

Tasks

- 1- install splunk**
- 2- install forwarder**
- 3- configure Domain Controller**
- 4- install Xampp Web app server**
- 5- install Pfsense firewall**
- 6- install Suricata IPS/IDS**
- 6- configure DVWA vulnerable Web app on xampp**
- 7- configure securityMod WAF To detect web app attacks**
- 8- write rule in splunk to generate alert**
- 9- detect Active Directory Attacks**

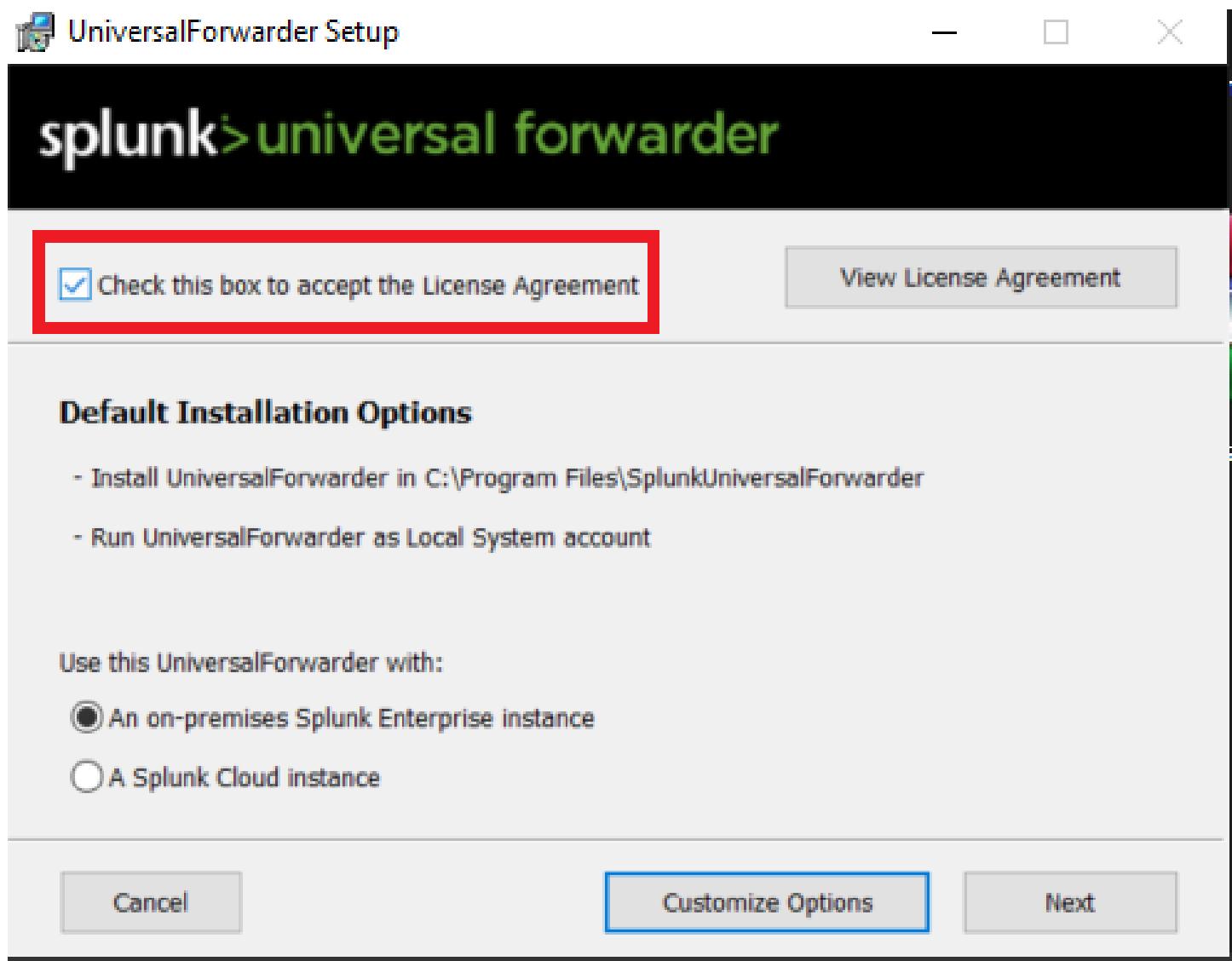
splunk install

- 1- Download [Splunk](#)**
- 2- sudo dpkg -i splunk.deb**
- 3- sudo /opt/splunk/bin/splunk start --accept-license**
- 4- sudo /opt/splunk/bin/splunk enable boot-start**

you can access splunk via web browser
http://127.0.0.1:8000

install forwarder

Download [Forwarder](#)



Add Splunk Machine IP Address And Default Port ==>
192.168.1.20:8089

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP

 :

*Enter the hostname or IP of your deployment server, e.g.
ds.splunk.com*

default is 8089

Add Splunk Machine IP Address And Default Port ==>

192.168.1.20:9997

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP

 :

*Enter the hostname or IP of your receiving indexer, e.g.
ds.splunk.com*

default is 9997

Configure Receiving In Splunk

Note:

Make sure allow traffic through Firewall port 8089, 9997 on Windows Machine And Linux Machine

The screenshot shows the Splunk web interface. At the top, there are navigation links: 'Administrator', 'Messages' (with 1 notification), 'Settings' (highlighted with a red box), 'Activity', 'Help', and 'Find'. Below the navigation is a search bar labeled 'Search settings...'. On the left, there's a sidebar with links: 'Created by you', 'Shared', 'Add Data' (with a plus icon), 'Explore Data' (with a magnifying glass icon), 'Monitoring Console' (with a bar chart icon), 'Visualize' (with a pie chart icon), 'Create dashboards', and 'Configure mobile devices'. The main content area is titled 'DATA' and contains several sections: 'KNOWLEDGE' (Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations), 'SYSTEM' (Server settings; Server controls; Health report manager; RapidDiag; Instrumentation; Licensing; Workload management; Mobile settings), 'DISTRIBUTED ENVIRONMENT' (OTel Collectors; Agent management; Indexer clustering; Federation; Distributed search), 'USERS AND AUTHENTICATION' (Roles; Users; Tokens; Password management; Authentication methods). The 'Forwarding and receiving' link under 'DATA' is also highlighted with a red box.

