/x86_64-linux-gnu/gnu/stubs.h:7:11: fatal error: 'gnu/stubs-32.h' file not found
# include <gnu/stubs-32.h>
          ^~~~~~
1 error generated.
make[1]: *** [Makefile:540: xdp_lb.bpf] Error 1
make[1]: Leaving directory '/root/libbpf/src/suricata/ebpf'
make: *** [Makefile:490: all-recursive] Error 1
make: *** Deleting directory '/root/libbpf/src/suricata'"
```

There was an error. Solution:

```
sudo apt-get install g++-multilib libc6-dev-i386
```

```
root@kali:~/libbpf/src/suricata# sudo apt-get install g++-multilib libc6-dev-i386
Trash
```

```

Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu cpp cpp-10 g++ g++-10 g++-10-multilib gcc gcc-10 gcc-10-base g
lib32atomic1c1 lib32gcc-10-dev lib32gcc-s1 lib32gomp1 lib32itm1 lib32quadmath0 lib32stdc++-10-dev lib32stdc++6 lib3
libbinutils libc6-dev-x32 libc6-x32 libcc1-0 libctf0 libgcc-10-dev libgcc-s1 libgfortran5 libgomp1 libitm1 liblsa
libstdc++-10-dev libstdc++6 libtsan0 libubsan1 libx32asan6 libx32atomic1 libx32gcc-10-dev libx32gcc-s1 libx32gomp
libx32stdc++-10-dev libx32stdc++6 libx32ubsan1
Suggested packages:
binutils-doc cpp-doc gcc-10-locales gcc-10-doc lib32stdc++6-10-dbg libx32stdc++6-10-dbg gcc-doc libstdc++-10-doc
lib32gcc1
The following NEW packages will be installed:
cpp-10 g++-10 g++-10-multilib g++-multilib gcc-10 gcc-10-multilib gcc-multilib lib32asan6 lib32atomic1 lib32gcc-1
lib32quadmath0 lib32stdc++-10-dev lib32ubsan1 libasan6 libc6-dev-i386 libc6-dev-x32 libc6-x32 libgcc-10-dev libst
libx32gcc-10-dev libx32gcc-s1 libx32gomp1 libx32itm1 libx32quadmath0 libx32stdc++-10-dev libx32stdc++6 libx32uba
The following packages will be upgraded:
binutils binutils-common binutils-x86_64-linux-gnu cpp g++ gcc gcc-10-base lib32gcc-s1 lib32stdc++6 libatomic1 li
libgfortran5 libgomp1 libitm1 liblsan0 libobjc4 libquadmath0 libstdc++6 libtsan0 libubsan1
23 upgraded, 31 newly installed, 1 to remove and 817 not upgraded.
Need to get 54.4 MB/58.8 MB of archives.
After this operation, 227 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
8% [Working]

```

```

Setting up cpp (4:10.1.0-1) ...
Setting up binutils-x86_64-linux-gnu (2.35-1) ...
Setting up libx32stdc++6 (10.1.0-6) ...
Setting up libstdc++-10-dev:amd64 (10.1.0-6) ...
Setting up libx32ubsan1 (10.1.0-6) ...
Setting up binutils (2.35-1) ...
Setting up lib32gcc-10-dev (10.1.0-6) ...
Setting up gcc-10 (10.1.0-6) ...
Setting up lib32stdc++-10-dev (10.1.0-6) ...
Setting up libx32gcc-10-dev (10.1.0-6) ...
Setting up g++-10 (10.1.0-6) ...
Setting up libx32stdc++-10-dev (10.1.0-6) ...
Setting up gcc (4:10.1.0-1) ...
Setting up gcc-10-multilib (10.1.0-6) ...
Setting up g++ (4:10.1.0-1) ...
Setting up g++-10-multilib (10.1.0-6) ...
Setting up gcc-multilib (4:10.1.0-1) ...
Setting up g++-multilib (4:10.1.0-1) ...
Processing triggers for kali-menu (2020.2.2) ...
Processing triggers for libc-bin (2.31-2) ...
Processing triggers for man-db (2.9.1-1) ...

```

Again:

```

root@kali:~/libbpf/src/suricata# make clean && make

```

```
llc-9 -march=bpf -filetype=obj xdp_filter.ll -o xdp_filter.bpf
rm -f xdp_filter.ll
clang -Wall -Iinclude -O2 \
    -I/usr/include/x86_64-linux-gnu/ \
    -D__KERNEL__ -D__ASM_SYSREG_H \
    -target bpf -S -emit-llvm xdp_lb.c -o xdp_lb.ll
llc-9 -march=bpf -filetype=obj xdp_lb.ll -o xdp_lb.bpf
rm -f xdp_lb.ll
clang -Wall -Iinclude -O2 \
    -I/usr/include/x86_64-linux-gnu/ \
    -D__KERNEL__ -D__ASM_SYSREG_H \
    -target bpf -S -emit-llvm vlan_filter.c -o vlan_filter.ll
llc-9 -march=bpf -filetype=obj vlan_filter.ll -o vlan_filter.bpf
rm -f vlan_filter.ll
make[1]: Leaving directory '/root/libbpf/src/suricata/ebpf'
make[1]: Entering directory '/root/libbpf/src/suricata'
make[1]: Nothing to be done for 'all-am'.
make[1]: Leaving directory '/root/libbpf/src/suricata'
```

problem is solved.

```
root@kali:~/libbpf/src/suricata# make install-full
Trash
```

```
root@kali:~/libbpf/src/suricata# sudo ldconfig
root@kali:~/libbpf/src/suricata#
```

```
sudo mkdir /usr/libexec/suricata/ebpf/
```

```
root@kali:/usr/libexec# sudo mkdir /usr/libexec/suricata/ebpf/
Trash
```

```
./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/ \ --enable-ebpf --enable-ebpf-build -
-with-clang=/usr/bin/clang
```

```
root@kali:~/libbpf/src/suricata# ./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/ --enable-ebpf --enable-ebpf-build --with-clang=/usr/
bin/clang
```

The clang compiler is needed if you want to build eBPF files as the build is done via a specific eBPF backend.

```
checking for special C compiler options needed for large files... no
checking for _FILE_OFFSET_BITS value needed for large files... no
checking host os... installation for x86_64-pc-linux-gnu OS... ok
checking for c11 support... yes
checking for thread local storage gnu __thread support... yes
checking for dlfcn.h... (cached) yes
checking for plugin support... yes
checking checking if gcc supports -march=native... yes
checking for g++... g++
checking whether we are using the GNU C++ compiler... yes
checking whether g++ accepts -g... yes
checking dependency style of g++... gcc3
checking how to run the C++ preprocessor... g++ -E
checking for ld used by g++... /usr/bin/ld -m elf_x86_64
checking if the linker (/usr/bin/ld -m elf_x86_64) is GNU ld... yes
checking whether the g++ linker (/usr/bin/ld -m elf_x86_64) supports shared libraries... yes
checking for g++ option to produce PIC... -fPIC -DPIC
checking if g++ PIC flag -fPIC -DPIC works... yes
checking if g++ static flag -static works... yes
checking if g++ supports -c -o file.o... yes
checking if g++ supports -c -o file.o... (cached) yes
checking whether the g++ linker (/usr/bin/ld -m elf_x86_64) supports shared libraries... yes
checking dynamic linker characteristics... (cached) GNU/Linux ld.so
checking how to hardcode library paths into programs... immediate
```

To build and install run 'make' and 'make install'.

You can run 'make install-conf' if you want to install initial configuration files to /etc/suricata/. Running 'make install-full' will install configuration and rules and provide you a ready-to-run suricata.

To install Suricata into /usr/bin/suricata, have the config in /etc/suricata and use /var/log/suricata as log dir, use:
./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/

13.2 Setup bypass

```
root@kali:~/libbpf/src/suricata# ls
aclocal.m4      compile    configure.ac  etc        m4        qa          suricata.yaml
acsite.m4       config.guess  contrib     install-sh  Makefile   README.md
appveyor.yml   config.log   COPYING     libhttp    Makefile.am  rules
autogen.sh      config.rpath depcomp     libtool   Makefile.cvs  rust
autom4te.cache config.status doc        LICENSE   Makefile.in  scripts
benches         config.sub   doxygen.cfg ltmain.sh missing   src
ChangeLog       configure   ebpf       lua       python   suricata-update
root@kali:~/libbpf/src/suricata# nano suricata.yaml
```

```
"stream:
memcap: 64mb
bypass:true
checksum-validation: yes      # reject incorrect csyms
inline: auto                  # auto will use inline mode in IPS mode, yes or no set it statically
reassembly:
memcap: 256mb
depth: 1mb                    # reassemble 1mb into a stream
toserver-chunk-size: 2560
toclient-chunk-size: 2560
randomize-chunk-size: yes
#randomize-chunk-range: 10
#raw: yes
#segment-prealloc: 2048
#check-overlap-different-data: true
```

```
app-layer:
protocols:
  rfb:
    enabled: yes
    detection-ports:
      dp: 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909
    # MQTT, disabled by default.
  mqtt:
    # enabled: no
    # max-msg-length: 1mb
  krb5:
    enabled: yes
  snmp:
    enabled: yes
  ikev2:
    enabled: yes
  tls:
    enabled: yes
    detection-ports:
      dp: 443
encryption-handling: bypass
```

13.3 Setup eBPF filter:

Suricata can load as eBPF filter any eBPF code exposing a filter section.

```
cp ebpf/vlan_filter.bpf /usr/libexec/ebpf/
```

```
root@kali:~/libbpf/src/suricata# cp ebpf/vlan_filter.bpf /usr/libexec/ebpf  
root@kali:~/libbpf/src/suricata#
```

suricata.yaml:

```
#copy-irule. ebnr  
# For eBPF and XDP setup including bypass, filter and load balancing, please  
# see doc/userguide/capture-hardware/ebpf-xdp.rst for more info.  
ebpf-filter-file: /usr/libexec/ebpf/vlan_filter.bpf
```

```
/usr/bin/suricata --pidfile /var/run/suricata.pid --af-packet=eth3 -vvv
```

Run suricata.

```
root@kali:~/libbpf/src/suricata# /usr/bin/suricata --pidfile /var/run/suricata.pid --af-packet=eth3 -vvv
```

```
[21126] 28/8/2020 -- 12:15:10 - (runmode-af-packet.c:706) <Config> (ParseAFPConfig) -- eth3: enabling zero copy mode by using data release call  
[21126] 28/8/2020 -- 12:15:10 - (util-runmodes.c:264) <Info> (RunModeSetLiveCaptureWorkersForDevice) -- Going to use 4 thread(s)  
[21126] 28/8/2020 -- 12:15:10 - (flow-manager.c:1063) <Config> (FlowManagerThreadSpawn) -- using 1 flow manager threads  
[21139] 28/8/2020 -- 12:15:10 - (flow-manager.c:806) <Notice> (FlowManager) -- FM FM#01/0 starting. min_timeout 30s. Full hash pass in 240s  
[21126] 28/8/2020 -- 12:15:10 - (flow-manager.c:1266) <Config> (FlowRecyclerThreadSpawn) -- using 1 flow recycler threads  
[21126] 28/8/2020 -- 12:15:10 - (unix-manager.c:132) <Info> (UnixNew) -- Using unix socket file '/var/run/suricata-command.socket'  
[21126] 28/8/2020 -- 12:15:10 - (tm-threads.c:1965) <Notice> (TmThreadWaitOnThreadInit) -- all 4 packet processing threads, 4 management threads initialized, engine started.
```

```
[2815] 28/8/2020 -- 12:37:13 - (runmode-af-packet.c:706) <Config> (ParseAFPConfig) -- eth3: enabling zero copy mode by using data release call  
[2815] 28/8/2020 -- 12:37:13 - (util-runmodes.c:264) <Info> (RunModeSetLiveCaptureWorkersForDevice) -- Going to use 4 thread(s)  
[2815] 28/8/2020 -- 12:37:13 - (flow-manager.c:1063) <Config> (FlowManagerThreadSpawn) -- using 1 flow manager threads  
[2826] 28/8/2020 -- 12:37:13 - (flow-manager.c:806) <Notice> (FlowManager) -- FM FM#01/0 starting. min_timeout 30s. Full hash pass in 240s  
[2815] 28/8/2020 -- 12:37:13 - (flow-manager.c:1266) <Config> (FlowRecyclerThreadSpawn) -- using 1 flow recycler threads  
[2815] 28/8/2020 -- 12:37:13 - (unix-manager.c:132) <Info> (UnixNew) -- Using unix socket file '/var/run/suricata-command.socket'  
[2815] 28/8/2020 -- 12:37:13 - (tm-threads.c:1965) <Notice> (TmThreadWaitOnThreadInit) -- all 4 packet processing threads, 4 management threads initialized, engine started.
```

```
/usr/bin/suricata --pidfile /var/run/suricata.pid --af-packet=eth0 -vvv
```

```
root@kali:~/libbpf/src/suricata# /usr/bin/suricata --pidfile /var/run/suricata.pid --af-packet=eth0 -vvv
```

```
[2924] 28/8/2020 -- 12:38:58 - (suricata.c:1066) <Notice> (LogVersion) -- This is Suricata version 6.0.0-dev (d3cf2c21d 2020-08-25) running in SYSTEM mode
[2924] 28/8/2020 -- 12:38:58 - (util-cpu.c:178) <Info> (UtilCpuPrintSummary) -- CPUs/cores online: 4
[2924] 28/8/2020 -- 12:38:58 - (app-layer-ntp.c:2419) <Config> (HTPConfigSetDefaultsPhase2) -- 'default' server has 'request-body-minimal-inspect-size' set to 32655 and 'request-body-inspect-window' set to 4045 after randomization.
[2924] 28/8/2020 -- 12:38:58 - (app-layer-ntp.c:2437) <Config> (HTPConfigSetDefaultsPhase2) -- 'default' server has 'response-body-minimal-inspect-size' set to 40498 and 'response-body-inspect-window' set to 16033 after randomization.
[2924] 28/8/2020 -- 12:38:58 - (app-layer-smb.c:316) <Config> (RegisterSMBParsers) -- SMB stream depth: 0
[2924] 28/8/2020 -- 12:38:58 - (app-layer-modbus.c:1514) <Config> (RegisterModbusParsers) -- Protocol detection and parser disabled for modbus protocol.
[2924] 28/8/2020 -- 12:38:58 - (app-layer-enip.c:464) <Config> (RegisterENIPUDPParsers) -- Protocol detection and parser disabled for enip protocol.
[2924] 28/8/2020 -- 12:38:58 - (app-layer-dnp3.c:1606) <Config> (RegisterDNP3Parsers) -- Protocol detection and parser disabled for DNP3.
[2924] 28/8/2020 -- 12:38:58 - (util-ioctl.c:112) <Info> (GetIfaceMTU) -- Found an MTU of 1500 for 'eth0'
[2924] 28/8/2020 -- 12:38:58 - (util-ioctl.c:112) <Info> (GetIfaceMTU) -- Found an MTU of 1500 for 'eth0'
```

13.4 Setup eBPF bypass

suricata.yaml:

```
ebpf-filter-file: /usr/libexec/ebpf/bypass_filter.bpf
```

```
bypass: yes
```

```
#copy-mode: ips
#copy-iface: eth1
# For eBPF and XDP setup including bypass, filter and load balancing, please
# see doc/userguide/capture-hardware/ebpf-xdp.rst for more info.
ebpf-filter-file: /usr/libexec/ebpf/vlan_filter.bpf
ebpf-filter-file: /usr/libexec/ebpf/bypass_filter.bpf
bypass: yes
```

```
root@kali:~/libbpf/src/suricata# cp ebpf/lb.bpf /usr/libexec/ebpf
root@kali:~/libbpf/src/suricata#
```

CHAPTER 14

Splunk Free for Suricata

14.1 What is Splunk?

It is a SIEM (log monitoring) solution that can collect logs from various sources (server, firewall), store the logs it collects, search, research and analyze the stored logs.

By quickly identifying potential problems, it can trigger human or automatic responses to stop attacks before they complete.

It is a statistical, visual program that is useful for monitoring the logs of suricata and similar programs.

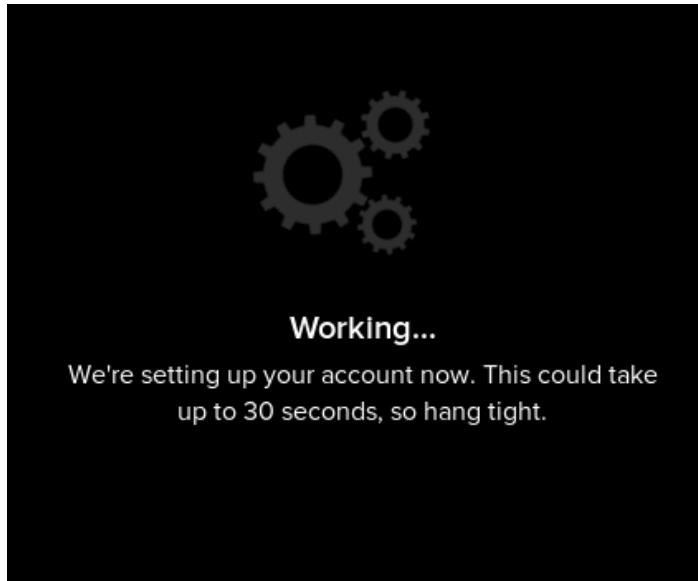
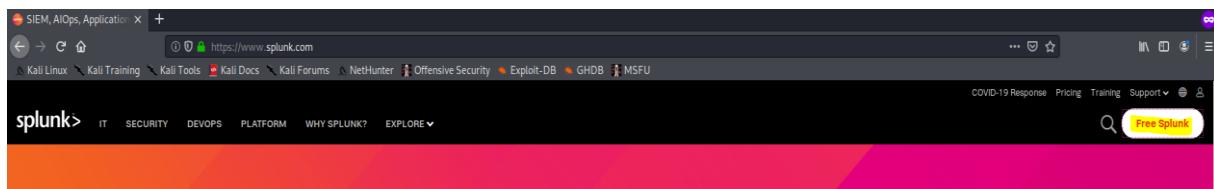
14.2 How does it work?

It centralizes security setting analytics, pulls relevant assets and identities from networks, endpoints, cloud applications and other sources, and displays them under a single dashboard. This means that IT managers can spend less time collecting data and more time analyzing incidents and determining response.

14.3 Splunk installation on Kali

Step 1: Go to the website and download.

www.splunk.com



Step 2: Choose to Download according to the operating system.

I chose .deb because Kali Linux is based on Debian.



Splunk Enterprise 8.0.5

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package



64-bit

2.6+, 3.x+, or 4.x+ kernel Linux distributions

.deb

376.61 MB

[Download Now](#)

.tgz

488.16 MB

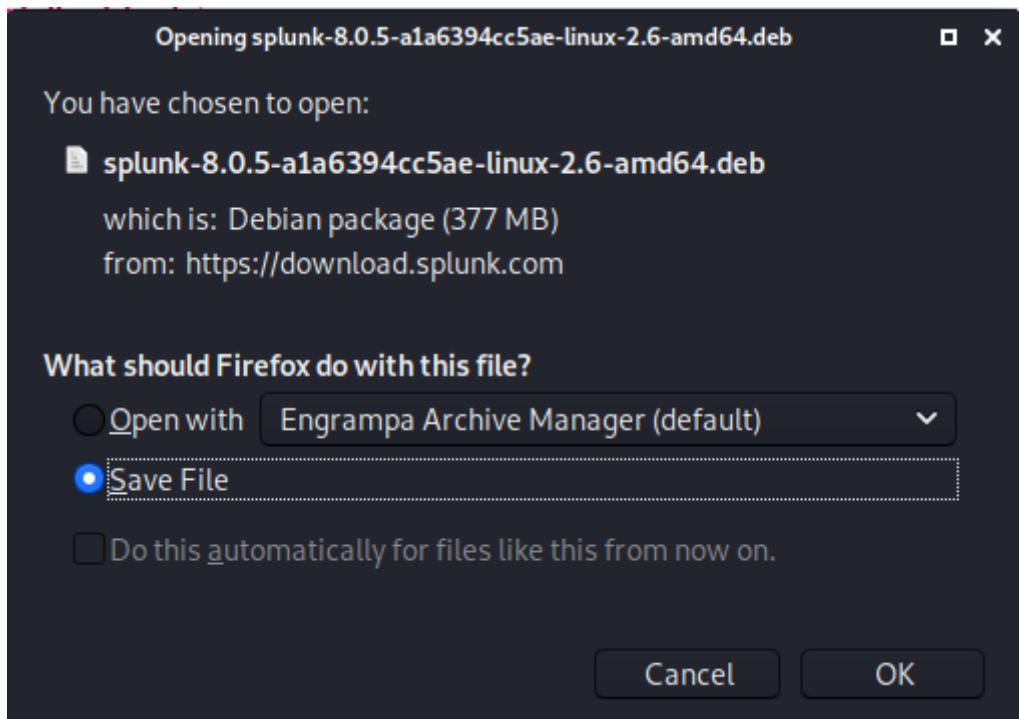
[Download Now](#)

.rpm

488.49 MB

[Download Now](#)

[Release Notes](#) | [System Requirements](#) | [Older Releases](#) | [All Other Downloads](#)



Step 3: Installing the package from the terminal.

dpkg : package manager for Debian

dpkg is the software that forms the basis of the Debian package management system.

Used to get information about .deb packages, install and uninstall them.

