



INSTITUTE FOR ADVANCED COMPUTING  
AND  
SOFTWARE DEVELOPMENT  
AKURDI, PUNE

DOCUMENTATION ON

**“Intrusion Detection System with  
OSSEC HIDS and monitoring  
with Splunk”**

PG-DITISS Mar-2023

**SUBMITTED BY:**

**GROUP NO: 24**

**ETI SARASWAT (233449)**

**JUI MULIK (233450)**

**MR. KARTIK AWARI  
PROJECT GUIDE**

**MR. ROHIT PURANIK  
CENTRE COORDINATOR**

## INDEX

Topics	Page No.
List of Abbreviations	
1. Introduction	1
2. Architecture	2
3. Key Features	4
4. Need	5
5. Technology Used	7
6. Key Benefits	8
7. Use Case Diagram	10
8. Configuration	11
9. Description of WUI Components	12
10. Implementation	13
11. Advantages of HIDS	24
12. Future Scope	25
13. Conclusion	26
14. References	27

**LIST OF ABBREVIATIONS**

<b>Sr no.</b>	<b>Abbreviation</b>	<b>Full-Form</b>
1.	OSSEC	Open Source HIDS SECURITY
2.	HIDS	Host BASED INTRUSION DETECTION SYSTEM
3.	SIEM	Security Information and Event Management
4.	SIM	Security Incident Management

# 1. INTRODUCTION

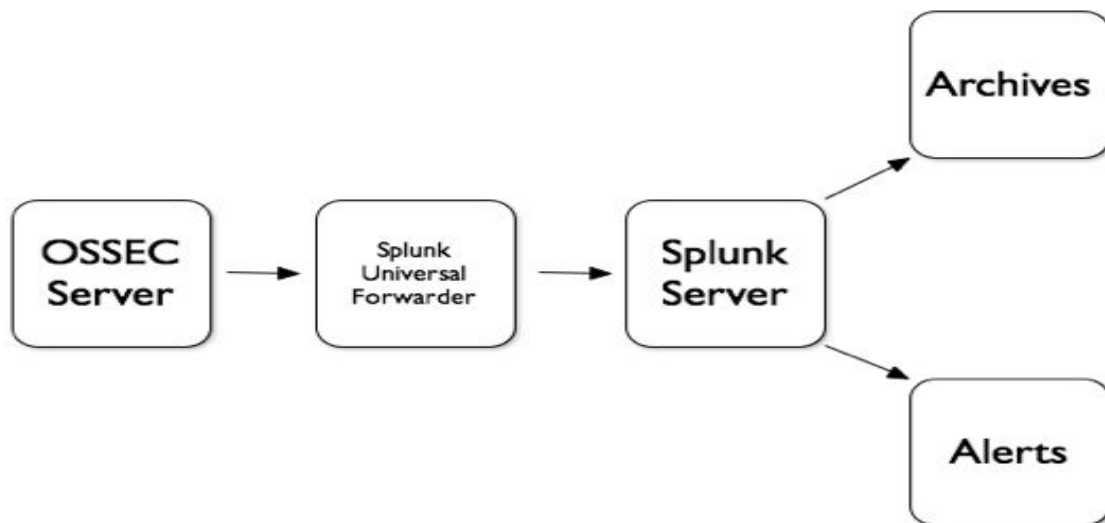
Implemented OSSEC based on server-agent architecture which offers host-based intrusion detection across multiple platforms. Aim of this project is to detect the problem of brute force attacks, unauthorized file modification, rootkit installation with the help of log-based intrusion detection, file integrity monitoring, active response, rootkit detection and to meet specific compliance requirements. It detects and alerts on unauthorized file system modification and malicious behavior that could make you non-compliant. With the help of this we can apply some preventive measures to the systems which will make them more secure.

OSSEC (Open Source HIDS Security) is a monitoring tool used to detect intrusion. It runs on most operating systems including Linux, Windows etc. OSSEC lets customers configure incidents they want to be alerted on, and lets them focus on raising the priority of critical incidents over the regular noise on any system. Active response options to block an attack immediately are also available. OSSEC offers the flexibility of agent based and agentless monitoring of systems and networking components such as routers and firewalls. Communication between agents and the OSSEC server generally occurs on port 1514/udp in secure mode.

Integrating OSSEC server with Splunk provides a powerful and comprehensive approach to security monitoring, threat detection, and incident response, while Splunk provides a centralized platform for collecting, analyzing, and visualizing security-related data.

Combining these two solutions can enhance your organization's security posture and improve your ability to detect and respond to threats effectively.

## 2. Architecture



OSSEC utilizes a client / server architecture. It has a central manager for monitoring and receiving information from agents.

### Manager (or Server)

The manager is the central piece of the OSSEC deployment. It stores the file integrity checking databases, the logs, events, and system auditing entries. All the rules, decoders, and major configuration options are stored centrally in the manager; making it easy to administer even a large number of agents

## **Agents**

The agent is a small program, or collection of programs, installed on the systems to be monitored. The agent will collect information and forward it to the manager for analysis and correlation. Note: The rules only exist on the manager. All analysis is done on the manager. Agents do not send alerts to the manager, they only send the raw logs.

## **Splunk**

Splunk is a powerful and widely used software platform that specializes in collecting, indexing, searching, and analyzing machine-generated data. Splunk is commonly used for log management, security information and event management (SIEM), monitoring, and data analysis across a wide range of industries.

## **Splunk Forwarder**

Splunk Forwarder, often referred to as "Splunk Universal Forwarder," is a lightweight component of the Splunk platform used for data collection and forwarding. It is specifically designed to gather data from various sources, such as log files, metrics, and other machine-generated data, and then send that data to a central Splunk instance (usually a Splunk indexer) for indexing, search, and analysis.

## 3. Key Features

### File Integrity checking

There is one thing in common to any attack to our networks and computers: they change our systems in some way. The goal of file integrity checking (or FIM - file integrity monitoring) is to detect these changes and alert you when they happen. It can be an attack, or a misuse by an employee or even by an admin, any file, directory or registry change will be alerted to us.

### Log Monitoring

Our operating system wants to speak to us, but do we know how to listen? Every operating system, application, and device on our network generate logs (events) to let us know what is happening. OSSEC collects, analyzes and correlates these logs to let us know if something suspicious is happening (attack, misuse, errors, etc). Do we want to know when an application is installed on our ossec agent? Or when someone changes a rule in our firewall? By monitoring our logs, OSSEC will notify us.

### Rootkit detection

Criminal hackers want to hide their actions, but using rootkit detection we can be notified when the system is modified in a way common to rootkits. A rootkit is a program developed to gain covert control over an operating system while hiding from and interacting with the system on which it is installed. An installed rootkit can hide services, processes, ports, files, directories, and registry keys from the rest of the operating system and from the user.