Forward data

Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

Write Default Port 9997

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

For example, 9997 will receive data on TCP port 9997.

Cancel **Save**

Add Date In Splunk

The screenshot shows the Splunk Enterprise home page. On the left, there's a sidebar with various app icons and names: Search & Reporting, Audit Trail, Data Management, Discover Splunk Observability Cloud, Imperva AppSecurity View, Splunk Secure Gateway, Splunk Security Essentials, and Upgrade Readiness App. The main area is titled "Hello, Administrator". It features a "Common tasks" section with several cards:

- Add data**: Add data from a variety of common sources. This card is highlighted with a red box.
- Search your data**: Turn data into doing with Splunk search.
- Visualize your data**: Create dashboards that work for your data.
- Manage alerts**: Manage the alerts that monitor your data.
- Add team members**: Add your team members to Splunk platform.
- Manage permissions**: Control who has access with roles.
- Configure mobile devices**: Login or manage mobile devices using Splunk Secure Gateway.

What data do you want to send to the Splunk platform?



Upload
files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



Monitor
files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



Forward
data from a Splunk forwarder

Files - TCP/UDP - Scripts

1- Select host from Available Host

2- Add A New Host Name

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class

New

Existing

Available host(s)

[add all >](#)

WINDOWS DC

Selected host(s)

[« remove all](#)

New Server Class Name

Add Data

Select Forwarders Select Source Input Settings Review Done

< Back Next >

Local Event Logs

Collect event logs from this machine.

Files & Directories

Upload a file, index a local file, or monitor an entire directory.

TCP / UDP

Configure the Splunk platform to listen on a network port.

Local Performance Monitoring

Collect performance data from this machine.

Scripts

Get data from any API, service, or database with a script.

checkapp

Systemd Journald Input for Splunk

This is the input that gets data from journald (systemd's logging component) into Splunk.

Load Input for the Splunk platform

Configure selected Splunk Universal Forwarders to monitor local Windows event log channels, which contain log data published by installed applications, services, and system processes. The event log monitor runs once for every event log input defined in the Splunk platform. [Learn More](#)

Select Event Logs Available item(s)

add all >

Selected item

Select the Windows Event Logs you want to index from the list.

Add Data

Select Forwarders Select Source Input Settings Review Done

< Back **Review >**

Input Settings

Optionally set additional input parameters for this data input as follows:

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Default ▾ **Create a new index**

FAQ

> How do indexes work?
 > How do I know when to create or use multiple indexes?

Create New Index Name PC-01

New Index X

General Settings

Index Name Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics
The type of data to store (event-based or metrics).

Home Path optional
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

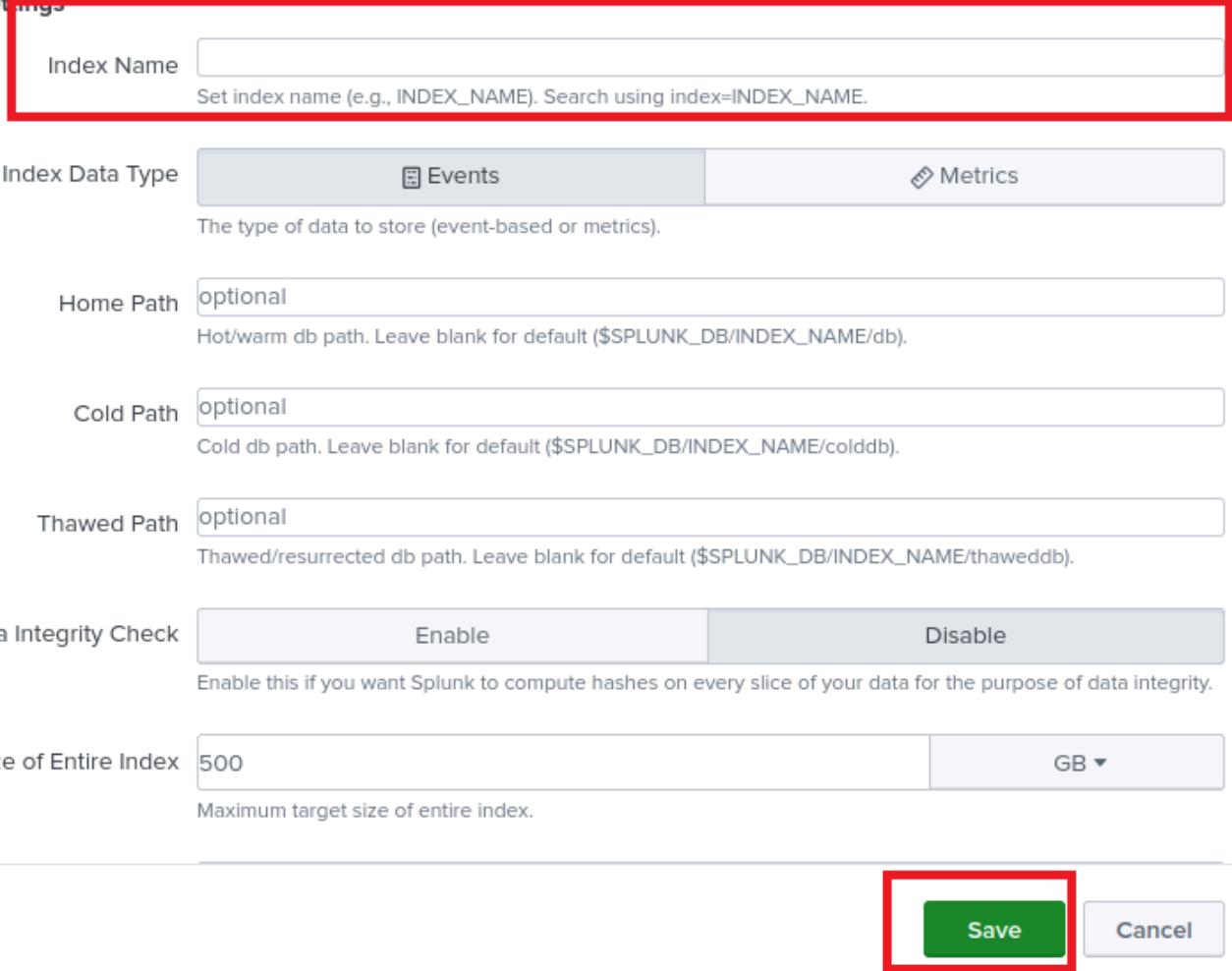
Cold Path optional
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path optional
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index GB ▾
Maximum target size of entire index.