```
sudo dpkg -i splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb
```

```
kali㉿kali:~$ cd Downloads
kali㉿kali:~/Downloads$ ls
splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb
kali㉿kali:~/Downloads$ sudo dpkg -i splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb
```

```
Selecting previously unselected package splunk.
(Reading database ... 282537 files and directories currently installed.)
Preparing to unpack splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb ...
Unpacking splunk (8.0.5) ...
Setting up splunk (8.0.5) ...
complete
```

Step 4: Start the Splunk

```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# cd /opt/
root@kali:/opt# ls
splunk
root@kali:/opt# cd splunk
root@kali:/opt/splunk# ls
bin          ftr      license-eula.txt  share
copyright.txt  include  openssl        splunk-8.0.5-a1a6394cc5ae-linux-2.6-x86_64-manifest
etc          lib      README-splunk.txt
root@kali:/opt/splunk# cd bin
root@kali:/opt/splunk/bin#
```

```
./splunk start
```

```
root@kali:/opt/splunk/bin# ./splunk start
[trash]

SPLUNK GENERAL TERMS (v1.2020)

Do you agree with this license? [y/n]: y

Signature ok
subject=/CN=kali/O=SplunkUser
Getting CA Private Key
writing RSA key
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://kali:8000
```

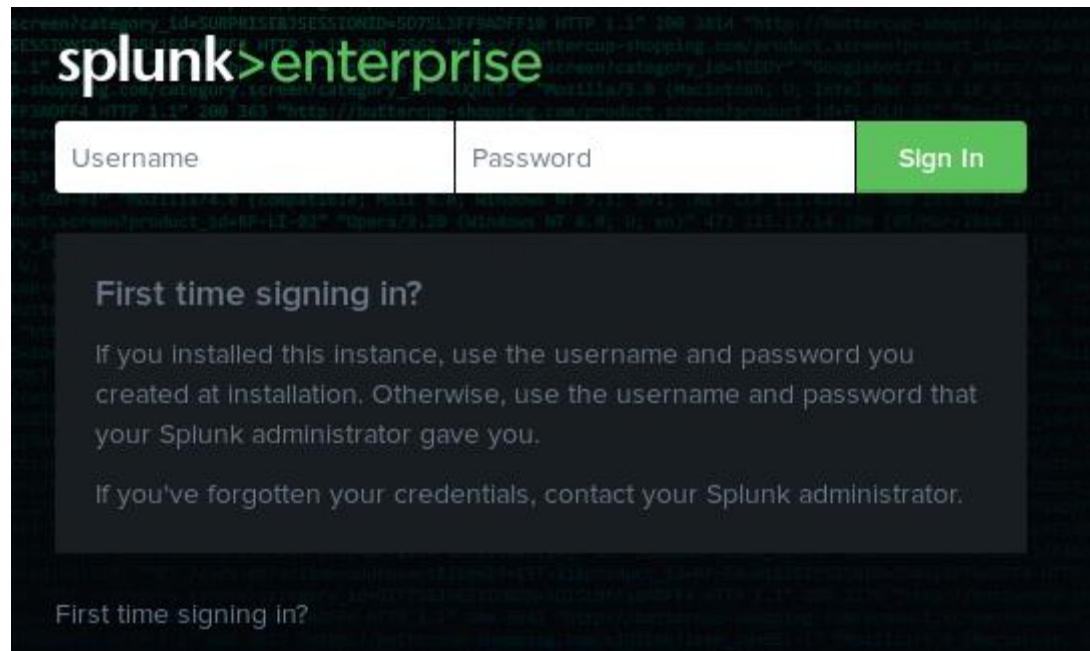
NOTE: For automatic start of splunk in case of force closing of splunk:

```
root@kali:/opt/splunk/bin# ./splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
```

Step 5: Register

go to this website.

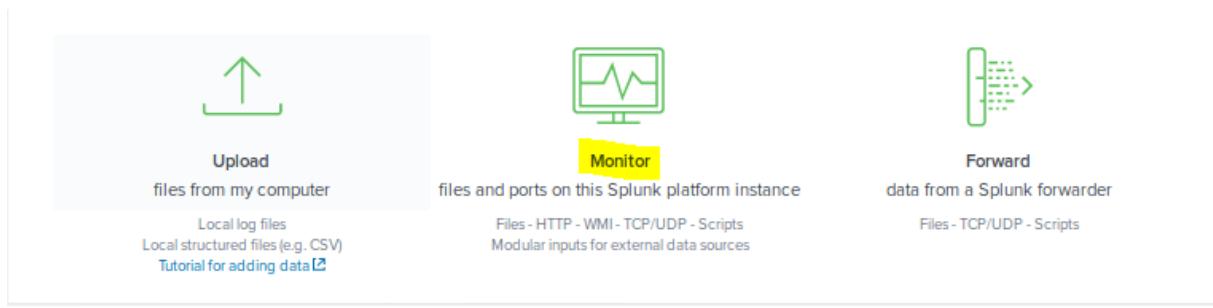
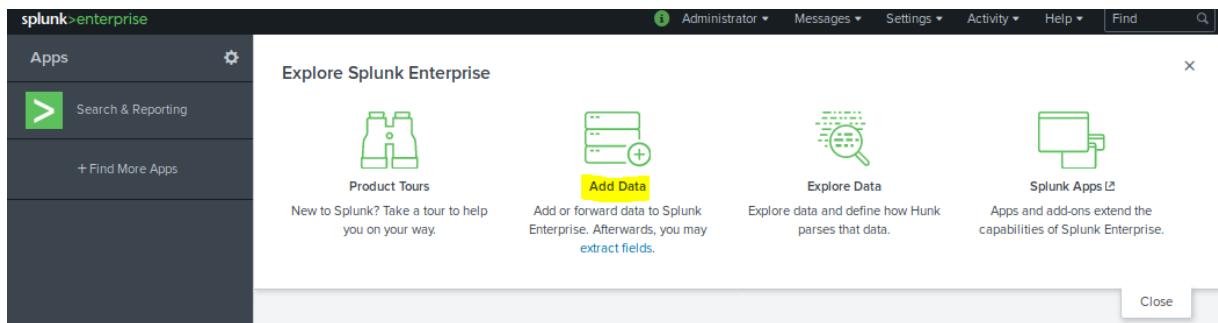
```
The Splunk web interface is at http://kali:8000
```



Installation complete.

14.4 How to use Splunk?

Add data to collect the logs of the server.



This screenshot shows the 'Add Data' configuration page. On the left, there's a sidebar with sections: 'Files & Directories' (highlighted in yellow), 'HTTP Event Collector', 'TCP / UDP', and 'Scripts'. The 'Files & Directories' section contains a sub-section: 'Upload a file, index a local file, or monitor an entire directory.' On the right, there's a large text input field with placeholder text: 'Select an option' and a left arrow icon.

- i** Data preview will be skipped, it is not supported for directories.

File or Directory ?	/var/log	Browse
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.		
Whitelist ?	optional	
Blacklist ?	optional	

Logs in linux are kept in this directory.

Review

Input Type Directory Monitor
Source Path /var/log
Whitelist N/A
Blacklist N/A
Source Type Automatic
App Context search
Host kali
Index default

After the necessary configuration, the search is started.

✓ File input has been created successfully.

Configure your inputs by going to [Settings > Data Inputs](#)

[Start Searching](#)

Search your data now or see [examples and tutorials](#).

[Add More Data](#)

Add more data inputs now or see [examples and tutorials](#).

[Download Apps](#)

Apps help you do more with your data. [Learn more](#).

[Build Dashboards](#)

Visualize your searches. [Learn more](#).

i	Time	Event
>	8/21/20 2:55:41:000 PM	[...] 43.842] x.Org X Server 1.20.8 X Protocol Version 11, Revision 0 [...] 43.843] Build Operating System: Linux 4.19.0-8-amd64 x86_64 Debian [...] 43.843] Current Operating System: Linux kali 5.5.0-kali2-amd64 #1 SMP Debian 5.5.17-1kali1 (2020-04-21) x86_64 Show all 6 lines host = kali source = /var/log/Xorg.0.log sourcetype = Xorg
>	8/21/20 2:55:01:000 PM	Aug 21 14:55:01 kali CRON[2987]: (root) CMD (command -v debian-sal > /dev/null && debian-sal 1 1) host = kali source = /var/log/syslog sourcetype = syslog
>	8/21/20 2:55:01:000 PM	Aug 21 14:55:01 kali CRON[2986]: pam_unix(cron:session): session closed for user root host = kali source = /var/log/auth.log sourcetype = syslog
>	8/21/20 2:55:01:000 PM	Aug 21 14:55:01 kali CRON[2986]: pam_unix(cron:session): session opened for user root by (uid=0) host = kali source = /var/log/auth.log sourcetype = syslog
>	8/21/20 2:54:41:000 PM	Aug 21 14:54:41 kali NetworkManager[639]: <info> [1598036081.3000] dhcp4 (eth1): state changed timeout -> done host = kali source = /var/log/syslog sourcetype = syslog
>	8/21/20 2:54:41:000 PM	Aug 21 14:54:41 kali NetworkManager[639]: <info> [1598036081.2998] dhcp4 (eth1): canceled DHCP transaction host = kali source = /var/log/syslog sourcetype = syslog
>	8/21/20 2:54:41:000 PM	Aug 21 14:54:41 kali NetworkManager[639]: <info> [1598036081.2764] device (eth1): state change: failed -> disconnected (reason 'none', sysiface-state: 'managed') host = kali source = /var/log/syslog sourcetype = syslog

14.5 Splunk for Suricata

Step 1 : Editing

Eve JSON Output

```
root@kali:/etc/suricata# nano eve.json
```

- eve-log:

```
    enabled: yes
    type: file #file|syslog|unix_dgram|unix_stream
    filename: eve.json
    # the following are valid when type: syslog above
    #identity: "suricata"
    #facility: local5
    #level: Info ## possible levels: Emergency, Alert, Critical,
    ## Error, Warning, Notice, Info, Debug
```

types:

- alert

- http:

```
    extended: yes # enable this for extended logging information
    # custom allows additional http fields to be included in eve-log
    # the example below adds three additional fields when uncommented
    #custom: [Accept-Encoding, Accept-Language, Authorization]
```

- dns

- tls:

```
    extended: yes # enable this for extended logging information
```

- files:

```
    force-magic: no # force logging magic on all logged files
```

```
    force-md5: no # force logging of md5 checksums
```

#- drop

- ssh

```
GNU nano 4.9.2                                         eve.json
File: /etc/suricata/eve.json
["timestamp": "2020-08-24T09:14:44.896558-0400", "event_type": "stats", "stats": {"uptime": 0, "decoder": {"pkts": 0, "bytes": 0}}, {"timestamp": "2020-08-24T09:19:00.293802-0400", "event_type": "stats", "stats": {"uptime": 0, "decoder": {"pkts": 0, "bytes": 0}}}

- eve-log:
  enabled: yes
  type: file #file|syslog|unix_dgram|unix_stream
  filename: eve.json
  # the following are valid when type: syslog above
  #identity: "suricata"
  #facility: local5
  #level: Info ## possible levels: Emergency, Alert, Critical,
  #           ## Error, Warning, Notice, Info, Debug
  types:
    - alert
    - http:
      extended: yes      # enable this for extended logging information
      # custom allows additional http fields to be included in eve-log
      # the example below adds three additional fields when uncommented
      #custom: [Accept-Encoding, Accept-Language, Authorization]
    - dns
    - tls:
      extended: yes      # enable this for extended logging information
    - files:
      force-magic: no   # force logging magic on all logged files
      force-md5: no     # force logging of md5 checksums
    #- drop
  - ssh
```

```
GNU nano 4.9.2                                         fast.log
File: /etc/suricata/fast.log
- fast:
  enabled: yes
  filename: fast.log
  append: yes
  #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'
```

```
GNU nano 4.9.2                                         ssh.json
File: /etc/suricata/ssh.json
- eve-log:
  enabled: yes
  filetype: regular
  filename: ssh.json
  types:
    - ssh
```

```
root@kali:~# sudo service suricata restart
root@kali:~#
```

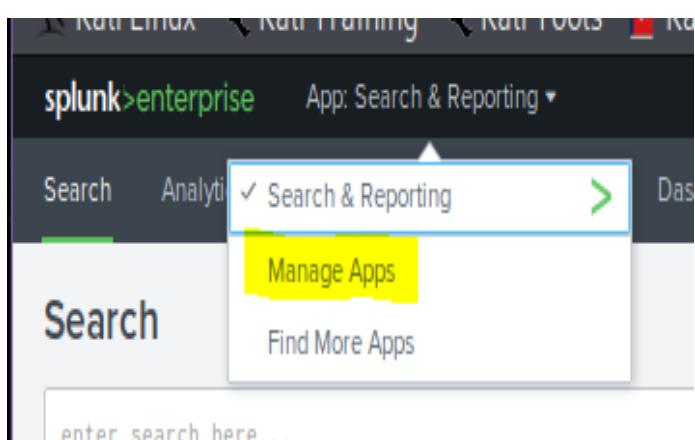
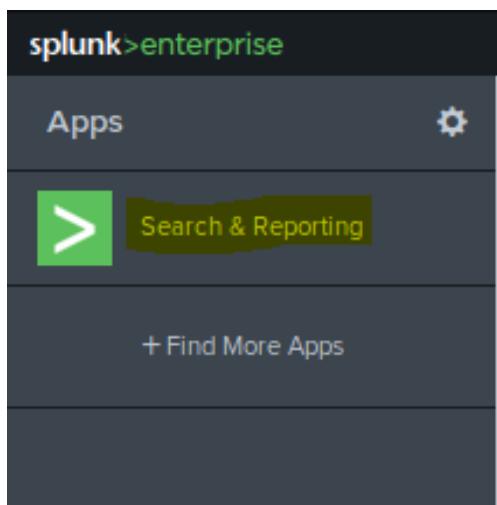
Step 2: Splunk adjustments/ add application

```
root@kali:~# cd /opt/splunk/bin
```

```
root@kali:/opt/splunk/bin# ./splunk start
The splunk daemon (splunkd) is already running.