## 4. Need

### 4.1 Why Ossec ?

- Open-Source
- log analysis
- Easy to install
- Easy to customize (rules and config in xml format)
- Scalable (client/server architecture)
- Multi-platform (Windows, Solaris, Linux, \*BSD, etc)
- Secure by default (need to create the certificate / private key for SSL )
- Ossec comes with many decoders/rules which analysis our logs: telnet, Su, Sudo, vsftpd, Postfix, Apache, syslog etc

### Host-Based Intrusion Detection

An HIDS detects events on a server or workstation and can generate alerts. An HIDS is capable of performing additional system level checks that only IDS software installed on a host machine can do, such as file integrity checking, registry monitoring, log analysis, rootkit detection, and active response.



## 4.2 Why Splunk ?

Integrating OSSEC server with Splunk provides a powerful and comprehensive approach to security monitoring, threat detection, and incident response, while Splunk provides a centralized platform for collecting, analyzing, and visualizing security-related data. Combining these two solutions can enhance your organization's security posture and improve your ability to detect and respond to threats effectively.

### **Splunk**

Splunk is a powerful and widely used software platform that specializes in collecting, indexing, searching, and analyzing machine-generated data. Splunk is commonly used for log management, security information and event management (SIEM), monitoring, and data analysis across a wide range of industries.

### **Splunk Forwarder**

Splunk Forwarder, often referred to as "Splunk Universal Forwarder," is a lightweight component of the Splunk platform used for data collection and forwarding. It is specifically designed to gather data from various sources, such as log files, metrics, and other machine-generated data, and then send that data to a central Splunk instance (usually a Splunk indexer) for indexing, search, and analysis.

## 5. Technology Used

### Hardware Requirements:

- RAM: 16 GB
- HDD: 512GB

### Software Requirements:

- Operating System: Linux (Debian 10)
- Tool: VMWare Workstation
- Tool : Splunk
- Tool : Ossec

## **6. Key Benefits**

### **Compliance Requirements**

OSSEC helps customers meet specific compliance requirements such as PCI and HIPAA. It lets customers detect and alert on unauthorized file system modifications and malicious behavior embedded in the log files of commercial products as well as custom applications. For PCI, it covers the sections of file integrity monitoring (PCI 11.5, 10.5), log inspection and monitoring (section 10), and policy enforcement/checking.

### **Multi platform**

OSSEC lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms such as Linux, Solaris, Windows, and Mac OS X.

### **Real-time and Configurable Alerts**

OSSEC lets customers configure incidents they want to be alerted on, and lets them focus on raising the priority of critical incidents over the regular noise on any system. Integration with smtp, sms, and syslog allows customers to be on top of alerts by sending them to e-mail enabled devices. Active response options to block an attack immediately are also available.

### **Integration with current infrastructure**

OSSEC will integrate with current investments from customers such as SIM/SEM (Security Incident Management/Security Events Management) products for centralized reporting and correlation of events.

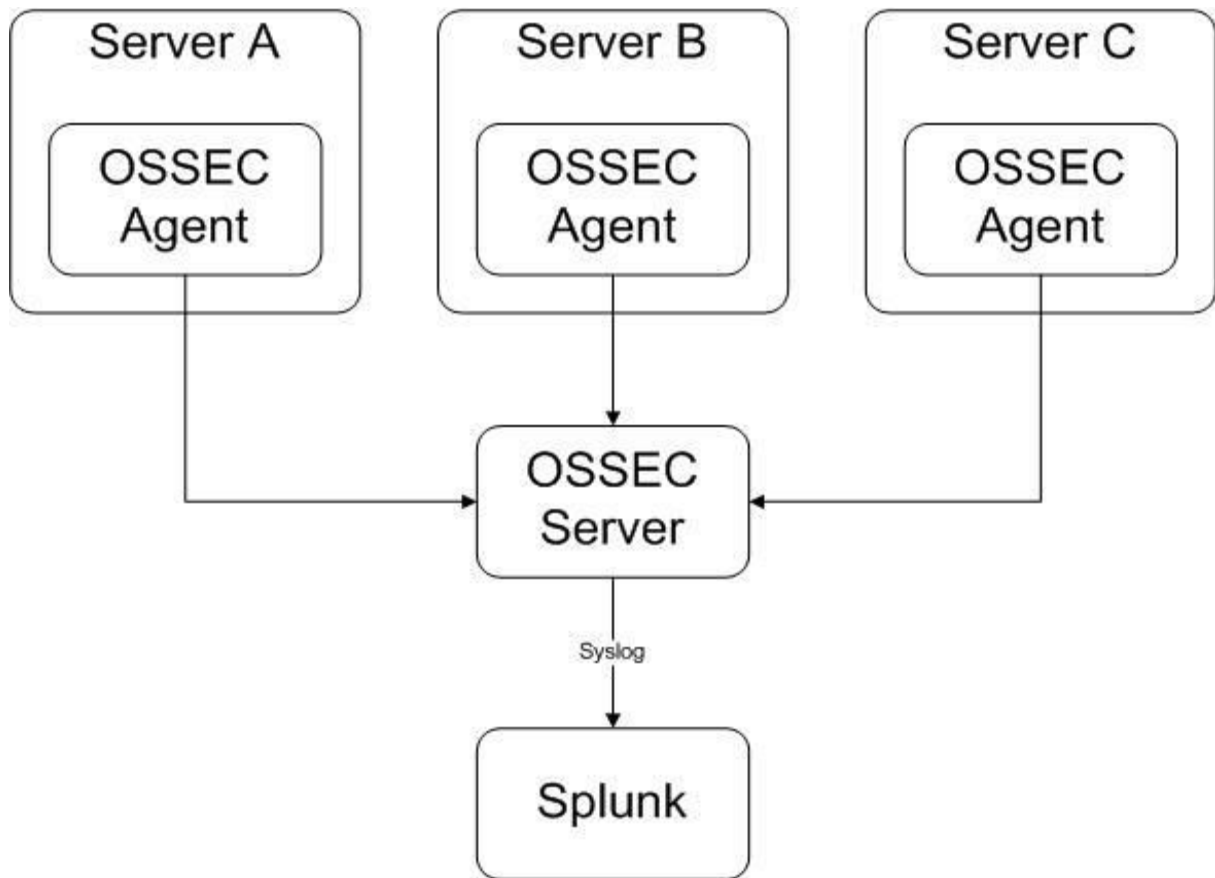
## **Centralized management**

OSSEC provides a simplified centralized management server to manage policies across multiple operating systems. Additionally, it also lets customers define server specific overrides for finer grained policies.

## **Agent and agentless monitoring**

OSSEC offers the flexibility of agent based and agentless monitoring of systems and networking components such as routers and firewalls. Agentless monitoring lets customers who have restrictions on software being installed on systems (such as FDA approved systems or appliances) meet security and compliance needs.