Save Cancel



After Create It Choose It And Click Rivew And Done

Install And Configure Sysmon:

Download [Sysmon](#)

Download [Configuration File](#)

Copy Configuration file to Sysmon Directory

Open PowerShell OR CMD As Administrator

Command:

Sysmon64.exe -accepteula -i sysmonconfig.xml

Send Sysmon Logs To Splunk

Go To This Path ==>

C:\ProgramFiles\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local

Open Inputs.conf file And Add this

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

disabled = false

renderXml = true

source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

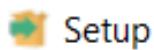
index = PC-01

Install Xampp Server On windows Server To Configure DVWA Lab

Download [Xampp](#)

Installation Process Like As Any exe File Click Next Next...BlaBlaBla

Note: Make Sure Choose this Options



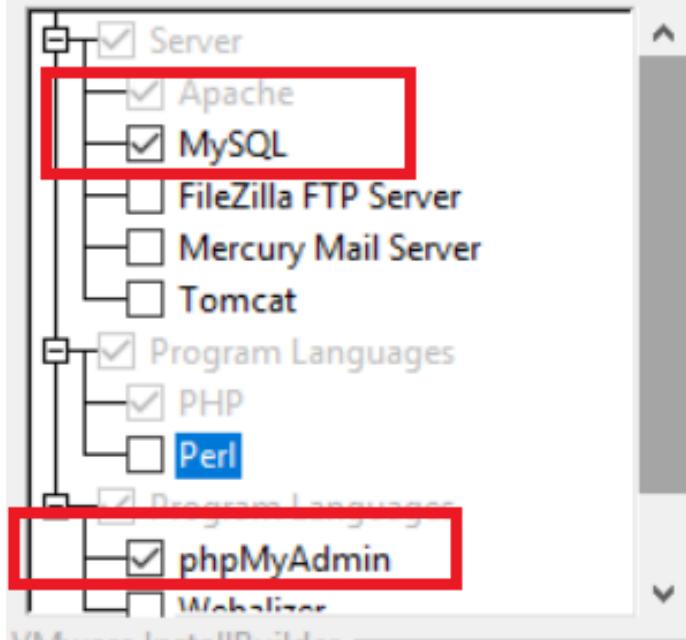
Setup

- X



Select Components

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.