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://kali:8000
```



Before install app from file, we will download the application.

Apps								
Showing 1-18 of 18 items								
Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions	
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable		
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable		
Log Event Alert Action	alert_logevent	8.0.5	Yes	No	App Permissions	Enabled Disable	Edit properties View objects	
Webhook Alert Action	alert_webhook	8.0.5	Yes	No	App Permissions	Enabled Disable	Edit properties View objects	
Apps Browser	appsbrowser	8.0.5	Yes	No	App Permissions	Enabled	Edit properties View objects	
introspection_generator_addon	introspection_generator_addon	8.0.5	Yes	No	App Permissions	Enabled Disable	Edit properties View objects	
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View c	
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects	
legacy	legacy		Yes	No	App Permissions	Disabled Enable		

Step 3: Download app for Suricata

The screenshot shows a web browser window with multiple tabs open. The active tab is titled 'Splunk Apps Browser' and shows the 'Suricata app for splunk' listing on the Splunkbase website. The app has a 5-star rating from 3 reviews. A screenshot of the app's interface is displayed, showing event search results and analysis panels.

www.splunkbase.splunk.com/app



Thank You

Downloading Suricata app for splunk

SHA256 checksum (suricata-app-for-splunk_10.tgz)

ce4706ce275c5c34a4058d516e5a948cc7e6510b8aa3dc8d29c400fbaa1c4ad8

To install your download

For instructions specific to your download, click the Details tab after closing this window.

OK



Accept License Agreements

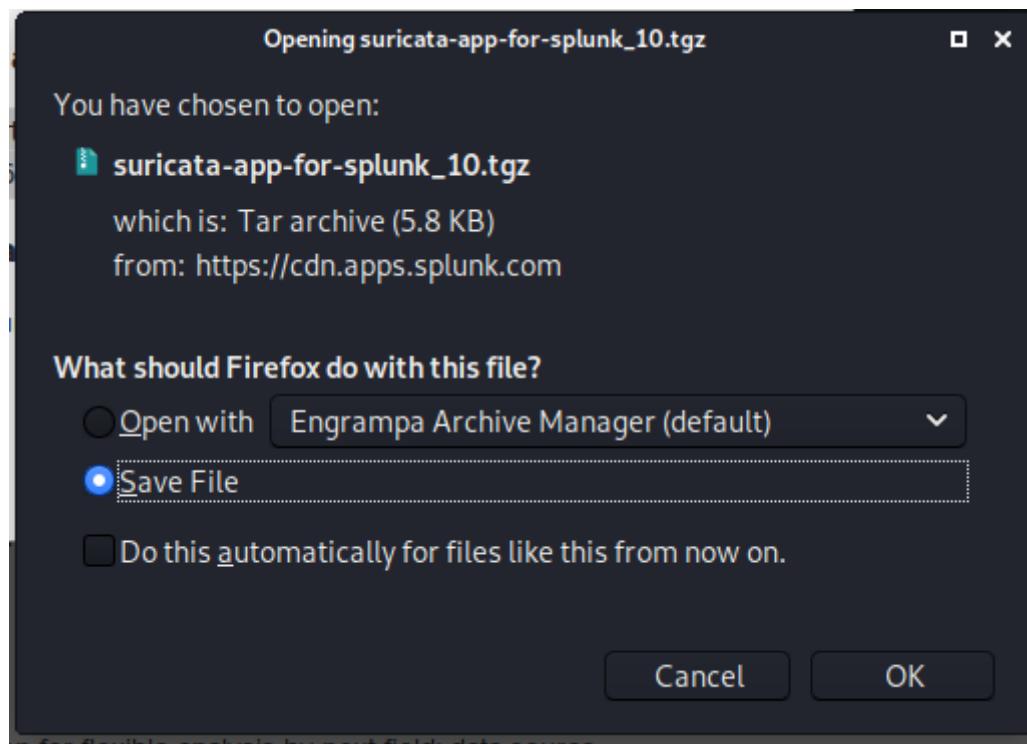
This app is provided by a third party and your right to use the app is in accordance with the license provided by that third-party licensor. Splunk is not responsible for any third-party apps and does not provide any warranty or support. If you have any questions, complaints or claims with respect to this app, please contact the licensor directly.

[GNU GPL 3.0](#)

[Splunk Websites Terms and Conditions of Use](#)

- I have read the terms and conditions of this license and agree to be bound by them.
- I consent to Splunk sharing my contact information with the publisher of this app so I can receive more information about the app directly from the publisher.

[Agree to Download](#)



Step 4: Setting up the downloaded file in splunk

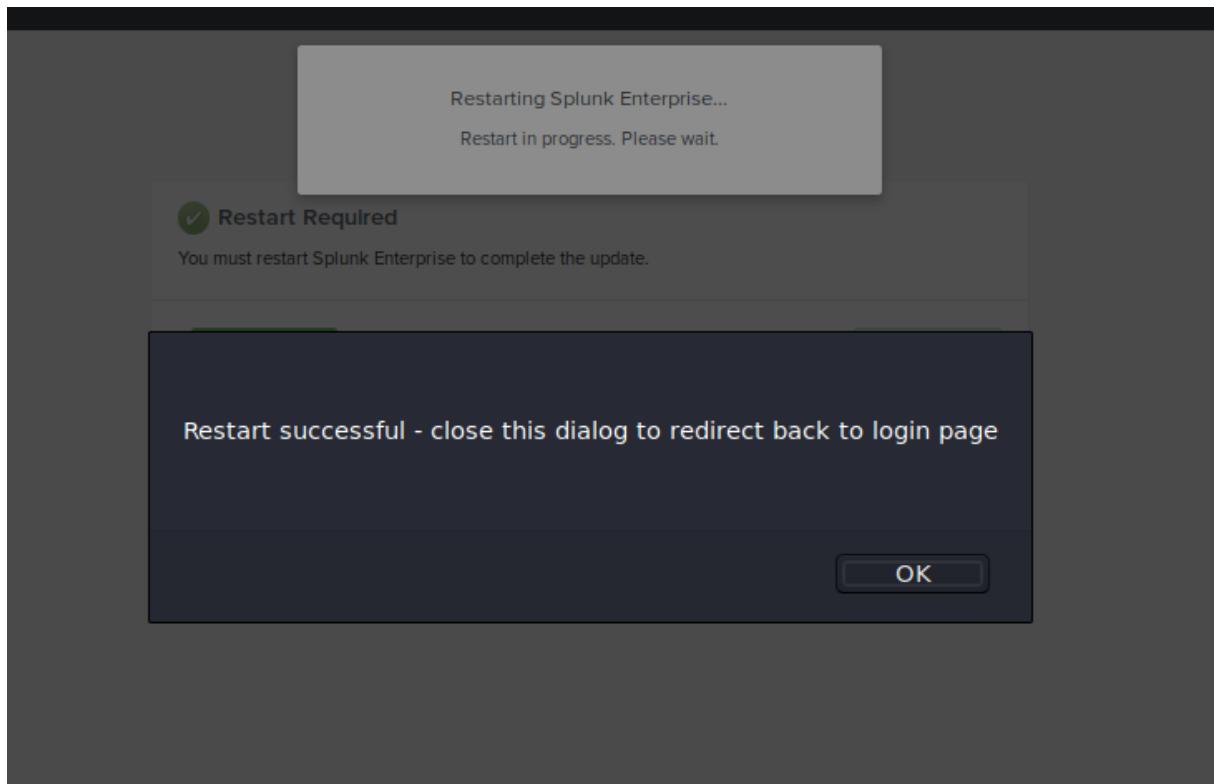
A file manager window is shown with the following details:

- Path: `kali` > `Downloads` > `suricataforsplunk` > `bin`
- File List:
 - `suricataforsplunk` (Archive, 22 Jun 2016)
 - `splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb` (Archive, 394.9 MB, Fri)
 - `suricata-app-for-splunk_10.tgz` (Archive, 5.9 kB, 18:11) - This file is highlighted in blue.

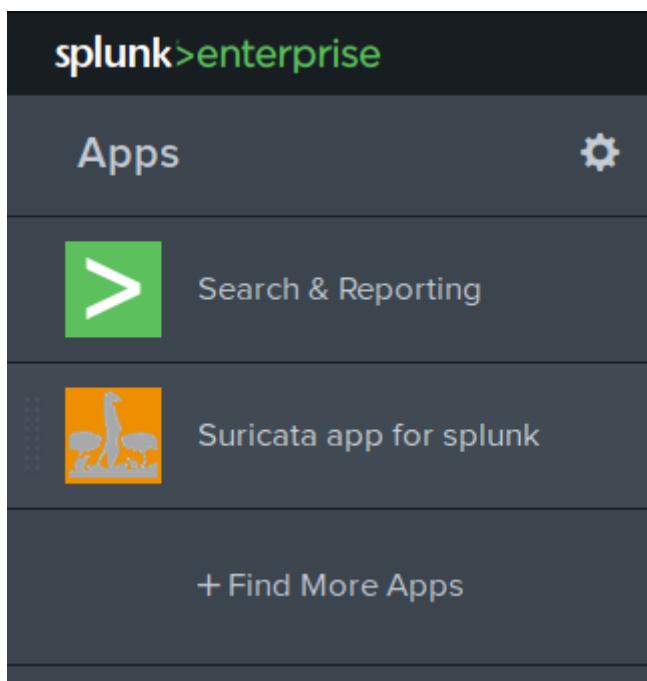
Below the file manager, a message box displays:

Restart Required
You must restart Splunk Enterprise to complete the update.

Restart Now



After restart



14.6 Search Details and Logs

What to Search

280,524 Events INDEXED	8 months ago EARLIEST EVENT	a few seconds ago LATEST EVENT
---------------------------	--------------------------------	-----------------------------------

[Data Summary](#)

Data Summary

X

[Hosts \(5\)](#) [Sources \(71\)](#) [Sourcetypes \(39\)](#)

filter		Hosts	
Host	Count	Last Update	Count
15.0	1	8/21/20 2:59:09.000 PM	
UTC	4	8/21/20 2:59:09.000 PM	
brd	6	8/21/20 2:59:09.000 PM	
kali	280,540	8/25/20 4:56:33.000 AM	
syslogd	1	8/21/20 2:59:08.000 PM	

Data Summary

X

Hosts (5)

Sources (71)

Sourcetypes (39)

filter



< Prev

1

2

Next >

Source	Count	Last Update
/var/log/Xorg.0.log	142	8/25/20 4:55:33.000 AM
/var/log/Xorg.1.log	4,636	8/24/20 4:30:13.000 PM
/var/log/alternatives.log	377	8/21/20 2:59:05.000 PM
/var/log/apt/history.log	80	8/22/20 8:38:56.000 AM
/var/log/apt/term.log	121	8/22/20 8:38:56.000 AM
/var/log/auth.log	1,329	8/25/20 4:55:01.000 AM
/var/log/auth.log.1	1,453	8/21/20 2:59:03.000 PM
/var/log/auth.log.2.gz	1,504	8/21/20 2:59:05.000 PM
/var/log/boot.log	2,661	8/25/20 4:36:53.000 AM
/var/log/daemon.log	13,080	8/25/20 4:55:48.000 AM

Data Summary

X

Hosts (5)

Sources (71)

Sourcetypes (39)

filter



Sourcetype	Count	Last Update
Xorg	3,750	8/23/20 8:16:15.000 AM
Xorg-2	148	8/25/20 4:55:33.000 AM
Xorg-too_small	4,617	8/24/20 4:30:13.000 PM
alternatives	377	8/21/20 2:59:05.000 PM
breakable_text	5,064	8/24/20 6:57:53.000 PM
dpkg	17,270	8/22/20 8:38:54.000 AM
eve.json	1,357	8/21/20 2:59:17.000 PM
fontconfig-too_small	94	8/21/20 2:58:55.000 PM
hardware-summary	5,579	8/21/20 2:59:08.000 PM
history	80	8/22/20 8:38:56.000 AM

host=UTC

Splunk+Enterprise App: Suricata app for splunk

Administrator Messages Settings Activity Help Find

Search Dashboards

New Search

host=SRC

✓ 4 events (before 8/25/20 4:52:57,000 AM) No Event Sampling

Events (4) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Desect

All time ▾ Smart Mode ▾

1 second per column

List Format 20 Per Page ▾

Time	Event
5/8/20 12:08:26 PM	May 8 12:08:26 debootstrap: Universal Time is now: Fri May 8 12:08:26 UTC 2020 host=UTC source=/var/log/installer/syslog sourcetype=syslog
5/8/20 12:08:26 PM	May 8 12:08:26 debootstrap: Local time is now: Fri May 8 12:08:26 UTC 2020 host=UTC source=/var/log/installer/syslog sourcetype=syslog
5/8/20 12:07:53 PM	May 8 12:07:53 clock-setup: Fri May 8 12:07:53 UTC 2020 host=UTC source=/var/log/installer/syslog sourcetype=syslog
5/8/20 12:06:19 PM	May 8 12:06:19 kernel: [1.539334] rtc_cmos 00:01: setting system clock to 2020-05-08T12:06:18 UTC (1588939578) host=UTC source=/var/log/installer/syslog sourcetype=syslog

SELECTED FIELDS
host
source
sourcetype

INTERESTING FIELDS
date_hour
date_minute
date_second
date_month
date_year
date_usec
date_wday
date_year1
offset_zone
index
linecount
process
punct
strukt_server
timestamppos
timestamppos1

host=kali

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** host=kali
- Time Range:** Last 24 hours
- Event Count:** 25,656 events (from 08/24/20 4:00:00 AM to 08/25/20 4:54:19.000 AM)
- Sampling:** No Event Sampling
- Job Status:** Job ▾
- Mode:** Smart Mode ▾
- Panel Tabs:** Events (25,656) (selected), Patterns, Statistics, Visualization
- Format Timeline:** Format Timeline ▾, Zoom Out, Zoom to Selection, Deselect, 1 hour per column
- Timeline View:** Shows event counts over time, with a callout for "2,631 events at 9 AM on Monday, August 24, 2020". A 1 day/1 hour scale bar is shown below the timeline.
- List View:** List ▾, Format, 20 Per Page ▾
- Page Navigation:** 1 (selected), 2, 3, 4, 5, 6, 7, 8, ... Next ▾
- Table View (Events):**

i	Time	Event
>	8/25/20 4:52:04.000 AM	[346.189] (!!) vmware(0): New layout. [346.190] (!!) vmware(0): 0: 0 0 1920 957 [346.190] (!!) vmware(0): [346.342] (EE) No surface to present from. host = kali source = /var/log/Xorg.0.log sourcetype = Xorg-2
>	8/25/20 4:51:58.000 AM	[340.758] (EE) No surface to present from. host = kali source = /var/log/Xorg.0.log sourcetype = Xorg-2
>	8/25/20 4:51:58.000 AM	[340.678] (!!) vmware(0): New layout. [340.680] (!!) vmware(0): 0: 0 0 1273 741 [340.680] (!!) vmware(0): host = kali source = /var/log/Xorg.0.log sourcetype = Xorg-2
>	8/25/20 4:50:00.000 AM	Aug 25 04:50:00 kali NetworkManager[641]: <info> [1598345400.9930] manager: startup complete host = kali source = /var/log/daemon.log sourcetype = syslog
>	8/25/20 4:50:00.000 AM	Aug 25 04:50:00 kali NetworkManager[641]: <info> [1598345400.9830] dhcpc (eth1): state changed timeout -> done host = kali source = /var/log/daemon.log sourcetype = syslog
>	8/25/20 4:50:00.000 AM	Aug 25 04:50:00 kali NetworkManager[641]: <info> [1598345400.9829] dhcpc (eth1): canceled DHCP transaction host = kali source = /var/log/daemon.log sourcetype = syslog
>	8/25/20 4:50:00.000 AM	Aug 25 04:50:00 kali NetworkManager[641]: <info> [1598345400.9551] device (eth1): state change: failed -> disconnected (reason 'none', sys-interface-state: 'managed') host = kali source = /var/log/daemon.log sourcetype = syslog
>	8/25/20 4:50:00.000 AM	Aug 25 04:50:00 kali NetworkManager[641]: <warn> [1598345400.9537] device (eth1): Activation: failed for connection 'Wired connection 1' host = kali source = /var/log/daemon.log sourcetype = syslog
>	8/25/20 4:50:00.000 AM	Aug 25 04:50:00 kali NetworkManager[641]: <info> [1598345400.9472] device (eth1): state change: ip-config -> failed (reason 'ip-config-unavailable', sys-interface-state: 'managed') host = kali source = /var/log/daemon.log sourcetype = syslog

host=kali

✓ 2,559 events (8/24/20 5:00:00.000 AM to 8/25/20 5:10:33.000 AM) Sampling 1: 10 ▾

Events (2,559) Patterns Statistics Visualization

Smaller Larger

17 patterns based on a sample of 2,558 events

⚠ Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.