## 7. UML Diagram



### Implementation of OSSEC HIDS and Monitoring with Splunk

## 8. Configuration

### Server Configuration

The Server installation type is recommended if we already have multiple Agent installations deployed throughout our organization and must collect the host-generated alerts. The role of an OSSEC server is to collect all alerts from deployed Agent installations and provide an overall view of what is being reported by all deployed Agent installations. For real time implementation in OSSEC Server we configure Splunk Forwarder to integrate with Splunk.

Splunk Forwarder, often referred to as "Splunk Universal Forwarder," is a lightweight component of the Splunk platform used for data collection and forwarding.

### Agent Configuration

To deploy the OSSEC HIDS on several systems in our organization. This installation type allows us to deploy the security and protection offered by OSSEC on the host of your choosing and centralizes your information by sending alerts back to a single OSSEC server. The Agent installation eliminates the overhead of logging on our deployed agent and ensures that generated alerts are not kept on the system.

### Splunk Configuration

Integrating OSSEC server with Splunk provides a powerful and comprehensive approach to security monitoring, threat detection, and incident response, while Splunk provides a centralized platform for collecting, analyzing, and visualizing security-related data.

## 9. Describing of Ossec WUI Components

The WUI has several tabs, each of which serves a specific purpose.

- **Main** The main dashboard page of the WUI.
- **Search** Allows you to search through collected OSSEC HIDS alerts.
- **Integrity Checking** Allows you to search through collected OSSEC HIDS sys-check alerts.
- **Stats** Displays statistics about the collected OSSEC HIDS alerts.
- **About** Displays license and copyright information about the OSSEC HIDS and the WUI.

Throughout this section, we will discuss each component in detail to provide you with a look into the importance of each tab within the WUI

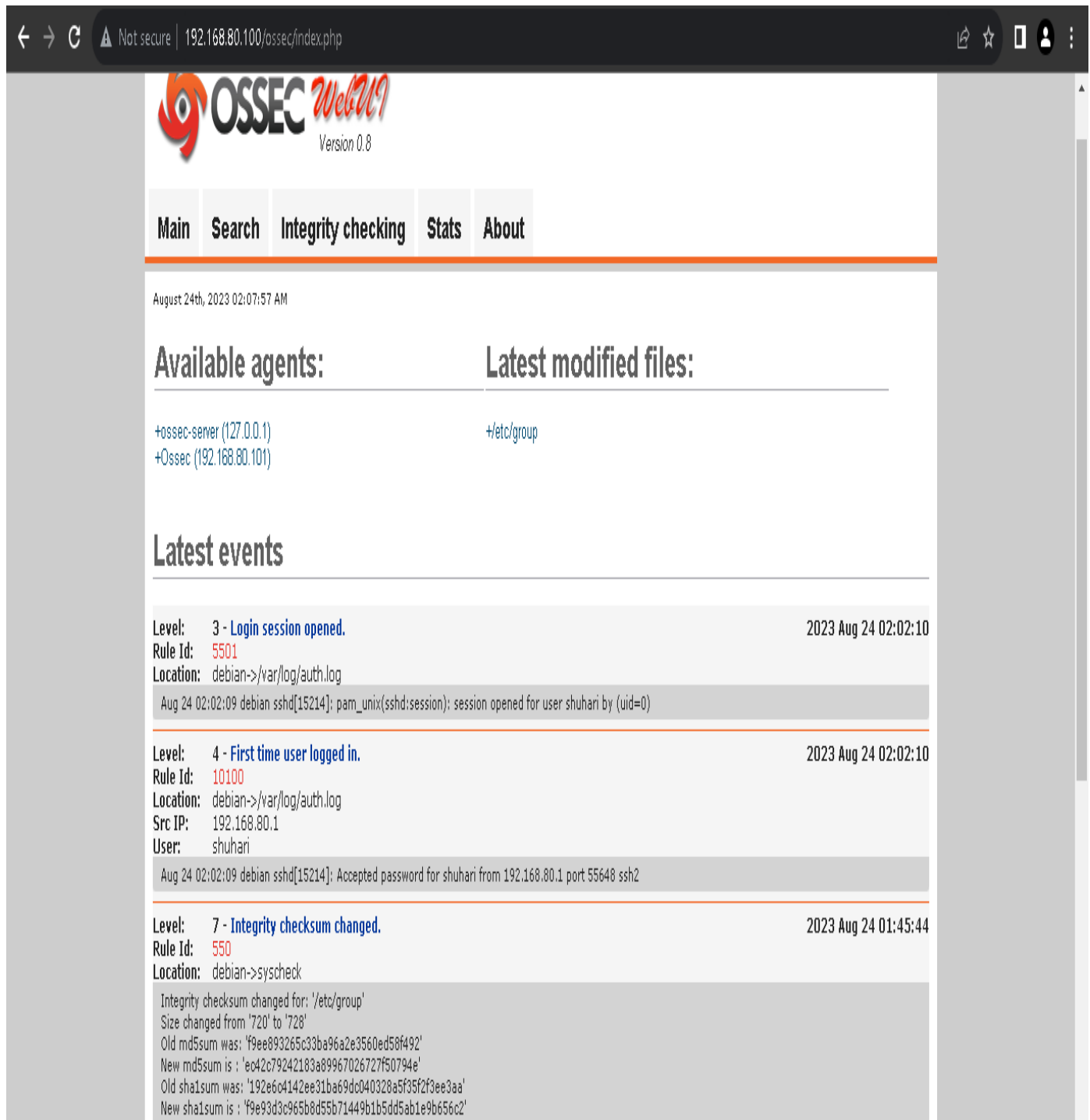
### Main

The Main tab is a dashboard for everything that is being reported to your OSSEC HIDS server. It allows anyone with valid WUI credentials to see what is happening in your OSSEC HIDS deployment. The Main tab details three sections, each with a specific purpose:

- Available agents
- Latest modified files
- Latest events

## 10. Implementation

### 10.1 OSSEC Server-Agent Setup:



The screenshot displays the OSSEC WebUI interface. The browser address bar shows the URL `192.168.80.100/ossec/index.php`. The page header includes the OSSEC logo and version 0.8. The navigation menu has tabs for Main, Search, Integrity checking, Stats, and About. The main content area is divided into three sections: Available agents, Latest modified files, and Latest events.