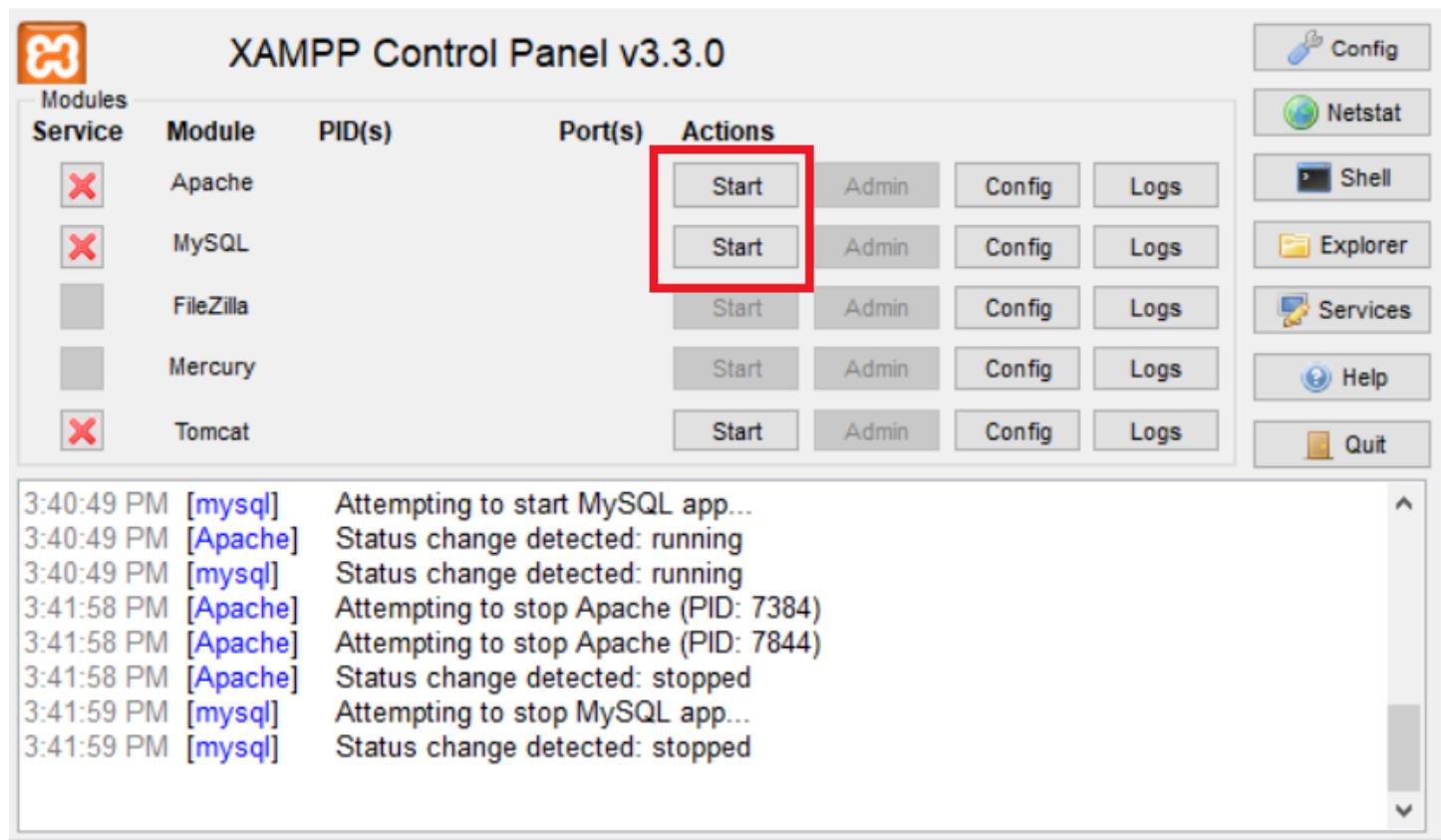
VMware InstallBuilder

< Back

Next >

Cancel

When Installation Complete Successfully Open App You will Show This, Click Start On Apache And MySQL



Configure DVWA Vulnerable Web App

Download [DVWA](#)

After Download It Extract File And Rename It **dvwa** And Copy To This Path ==> **C:\xampp\htdocs**

now you need edit **dvwa** configuration file from this path ==> **C:\xampp\htdocs\dvwa\config**

you can see file name **config.inc.php.dist** rename it **config.inc.php** and open file

Add username and password you will use it to login

```
config.inc.php - Notepad
File Edit Format View Help

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ] = getenv('DB_USER') ?: 'dvwa';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'admin';
$_DVWA[ 'db_port' ] = getenv('DB_PORT') ?: '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ] = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';

# Default security level
# Default value for the security level with each session
<

Unix (LF) Ln 24, Col 21 100%
```

now we will configure Database open <http://127.0.0.1/phpmyadmin/> in your browser to create dvwa Database

The screenshot shows the phpMyAdmin interface with the following details:

- Left Sidebar:** Shows a tree view of databases: New, dvwa, information_schema, mysql, performance_schema, phpmyadmin, and test. The "New" button is highlighted with a red box.
- Top Bar:** Shows "Server: 127.0.0.1" and tabs for Databases, SQL, Status, User accounts, Export, Import, and a gear icon.
- Main Area:** Title "Databases". A modal window titled "Create database" is open, showing a "Database name" input field containing "utf8mb4_general_ci" and a "Create" button, both highlighted with red boxes.
- Table:** Displays a list of databases with their collations and actions:

Database	Collation	Action
dvwa	utf8mb4_general_ci	<input type="button" value="Check privileges"/>
information_schema	utf8_general_ci	<input type="button" value="Check privileges"/>
mysql	utf8mb4_general_ci	<input type="button" value="Check privileges"/>
performance_schema	utf8_general_ci	<input type="button" value="Check privileges"/>
phpmyadmin	utf8_bin	<input type="button" value="Check privileges"/>
test	latin1_swedish_ci	<input type="button" value="Check privileges"/>
- Total:** 6
- Bottom Alert:** A note: "Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server." with a "Enable statistics" button.

Now Open dvwa in your browser <http://127.0.0.1/dvwa/> And scroll Down And click **Create / Reset Database**

Database password: *****
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306

API
This section is only important if you want to use the API module.
Vendor files installed: **Not Installed**

For information on how to install these, see the [README](#).

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

[Create / Reset Database](#)

Now Refresh browser and login via this credential **admin:password**

Congratulations



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with various levels of **difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken

now create a new index in splunk name **webapp** to send logs add this configuration in inputs.conf >> C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local

```
[monitor://C:\xampp\apache\logs\access.log]
sourcetype = apache:access
index = webapp
disabled = false
```

```
[monitor://C:\xampp\apache\logs\error.log]
sourcetype = apache:error
index = webapp
disabled = false
```

install WAF

download mod security WAF from [here](#)

unzip file and copy **mob_security2.so** to >> C:\xampp\apache\modules

create config file name **modsecurity.conf** in >> C:\xampp\apache\conf and add this settings

```
SecAuditLog "C:/xampp/apache/logs/modsec_audit.log"
```

```
SecDebugLog "C:/xampp/apache/logs/modsec_debug.log"
```

```
SecRuleEngine DetectionOnly
```

```
SecRequestBodyAccess On
```

```
SecAuditEngine On
```

```
SecAuditLogParts ABC
```

Note: We will use the WAF here to capture the request body, and we will not rely on the default rules because we want to try writing custom rules by hand and generate alert

now create a new index in splunk name **waf** to send logs to splunk add this configuration in **inputs.conf** >> C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local

[monitor://C:/xampp/apache/logs/modsec_audit.log]