```

14.46% <timestamp> kali NetworkManager[641]: <info> [1598346360.9783] dhcpc (eth1): state changed timeout -> done
12.86% <timestamp> kali system[1]: phpsessionclean.service: Succeeded.
3.17% <timestamp> kali kernel: [ 0.581854] ACPI: Added _OSI(Linux-Lenovo-NV-HDMI-Audio)
2.74% <timestamp> kali dbus-daemon[1035]: [session uid=1000 pid=1035] Activating via systemd: service name='org.blueman.Applet' unit='blueman-applet.service' requested by ':1.79' (uid=1000 pid=1905 comm='/usr/bin/python3 /usr/bin/blueman-tray ')
1.56% (*timestamp*:<timestamp>, "event_type": "stats", "stats": {"uptime": 3953, "decoder": {"pkts": 0, "bytes": 0, "invalid": 0, "ipv4": 0, "ipv6": 0, "ethernet": 0, "raw": 0, "null": 0, "sll": 0, "tcp": 0, "udp": 0, "sctp": 0, "icmpv4": 0, "icmpv6": 0, "ppp": 0, "gre": 0, "vlan": 0, "vxlan": 0, "ieee8021ah": 0, "teredo": 0, "ipv4_in_ip6": 0, "ipv6_in_ip6": 0, "mpls": 0, "avg_pkts_size": 0, "max_pkts_size": 0, "erspan": 0, "event": {"ipv4": {"pkt_too_small": 0, "hlen_too_small": 0, "iplen_smaller_than_hlen": 0, "trunc_pkts": 0, "lost_pkts": 0, "not_pkts_received": 0, "not_pkts_repeated": 0, "not_pkts_duplicated": 0, "not_pkts_unknown": 0, "none": 0}, "version": 0, "icmp6": 0, "frag_too_large": 0, "frag_overlap": 0, "frag_improper": 0, "icmp4": 0, "pkt_too_small": 0}}, "date": <timestamp> (uptime: 0d, 0h 05m 13s)
1.52% -----
1.49% -----
1.29% <timestamp> kali rtkit-daemon[867]: Supervising 3 threads of 1 processes of 2 users.
1.25% -----
0.78% [<0.09s> DEBUG: Seat seat8: Starting
0.82% [ 2613.038] Module class: X.Org Video Driver
0.74% [ 2615.040] (II) Initializing extension XInputExtension
0.94% <timestamp> kali kernel: [ 0.089421] [Firmware Bug]: CPU1: APIC id mismatch. Firmware: 1 APIC: 2
0.55% [ 2615.010] (II) vmsware(0): Modeline "1440x900x59.9 106.50 1440 1520 1672 1904 900 903 905 934 -hsync +vsync (35.9 kHz e)
```

New Search

Save As ▾ Close

Last 24 hours ▾

142,888 events (8/24/20 5:00:00.000 AM to 8/25/20 5:12:37.000 AM) No Event Sampling ▾

Events (142,888) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out

1 hour per column

Time	Event
8/25/20 5:12:36.817 AM	<pre> SELECTED FIELDS # RootObject.date_hour 19 # RootObject.date_minute 2 # RootObject.date_month 60 # RootObject.date_second 60 # RootObject.date_year 19 # RootObject.date_zone 3 # RootObject.index 5 # RootObject.linecount 15 # RootObject.pid 100+ # RootObject.splunk_server 1 # RootObject.timeendpos 23 INTERESTING FIELDS # RootObject.date_hour 19 # RootObject.date_minute 2 # RootObject.date_month 60 # RootObject.date_second 60 # RootObject.date_year 19 # RootObject.date_zone 3 # RootObject.index 5 # RootObject.linecount 15 # RootObject.pid 100+ # RootObject.splunk_server 1 # RootObject.timeendpos 23 <i>host = kali source = /opt/splunk/var/log/introspection/resource_usage.log sourcetype = splunk_resource_usage</i></pre>
8/25/20 5:12:36.817 AM	<pre> SELECTED FIELDS # RootObject.date_hour 19 # RootObject.date_minute 2 # RootObject.date_month 60 # RootObject.date_second 60 # RootObject.date_year 19 # RootObject.date_zone 3 # RootObject.index 5 # RootObject.linecount 15 # RootObject.pid 100+ # RootObject.splunk_server 1 # RootObject.timeendpos 23 INTERESTING FIELDS # RootObject.date_hour 19 # RootObject.date_minute 2 # RootObject.date_month 60 # RootObject.date_second 60 # RootObject.date_year 19 # RootObject.date_zone 3 # RootObject.index 5 # RootObject.linecount 15 # RootObject.pid 100+ # RootObject.splunk_server 1 # RootObject.timeendpos 23 <i>host = kali source = /opt/splunk/var/log/introspection/resource_usage.log sourcetype = splunk_resource_usage</i></pre>

< Prev 1 2 3 4 5 6 7 8 Next >

sourcetype="eve.json"

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** sourcetype="eve.json"
- Results Summary:** 1,357 events (before 8/25/20 4:57:42.000 AM) No Event Sampling
- Time Range:** All time
- Event List:** Events (1,357) | Patterns | Statistics | Visualization
- Event Timeline:** Format Timeline | Zoom Out | +Zoom to Selection | X Deselect
- Event View Headers:** i Time Event
- Event 1:** 8/9/20 1:37:04.367 PM { [-] event_type: stats stats: { [+] } timestamp: 2020-08-09T13:37:04.367878-0400 }
- Event 2:** 8/9/20 1:37:04.112 PM { [-] event_type: stats stats: { [+] } timestamp: 2020-08-09T13:37:04.112426-0400 }
- Event 3:** 8/9/20 1:36:56.111 PM { [-] event_type: stats stats: { [+] } timestamp: 2020-08-09T13:36:56.111352-0400 }
- Event 4:** 8/9/20 1:36:48.110 PM { [-] event_type: stats stats: { [+] } timestamp: 2020-08-09T13:36:48.110056-0400 }
- Event Details:** host = kali | source = /var/log/suricata/eve.json.1 | sourcetype = eve.json

var/log/suricata

Data Summary X

Hosts (5) Sources (71) Sourcetypes (39)

var/log/suricata X

Source	Count	Last Update
/var/log/suricata/eve.json	721	8/24/20 6:57:53.000 PM
/var/log/suricata/eve.json.1	1,357	8/21/20 2:59:17.000 PM
/var/log/suricata/stats.log	7,469	8/24/20 6:57:53.000 PM
/var/log/suricata/stats.log.1	4,071	8/21/20 2:59:12.000 PM
/var/log/suricata/suricata.log	343	8/24/20 6:57:54.000 PM
/var/log/suricata/suricata.log.1	60	8/21/20 2:59:12.000 PM

source="/var/log/suricata/stats.log"

i	Time	Event
>	8/24/20 6:57:52.000 PM	flow.spare Total 10000 flow_mgr.rows_checked Total 65536 flow_mgr.rows_skipped Total 65536 tcp.memuse Total 2293760 Show all 7 lines host = kali source = /var/log/suricata/stats.log sourcetype = breakable_text
>	8/24/20 6:57:52.000 PM	Counter TM Name Value host = kali source = /var/log/suricata/stats.log sourcetype = breakable_text
>	8/24/20 6:57:52.000 PM	Date: 8/24/2020 -- 18:57:52 (uptime: 0d, 01h 06m 00s) host = kali source = /var/log/suricata/stats.log sourcetype = breakable_text
>	8/24/20 6:57:45.000 PM	flow.spare Total 10000 flow_mgr.rows_checked Total 65536 flow_mgr.rows_skipped Total 65536 tcp.memuse Total 2293760 Show all 7 lines host = kali source = /var/log/suricata/stats.log sourcetype = breakable_text

CHAPTER 15

Suricata on pfSense

15.1 What is pfSense?

pfSense is an firewall/router computer software distribution.

pfSense can act in an Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) role with add-on packages like Suricata.

15.2 What is firewall?

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

15.3 What is router?

Routers are devices that connect different devices or networks and direct network traffic.

15.4 Installing pfSense on VMWare

Step 1 : Download pfSense

www.pfsense.org/download/

Select Image To Download

Version: 2.4.5-p1

Architecture: AMD64 (64-bit) ?

Installer: CD Image (ISO) Installer

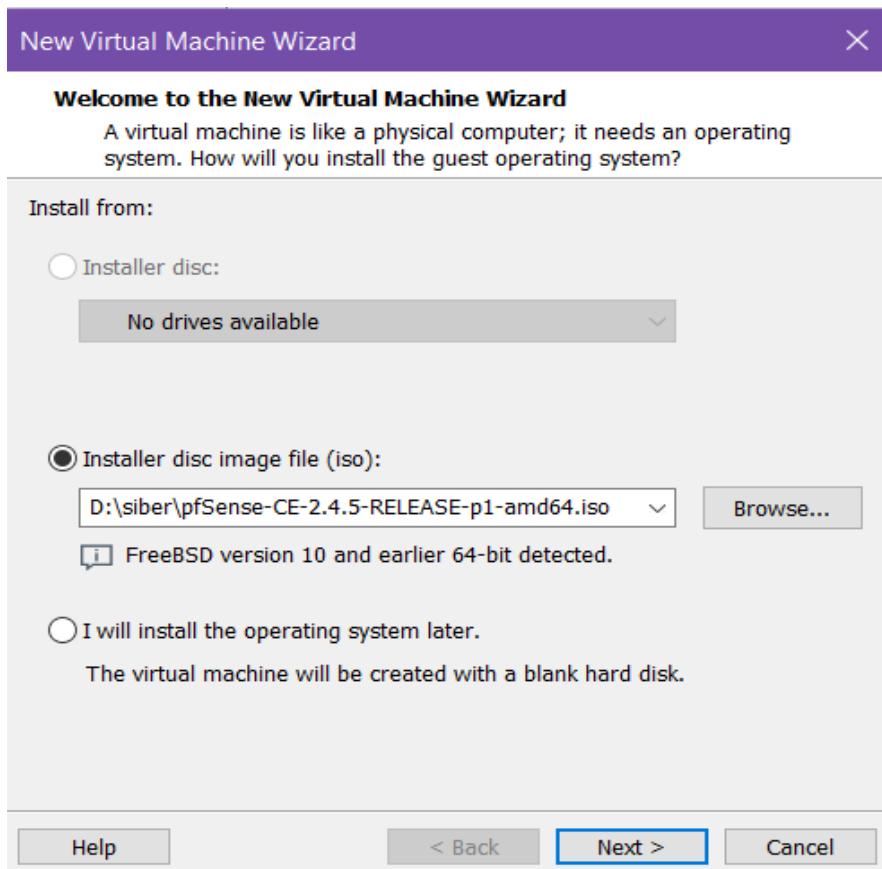
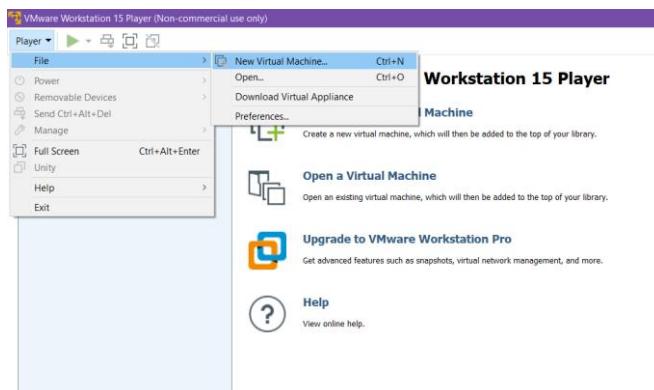
Mirror: New York City, USA

Supported by **netgate**

[SHA256 Checksum](#) for compressed (.gz) file:
0a09a7748419c86c665eb8d908f584e96d54859aa13f4eeb175a60548c70e228

It must be in iso setting to open in vmware.

Step 2 : Installing in VMWare



New Virtual Machine Wizard

X

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

FreeBSD version 10 and earlier 64-bit

Location:

D:\PFSense

[Browse...](#)

[< Back](#)

[Next >](#)

[Cancel](#)

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 

Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

Store virtual disk as a single file

Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

[Help](#)

[< Back](#)

[Next >](#)

[Cancel](#)

New Virtual Machine Wizard

X

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing FreeBSD version 10 and earlier 64-bit.

The virtual machine will be created with the following settings:

Name: FreeBSD version 10 and earlier 64-bit

Location: D:\PFSense

Version: Workstation 15.x

Operating System: FreeBSD version 10 and earlier 64-bit

Hard Disk: 20 GB, Split

Memory: 256 MB

Network Adapter: NAT

Other Devices: CD/DVD, USB Controller, Printer, Sound Card

[Customize Hardware...](#)

Power on this virtual machine after creation

< Back

Finish

Cancel

NAT->network adapter

Device	Summary
Memory	256 MB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file D:\siber\pfSense...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

Connected
 Connect at power on

Network connection

Bridged: Connected directly to the physical network
 Replicate physical network connection state

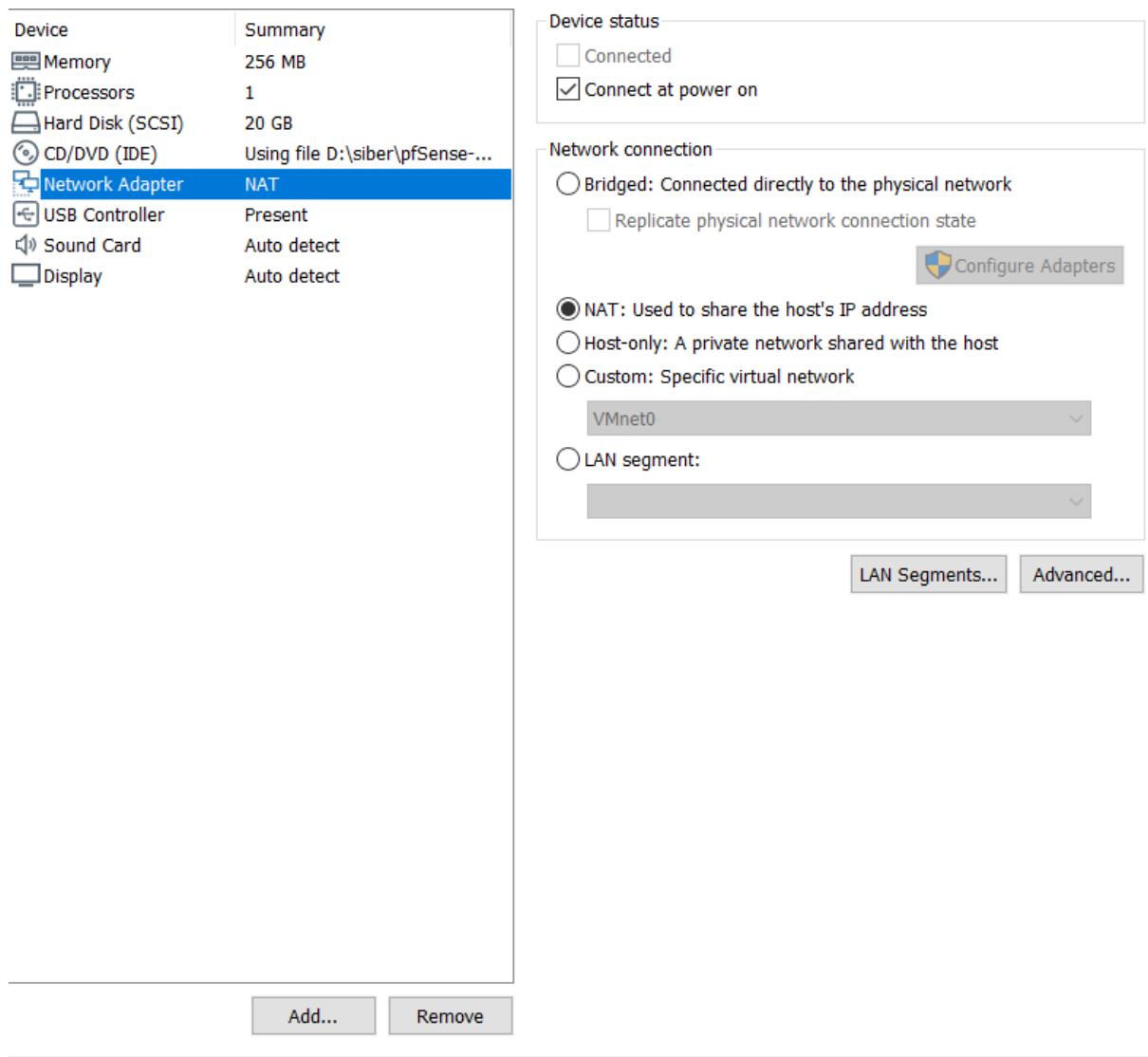
NAT: Used to share the host's IP address
 Host-only: A private network shared with the host
 Custom: Specific virtual network

VMnet0

LAN segment:

LAN Segments... **Advanced...**

Add... Remove



Add network adapter

Add Hardware Wizard

X

Hardware Type

What type of hardware do you want to install?

Hardware types:

- CD/DVD Drive
- Floppy Drive
- Network Adapter
- USB Controller
- Sound Card
- Parallel Port
- Serial Port
- Printer
- Generic SCSI Device

Explanation

Add a network adapter.

Finish

Cancel

Device status

- Connected
- Connect at power on

Network connection

Bridged: Connected directly to the physical network

Replicate physical network connection state



NAT: Used to share the host's IP address

Host-only: A private network shared with the host

Custom: Specific virtual network

VMnet1

LAN segment:

[LAN Segments...](#)

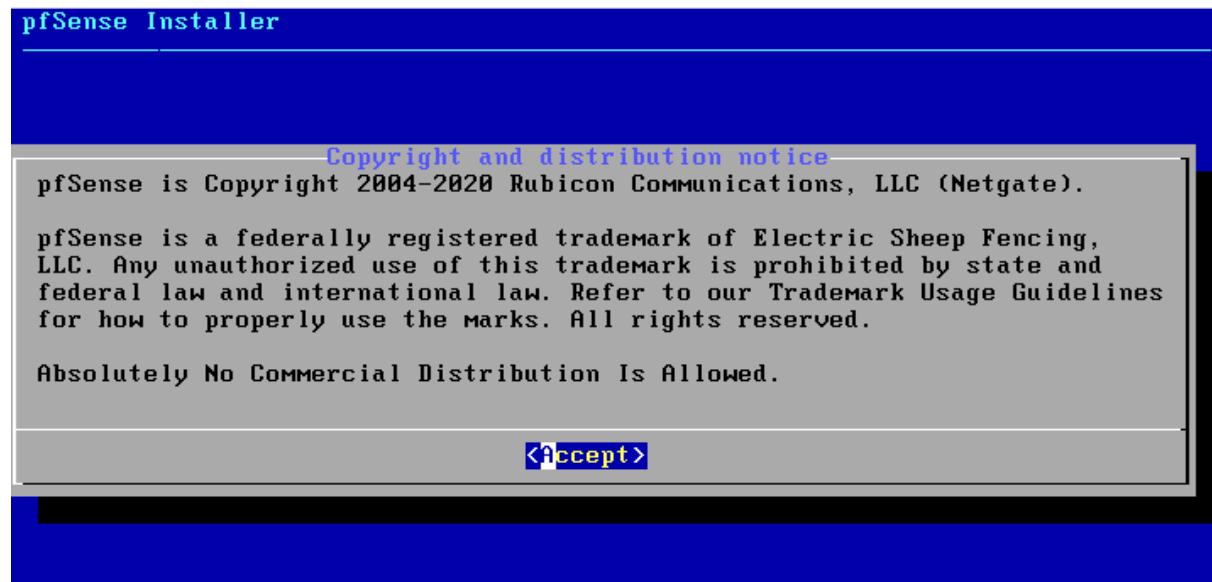
[Advanced...](#)

Device	Summary
Memory	256 MB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file D:\siber\pfSense-...
Network Adapter	NAT
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

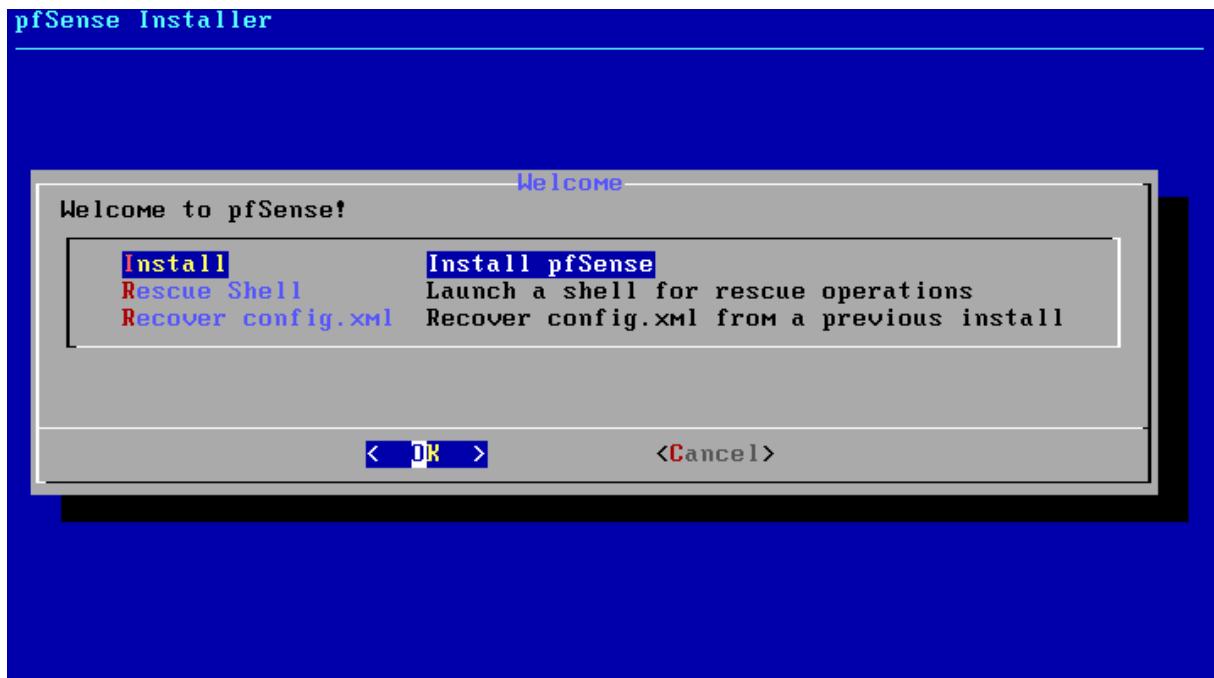
2 network adapters must be added. One should be WAN and one should be LAN.

Step 3 : pfSense installation

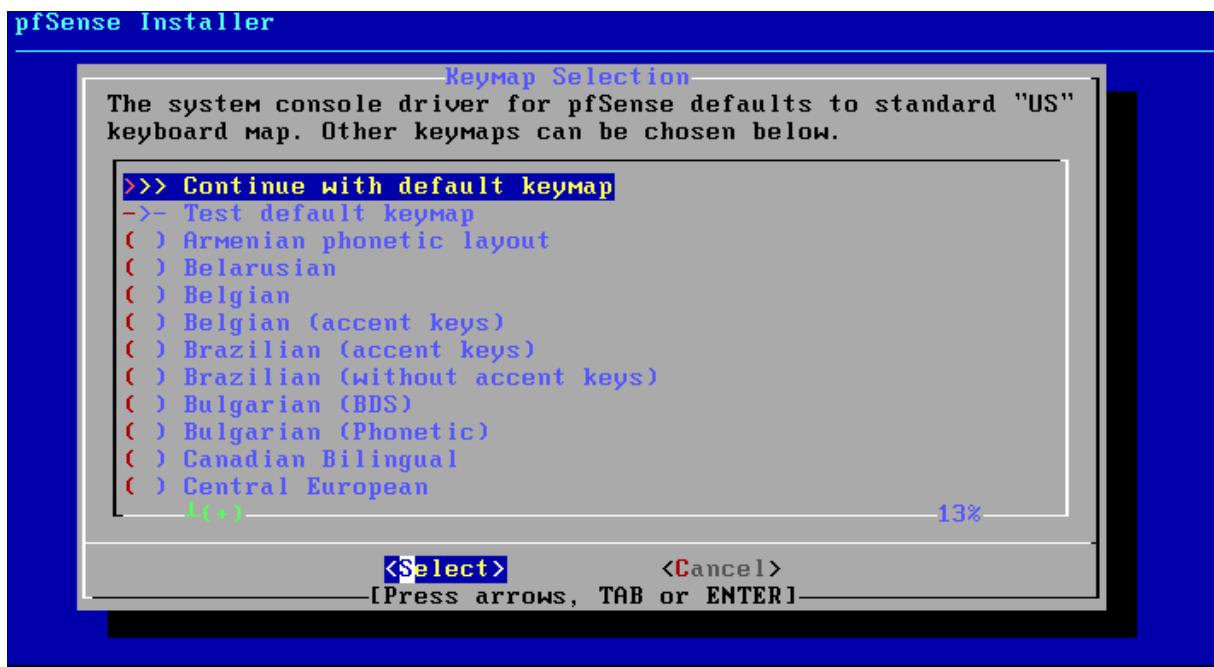
```
psm0: Model IntelliMouse, device ID 3
acpi_syscontainer0: <System Container> on acpi0
orM0: <ISA Option ROMs> at iomem 0xc0000-0xc7fff,0xc8000-0xc9fff,0xca000-0xcffff
,0xcb000-0xcbfff,0xcc000-0xccffff,0xdc000-0xdffff,0xe0000-0xe7fff on isa0
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
ppc0: cannot reserve I/O port range
Timecounters tick every 10.000 msec
em2: link state changed to UP
usbus0: 12Mbps Full Speed USB v1.0
usbust1: 480Mbps High Speed USB v2.0
ugen1.1: <0x15ad EHCI root HUB> at usbus1
uhub0: <0x15ad EHCI root HUB, class 9/0, rev 2.00/1.00, addr 1> on usbus1
ugen0.1: <0x15ad UHCI root HUB> at usbus0
uhub1: <0x15ad UHCI root HUB, class 9/0, rev 1.00/1.00, addr 1> on usbus0
uhub1: 2 ports with 2 removable, self powered
ugen0.2: <VMware VMware Virtual USB Mouse> at usbus0
uhid0 on uhub1
uhid0: <VMware> on usbus0
uhid1 on uhub1
uhid1: <VMware> on usbus0
ugen0.3: <VMware, Inc. VMware Virtual USB Hub> at usbus0
uhub2 on uhub1
uhub2: <VMware, Inc.> on usbus0
uhub0: 6 ports with 6 removable, self powered
```



pfSense Installer



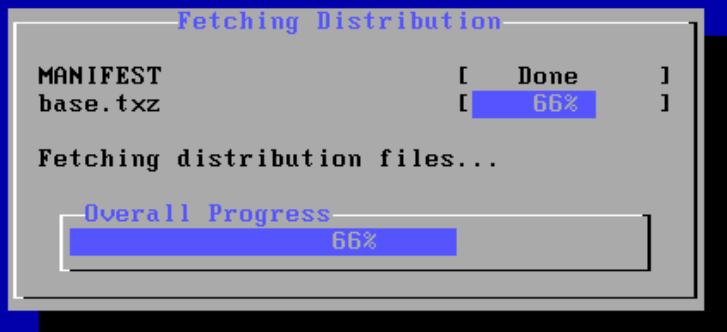
pfSense Installer



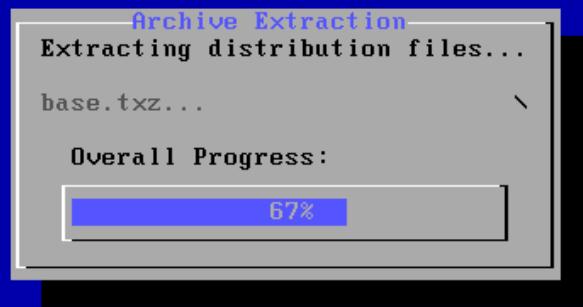
pfSense Installer



pfSense Installer

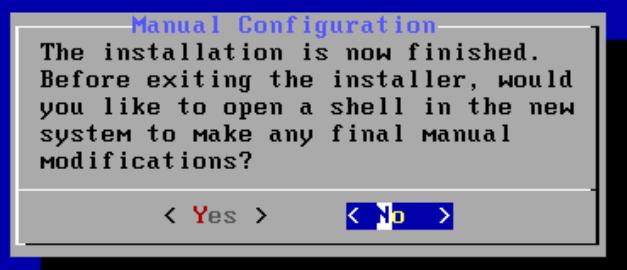


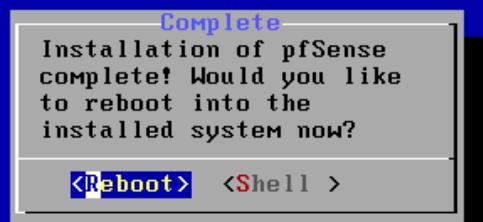
pfSense Installer



15689 files read @ 364.0 files/sec.

pfSense Installer