**Available agents:**

- +ossec-server (127.0.0.1)
- +Ossec (192.168.80.101)

**Latest modified files:**

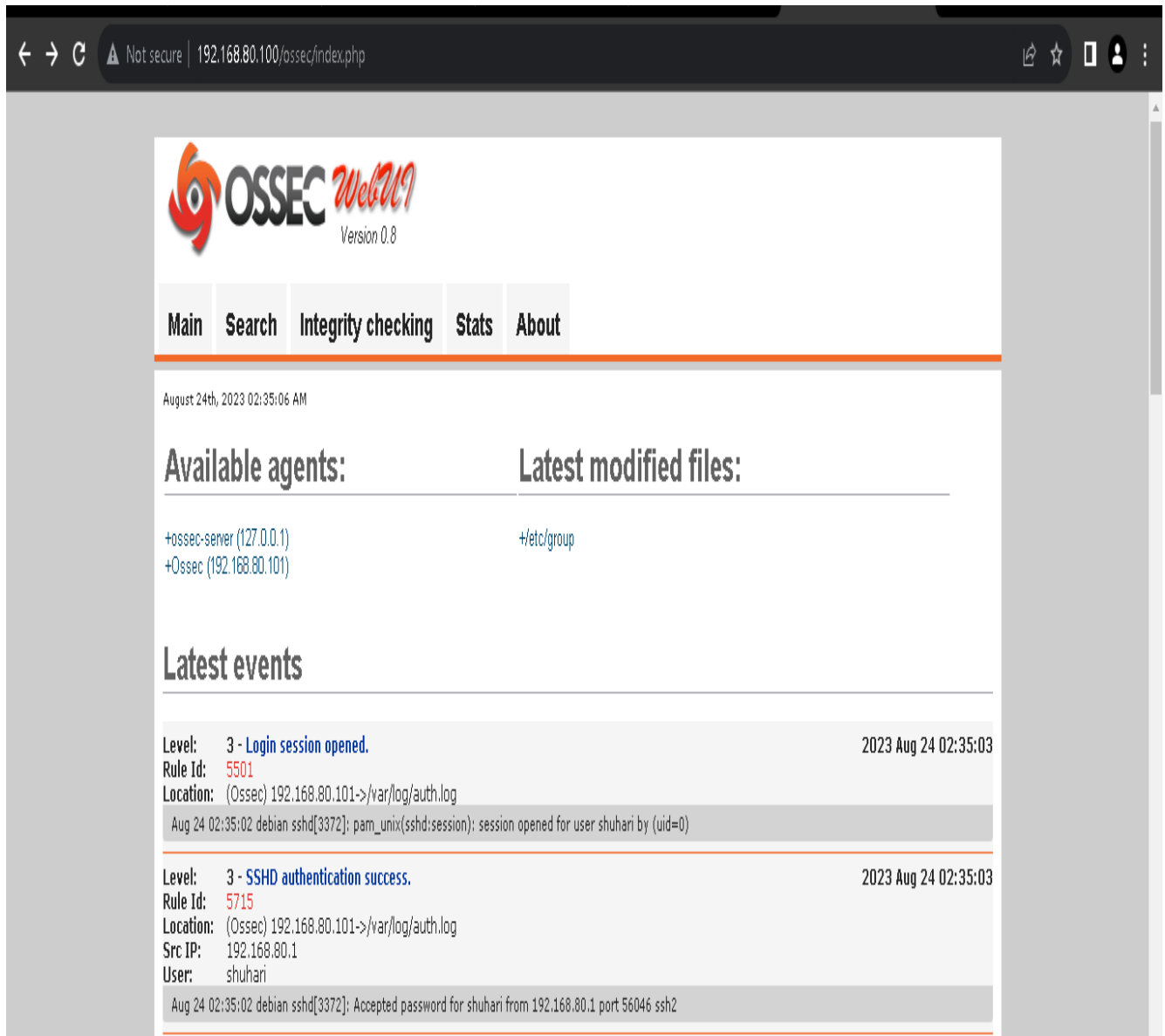
- +etc/group

**Latest events**

Level	Message	Time
3 - Login session opened.	Rule Id: 5501 Location: debian->/var/log/auth.log Aug 24 02:02:09 debian sshd[15214]: pam_unix(sshd:session): session opened for user shuhari by (uid=0)	2023 Aug 24 02:02:10
4 - First time user logged in.	Rule Id: 10100 Location: debian->/var/log/auth.log Src IP: 192.168.80.1 User: shuhari Aug 24 02:02:09 debian sshd[15214]: Accepted password for shuhari from 192.168.80.1 port 55648 ssh2	2023 Aug 24 02:02:10
7 - Integrity checksum changed.	Rule Id: 550 Location: debian->syscheck Integrity checksum changed for: '/etc/group' Size changed from '720' to '728' Old md5sum was: 'f9ee893265c33ba96a2e3560ed58f492' New md5sum is: 'e042c79242183a89967026727f50794e' Old sha1sum was: '192e6c4142ee31ba69dc040328a5f35f2f3ee3aa' New sha1sum is: 'f9e93d3c965b8d55b71449b1b5dd5ab1e9b656c2'	2023 Aug 24 01:45:44



## 10.2 Authentication Logs:



The screenshot displays the OSSEC WebUI interface in a web browser. The browser's address bar shows the URL `192.168.80.100/ossec/index.php` with a "Not secure" warning. The OSSEC logo and "Version 0.8" are visible at the top. A navigation menu includes "Main", "Search", "Integrity checking", "Stats", and "About". The "Main" section shows the current date and time: "August 24th, 2023 02:35:06 AM". Below this, there are two sections: "Available agents:" and "Latest modified files:". The "Available agents:" section lists two agents: "+ossec-server (127.0.0.1)" and "+Ossec (192.168.80.101)". The "Latest modified files:" section lists "+etc/group". The "Latest events" section displays two log entries. The first entry is a "Login session opened" event with Level 3, Rule Id 5501, and Location (Ossec) 192.168.80.101->/var/log/auth.log. The second entry is an "SSH authentication success" event with Level 3, Rule Id 5715, and Location (Ossec) 192.168.80.101->/var/log/auth.log. Both events occurred on August 24, 2023, at 02:35:03.

OSSEC WebUI Version 0.8

Main Search Integrity checking Stats About

August 24th, 2023 02:35:06 AM

Available agents: Latest modified files:

+ossec-server (127.0.0.1)  
+Ossec (192.168.80.101)