disabled = false

index = waf

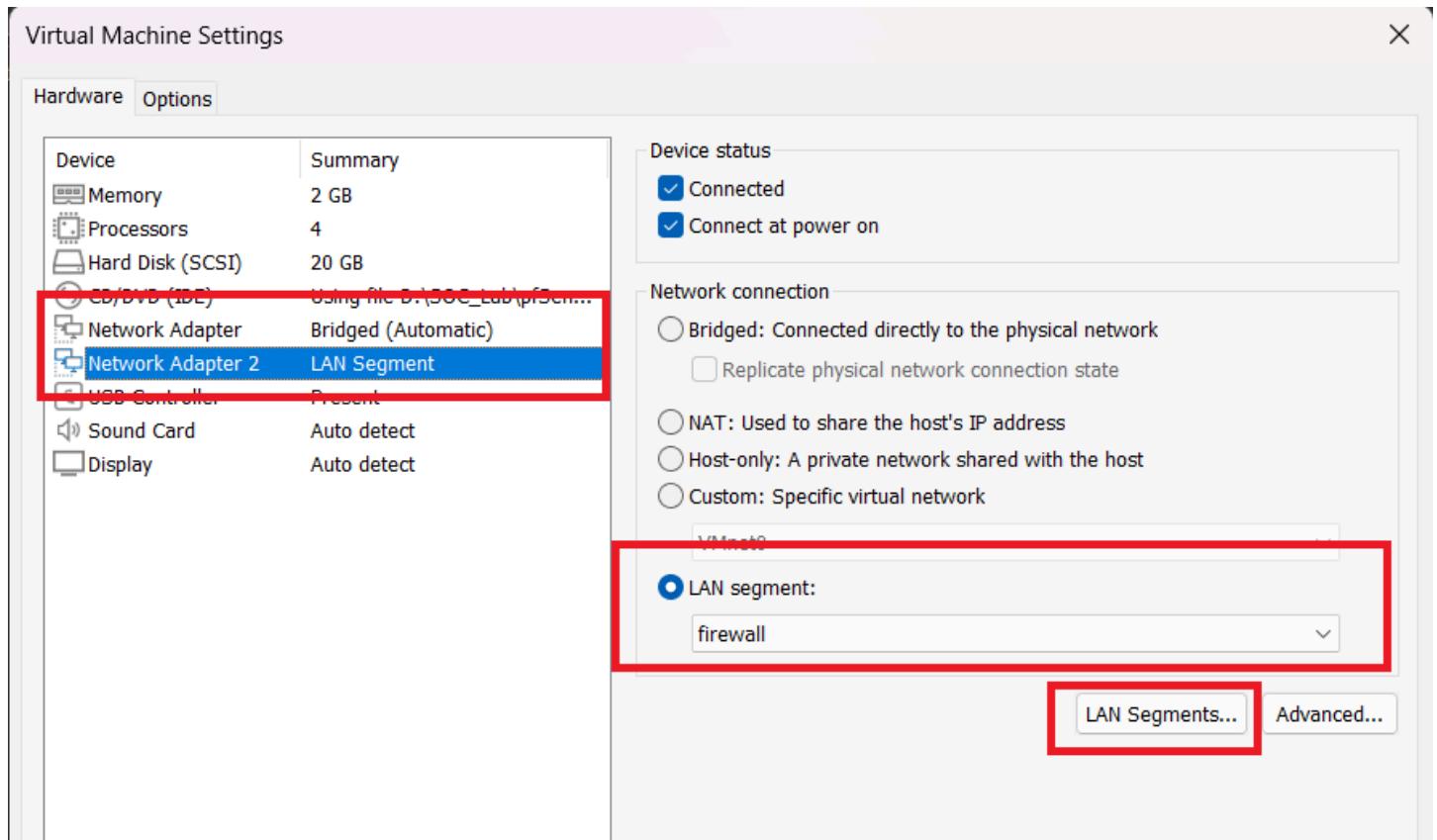
sourcetype = modsecurity:json

Install pfSense FW

download [pfSense](#)

install it in VMware

create a 2 network card (**LAN, Bridge**) Ip some thing like 10.10.10.1/24 WAN 192.168.1.0/24 after installation complete access PfSense from any Machine in NAT card via web browser by pfSense ip 10.10.10.1



The screenshot shows the pfSense Status/Dashboard page. At the top, it displays the pfSense logo and navigation links: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help. Below the header, there are two main sections: 'System Information' and 'Netgate Services And Support'. The 'System Information' section provides details like Name (pfSense.home.arpa), User (admin@10.10.10.15), System (VMware Virtual Machine), BIOS (Phoenix Technologies LTD), and Version (2.7.0 RELEASE). The 'Netgate Services And Support' section shows Contract type (Community Support) and a link to NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES. A note at the bottom explains the benefits of Netgate support.

require check update from Tab >> System >> update

Notes: add all VM machine in LAN Network add static IP Range
192.168.200.0/24 Subnet 255.255.255.0 Default Gateway firewall IP like 192.168.200.1

now send logs to splunk

Not secure 192.168.200.1/status_logs_settings.php

Status / System Logs / Settings

System Firewall DHCP Authentication IPsec PPP PPPoE/L2

General Logging Options

Log Message Format syslog (RFC 5424, with RFC 3339 microsecond-precision timestamp)

The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled).

Forward/Reverse Display Show log entries in reverse order (newest entries on top)

GUI Log Entries 500

This is only the number of log entries displayed in the GUI. It does not affect the number of log entries contained in the actual log files.

Log firewall default blocks Log packets matched from the default block rules in the ruleset

Log packets that are blocked by the implicit default block rule. - Policies still respected.

Log packets matched from the default pass rules put in the ruleset

Log packets that are allowed by the implicit default pass rule. - Policies still respected.

Log packets blocked by 'Block Bogon Networks' rules

Log packets blocked by 'Block Private Networks' rules

Web Server Log Log errors from the web server process

If this is checked, errors from the web server process for the GUI or Captive Portal will appear in the main system log.

scroll down to

The number of log files to keep before the oldest copy is removed on rotation.

Remote Logging Options

Enable Remote Logging Send log messages to remote syslog server

Source Address Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers 192.168.200.10:514

IP[:port] IP[:port]

Remote Syslog Contents

Everything

System Events

Firewall Events

- DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- General Authentication Events
- Captive Portal Events
- VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- Gateway Monitor Events
- Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- Network Time Protocol Events (NTP Daemon, NTP Client)
- Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslog on the remote server to receive these logs.

and click save

now configure receiving in splunk >> settings >> data inputs >> UDP

Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

Local inputs

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	19	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	1	+ Add new

UDP

Data inputs > UDP

Showing 1-1 of 1 item



New Local UDP

UDP port	Source type	Status	Actions
192.168.200.1:514	pfsense	Enabled Disable	Clone Delete

Add Data

Select Source Input Settings Review Done

< Back

Next >

Files & Directories

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

Configure the Splunk platform to listen on a network port.

Scripts

Get data from any API, service, or database with a script.

checkapp

Systemd Journald Input for Splunk

This is the input that gets data from journald (systemd's logging component) into Splunk.