```
Checking config backups consistency...done.  
Setting up extended sysctls...done.  
Setting timezone...done.  
Configuring loopback interface...lo0: link state changed to UP  
done.  
Starting syslog...done.  
Starting Secure Shell Services...done.  
Setting up interfaces microcode...done.  
Configuring loopback interface...done.  
Creating wireless clone interfaces...done.  
Configuring LAGG interfaces...done.  
Configuring VLAN interfaces...done.  
Configuring QinQ interfaces...done.  
Configuring IPsec VTI interfaces...done.  
Configuring WAN interface...done.  
Configuring LAN interface...done.  
Configuring CARP settings...done.  
Syncing OpenVPN settings...done.  
Configuring firewall.....done.  
Starting PFLOG...done.  
Setting up gateway Monitors...done.  
Setting up static routes...done.  
Setting up DNSs...  
Starting DNS Resolver...done.  
Synchronizing user settings...■
```

Change LAN

Reason for change: An address appropriate for the WAN must be set.

192.168.40.x , x can be between 1 and 253.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: f24c06273e70d3b392ee

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.40.130/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2
```

```
Enter an option: 2
```

```
Available interfaces:
```

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
```

```
Enter the number of the interface you wish to configure: 2
```

```
Enter the number of the interface you wish to configure: 2
```

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.40.8
```

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8
```

```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

```
Enter the new LAN IPv6 address. Press <ENTER> for none:  
>  
Do you want to enable the DHCP server on LAN? (y/n) n  
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
The IPv4 LAN address has been set to 192.168.40.8/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
http://192.168.40.8/  
Press <ENTER> to continue.
```

```
Press <ENTER> to continue.  
VMware Virtual Machine - Netgate Device ID: e8cc7ad070d9652c7683  
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***  
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.40.142/24  
LAN (lan)      -> em1          -> v4: 192.168.40.8/24  
  
0) Logout (SSH only)          9) pfTop  
1) Assign Interfaces          10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults 13) Update from console  
5) Reboot system              14) Enable Secure Shell (sshd)  
6) Halt system                15) Restore recent configuration  
7) Ping host                  16) Restart PHP-FPM  
8) Shell
```

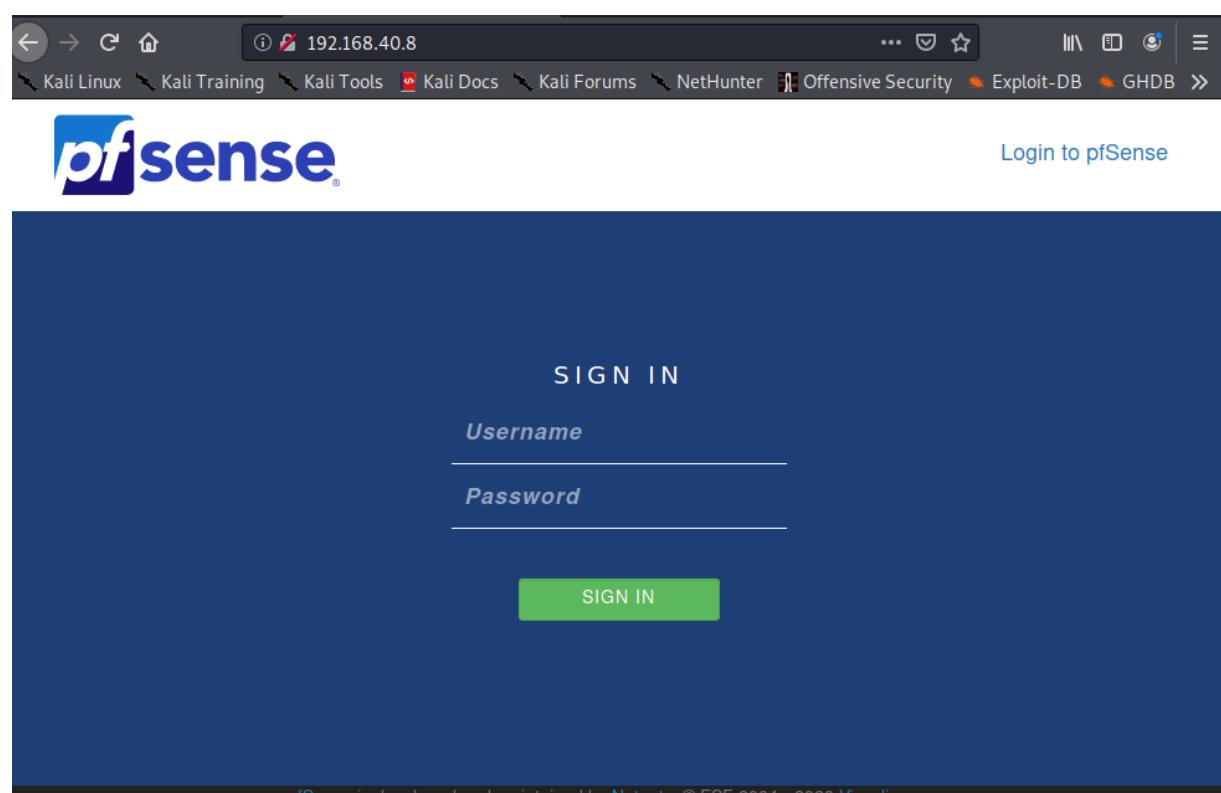
My browser is <http://192.168.40.8/>

15.5 Setup Suricata on pfSense

Step 1 : Login

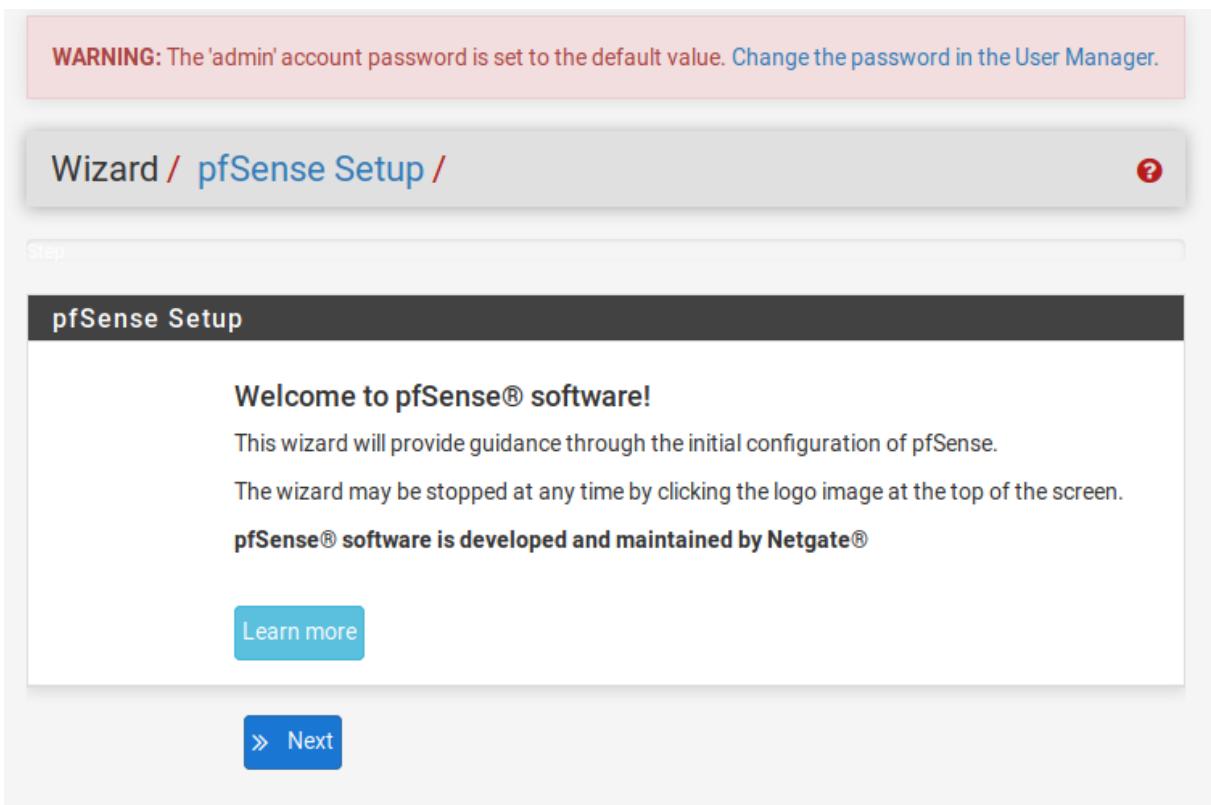
Default username: admin

Default password : pfsense



```
Message from syslogd@pfSense at Aug 27 08:27:01 ...
php-fpm[3750]: /index.php: Successful login for user 'admin' from: 192.168.40.13
5 (Local Database)
```

Step 2 : Install the Suricata Package



Change password.

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by	SYSTEM	
Disabled	<input type="checkbox"/> This user cannot login	
Username	admin	
Password	••••••••••	••••••••••
Full name	System Administrator	User's full name, for administrative information only
Expiration date		Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.	
Group membership	Not member of	Member of
» Move to 'Member of' list		« Move to 'Not member of' list
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.		

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: suricata Both [Search](#) [Clear](#)

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
suricata	5.0.3	High Performance Network IDS, IPS and Security Monitoring engine by OISF. Package Dependencies: suricata-5.0.3	+ Install

Installed Packages Available Packages Package Installer

Confirmation Required to install package pfSense-pkg-suricata.

Confirm

Installed Packages Available Packages Package Installer

Package Installation

```
lzo: 2.0.5 [pfSense]  
libnet: 1.1.6_5,1 [pfSense]  
libpcap: 1.9.1_1 [pfSense]  
libyaml: 0.2.2 [pfSense]  
nspr: 4.25 [pfSense]  
nss: 3.51 [pfSense]  
pfSense-pkg-suricata: 5.0.3 [pfSense]  
py37-yaml: 5.3.1 [pfSense]  
suricata: 5.0.3 [pfSense]
```

Number of packages to be installed: 12

The process will require 38 MiB more space.

7 MiB to be downloaded.

[1/12] Fetching pfSense-pkg-suricata-5.0.3.txz:

[2/12] Fetching suricata-5.0.3.txz:

pfSense-pkg-suricata installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

Title to run in `neuimap(4)` mode.

RULES: `Suricata` IDS/IPS Engine comes without rules by default. You should add rules by yourself and set an updating strategy. To do so, please visit:

<http://www.openinfosecfoundation.org/documentation/rules.html>
<http://www.openinfosecfoundation.org/documentation/emerging-threats.html>

You may want to try BPF in `zerocopy` mode to test performance improvements:

`sysctl -w net.bpf.zerocopy_enable=1`

Don't forget to add `net.bpf.zerocopy_enable=1` to `/etc/sysctl.conf`
->> Cleaning up cache... done.

Success

pfSense
COMMUNITY EDITION

System ▾

Interfaces ▾

Firewall ▾

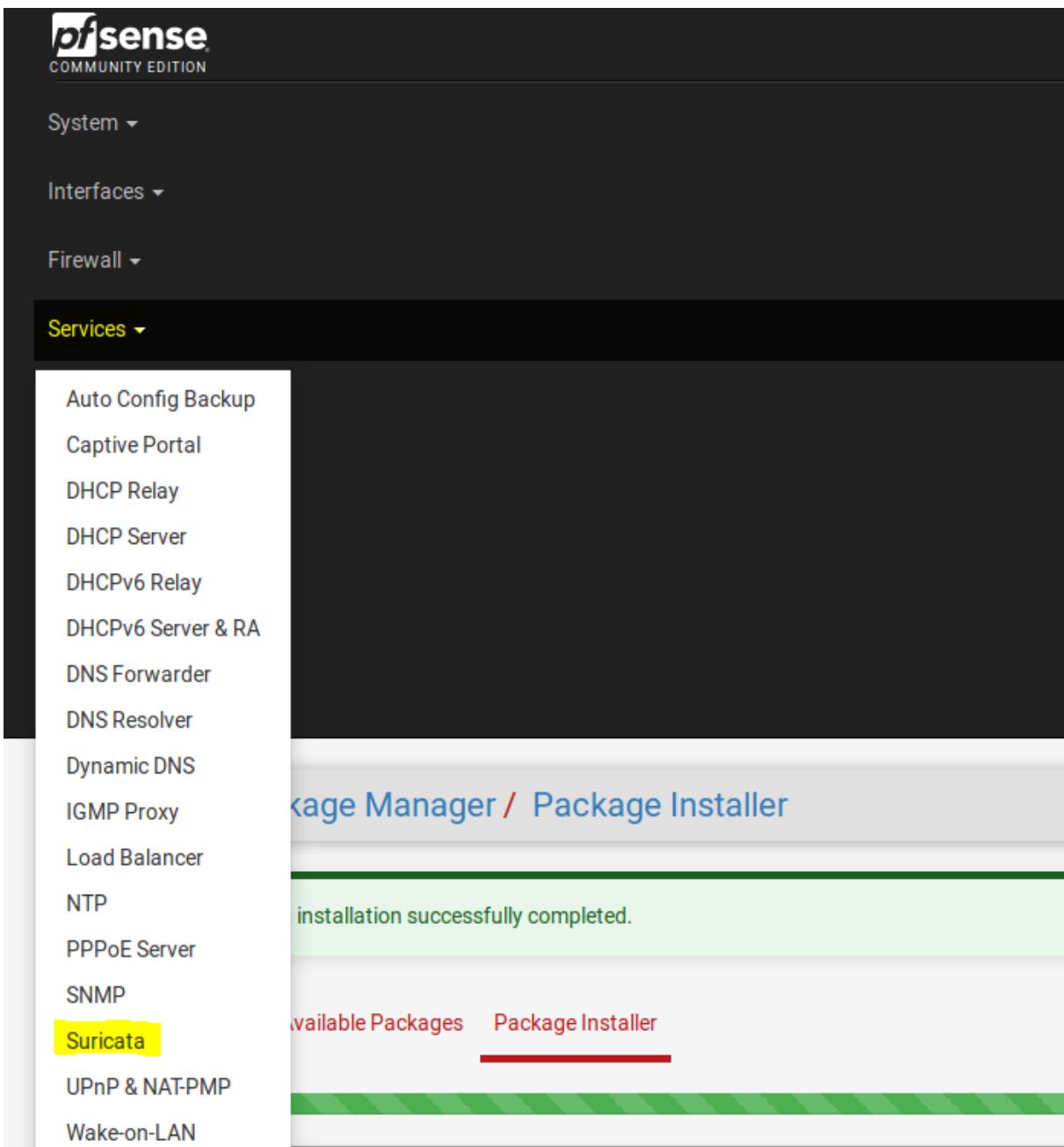
Services ▾

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server & RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- Load Balancer
- NTP
- PPPoE Server
- SNMP
- Suricata**
- UPnP & NAT-PMP
- Wake-on-LAN

Package Manager / Package Installer

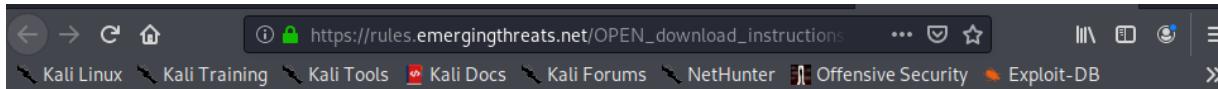
installation successfully completed.

Available Packages Package Installer



Step 3 : Enable rule download

The screenshot shows the 'Global Settings' tab selected in the Suricata configuration interface. A sub-menu at the bottom includes 'Logs Mgmt', 'SID Mgmt', 'Sync', and 'IP Lists'. Below this, a section titled 'Please Choose The Type Of Rules You Wish To Download' contains two options: 'Install ETOpen Emerging Threats rules' and 'ETOpen Custom Rule Download URL'. The 'ETOpen Custom Rule Download URL' field is populated with 'https://rules.emergingthreats.net/open/suricata-5.0.0/emerging.rules.tar.gz'. A note below the URL states: 'You must provide the complete URL including the filename! The code will assume a matching filename exists at the same URL with an additional extension of ".md5"'.



ET OPEN Ruleset Download Instructions

To download your **OPEN** ruleset use the following url format

Suricata: [https://rules.emergingthreats.net/open/suricata-\\$version/emerging.rules.tar.gz](https://rules.emergingthreats.net/open/suricata-$version/emerging.rules.tar.gz)

Snort: [https://rules.emergingthreats.net/open/snort-\\$version/emerging.rules.tar.gz](https://rules.emergingthreats.net/open/snort-$version/emerging.rules.tar.gz)

\$version above is customer supplied. It is the version of your Suricata or Snort IDS.

Examples:

- <https://rules.emergingthreats.net/open/suricata-5.0.0/emerging.rules.tar.gz>
- <https://rules.emergingthreats.net/open/snort-2.9.7.0/emerging.rules.tar.gz>

Changelogs: <http://rules.emergingthreats.net/changelogs/>

**Install Snort GPLv2
Community rules**

The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.

Use a custom URL for Snort GPLv2 rule downloads

This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.

**Snort
Oinkmaster
Code**

Obtain a snort.org Oinkmaster code and paste it here.

[Sign up and get the code:](#)

Snort - Network Intrusion Detection System

https://snort.org/users/sign_up

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

SNORT

Sign up

Email
Please enter your Email address

Password

Password confirmation

Agree to Snort license

Subscribe to Snort mailing lists?

Snort-users Snort-sigs Snort-devel Snort-openappid

You will receive an email confirmation that will require your action if you select any of these boxes

Sign up

Sign in

Didn't receive confirmation instructions?

Install Snort rules

Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)

[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Use a custom URL for Snort rule downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.

Snort Rules Filename	<input type="text" value="snortrules-snapshot-29160.tar.gz"/>
Enter the rules tarball filename (filename only, do not include the URL.)	
Example: snortrules-snapshot-29151.tar.gz	
DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!	
Snort Oinkmaster Code	<input type="text" value="392ede42fca4032d4f64a03ac072402f2964cb4b"/>
Obtain a snort.org Oinkmaster code and paste it here.	