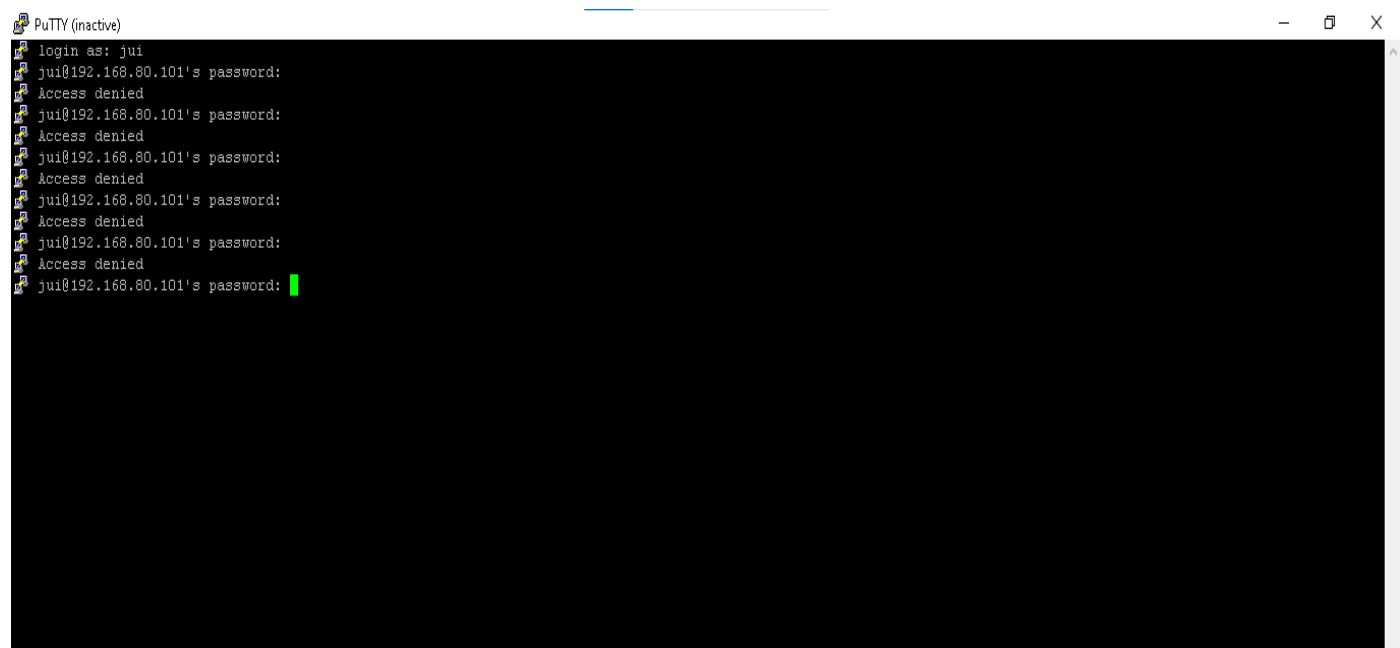
+etc/group

Latest events

Level: 3 - Login session opened. 2023 Aug 24 02:35:03  
Rule Id: 5501  
Location: (Ossec) 192.168.80.101->/var/log/auth.log  
Aug 24 02:35:02 debian sshd[3372]: pam\_unix(sshd:session): session opened for user shuhari by (uid=0)

Level: 3 - SSHD authentication success. 2023 Aug 24 02:35:03  
Rule Id: 5715  
Location: (Ossec) 192.168.80.101->/var/log/auth.log  
Src IP: 192.168.80.1  
User: shuhari  
Aug 24 02:35:02 debian sshd[3372]: Accepted password for shuhari from 192.168.80.1 port 56046 ssh2

10.3 Login Failed Attempts and Ip Blocked:



+ossec-server (127.0.0.1)		+etc/group
+Ossec (192.168.80.101)		
Latest events		
Level:	5 - Attempt to login using a non-existent user	2023 Aug 24 02:30:58
Rule Id:	5710	
Location:	(Ossec) 192.168.80.101->/var/log/auth.log	
Src IP:	192.168.80.1	
Aug 24 02:30:57 debian sshd[3358]: Failed password for invalid user jui from 192.168.80.1 port 55992 ssh2		
Level:	5 - Attempt to login using a non-existent user	2023 Aug 24 02:30:50
Rule Id:	5710	
Location:	(Ossec) 192.168.80.101->/var/log/auth.log	
Src IP:	192.168.80.1	
Aug 24 02:30:49 debian sshd[3358]: Failed password for invalid user jui from 192.168.80.1 port 55992 ssh2		
Level:	5 - Attempt to login using a non-existent user	2023 Aug 24 02:30:44
Rule Id:	5710	
Location:	(Ossec) 192.168.80.101->/var/log/auth.log	
Src IP:	192.168.80.1	
Aug 24 02:30:43 debian sshd[3358]: Failed password for invalid user jui from 192.168.80.1 port 55992 ssh2		
Level:	5 - Attempt to login using a non-existent user	2023 Aug 24 02:30:38
Rule Id:	5710	
Location:	(Ossec) 192.168.80.101->/var/log/auth.log	
Src IP:	192.168.80.1	
Aug 24 02:30:37 debian sshd[3358]: Failed password for invalid user jui from 192.168.80.1 port 55992 ssh2		
Level:	5 - Attempt to login using a non-existent user	2023 Aug 24 02:30:28
Rule Id:	5710	
Location:	(Ossec) 192.168.80.101->/var/log/auth.log	
Src IP:	192.168.80.1	
Aug 24 02:30:26 debian sshd[3358]: Failed password for invalid user jui from 192.168.80.1 port 55992 ssh2		
Level:	5 - User login failed.	2023 Aug 24 02:30:26
Rule Id:	5503	
Location:	(Ossec) 192.168.80.101->/var/log/auth.log	
Aug 24 02:30:24 debian sshd[3358]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.80.1		



## 10.4 File Integrity:

← → ↻

Not secure | 192.168.80.100/ossec/

Main

Search

Integrity checking

Stats

About

August 26th, 2023 02:01:56 AM

Available agents:

Latest modified files:

+ossec-server (127.0.0.1)  
+Ossec (192.168.80.101)

+var/ossec/etc/ossec.conf  
+etc/group

Latest events

Level: 3 - Login session opened.

Rule Id: 5501

Location: (Ossec) 192.168.80.101->/var/log/auth.log

Aug 26 02:01:47 debian login[420]: pam\_unix(login:session): session opened for user shuhari by LOGIN(uid=0)

2023 Aug 26 02:01:48

Level: 5 - User authentication failure.

Rule Id: 2501

Location: (Ossec) 192.168.80.101->/var/log/auth.log

Aug 26 02:01:38 debian login[420]: FAILED LOGIN (1) on '/dev/tty1' FOR 'shuhari', Authentication failure

2023 Aug 26 02:01:38

Level: 5 - User login failed.

Rule Id: 5503

Location: (Ossec) 192.168.80.101->/var/log/auth.log

Aug 26 02:01:35 debian login[420]: pam\_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=shuhari

2023 Aug 26 02:01:36

Level: 7 - Integrity checksum changed.