Log Input for the Splunk platform

This input collects data from logd on macOS and sends it to the Splunk platform.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP

UDP

Port ?

514

Example: 514

Source name override ?

optional

host:port

Only accept connection

from ?

optional

example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

FAQ

> How should I configure the Splunk platform for syslog traffic?

and click next

source Type pfsense

Add Data

Select Source Input Settings Review Done

< Back

Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Source Type Select New

Source Type Category Application ▾

Source Type Description

App context

scroll down to

determines the available configuration options. [Learn More](#) ↗

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#) ↗

Index Create a new index

New Index

X

General Settings

Index Name fw-01

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type

Events

Metrics

The type of data to store (event-based or metrics).

Home Path

optional

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index

fw-01 ▾

Create a new index

click Review >> submit

check logs send succefuly

Time	Event
Dec 24 17:28:16 192.168.200.1	Dec 24 17:23:20 filterlog[68461]: 74.,,100000101,em1,match,pass,in,4,0x2,0,128,48087,0,0F,6,tcp,52,192.168.200.150,192.168.1.10,50381,999 5:28:16.000 PM 7,0,SEC,1691047768,,64240,,mss;nop;wscale;nop;nop;sackOK host = 192.168.200.1 : sourcetype = pfSense
Dec 24 17:28:11 192.168.200.1	Dec 24 17:23:15 filterlog[68461]: 74.,,100000101,em1,match,pass,in,4,0x0,,64,12550,0,none,17,udp,80,192.168.200.10,8.8.8.8,53156,53,60 5:28:11.000 PM host = 192.168.200.1 : sourcetype = pfSense
Dec 24 17:28:11 192.168.200.1	Dec 24 17:23:15 filterlog[68461]: 74.,,100000101,em1,match,pass,in,4,0x0,,64,26665,0,none,17,udp,109,192.168.200.10,8.8.8.8,44923,53,89 5:28:11.000 PM

Install Suricata IPS/IDS System

from pfSense web GUI >> System >> Package Manager

Name	Version	Description
suricata	7.0.8_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF. Package Dependencies: suricata-7.0.8

after installation complete go to suricata from >>Services >> Suricata >> Global Settings

to do some configuration

Link in First image >> wget

<http://rules.emergingthreats.net/open/suricata-7.0.3/emerging-all.rules.tar.gz>

The screenshot shows the 'Global Settings' tab selected in the Suricata configuration interface. It displays several sections for rule updates:

- Please Choose The Type Of Rules You Wish To Download:**
 - Install ETOpen Emerging Threats rules:** Includes checkboxes for selecting ETOpen rules and choosing a custom URL.
 - ETOpen Custom Rule Download URL:** A text input field contains the command "wget http://rules.emergingthreats.net/open/suricata-7.0.3/emerging-all.rules".
 - Install ETPro Emerging Threats rules:** Includes checkboxes for selecting ETPro rules and choosing a custom URL.
 - Install Snort rules:** Includes checkboxes for selecting Snort rules and choosing a custom URL.
 - Install Snort GPLv2 Community rules:** Includes checkboxes for selecting Snort GPLv2 rules and choosing a custom URL.
- Install Feodo Tracker Botnet C2 IP rules:** Includes a checkbox for selecting Feodo Tracker rules.
- Install ABUSE.ch SSL Blacklist rules:** Includes a checkbox for selecting ABUSE.ch SSL Blacklist rules.
- Hide Deprecated Rules Categories:** Includes a checkbox for hiding deprecated rules categories.
- Download Extra Rules:** Includes a checkbox for downloading extra rules and a note about MD5 checksums.
- Rules Update Settings:** Includes an 'Update Interval' dropdown set to '1 DAY' and notes about auto-updates.

General Settings

Remove Blocked Hosts Interval	1 HOUR	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	<input type="checkbox"/> Copy Suricata messages to the firewall system log.	
Keep Suricata Settings After Deinstall	<input checked="" type="checkbox"/> Settings will not be removed during package deinstallation.	
Clear Blocked Hosts After Deinstall	<input checked="" type="checkbox"/> Click to clear all blocked hosts added by Suricata when removing the package. Default is checked.	

Click save and go to >> services >> Suricata >> update to apply rule and configuration

Services / Suricata / Updates

Interfaces	Global Settings	Updates	Alerts	Blocks	Files	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 Enabled	Not Enabled
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Unknown
Result: Unknown

Update Force

WARNING: No rule types have been selected for download. Visit the Global Settings Tab to select rule types.

Now go to >> System >> Advanced >> Networking to enable suricate got on Raw Traffic without any edit from firewall

pfSense COMMUNITY EDITION

System / Advanced / Networking

Admin Access	Firewall & NAT	Networking	Miscellaneous	System Tunables	Notifications
--------------	----------------	------------	---------------	-----------------	---------------

IPv6 Options

Allow IPv6 All IPv6 traffic will be blocked by the firewall unless this box is checked
NOTE: This does not disable any IPv6 features on the firewall, it only blocks traffic.

IPv6 over IPv4 Tunneling Enable IPv6 over IPv4 tunneling

scroll down to

Network Interfaces

Hardware Checksum Offloading	<input checked="" type="checkbox"/> Disable hardware checksum offload
Checking this option will disable hardware checksum offloading.	
Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs. This will take effect after a machine reboot or re-configure of each interface.	
Hardware TCP Segmentation Offloading	<input checked="" type="checkbox"/> Disable hardware TCP segmentation offload
Checking this option will disable hardware TCP segmentation offloading (TSO, TS04, TS06). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.	
Hardware Large Receive Offloading	<input checked="" type="checkbox"/> Disable hardware large receive offload
Checking this option will disable hardware large receive offloading (LRO). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.	
hn ALTQ support	<input checked="" type="checkbox"/> Enable the ALTQ support for hn NICs.
Checking this option will enable the ALTQ support for hn NICs. The ALTQ support disables the multiqueue API and may reduce the system capability to handle traffic. This will take effect after a machine reboot.	
ARP Handling	<input type="checkbox"/> Suppress ARP messages
This option will suppress ARP log messages when multiple interfaces reside on the same broadcast domain.	
Reset All States	<input type="checkbox"/> Reset all states if WAN IP Address changes
This option resets all states when a WAN IP Address changes instead of only states associated with the previous IP Address.	