**Snort
Oinkmaster
Code**

392ede42fca4032d4f64a03ac072402f2964cb4b

Obtain a snort.org Oinkmaster code and paste it here.

**Hide Deprecated
Rules Categories**

Hide deprecated rules categories in the GUI and remove them from the configuration. Default is Not Checked.

General Settings

**Remove Blocked
Hosts Interval**

Please select the amount of time you would like hosts to be blocked. Note this setting is only applicable when using Legacy Mode blocking! This setting is ignored when using Inline IPS Mode.

Hint: in most cases, 1 hour is a good choice.

Log to System Log

Copy Suricata messages to the firewall system log.

**Keep Suricata
Settings After
Deinstall**

Settings will not be removed during package deinstallation.

 Save

Update rules

Services / Suricata / Update Rules Set Files ?

Interfaces Global Settings Updates Alerts Blocks Pass Lists Suppress Logs View

Logs Mgmt SID Mgmt Sync IP Lists

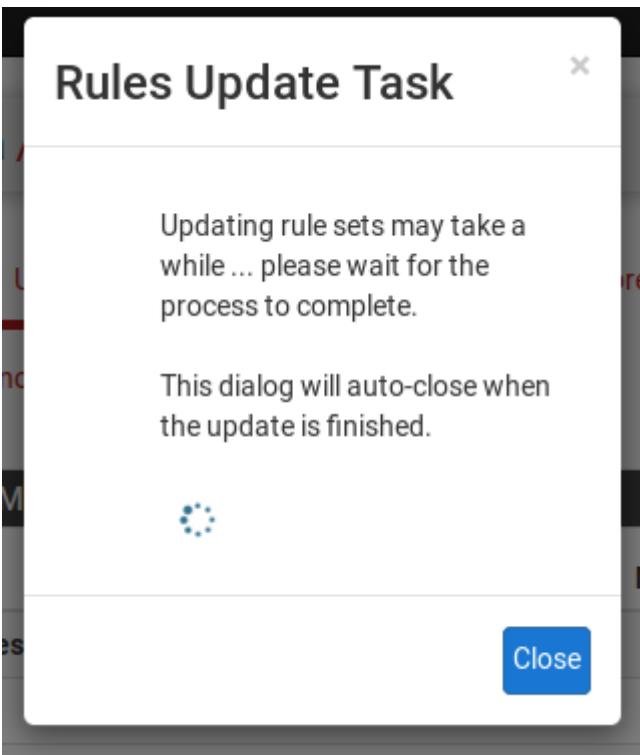
INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort Subscriber Rules	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Unknown
Result: Unknown

✓ Update ⬇ Force



Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
-----------------------------	----------------	----------------

INSTALLED RULE SET MD5 SIGNATURES		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	b87608ac90fc3a524c9072c89fc60007	Thursday, 27-Aug-20 09:06:27 UTC
Snort Subscriber Rules	1aa231e5b10d3d8a269afde3b4563168	Thursday, 27-Aug-20 09:06:29 UTC

Step 4 : Create lists

A list representing the home network is created.

Services / Suricata / Pass Lists

Interfaces Global Settings Updates Alerts Blocks Pass Lists Suppress Logs View

Logs Mgmt SID Mgmt Sync IP Lists

Configured Pass Lists

List Name	Assigned Alias	Description	Actions
HomeNetwork			Add

General Information

Name	HomeNetwork
The list name may only consist of the characters 'a-z, A-Z, 0-9 and _'.	
Description	
You may enter a description here for your reference.	

Auto-Generated IP Addresses

Local Networks	<input checked="" type="checkbox"/> Add firewall Locally-Attached Networks to the list (excluding WAN). Default is checked (but see warning below). If creating a custom HOME_NET list, then this box should usually be checked.
WAN IP	<input checked="" type="checkbox"/> Add WAN interface IP to the list. Default is checked. If creating a custom HOME_NET list and using NAT, then this box should usually be checked.
WAN Gateways	<input checked="" type="checkbox"/> Add WAN Gateways to the list. Default is checked.
WAN DNS Servers	<input checked="" type="checkbox"/> Add WAN DNS servers to the list. Default is checked.
Virtual IP Addresses	<input checked="" type="checkbox"/> Add Virtual IP Addresses to the list. Default is checked.
VPN Addresses	<input checked="" type="checkbox"/> Add VPN Addresses to the list. Default is checked. If creating a custom HOME_NET list, then this box should usually be checked.

Configured Pass Lists			
List Name	Assigned Alias	Description	Actions
<input type="checkbox"/> HomeNetwork			
			Add Delete

Also, since there are a lot of False Positives at startup, a suppression list is created to suppress specific Snort and ET signatures.

Services / Suricata / Suppression Lists			
Interfaces	Global Settings	Updates	Alerts
Blocks	Pass Lists	Suppress	Logs View
Configured Suppression Lists			
List Name	Description	Actions	
		Add	

General Information	
Name	<input type="text" value="WAN_List"/> <small>The list name may only consist of the characters 'a-z, A-Z, 0-9 and '_.'</small>
Description	<input type="text"/> <small>You may enter a description here for your reference.</small>

Configured Suppression Lists			
List Name	Description	Actions	
<input type="checkbox"/> WAN_List			
			Add Delete

General Information

Name The list name may only consist of the characters 'a-z, A-Z, 0-9 and _'.

Description You may enter a description here for your reference.

Suppression List Content

Suppression Rules

```
#disable SURICATA UDPv4 invalid checksum
suppress gen_id 1, sig_id 2200075,
track by_src, ip x.x.x.x
#disable SURICATA IPv4 invalid checksum
```

Valid keywords are 'suppress', 'event_filter' and 'rate_filter'.
Example 1: suppress gen_id 1, sig_id 1852, track by_src, ip 10.1.1.54
Example 2: event_filter gen_id 1, sig_id 1851, type limit, track by_src, count 1, seconds 60
Example 3: rate_filter gen_id 135, sig_id 1, track by_src, count 100, seconds 1, new_action log, timeout 10

 **Save**

```
#disable SURICATA UDPv4 invalid checksum

suppress gen_id 1, sig_id 2200075, track by_src, ip x.x.x.x

#disable SURICATA IPv4 invalid checksum
```

Step 5 : Enable rule categories

The screenshot shows the 'Services / Suricata / Interfaces' interface. The top navigation bar includes links for 'Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocks', 'Pass Lists', 'Suppress', 'Logs View', 'Logs Mgmt', 'SID Mgmt', 'Sync', and 'IP Lists'. Below this is a table titled 'Interface Settings Overview' with columns: 'Interface', 'Suricata Status', 'Pattern Match', 'Blocking Mode', 'Description', and 'Actions'. A green 'Add' button is located at the bottom right of the table area.

The screenshot shows the 'Suricata IDS / Interface - Categories' interface. The top navigation bar includes links for 'Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocks', 'Pass Lists', 'Suppress', 'Logs View', 'Logs Mgmt', 'SID Mgmt', 'Sync', and 'IP Lists'. Below this is a menu with options: 'Iface Settings', 'Iface Categories', 'Iface Rules', 'Iface Flow/Stream', 'Iface App Parsers', 'Iface Variables', and 'Iface IP Rep'. A section titled 'Automatic flowbit resolution' contains a 'Resolve Flowbits' checkbox which is checked. A note states: 'Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.' Below this is a 'View rules' section with a 'View' button and a note: 'Click to view auto-enabled rules required to satisfy flowbit dependencies'. A note at the bottom says: 'Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.'

Automatic flowbit resolution

Resolve Flowbits Auto-enable rules required for checked flowbits
 Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

View rules  Click to view auto-enabled rules required to satisfy flowbit dependencies

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Select the rulesets (Categories) Suricata will load at startup

▲ - Category is auto-enabled by SID Mgmt conf files
▼ - Category is auto-disabled by SID Mgmt conf files

Enabled	Ruleset: Snort GPLv2 Community Rules	
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos-certified)	
Enabled	Ruleset: ET Open Rules	Snort Rules have not been downloaded.
<input checked="" type="checkbox"/>	emerging-3coresec.rules	
<input checked="" type="checkbox"/>	emerging-activex.rules	
<input checked="" type="checkbox"/>	emerging-adware_pup.rules	
<input checked="" type="checkbox"/>	emerging-attack_response.rules	
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	
<input checked="" type="checkbox"/>	emerging-botcc.rules	
<input checked="" type="checkbox"/>	emerging-chat.rules	
<input checked="" type="checkbox"/>	emerging-clarmy.rules	
<input checked="" type="checkbox"/>	emerging-coinminer.rules	
<input checked="" type="checkbox"/>	emerging-compromised.rules	
<input checked="" type="checkbox"/>	emerging-current_events.rules	
<input checked="" type="checkbox"/>	emerging-deleted.rules	
<input checked="" type="checkbox"/>	emerging-dns.rules	

Available Rule Categories

Category: emerging-dns.rules

Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions:

When finished, click APPLY to save and send any SID state/action changes made on this tab to Suricata.

Rules View Filter

Rule Signature ID (SID) Enable/Disable Overrides

Legend: ✓ Default Enabled ✓ Enabled by user 🕒 Auto-enabled by SID Mgmt ⚠ Action/content modified by SID Mgmt ⚠ Rule action is alert ⚠ Rule contains noalert option
⌚ Default Disabled ⌚ Disabled by user 🕒 Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
⌚	⚠	1	2008446	udp	any	53	\$DNS_SERVERS	any	ET DNS Excessive DNS Responses with 1 or more RR's (100+ in 10 seconds) - possible Cache Poisoning Attempt
⌚	⚠	1	2008475	udp	any	53	\$HOME_NET	any	ET DNS Query Responses with 3 RR's set (50+ in 2 seconds) - possible A RR Cache Poisoning Attempt
⌚	⚠	1	2008447	udp	any	53	\$HOME_NET	any	ET DNS Query Responses with 3 RR's set (50+ in 2 seconds) - possible NS RR Cache Poisoning Attempt
✓	⚠	1	2101948	udp	\$EXTERNAL_NET	any	\$HOME_NET	53	GPL DNS zone transfer UDP
✓	⚠	1	2101616	udp	\$EXTERNAL_NET	any	\$HOME_NET	53	GPL DNS named version attempt
✓	⚠	1	2100252	udp	\$EXTERNAL_NET	any	\$HOME_NET	53	GPL DNS named iqury attempt

Available Rule Categories

Category: emerging-scan.rules

Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions:

When finished, click APPLY to save and send any SID state/action changes made on this tab to Suricata.

Rules View Filter

Rule Signature ID (SID) Enable/Disable Overrides

Legend: ✓ Default Enabled ✓ Enabled by user 🕒 Auto-enabled by SID Mgmt ⚠ Action/content modified by SID Mgmt ⚠ Rule action is alert ⚠ Rule contains noalert option
⌚ Default Disabled ⌚ Disabled by user 🕒 Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	⚠	1	2010371	tcp	\$EXTERNAL_NET	any	\$HOME_NET	any	ET SCAN Amap TCP Service Scan Detected
✓	⚠	1	2010372	udp	\$EXTERNAL_NET	any	\$HOME_NET	any	ET SCAN Amap UDP Service Scan Detected
✓	⚠	1	2008414	udp	\$EXTERNAL_NET	any	\$HOME_NET	69	ET SCAN Cisco Torch TFTP Scan
✓	⚠	1	2010642	tcp	\$EXTERNAL_NET	any	\$HOME_NET	21	ET SCAN Multiple FTP Root Login Attempts from Single Source - Possible Brute Force Attempt
✓	⚠	1	2010643	tcp	\$EXTERNAL_NET	any	\$HOME_NET	21	ET SCAN Multiple FTP Administrator Login Attempts from Single Source - Possible Brute Force Attempt
✓	⚠	1	2007802	tcp	any	any	any	21	ET SCAN Grim's Ping ftp scanning tool

Step 6 : Configure Logging

Services / Suricata / Edit Interface Settings - WAN

Interfaces Global Settings Updates Alerts Blocks Pass Lists Suppress Logs View Logs Mgmt SID Mgmt Sync IP Lists

WAN Settings WAN Categories WAN Rules WAN Flow/Stream WAN App Parsers WAN Variables WAN IP Rep

General Settings

Enable Checking this box enables Suricata inspection on the interface.

Interface Choose which interface this Suricata instance applies to. In most cases, you will want to use WAN here if this is the first Suricata-configured interface.

Description Enter a meaningful description here for your reference. The default is the interface name.

Logging Settings

Send Alerts to System Log Suricata will send Alerts from this interface to the firewall's system log.
NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.

Log Facility Select system log Facility to use for reporting. Default is LOCAL1.

Log Priority Select system log Priority (Level) to use for reporting. Default is NOTICE.

Networks Suricata Should Inspect and Protect

Home Net Choose the Home Net you want this interface to use.
Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.
Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

External Net Choose the External Net you want this interface to use.
External Net is networks that are not Home Net. Most users should leave this setting at default.
Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

Alert Suppression and Filtering

Alert Suppression and Filtering Choose the suppression or filtering file you want this interface to use. Default option disables suppression and filtering.

Enable Stats Collection	<input type="checkbox"/> Suricata will periodically gather performance statistics for this interface. Default is Not Checked.
Enable HTTP Log	<input checked="" type="checkbox"/> Suricata will log decoded HTTP traffic for the interface. Default is Checked.
Append HTTP Log	<input checked="" type="checkbox"/> Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.
Log Extended HTTP Info	<input type="checkbox"/> Suricata will log extended HTTP information. Default is Checked.
Enable TLS Log	<input type="checkbox"/> Suricata will log TLS handshake traffic for the interface. Default is Not Checked.
Enable File-Store	<input type="checkbox"/> Suricata will extract and store files from application layer streams. Default is Not Checked. WARNING: Enabling file-store will consume a significant amount of disk space on a busy network!
Enable Packet Log	<input type="checkbox"/> Suricata will log decoded packets for the interface in pcap-format. Default is Not Checked. This can consume a significant amount of disk space when enabled.

EVE Output Settings

EVE JSON Log	<input checked="" type="checkbox"/> Suricata will output selected info in JSON format to a single file or to syslog. Default is Not Checked.
EVE Output Type	<input type="text" value="SYSLOG"/>
Select EVE log output destination. Choosing FILE is suggested, and is the default value.	
EVE Syslog Output Facility	<input type="text" value="LOCAL1"/>
Select EVE syslog output facility.	
EVE Syslog Output Priority	<input type="text" value="NOTICE"/>
Select EVE syslog output priority.	
EVE HTTP XFF Support	<input type="checkbox"/> Log X-Forwarded-For IP addresses. Default is Not Checked.
EVE Log Alerts	<input checked="" type="checkbox"/> Suricata will output Alerts via EVE

Review Log

Services / Suricata / Alerts

Interfaces	Global Settings	Updates	Alerts	Blocks	Pass Lists	Suppress	Logs View	Logs Mgmt	SID Mgmt	Sync																					
IP Lists																															
Alert Log View Settings																															
<table border="1"> <tr> <td>Instance to View</td> <td><input type="text" value="(WAN) WAN"/></td> <td>Choose which instance alerts you want to inspect.</td> </tr> <tr> <td>Save or Remove Logs</td> <td><input type="button" value="Download"/></td> <td><input type="button" value="Clear"/></td> </tr> <tr> <td colspan="2">All alert log files for selected interface will be downloaded</td> <td>All log files will be cleared</td> </tr> <tr> <td>Save Settings</td> <td><input type="button" value="Save"/></td> <td><input checked="" type="checkbox"/> Refresh</td> </tr> <tr> <td colspan="2">Save auto-refresh and view settings</td> <td>Default is ON</td> </tr> <tr> <td colspan="2"></td> <td><input type="text" value="250"/></td> </tr> <tr> <td colspan="2"></td> <td>Number of alerts to display. Default is 250</td> </tr> </table>											Instance to View	<input type="text" value="(WAN) WAN"/>	Choose which instance alerts you want to inspect.	Save or Remove Logs	<input type="button" value="Download"/>	<input type="button" value="Clear"/>	All alert log files for selected interface will be downloaded		All log files will be cleared	Save Settings	<input type="button" value="Save"/>	<input checked="" type="checkbox"/> Refresh	Save auto-refresh and view settings		Default is ON			<input type="text" value="250"/>			Number of alerts to display. Default is 250
Instance to View	<input type="text" value="(WAN) WAN"/>	Choose which instance alerts you want to inspect.																													
Save or Remove Logs	<input type="button" value="Download"/>	<input type="button" value="Clear"/>																													
All alert log files for selected interface will be downloaded		All log files will be cleared																													
Save Settings	<input type="button" value="Save"/>	<input checked="" type="checkbox"/> Refresh																													
Save auto-refresh and view settings		Default is ON																													
		<input type="text" value="250"/>																													
		Number of alerts to display. Default is 250																													
Alert Log View Filter																															
Last 250 Alert Entries. (Most recent entries are listed first)																															
Date	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description																						

Date	Pri	Proto	Class	DPort	GID:SID	Description
08/27/2020 18:52:34	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:52:21	3	TCP	Generic Protocol Command Decode	31043	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:50:26	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:50:23	3	TCP	Generic Protocol Command Decode	57734	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:50:13	3	TCP	Generic Protocol Command Decode	31043	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:49:22	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:49:09	3	TCP	Generic Protocol Command Decode	31043	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:50	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:37	3	TCP	Generic Protocol Command Decode	31043	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:34	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:26	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:22	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:21	3	TCP	Generic Protocol Command Decode	31043	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:20	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘
08/27/2020 18:48:19	3	TCP	Generic Protocol Command Decode	17429	1:2210032	SURICATA STREAM FIN1 FIN with wrong seq ⊕ ✘

Step 7 : Enable Watchdog

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Service_Watchdog Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	Action
Service_Watchdog	1.8.7	Monitors for stopped services and restarts them.	+ Install

pfSense-pkg-Service_Watchdog installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
[1/1] Fetching pfSense-pkg-Service_Watchdog-1.8.7.txz: ... done
Checking integrity... done (0 conflicting)
[1/1] Installing pfSense-pkg-Service_Watchdog-1.8.7...
[1/1] Extracting pfSense-pkg-Service_Watchdog-1.8.7: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Menu items... done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

Confirmation Required to install package pfSense-pkg-Service_Watchdog.

Confirm

Services / Service Watchdog

This page allows selecting services to be monitored so that they may be automatically restarted if they crash or are stopped.

Notify	Service Name	Description	Actions
No services have been defined for monitoring.			

[+ Add New Service](#) [Save Notification Settings](#)

Services / Service Watchdog / Add

Add Service to Monitor

Service to Add: suricata: Suricata IDS/IPS Daemon

Select a service to add to the monitoring list.

[Add](#)

Notify	Service Name	Description	Actions
<input type="checkbox"/>	<input type="checkbox"/> suricata	Suricata IDS/IPS Daemon	Edit

What is Watchdog?

A watchdog is a device used to protect a system from specific software or hardware failures that may cause the system to stop responding.

Setup and tune is done.