Rule Id: 550

Location: (Ossec) 192.168.80.101->syscheck

Integrity checksum changed for: '/var/ossec/etc/ossec.conf'  
Size changed from '2944' to '3034'  
Old md5sum was: 'b73e8518c1ed8f6f7802d828bd48146c'  
New md5sum is: '5cfb1850c0c814ec6a1dce15d93a12f3'  
Old sha1sum was: 'dd9694391369da40bc928e362f037cef31ade690'  
New sha1sum is: 'ef60cabe8667724c451bb726e3adf478c3571be0'

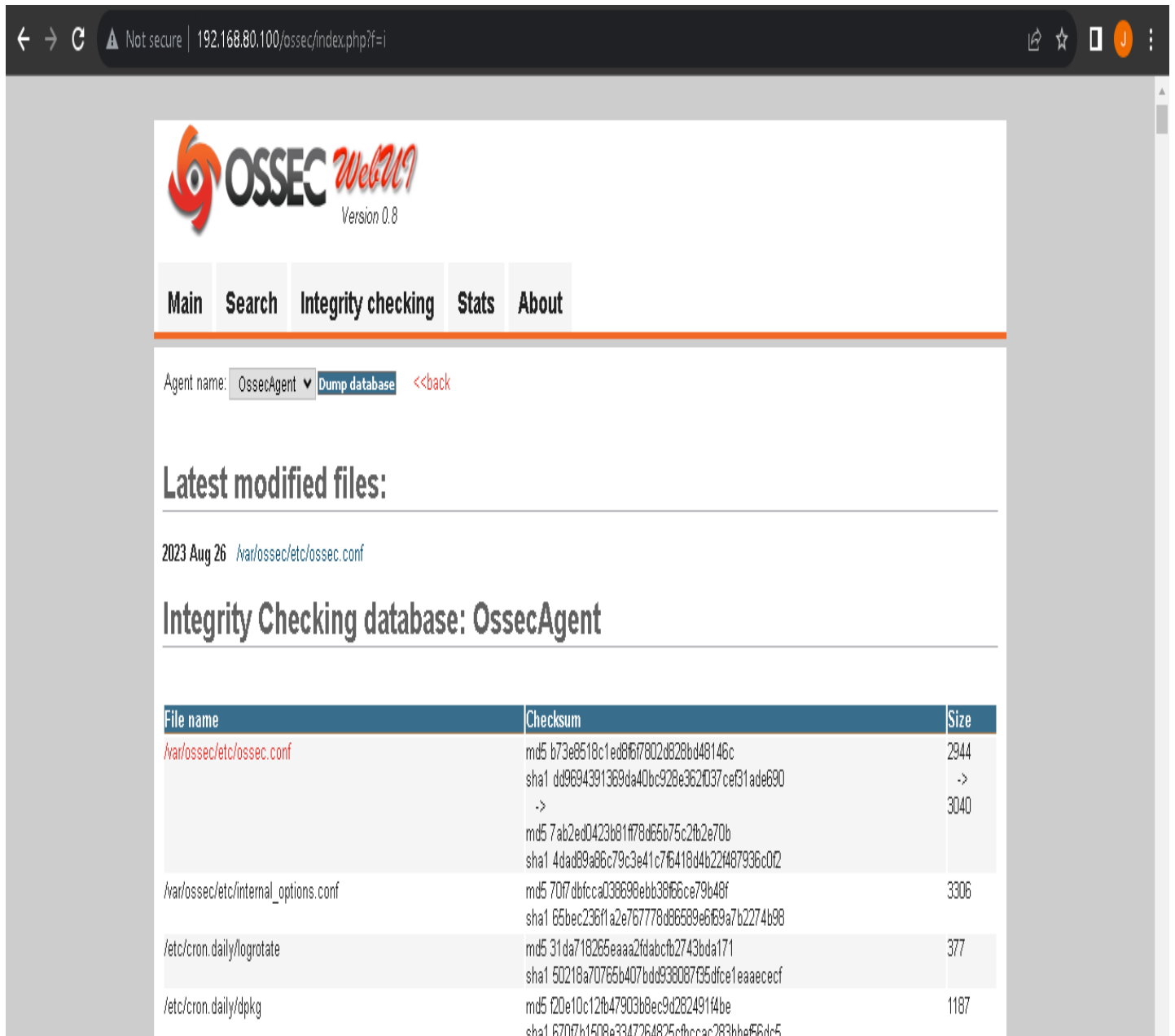
2023 Aug 26 02:01:27

17 | Page

## 10.4.1 File Integrity Testing of /etc/hosts and /etc/timezone

← → ↻ ⚠ Not secure   192.168.80.100/ossec/index.php?f=i			sha1 10eac917ce579c1919670765e2901c1402136b11	
/etc/init.d/apparmor	md5 42e157dc91f6554abefa2160c2bc42db	3740	sha1 078f66498790123b7b088b62596a3f3d7bea9	
/etc/init.d/rsyslog	md5 bd41a0654a192d74dfb9c551b06fa855	2864	sha1 08e34ce46a988013dd451e21178a517388a02101	
/etc/init.d/console-setup.sh	md5 510488b5120b580b673a15b75a5498b0	1232	sha1 0f667545ae788ae46ccc7045dc7975f044a76fd2	
/etc/init.d/sudo	md5 1153f6e6fa7c0e2166779df6ad43f1a8	1030	sha1 102ef71e497f33578e0865b678818ae552f9e1a6	
/etc/init.d/cron	md5 4824366b523de668591f5b6e258c7043	3059	sha1 33c891544bcd7dd27cb83830f512c58d02418f21	
/etc/init.d/apache-htcacheclean	md5 29fe315052a1c5fbc9dc9f29485e9906	2489	sha1 a5e4cc7c41296288d9f940e96652cdeb1e4441f9	
/etc/init.d/ossec	md5 fd0ebdfe02b3d897634c364376a5b0b	962	sha1 12f99eb61110eaf0270444db9f3497c78c6c0b	
/etc/init.d/hwclock.sh	md5 1ca5c0743fa797ffa364db95b6b8d8d8e	3809	sha1 6de496930f0e00e705fa244d77e7dfa2d1c6aefb	
/etc/init.d/kmod	md5 82698019c962069b438bd2a82d9fa1e7	2044	sha1 2ad758cc8614f4c8368e8e7eb71b92f0f2e8305	
/etc/hosts	md5 805a058046564c84c22a075e25856cb	211	sha1 352e3f54c842651ad25796a69b7c91acb54d1837	->
	md5 4215522397ce570216c2a61388e6d1a3	205	sha1 5bec84f4df3566ded38e0a4b8abc1f2578e66c86	->
/etc/timezone	md5 1ca57c569f6244553b280c8f47bbe777	11	sha1 426fb78333a020c0ca8f3cd9ea6ca4993dda00	->
	md5 53e7bc806959748b0d79eb667e7b0851	13	sha1 568cb2a8e8c9e1f668195812eee8c918b8283c6e	->
/etc/crontab	md5 44df62f6c671c9306a620e2839cd4a53	1042	sha1 90db86feb0aa6d41208eab8097929407d79d95cc	
/etc/apparmor.d/tunables/global	md5 30051273dfdb88155135f0890579293a	720	sha1 dec62356c89a192b4db0b6a98f0610d9bfb0644b	
/etc/apparmor.d/tunables/securityfs	md5 45d73edb5f03d141634ec6a5ba2b10f3	405	sha1 97a20f6fa834aac0fe386b7418deede161051cd	
/etc/apparmor.d/tunables/home	md5 ec0b11e815b30dc6fb4d05a41aff9f5	983	sha1 0f4471d5949a9d2bb4f6cfc7899f3f3778b37d7	
/etc/apparmor.d/tunables/xdg-user-dirs	md5 602eaa969d2dfa00a0ec16eed9b60b7f	868	sha1 811400d6868d66be1483c623acac25bca1610907	