Save

Click save and go to >> Services >> Suricata >> Interfaces

to allow this configuration in specific interface

Services / Suricata

Interfaces	Global Settings	Updates	Alerts	Blocks	Files	Pass Lists	Suppress	Logs View	Logs Mgmt	SID Mgmt
Sync	IP Lists									

Interface Settings Overview

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
					Add

i

Services / Suricata / WAN - Interface Settings

Interfaces	Global Settings	Updates	Alerts	Blocks	Files	Pass Lists	Suppress	Logs View	Logs Mgmt	SID Mgmt
Sync	IP Lists									

WAN Settings

General Settings

Enable	<input checked="" type="checkbox"/> Checking this box enables Suricata inspection on the interface.
Interface	LAN (em1)
Chooses which interface this Suricata instance applies to. If you are only using one interface, you will want to choose LAN here if this is the first Suricata-configured interface.	
Description	LAN
Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.	

scroll down to

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="button" value="FILE"/> Select EVE log output destination. Choosing FILE is suggested and is the default value. "Redis" is used for output to a Redis server, and the UNIX Socket options output to a user-created socket.				
EVE HTTP XFF Support	<input type="checkbox"/> Log X-Forwarded-For IP addresses. Default is Not Checked.				
EVE Ethernet MAC	<input type="checkbox"/> Log Ethernet header in events when available. Default is Not Checked.				
EVE Log Alerts	<input checked="" type="checkbox"/> Suricata will output Alerts via EVE				
EVE Log Alert Payload Data Formats	<input type="button" value="BOTH"/> Log the payload data with alerts. Options are No (disable payload logging), Only Printable (lossy) format, Only Base64 encoded or Both. See Suricata documentation.				
EVE Log Alert details	<input checked="" type="checkbox"/> Log a packet dump with alerts.	<input checked="" type="checkbox"/> Log additional HTTP data.	<input checked="" type="checkbox"/> Include App Layer metadata.	<input type="checkbox"/> Log final action taken on packet by the engine	<input type="checkbox"/> Log packets for rules using the "tag" keyword
EVE Log Drops	<input checked="" type="checkbox"/> Suricata will output Drops via EVE				
EVE Log Drops Options	<input checked="" type="checkbox"/> Log alerts that caused drops. Default is "Checked".		<input type="checkbox"/> Log final action taken on packet by the engine	<input type="button" value="All"/> "Start" logs only a single drop per flow direction. "All" logs each dropped pkt.	
EVE Log Anomalies	<input type="checkbox"/> Suricata will log packet anomalies such as truncated packets, packets with invalid IP/UDP/TCP length values and other events that render the packet invalid for further processing. Networks with high rates of anomalies may experience packet processing degradation.				
EVE Loaded Traffic	<input type="checkbox"/> BitTorrent	<input checked="" type="checkbox"/> DNS	<input checked="" type="checkbox"/> FTP	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> HTTP2
	<input checked="" type="checkbox"/> IKE	<input checked="" type="checkbox"/> Kerberos	<input checked="" type="checkbox"/> NFS	<input type="checkbox"/> PostareSOL	

Click save and go to check logs gerated successfly

Services / Suricata										
Interfaces	Global Settings	Updates	Alerts	Blocks	Files	Pass Lists	Suppress	Logs View	Logs Mgmt	SID Mgmt
<input type="button" value="Sync"/>	<input type="button" value="IP Lists"/>									
Interface Settings Overview										
Interface	Suricata Status	Pattern Match		Blocking Mode	Description		Actions			
<input type="checkbox"/> LAN (em1)	<input type="button" value="X"/> <input type="button" value="Play"/>	AUTO		DISABLED	LAN		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Add"/>	<input type="button" value="Delete"/>
<input type="button" value="i"/>										

go to this url to make suricata generate alert >> <http://testmyids.com>

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt
Sync IP Lists

Logs Browser Selections

Instance to View	(LAN) LAN
Choose which instance logs you want to view.	
Log File to View	alerts.log
Choose which log you want to view..	
Status/Result	File successfully loaded. Log File Path: /var/log/suricata/suricata_em122914/alerts.log
Refresh	

Log Contents

```
:53.634945 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:57335 -> 96.16.249.40:443
:54.717614 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:60248 -> 162.159.61.3:443
:54.717998 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:60248 -> 162.159.61.3:443
:54.735282 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:55206 -> 162.159.61.3:443
:54.735815 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:55206 -> 162.159.61.3:443
:54.735816 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:55206 -> 162.159.61.3:443
:54.781016 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 162.159.61.3:443 -> 10.10.10.15:60248
:54.781915 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:60248 -> 162.159.61.3:443
:54.808614 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 162.159.61.3:443 -> 10.10.10.15:55206
:54.809310 [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 10.10.10.15:55206 -> 162.159.61.3:443
```

now lets go to send logs to splunk

install Syslog-ng From package manger to send logs

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Both [Search](#) [Clear](#)

Enter a search string or *nix regular expression to search package names and descriptions.

Packages			
Name	Version	Description	
syslog-ng	1.16	Syslog-ng syslog server. This service is not intended to replace the default pfSense syslog server but rather acts as an independent syslog server.	+ Install
Package Dependencies:			
syslog-ng-4.4.0 logrotate-3.13.0_1			

go to >> services >> syslog-ng

General Advanced Log Viewer

General Options

Enable Select this option to enable syslog-ng

Interface Selection

LAN
WAN
loopback

Select interfaces you want to listen on

Default Protocol

UDP

Select the default protocol you want to listen on

CA

Select Certificate Authority for TLS protocol.

You can use it in your object definition as ca-dir('/var/etc/syslog-ng/ca.d') option of tls().