15.6 Check Out the Config

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 8
```

```
[2.4.5-RELEASE][root@pfSense.locaLdomain]#
```

```
top -CPz -o cpu -n
```

```
[2.4.5-RELEASE][root@pfSense.locaLdomain]# top -CPz -o cpu -n
```

PID	USERNAME	THR	PRI	NICE	SIZE	RES	STATE	TIME	CPU	COMMAND
84774	root	5	20	0	111M	22600K	nanslp	0:03	0.00%	suricata
49478	root	1	20	0	10928K	2172K	select	0:01	0.00%	ntpd
362	root	1	20	0	171M	7088K	kqread	0:00	0.00%	php-fpm
46489	root	1	20	0	13440K	0K	kqread	0:00	0.00%	<nginx>
14473	root	1	20	0	6964K	1164K	bpf	0:00	0.00%	filterlog
92520	root	1	20	0	6412K	1256K	select	0:00	0.00%	syslogd
284	root	5	52	0	6904K	1572K	uwait	0:00	0.00%	dpinge
439	root	1	20	0	9156K	80K	select	0:00	0.00%	devd
400	root	1	40	20	6752K	0K	kqread	0:00	0.00%	<check_reload
<pre>_stat></pre>										
48785	root	1	23	0	6376K	576K	nanslp	0:00	0.00%	cron
36410	root	1	20	0	7280K	2724K	pause	0:00	0.00%	tcsh
46588	root	1	20	0	13440K	0K	kqread	0:00	0.00%	<nginx>
15930	root	1	20	0	12016K	1556K	piperd	0:00	0.00%	sshg-parser
19309	unbound	1	52	0	25152K	0K	kqread	0:00	0.00%	<unbound>
16241	root	2	20	0	6536K	1124K	piperd	0:00	0.00%	sshg-blocker
29628	root	1	52	20	6976K	1704K	wait	0:00	0.00%	sh
13924	root	1	52	0	6724K	0K	wait	0:00	0.00%	<login>
16682	root	1	52	0	6976K	0K	wait	0:00	0.00%	<sh>

```
ps auwwx | grep suricata
```

```
[2.4.5-RELEASE][root@pfSense.locaLdomain]# ps auwx | grep suricata
```

```
root 84774 0.0 15.6 120136 31932 - Ss 17:17 0:04.83 /usr/local/bin/
suricata -i em0 -D -c /usr/local/etc/suricata/suric
root 34297 0.0 0.9 6560 1792 v0 S+ 17:26 0:00.00 grep suricata
```

Check out all the logs

```
[3]: /var/log/Suricata/Suricata_0005155/alerts.log: no such file or directory  
[2.4.5-RELEASE][root@pfSense.localdomain]# ls /var/log/suricata  
suricata_em04761 suricata_rules_update.log  
[2.4.5-RELEASE][root@pfSense.localdomain]#
```

```
[2.4.5-RELEASE][root@pfSense.localdomain]# ls /var/log/suricata/suricata_em  
04761  
alerts.log http.log suricata.log  
[2.4.5-RELEASE][root@pfSense.localdomain]#
```

```
ls -1 /var/log/suricata/suricata_em04761/alerts.log
```

```
alerts.log http.log suricata.log  
[2.4.5-RELEASE][root@pfSense.localdomain]# ls -1 /var/log/suricata/suricata_em04761/alerts.log  
[2.4.5-RELEASE][root@pfSense.localdomain]#
```

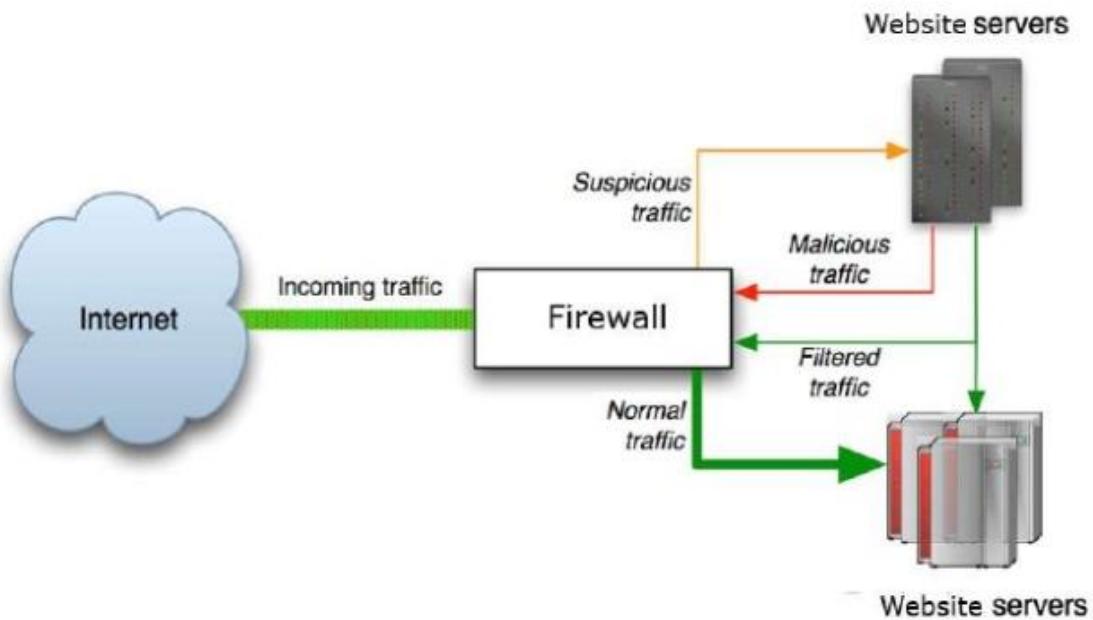
```
[2.4.5-RELEASE][root@pfSense.localdomain]# ls -1 /var/log/suricata/suricata_em04761/alerts.log  
[2.4.5-RELEASE][root@pfSense.localdomain]#
```

```
[2.4.5-RELEASE][root@pfSense.localdomain]# grep watch /etc/crontab  
*/1 * * * * root /usr/local/pkg/servicewatchdog_cron.php  
[2.4.5-RELEASE][root@pfSense.localdomain]#
```

Malware(**Malicious Software**) & Malicious Traffic

16.1 What is Malicious Traffic?

Malicious traffic or malicious network traffic is any suspicious link, file or connection that is being created or received over the network.



16.2 Malicious Traffic Types

- Scanners
- Worms
- Malicious Spam
- Backscatters
- DOS,DDOS

16.3 How does malicious traffic work?

When bad HTTP requests reach the command and control servers, these issue a communication to your compromised PC and make it a part of their larger zombie army known as botnets.

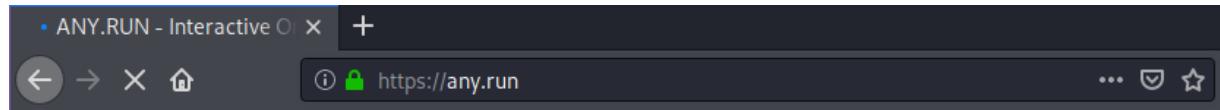
16.4 Detecting malicious traffic

Malicious traffic detection technology constantly monitors traffic for possible signs of suspicious links, files or links being created or received.

IPS systems are provided with suricata for example.

16.5 Any.run

- Any.run enables you to run and analyze all kinds of content (exe, js, pdf, office files, mail, script, URL) interactively in a real time environment.
- **Any.run uses suricata to analyze traffic.**
- Any.run also allows you to analyze compressed files.
- Any.run is also useful in analyzing macro viruses. The results can be observed by interactively running the suspect office file.





Register

You need to sign in for those awesome features



Welcome to ANY.RUN – first Interactive Malware Sandbox!

What's your name?

e



- Terms of Service & Privacy Policy *
- Subscribe to receive our newsletter

ANY.RUN – interactive sandbox gives you many advantages to research malicious files. Run simulation by launching various programs, rebooting the system and running various scenarios. Enjoy the speed and understandability of all processes.

If you already have an account [sign in](#)

[Next](#)

Thousands of samples that we receive from our users are analyzed by our machine learning system.



New Task

Let's create a new task

Advanced mode →

Choose operating system to start

Windows 7 ▾ 32bit 64bit

Type URL or choose a file to run

suriwire-suriwire-0.2.tar.gz (153.95 Kb) ×

File should contain extension otherwise use "Change extension to valid" option of Advanced mode

Task will be shared on the Public Submission Run

[← Get back to user mode](#)

STATISTICS FOR 24 HOURS 

CHOOSE OPERATING SYSTEM

Windows 7 32bit 64bit

Auto-confirm UAC ON OFF

Pre-installed soft set complete

Edition Professional

Build 7601

Locale United States (en-US)

ENVIRONMENT

APPLICATIONS		HOT FIXES
Internet Explorer	8.0.7601.175...	
Microsoft Visual C++ 2013 x86 Additional Ru...	12.0.21005	
Microsoft Visual C++ 2013 Redistributable (x...	12.0.30501.0	
Microsoft Visual C++ 2010 x86 Redistributabl...	10.0.40219	
Adobe Acrobat Reader DC MUI	15.023.20070	
Adobe Refresh Manager	1.8.0	
Microsoft Visual C++ 2008 Redistributable - x...	9.0.30729.61...	
Update for Microsoft .NET Framework 4.7.2 (...	1	
Microsoft .NET Framework 4.7.2	4.7.03062	
Microsoft Office Access Setup Metadata MUI (...	14.0.6029.10...	
Microsoft Office Shared Setup Metadata MUI (...	14.0.6029.10...	

OBJECT

Type URL or choose a file to run
 Type URL to file or Choose a file

Open in browser Internet Explorer

Download with User Agent Type User Agent Hide source of sample

Change extension to valid ON OFF

Command Line:
 Optional command line * Type %FILENAME% for replacing on path to the uploaded file in testing system

Start object from Temp directory

OPTIONS

Duration: 60 or SMART

Privacy: Public submission Who has a link Only me

NETWORK

Connected Disconnected

HTTPS MITM proxy Fake Net

Route internet traffic through (optional):
 Route via TOR User's VPN (OpenVPN)
Fastest geo

Save as default configuration

⚠ Task will be shared on the [Public Submission](#)

WINDOWS 7 PROFESSIONAL 32 bit

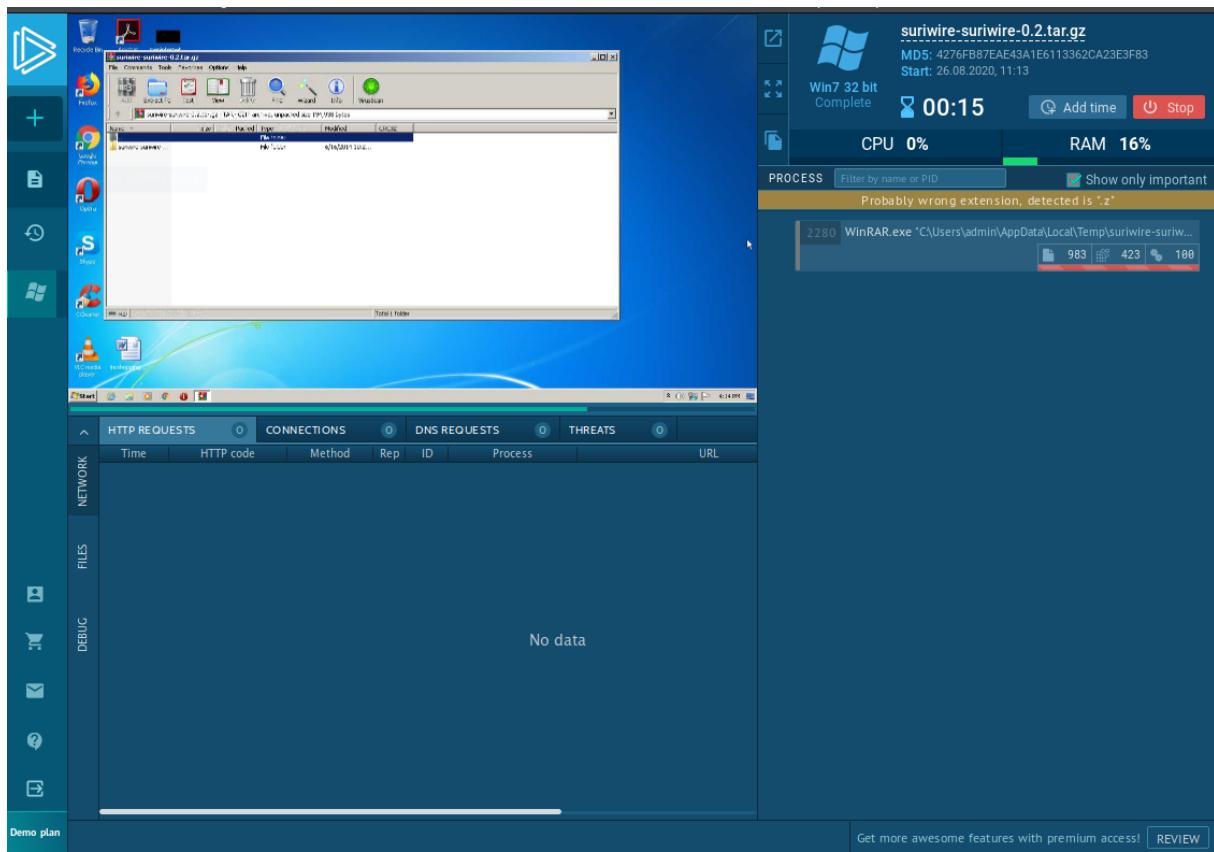


- ✓ Loading analyzed objects
- ✓ Allocating a new environment
- ↻ Creating a network connection
- Preparing to start
- Connecting to the incident!



Technical advice

Our service uses Suricata IDS. We offer the most accurate and fresh rulesets from premium providers, such as Proofpoint (Emerging Threats) and Positive Technologies at paid rates.



By examining the processes running in the right section, the reflections of the run file or URL on the system can be seen.

Likewise, with the help of the buttons on the Process section; File samples can be downloaded (**Sample**), the detected IOC data can be listed in bulk (**IOC**), the task can be re-run (**Re-run**), the report can be obtained as a pdf (**Text report**), its processes can be examined in graphics (**Processes graph**), Miter ATT & CK matches can be seen. (**ATT & CK™ matrix**).

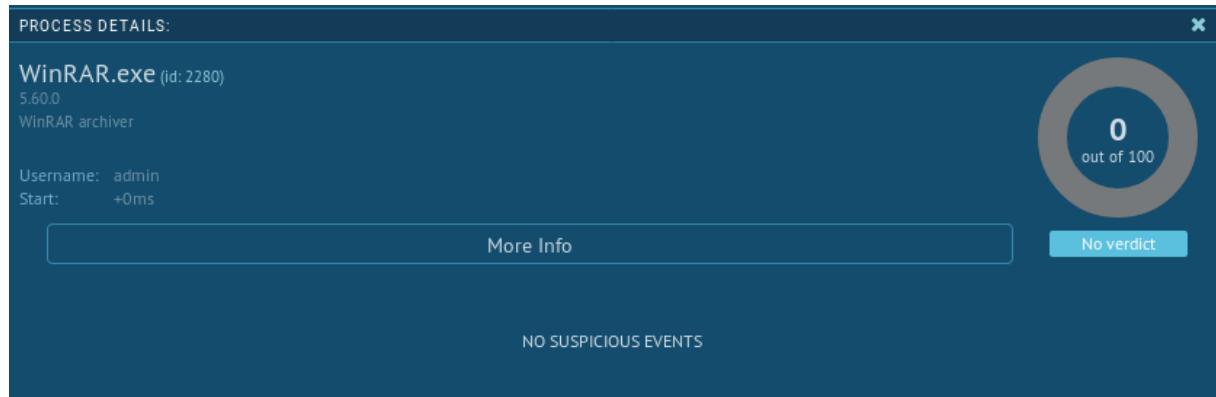
Tabs at the bottom of the interface:

HTTP Requests: You can see the http requests of the file / URL being run. There may be domains that malwares communicate as C&C servers.

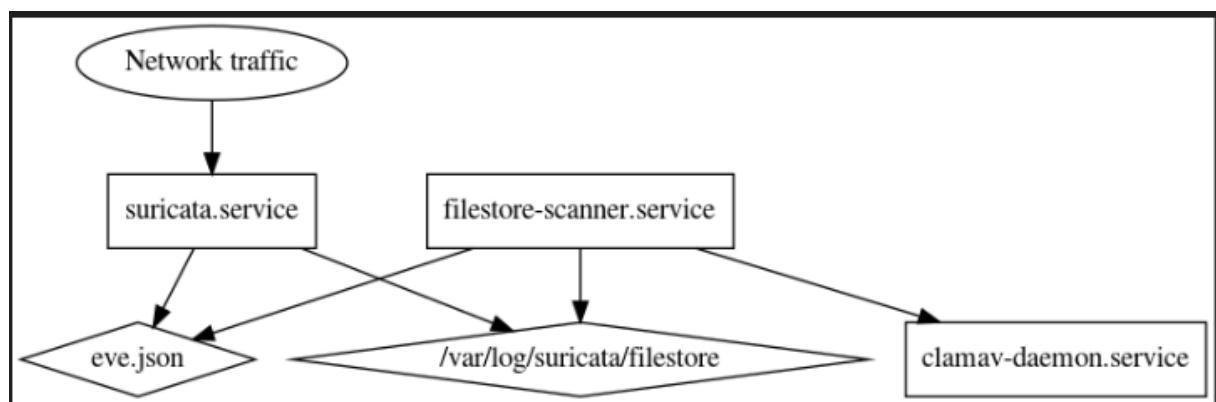
Connection: In this section, the data flows with which the connection is established - traffic can be examined and evidence can be collected about the communicated IP / domain.

DNS Requests: DNS queries can be viewed from this screen.

Threats: Malicious activities detected by Suricata IDS can be viewed here. This is a kind of conclusion part of the analysis.



16.6 Monitoring Network Traffic with Suricata and ClamAV



Install ClamAV

What is ClamAV?

ClamAV is anti-virus program.

```
clamdscan clamav-daemon|| clamav clamav-base clamav-freshclam clamdscan clamav-daemon
```

```
kali㉿kali:~$ sudo apt install clamav clamav-base clamav-freshclam clamdscan clamav-daemon
Trash
```

```
After this operation, 5,413 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 clamav-base all 0.102.4+dfsg-1 [119 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libtfm1 amd64 0.13-4 [60.5 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libclamav9 amd64 0.102.4+dfsg-1 [839 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 clamav-freshclam amd64 0.102.4+dfsg-1 [193 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 clamav amd64 0.102.4+dfsg-1 [174 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 clamav-daemon amd64 0.102.4+dfsg-1 [280 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 clamdscan amd64 0.102.4+dfsg-1 [131 kB]
Fetched 1,797 kB in 37s (48.4 kB/s)
Preconfiguring packages ...
Selecting previously unselected package clamav-base.
(Reading database ... 304496 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.102.4+dfsg-1_all.deb ...
Unpacking clamav-base (0.102.4+dfsg-1) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../1-libtfm1_0.13-4_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../2-libclamav9_0.102.4+dfsg-1_amd64.deb ...
Unpacking libclamav9:amd64 (0.102.4+dfsg-1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../3-clamav-freshclam_0.102.4+dfsg-1_amd64.deb ...
Unpacking clamav-freshclam (0.102.4+dfsg-1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../4-clamav_0.102.4+dfsg-1_amd64.deb ...
Unpacking clamav (0.102.4+dfsg-1) ...
Selecting previously unselected package clamav-daemon.
Preparing to unpack .../5-clamav-daemon_0.102.4+dfsg-1_amd64.deb ...
Unpacking clamav-daemon (0.102.4+dfsg-1) ...
Selecting previously unselected package clamdscan.
Preparing to unpack .../6-clamdscan_0.102.4+dfsg-1_amd64.deb ...
Unpacking clamdscan (0.102.4+dfsg-1) ...
Setting up libtfm1:amd64 (0.13-4) ...
Setting up libclamav9:amd64 (0.102.4+dfsg-1) ...
Setting up clamav-base (0.102.4+dfsg-1) ...
id: 'clamav': no such user
[Progress: [ 66%] [########################################.....]]
```

```
Setting up clamav-freshclam (0.102.4+dfsg-1) ...
clamav-freshclam.service is a disabled or a static unit, not starting it.
update-rc.d: We have no instructions for the clamav-freshclam init script.
update-rc.d: It looks like a non-network service, we enable it.
Setting up clamdscan (0.102.4+dfsg-1) ...
Setting up clamav-daemon (0.102.4+dfsg-1) ...
update-rc.d: We have no instructions for the clamav-daemon init script.
update-rc.d: It looks like a non-network service, we enable it.
clamav-daemon.service is a disabled or a static unit, not starting it.
Setting up clamav (0.102.4+dfsg-1) ...
Processing triggers for libc-bin (2.31-2) ...
Processing triggers for systemd (245.4-3) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for kali-menu (2020.2.2) ...

```

```
systemctl enable --now clamav-daemon
```

```
root@kali:~# systemctl enable --now clamav-daemon
```

```
Synchronizing state of clamav-daemon.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable clamav-daemon  
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-daemon.service → /lib/systemd/system/clamav-daemon.service.
```

Test service:

```
sudo clamdscan /fileName –fdpass
```

```
root@kali:/home/kali/Downloads# sudo clamdscan /home/kali/Downloads --fdpass  
/home/kali/Downloads: OK  
----- SCAN SUMMARY -----  
Infected files: 0  
Time: 0.407 sec (0 m 0 s)  
root@kali:/home/kali/Downloads#
```

Suricata:

```
sudo add-apt-repository ppa:oisf/suricata-stable
```

```
kali@kali:~$ sudo add-apt-repository ppa:oisf/suricata-stable
```

```
sudo: add-apt-repository: command not found
```

Command not found!