## 10.4.2 File Integrity Testing of /var/ossec/etc/ossec.conf file



OSSEC WebUI Version 0.8

Main Search Integrity checking Stats About

Agent name: OssecAgent Dump database <<back

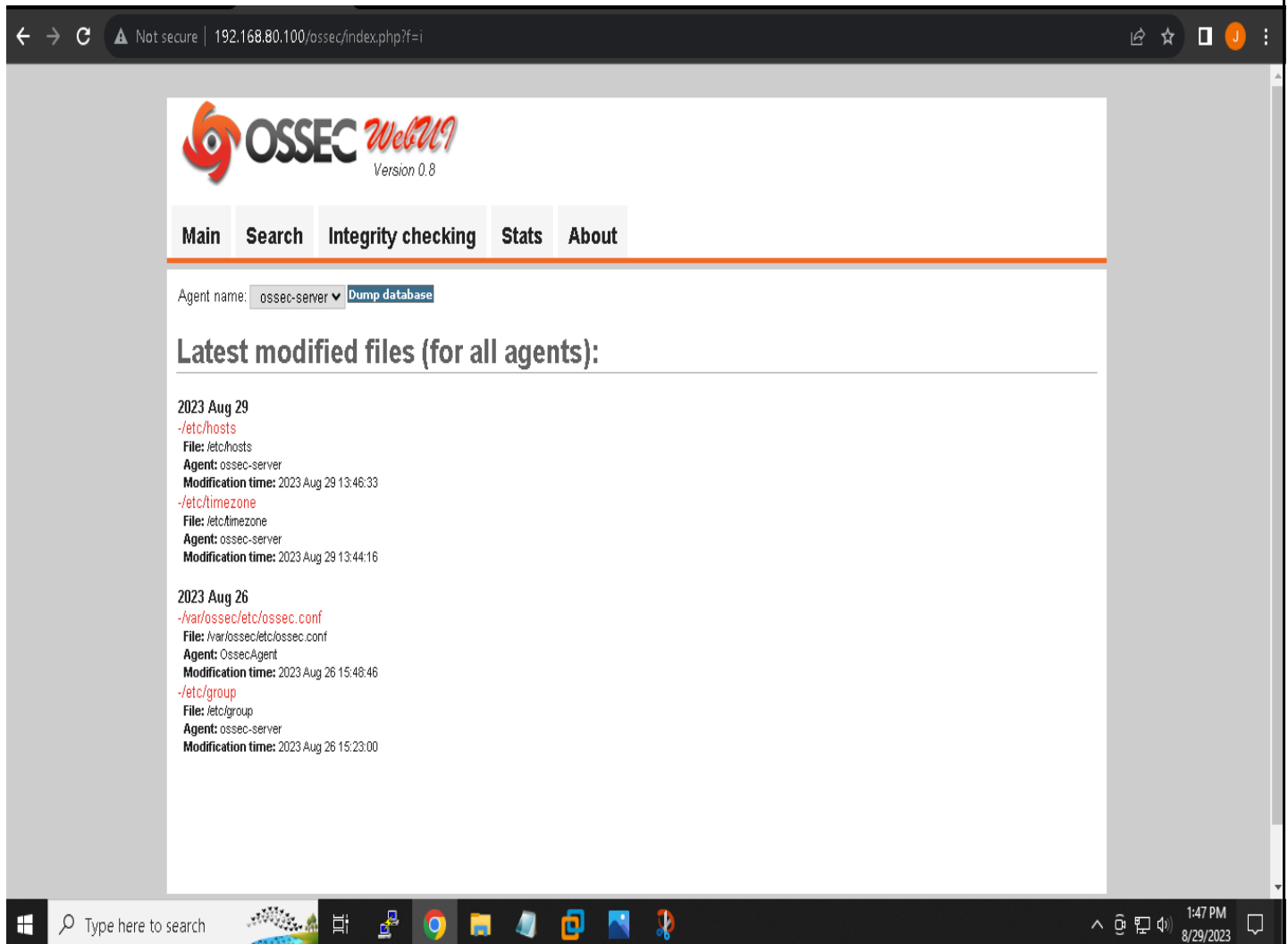
Latest modified files:

2023 Aug 26 [/var/ossec/etc/ossec.conf](#)

Integrity Checking database: OssecAgent

File name	Checksum	Size
<a href="#">/var/ossec/etc/ossec.conf</a>	md5 b73e8518c1ed8f67802d828bd48146c sha1 dd9694391369da40bc928e362f037cef31ade690 -> md5 7ab2ed0423b81f78d65b75c2fb2e70b sha1 4dad89a86c79c3e41c7f6418d4b22f487936c0f2	2944 -> 3040
<a href="#">/var/ossec/etc/internal_options.conf</a>	md5 70f7dbfcca038698ebb38f66ce79b48f sha1 65bec236f1a2e767778d86689e6f69a7b2274b98	3306
<a href="#">/etc/cron.daily/logrotate</a>	md5 31da718265eaaa2fdabcfb2743bda171 sha1 50218a70765b407bdd938087f35dfce1eaaeccef	377
<a href="#">/etc/cron.daily/dpkg</a>	md5 f20e10c12fb47903b8ec9d282491f4be sha1 670f7b1508e3347264825cfbcccac283bbe956dc5	1187

## 10.5 History of file integrity checking



The screenshot shows the OSSEC WebUI interface in a web browser. The browser's address bar displays the URL `192.168.80.100/ossec/index.php?f=i`. The OSSEC logo and "Version 0.8" are visible at the top of the page. A navigation bar contains links for "Main", "Search", "Integrity checking", "Stats", and "About". Below the navigation bar, the "Agent name" is set to "ossec-server", and a "Dump database" button is present. The main section is titled "Latest modified files (for all agents):". It lists two sets of file integrity data:

- 2023 Aug 29**
  - `-/etc/hosts`
    - File: `/etc/hosts`
    - Agent: `ossec-server`
    - Modification time: `2023 Aug 29 13:46:33`
  - `-/etc/timezone`
    - File: `/etc/timezone`
    - Agent: `ossec-server`
    - Modification time: `2023 Aug 29 13:44:16`
- 2023 Aug 26**
  - `-/var/ossec/etc/ossec.conf`
    - File: `/var/ossec/etc/ossec.conf`
    - Agent: `OssecAgent`
    - Modification time: `2023 Aug 26 15:48:46`
  - `-/etc/group`
    - File: `/etc/group`
    - Agent: `ossec-server`
    - Modification time: `2023 Aug 26 15:23:00`

The Windows taskbar at the bottom shows the search bar, task view, and several application icons. The system clock indicates the time is 1:47 PM on 8/29/2023.