General Advanced Log Viewer

Object Type	Object Name	Description
destination	d_splunk_suricata	 
destination	_DEFAULT	 
log	log_suricata_alerts	 
log	_DEFAULT	 
source	s_suricata_alerts	 
source	_DEFAULT	 

 Add

 Save

now we will create three object to send logs to splunk

1- monitor file

object name: s_suricata_alerts

object type: Source

object Parameters:

{

wildcard-file(

base-dir("/var/log/suricata/suricata_em153486")

filename-pattern("*")

```

recursive(yes)
follow-freq(1)
flags(no-parse)
program-override("suricata")
);
};


```

Services: Syslog-NG Advanced / Edit / Advanced

General Advanced Log Viewer

General Options

Object Name: s_suricata_alerts
Enter the object name

Object Type: Source
Select the object type

Object Parameters: {
wildcard-file(
base-dir("/var/log/suricata/suricata_em153486")
filename-pattern("*")
recursive(yes)
Enter the object parameters

Description: Enter the description for this item

Save

and click save

2- create socket

object name: d_splunk_suricata

object type: destination

object Parameters:

```
{
    syslog("splunk-ip" port(5141) transport("udp"));
};
```

[General](#) [Advanced](#) [Log Viewer](#)

General Options

<u>Object Name</u>	<input type="text" value="d_splunk_suricata"/> Enter the object name
<u>Object Type</u>	<input type="text" value="Destination"/> Select the object type
<u>Object Parameters</u>	{ syslog("10.10.10.10" port(5141) transport("udp")); }; Enter the object parameters
<u>Description</u>	<input type="text"/> Enter the description for this item

Save

and click save

3- forward logs

object name: log_suricata_alerts

object type: Logs

object Parameters:

{

source(s_suricata_alerts);

destination(d_splunk_suricata);

};

General Advanced Log Viewer

General Options

Object Name

Enter the object name

Object Type

Log

Select the object type

Object Parameters

```
{
    source(s_suricata_alerts);
    destination(d_splunk_suricata);
};
```

Enter the object parameters

Description

Enter the description for this item

 Save

and click save

General Advanced Log Viewer

Object Type	Object Name	Description
destination	d_splunk_suricata	 
destination	_DEFAULT	 
log	log_suricata_alerts	 
log	_DEFAULT	 
source	s_suricata_alerts	 
source	_DEFAULT	 
 Add		
 Save		

configure splunk forward and make sure port is 5141
source type json and create new index suricata

go to this url to make suricata generate alert >> <http://testmyids.com>

check logs send successfully to splunk

New Search

index="suricata"

539 of 539 events matched No Event Sampling ▾

Time range: All time (real-time) ▾ Save As ▾ Create Table View Close

Events (539) Patterns Statistics Visualization

Timeline format ▾ Zoom Out + Zoom to Selection × Deselect 1 minute per column

Format Show: 50 Per Page ▾ View: List ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

◀ Hide Fields	>All Fields	i Time	Event
SELECTED FIELDS		> 12/25/25 3:28:00.000 PM	Dec 25 15:28:00 10.10.10.1 1 2025-12-25T13:28:00+00:00 pfSense suricata -- [meta sequenceId="1078"] (*timestamp*: "2025-12-25T13:28:00.429133+0000", "flow_id": 223349948775667, "in_iface": "em1", "event_type": "quic", "src_ip": "10.10.10.10", "src_port": 54255, "dest_ip": "34.36.137.203", "dest_port": 443, "proto": "UDP", "pkt_src": "wire/pcap", "quic": {"version": "1"}), host = 10.10.10.1 sourcetype = json
INTERESTING FIELDS		> 12/25/25 3:28:00.000 PM	Dec 25 15:28:00 10.10.10.1 1 2025-12-25T13:28:00+00:00 pfSense suricata -- [meta sequenceId="1077"] (*timestamp*: "2025-12-25T13:28:00.429133+0000", "flow_id": 223349948775667, "in_iface": "em1", "event_type": "alert", "src_ip": "10.10.10.10", "src_port": 54255, "dest_ip": "34.36.137.203", "dest_port": 443, "proto": "UDP", "pkt_src": "wire/pcap", "tx_id": 9, "alert": {"action": "allowed", "gid": 1, "signature_id": 2231000, "rev": 1, "signature": "SURICATA QUIC failed decrypt", "category": "Generic Protocol Command Decode", "severity": 3}, "quic": {"version": "1"}, "app_proto": "quic", "direction": "to_server", "flow": {"pkts_to_server": 6, "pkts_to_client": 6, "bytes_to_server": 3057, "bytes_to_client": 5708}, "start_time": "2025-12-25T13:28:00.314146+0000", "src_ip": "10.10.10.10", "dest_ip": "34.36.137.203", "src_port": 54255, "dest_port": 443), "payload": "7wAAAEI/uW02KrlXmo0TERxQh9TihxsU2VhKfbUhU2sXxVR3VZJNv06phCyyGP8ocsdpBPyUgn/nLViw4YxpUl3PmgslNQRLnj+5ajYqshekQ0k0pLd0LA9xQ2OTVsHfpqrqqPK1uhJ/8QxD@whAEssxtZlhQqg6A0d50u-", "payload_printable": "..."), .Dq88)N(W.M.4r.mA...U..d.o.a./?....A%....h...IR...\\5...x.....JC..K.2...69510Zr...<.n...C...@..1.FH.\n..r.KE", "stream": 0, "packet": "AAwpec0yAAwpLG22CABFACTAAABAEAREksKCGoK1Sj9PvAbsA1+1T7wAAAEl/uW02KrlXmo0TERxQh9TihxsU2VhKfbUhU2sXxVR3VZJNv06phCyyGP8ocsdpBPyUgn/nLViw4YxpUl3PmgslNQRLnj+5ajYqshekQ0k0pLuDiA9xQ2OTVsMFnvronnP1uhJ/80+0/whAFssxt87ThDnn6A0d50u-", "packet_info": {"linktype": "1"}}