```
sudo apt-get install software-properties-common
```

```
sudo: add-apt-repository: command not found  
kali@kali:~$ sudo apt-get install software-properties-common
```

```

After this operation, 957 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 python3-distro-info all 0.23 [8,004 B]
Get:2 http://kali.download/kali kali-rolling/main amd64 python3-software-properties all 0.96.20.2-2.1 [49.7 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 software-properties-common all 0.96.20.2-2.1 [83.4 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 unattended-upgrades all 2.7 [88.4 kB]
Fetched 230 kB in 31s (7,460 B/s)
Preconfiguring packages ...
Selecting previously unselected package python3-distro-info.
(Reading database ... 304609 files and directories currently installed.)
Preparing to unpack .../python3-distro-info_0.23_all.deb ...
Unpacking python3-distro-info (0.23) ...
Selecting previously unselected package python3-software-properties.
Preparing to unpack .../python3-software-properties_0.96.20.2-2.1_all.deb ...
Unpacking python3-software-properties (0.96.20.2-2.1) ...
Selecting previously unselected package software-properties-common.
Preparing to unpack .../software-properties-common_0.96.20.2-2.1_all.deb ...
Unpacking software-properties-common (0.96.20.2-2.1) ...
Selecting previously unselected package unattended-upgrades.
Preparing to unpack .../unattended-upgrades_2.7_all.deb ...
Unpacking unattended-upgrades (2.7) ...
Setting up python3-software-properties (0.96.20.2-2.1) ...
Setting up python3-distro-info (0.23) ...
Setting up software-properties-common (0.96.20.2-2.1) ...
Setting up unattended-upgrades (2.7) ...

Creating config file /etc/apt/apt.conf.d/50unattended-upgrades with new version
update-rc.d: We have no instructions for the unattended-upgrades init script.
update-rc.d: It looks like a non-network service, we enable it.
Synchronizing state of unattended-upgrades.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable unattended-upgrades
Created symlink /etc/systemd/system/multi-user.target.wants/unattended-upgrades.service → /lib/systemd/system/unattended-upgrades.service.
Processing triggers for kali-menu (2020.2.2) ...
Processing triggers for systemd (245.4-3) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for dbus (1.12.16-2) ...

```

```

kali@kali:~$ sudo apt-get update

```

again:

```

kali@kali:~$ sudo add-apt-repository ppa:oisf/suricata-stable

```

```

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
- IDS runmode
- IPS runmode
- IDPS runmode
- NSM runmode
- eBPF/XDP
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRB
5, DHCP, IKEv2, SNMP, SIP, RDP
- SCADA automatic protocol detection - ENIP/DNP3/MODBUS
- File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted from live traffic.
- File MD5/SHA1/SHA256 matching
- Gzip Decompression
- Fast IP Matching
- Datasets matching
- Rustlang enabled protocol detection
- Lua scripting

and many more great features -
http://suricata-ids.org/features/all-features/
More info: https://launchpad.net/~oisf/+archive/ubuntu/suricata-stable
Press [ENTER] to continue or ctrl-c to cancel adding it

```

```
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keybox '/tmp/tmp_14ifeb/pubring.gpg' created
gpg: /tmp/tmp_14ifeb/trustdb.gpg: trustdb created
gpg: key D7F87B2966EB736F: public key "Launchpad PPA for Peter Manev" imported
gpg: Total number processed: 1
gpg:          imported: 1
gpg: no valid OpenPGP data found.
```

```
curl -s https://updates.signal.org/desktop/apt/keys.asc | sudo apt-key add -
root@kali:~# curl -s https://updates.signal.org/desktop/apt/keys.asc | sudo apt-key add -
root@kali:~# curl -vs https://updates.signal.org/desktop/apt/keys.asc
```

And reboot

```
root@kali:~# sudo -E add-apt-repository ppa:oisf/suricata-stable
```

```
sudo apt instal suricata
```

```
root@kali:~# sudo apt install suricata

Reading package lists ... Done
Building dependency tree
Reading state information ... Done
suricata is already the newest version (1:5.0.3-1).
0 upgraded, 0 newly installed, 0 to remove and 878 not upgraded.
```

```
root@kali:~# sudo suricata-update
```

```
les
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dhcp-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dnp3-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dns-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/files.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ipsec-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/kerberos-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/modbus-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/nfs-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ntp-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/smb-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/smtp-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/stream-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/tls-events.rules
29/8/2020 -- 09:46:00 - <Info> -- Ignoring file rules/emerging-deleted.rules
29/8/2020 -- 09:46:06 - <Info> -- Loaded 27804 rules.
29/8/2020 -- 09:46:07 - <Info> -- Disabled 14 rules.
29/8/2020 -- 09:46:07 - <Info> -- Enabled 0 rules.
29/8/2020 -- 09:46:07 - <Info> -- Modified 0 rules.
29/8/2020 -- 09:46:07 - <Info> -- Dropped 0 rules.
29/8/2020 -- 09:46:07 - <Info> -- Enabled 141 rules for flowbit dependencies.
29/8/2020 -- 09:46:07 - <Info> -- Backing up current rules.
29/8/2020 -- 09:46:12 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 27804; enabled: 20951; added: 203; removed 27; modified: 2626
29/8/2020 -- 09:46:13 - <Info> -- Testing with suricata -T.
```

```
29/8/2020 -- 13:30:15 - <Info> -- Done.
```

Update the basic rules and reload the service.

```
sudo kill -USR2 `pidof suricata`
```

```
kali㉿kali:~$ sudo kill -USR2 `pidof suricata`  
Usage:  
  kill [options] <pid> [...]  
  
Options:  
  <pid> [...]           send signal to every <pid> listed  
  -<signal>, -s, --signal <signal>  
                        specify the <signal> to be sent  
  -l, --list=[<signal>]  list all signal names, or convert one to a name  
  -L, --table            list all signal names in a nice table  
  
  -h, --help              display this help and exit  
  -V, --version           output version information and exit  
  
For more details see kill(1).
```

```
root@kali:~# nano /etc/suricata/suricata.yaml
```

```
outputs:
```

```
...
```

```
- eve-log:
```

```
    enabled: yes
```

```
    filetype: regular
```

```
    filename: eve.json
```

```
...
```

```
types:
```

```
...
```

```
- files:
```

```
    force-magic: yes
```

```
    force-hash: ["sha256"]
```

```

outputs:
  # a line based alerts log similar to Snort's fast.log
  - fast:
      enabled: yes
      filename: fast.log
      append: yes
      #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'

  # Extensible Event Format (nicknamed EVE) event log in JSON format
  - eve-log:
      enabled: yes
      filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
      filename: eve.json
      #prefix: "@eve: " # prefix to prepend to each log entry

  #custom. [subject, issuer, session_resumed, serial, fingerprint]
  - files:
      force-magic: yes    # force logging magic on all logged files
      force-hash:["sha256"]
      # force logging of checksums, available hash functions are md5,
      # sha1 and sha256
      #force-hash: [md5]

```

After editing surita.yaml, restart suricata service.

```
systemctl restart suricata
```

```
root@kali:~# systemctl restart suricata
[1] 1188877

```

Create a request that will return a plain text file to see it in action:

```
root@kali:~# curl http://google.ca
```

```
root@kali:~# curl http://google.ca
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.ca/">here</A>.
</BODY></HTML>
root@kali:~#
```

Grep:

```
sudo grep "fileinfo" /var/log/suricata/eve.json | jq
```

```
root@kali:~# grep "fileinfo" /var/log/suricata/eve.json | jq
```

```
-bash: jq: command not found
root@kali:~#
```

```
root@kali:~# apt-get install jq
```

```
Selecting previously unselected package jq.
Preparing to unpack ... /archives/jq_1.6-1_amd64.deb ...
Unpacking jq (1.6-1) ...
Setting up libonig5:amd64 (6.9.5-2) ...
Setting up libjq1:amd64 (1.6-1) ...
Setting up jq (1.6-1) ...
Processing triggers for libc-bin (2.30-4) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for kali-menu (2020.2.2) ...
root@kali:~#
```

```
root@kali:~# cat grep "fileinfo" /var/log/suricata/eve.json | jq
      Trash
```

Output:

```
{
  "timestamp": "2020-08-29T13:42:03.877935-0400",
  "event_type": "stats",
  "stats": {
    "uptime": 464,
    "capture": {
      "kernel_packets": 0,
      "kernel_drops": 0,
      "errors": 0
    },
    "processes": {
      "idle": 0
    }
  }
}
```

```
"flows_checked": 0,
"flows_notimeout": 0,
"flows_timeout": 0,
"flows_timeout_inuse": 0,
"flows_removed": 0,
"rows_checked": 65536,
"rows_skipped": 65536,
"rows_empty": 0,
"rows_busy": 0,
"rows maxlen": 0
},
"http": {
    "memuse": 0,
    "memcap": 0
},
"ftp": {
    "memuse": 0,
    "memcap": 0
}
}
```

Scanning Malware Files

```
kali㉿kali:/etc/suricata$ sudo nano suricata.yaml
```

```
w prune - command which can delete files over a certain age.
- file-store:
    version: 2
    enabled: no

# Set the directory for the filestore. If the path is not
# absolute will be relative to the default-log-dir.
#dir: filestore

# Write out a fileinfo record for each occurrence of a
# file. Disabled by default as each occurrence is already logged
# as a fileinfo record to the main eve-log.
write-fileinfo: yes

# Force storing of all files. Default: no.
force-filestore: yes
```

Download test file:

```
root@kali:~# wget http://2016.eicar.org/download/eicar.com
```

```
--2020-08-29 13:53:25-- http://2016.eicar.org/download/eicar.com
Resolving 2016.eicar.org (2016.eicar.org) ... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to 2016.eicar.org (2016.eicar.org)|89.238.73.97|:80 ... connected.
HTTP request sent, awaiting response ... 301 Moved Permanently
Location: https://www.eicar.org/download/eicar.com [following]
--2020-08-29 13:53:26-- https://www.eicar.org/download/eicar.com
Resolving www.eicar.org (www.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to www.eicar.org (www.eicar.org)|89.238.73.97|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 68 [application/x-msdownload]
Saving to: 'eicar.com'

eicar.com          100%[=====]      68  --KB/s    in 0s

2020-08-29 13:53:27 (31.0 MB/s) - 'eicar.com' saved [68/68]
```

```
root@kali:~# sudo cat grep "fileinfo" /var/log/suricata/eve.json | jq
```

```
"timestamp": "2020-08-29T14:33:09.549144-0400",
"event_type": "stats",
"stats": {
    "uptime": 2561,
    "capture": {
        "kernel_packets": 0,
        "kernel_drops": 0,
        "errors": 0
    }
}.
```

File captured by the suricata:

```
kali@kali:~$ sudo clamdscan Downloads --fdpass
/home/kali/Downloads/eicar.com: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Infected files: 1
Time: 0.288 sec (0 m 0 s)
```

```
GNU nano 4.9.2                               suricata.log
29/8/2020 -- 14:49:52 - <Notice> - rule reload complete
29/8/2020 -- 14:50:04 - <Notice> - Signal Received. Stopping engine.
29/8/2020 -- 14:50:04 - <Info> - time elapsed 3575.940s
29/8/2020 -- 14:50:04 - <Info> - Alerts: 0
29/8/2020 -- 14:50:05 - <Info> - cleaning up signature grouping structure... complete
29/8/2020 -- 14:50:05 - <Notice> - Stats for 'eth0': pkts: 0, drop: 0 (-nan%), invalid: 0, errors: 0, bytes: 0, rate: 0 B/s
29/8/2020 -- 14:50:05 - <Notice> - This is Suricata version 5.0.3 RELEASE running in monitor mode
29/8/2020 -- 14:50:05 - <Info> - CPUs/cores online: 2
29/8/2020 -- 14:50:06 - <Info> - Found an MTU of 1500 for 'eth0'
29/8/2020 -- 14:50:06 - <Info> - Found an MTU of 1500 for 'eth0'
29/8/2020 -- 14:50:06 - <Info> - fast output device (regular) initialized: fast.log
29/8/2020 -- 14:50:06 - <Info> - eve-log output device (regular) initialized: eve.js
29/8/2020 -- 14:50:06 - <Info> - stats output device (regular) initialized: stats.log
29/8/2020 -- 14:50:06 - <Warning> - [ERRCODE: SC_ERR_NO_RULES(42)] - No rule files in /etc/suricata/rules.d
29/8/2020 -- 14:50:06 - <Warning> - [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - 1 rule file was not loaded
29/8/2020 -- 14:50:06 - <Info> - Threshold config parsed: 0 rule(s) found
29/8/2020 -- 14:50:06 - <Info> - 0 signatures processed. 0 are IP-only rules, 0 are domain-only rules
29/8/2020 -- 14:50:06 - <Info> - Going to use 2 thread(s)
29/8/2020 -- 14:50:06 - <Info> - Using unix socket file '/var/run/suricata-command.sock'
29/8/2020 -- 14:50:06 - <Notice> - all 2 packet processing threads, 4 management threads are running
29/8/2020 -- 14:50:06 - <Info> - All AFP capture threads are running.
```

CHAPTER 17

References

- <http://temelag.blogspot.com>
- <https://docs.vmware.com>
- <https://superuser.com>
- <https://geekflare.com/pfsense-installation-guide/>
- <https://www.malware-traffic-analysis.net>
- <https://nullsecure-org.cdn.ampproject.org/>
- <https://www.reviversoft.com/tr/file-extensions pcap>
- <http://furkankayar.net/interaktif-malware-analiz-tool-anyrun/>
- <https://www.linuxquestions.org>
- <https://www.bitlyft.com/what-is-the-difference-between-ids-and-ips/>
- <https://bibliothequer.com/technologie/suricata/>
- <https://www.aldeid.com/wiki/Suricata-vs-snort>
- <https://fordefence.com/saldiri-tespit-ve-onleme-sistemleri-ids-ips/>
- <https://www.pona.com.tr/ips-ids-nedir/>
- <https://averagelinuxuser.com/linux-firewall/>
- <https://www.prismacsi.com/ips-ids-nedir/>
- <https://sibertehdit.com/ips-ve-ids-nedir-bu-sistemler-nasil-atlatilir/>
- <https://searchvmware.techtarget.com/definition/VMware>
- <https://www.stamus-networks.com/blog/2014/07/30/a-suricata-application-for-splunk>
- <https://pdfslide.net/documents/suricata-tutorial.html>
- <https://splunkbase.splunk.com/app/3202/>
- <https://home.regit.org/2014/03/suricata-ulogd-splunk-logstash/>
- <https://elatov.github.io/2015/01/suricata-on-freebsd-10/>
- <https://cse.sc.edu/~huangct/CSCE715S17/07346821.pdf>
- <https://www.systutorials.com>
- <https://www.hurricanelabs.com/splunk-tutorials/how-to-set-up-pfsense-and-suricata-in-splunk>
- <https://stackoverflow.com>

- <https://www.researchgate.net>
- <https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview>
- <https://www.btkakademi.gov.tr>
- <https://medium.com/@alpinoacademy/creating-custom-suricata-signatures-260fc049b56a>
- <http://magcyber.blogspot.com/2018/03/install-and-configuring-pfsense-on.html?m=1>
- <https://nbailey.ca/post/malware-on-the-wire/>
- <https://www.proofpoint.com/us/corporate-blog/post/emerging-threats-announcing-support-suricata-50>
- <https://www.bilgisayarnedir.com/>
- <https://berqnet.com>
- <https://searchvmware.techtarget.com>
- <https://www.vmware.com>
- <https://www.varonis.com>
- <https://purplesec.us>
- <https://fordefence.com>
- <https://www.bitlyft.com>
- <https://www.dnsstuff.com>
- <https://www.okanhazirci.com>
- <https://blog.rapid7.com/2017/02/21/suricata-overview/>
- <https://www.proofpoint.com/us/corporate-blog/post/emerging-threats-announcing-support-suricata-50>
- <https://wiki.archlinux.org/index.php/Suricata>
- [https://en.wikipedia.org/wiki/Suricata_\(software\)](https://en.wikipedia.org/wiki/Suricata_(software))
- <https://resources.infosecinstitute.com/configure-use-suricata-threat-detection/>
- <https://www.aldeid.com>
- <https://tacticalflex.zendesk.com>
- <https://redmine.openinfosecfoundation.org/>
- <https://linuxhint.com/>
- <https://home.regit.org/software/suriwire/>
- <https://sibertehtdit.com/>
- <http://sistemdostu.com/pfsense>
- <https://medium.com/@exnovan/pfsense-firewall-kurulumu-ve-ip-adresi%CC%87-yapilandirmasi-27f23af42bac>
- <https://techbast.com>
- <https://billysoftacademy.com/how-to-install-pfsense-2-4-4-on-vmware-workstation-15-5-pro/>
- <http://magcyber.blogspot.com/2018/03/install-and-configuring-pfsense-on.html?m=1>
- <https://www.webopedia.com/>
- <https://www.cisco.com/>
- <https://suricata-ids.org/features/>

- <https://technologyevangelist.co/2015/03/18/a-10gbe-capture-platform-snort-bro-suricata-wireshark/>
- <https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview>
- <https://resources.infosecinstitute.com/configure-use-suricata-threat-detection/>
- <https://www.slideshare.net/KurtuluKarasu/suricata-ile-siber-tehdit-avcl>
- <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
- <https://www.niobeweb.net/blog/firewall/>
- <https://www.webopedia.com/TERM/W/watchdog.html#:~:text=A%20watchdog%20is%20a%20device,information%20to%20the%20watchdog%20device.>
- <https://billysoftacademy.com/how-to-install-pfsense-2-4-4-on-vmware-workstation-15-5-pro/>
- <https://docs.netgate.com/pfsense/en/latest/install/installing-pfsense.html#pfsense-default-configuration>
- <http://magcyber.blogspot.com/2018/03/install-and-configuring-pfsense-on.html?m=1>
- <https://www.digitalocean.com/community/questions/after-installing-the-firewall-can-not-log-in-with-ssh>
- <https://techbast.com/2019/05/pfsense-how-to-install-firewall-pfsense-virtual-on-vmware.html>
- <https://buildmedia.readthedocs.org/media/pdf/suricata/latest/suricata.pdf>
- <https://suricata.readthedocs.io/en/suricata-3.2.5/performance/packet-profiling.html>
- <https://wiki.wireshark.org/Tools>
- https://github.com/alperensahin/suricata/blob/master/STS_Suricata.pdf
- https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Adding_Your_Own_Rules
- https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Rules
- <https://nbailey.ca/post/malware-on-the-wire/>
- <https://itsfoss.com/add-apt-repository-command-not-found/>
- <https://www.slideshare.net/ishraqabd/malicious-traffic>
- <https://home.sophos.com/en-us/security-news/2020/undetected-malicious-traffic.aspx#:~:text=Malicious%20traffic%20or%20malicious%20network,may%20compromise%20your%20personal%20computer.>