## 10.6 Monitoring with Splunk

### 10.6.1 Host Added

The screenshot shows the Splunk Enterprise web interface. A 'Data Summary' modal is open, displaying information for the 'debian' host. The modal has tabs for 'Hosts (1)', 'Sources (4)', and 'Sourcetypes (4)'. The 'Hosts' tab is selected, showing a table with the following data:

Host	Count	Last Update
debian	1,650	8/29/23 10:36:00 PM

The background interface shows the 'Search' sidebar with a search bar and 'Search History'. The main content area has a 'How to Search' section and an 'Analyze Your Data with Table Views' section.

### 10.6.2 Analyze Logs

The screenshot shows the Splunk Enterprise web interface with a search for 'host=debian'. The search results show 145 events. The 'Events' tab is selected, displaying a list of events. The first event is highlighted, showing the following details:

Time	Event
8/29/23 10:09:32.000 AM	Aug 29 00:39:32 debian sudo: pam_unix(sudo:session): session opened for user root by shuhari(uid=0) host = debian   source = /var/log/authlog   sourcetype = auth-too_small
8/29/23 10:09:32.000 AM	Aug 29 00:39:32 debian sudo: shuhari : TTY=pts/0 ; PWD=/opt/splunkforwarder/bin ; USER=root ; COMMAND=./splunk restart host = debian   source = /var/log/authlog   sourcetype = auth-too_small
8/29/23 10:09:07.000 AM	Aug 29 00:39:07 debian systemd[1]: Started Clean php session files. host = debian   source = /var/log/syslog   sourcetype = syslog
8/29/23 10:09:07.000 AM	Aug 29 00:39:07 debian systemd[1]: phpsessionclean.service: Succeeded.

The interface also shows a 'New Search' bar with the query 'host=debian' and a 'Visualize' button. The 'Events' tab is selected, and the 'List' view is active, showing a table of events with columns for 'Time' and 'Event'.



10.6.3 Source and source type

←

→

↺

Not secure | 192.168.80.110:8000/en-US/app/search/search

☆

splunkenterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Search & Reporting

Search

enter search here...

No Event Sampling

Search History

How to Search

If you are not familiar with the search features, see one of the following resources.

Documentation

Tutorial

Data Summary

Data Summary

Hosts (1)Sources (4)Source types (4)

filter

Source		Count	Last Update
/var/log/apt/history.log.gz		10	8/29/23 9:45:26.000 AM
/var/log/apt/term.log.gz		11	8/29/23 9:45:26.000 AM
/var/log/auth.log		62	8/29/23 1:09:02.000 PM
/var/log/syslog		1,567	8/29/23 1:09:36.000 PM

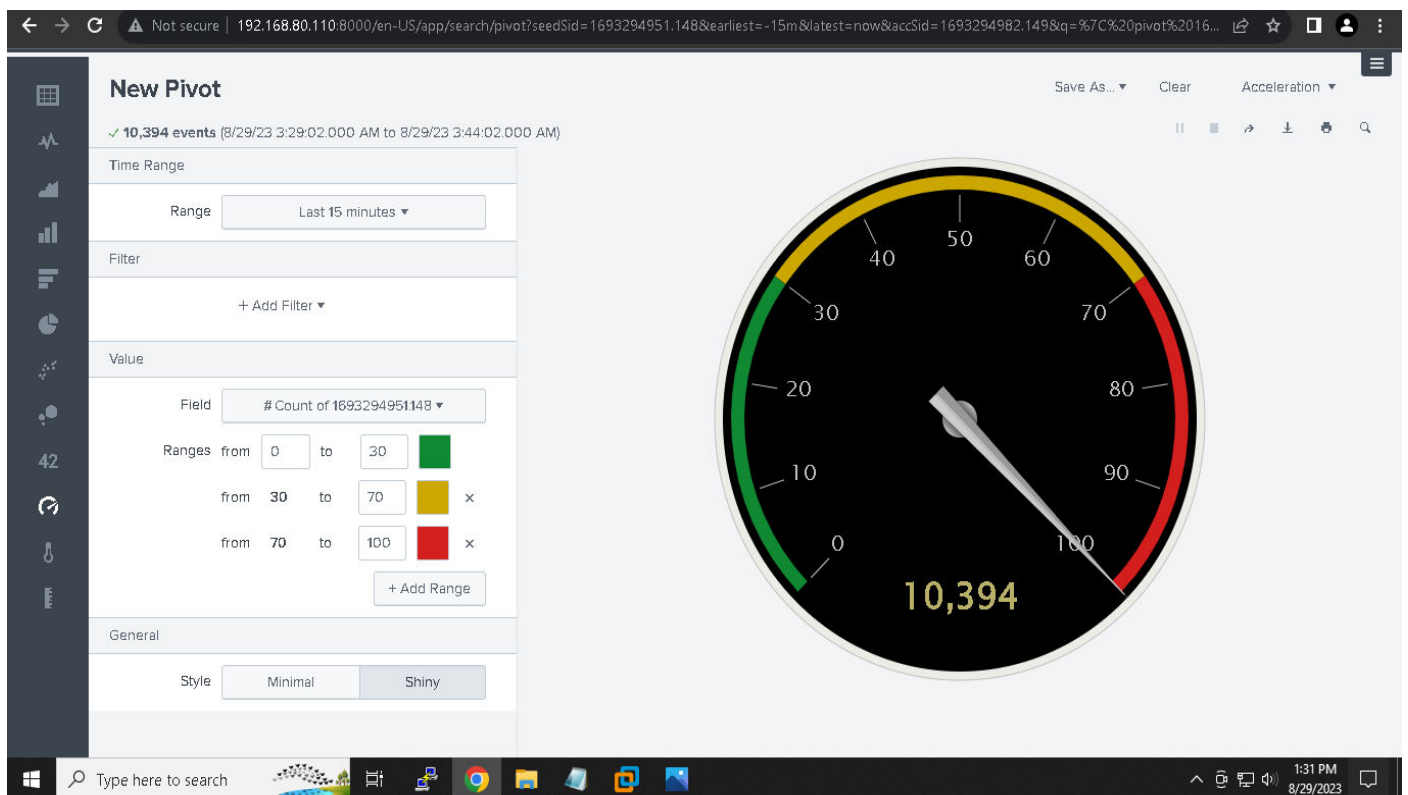
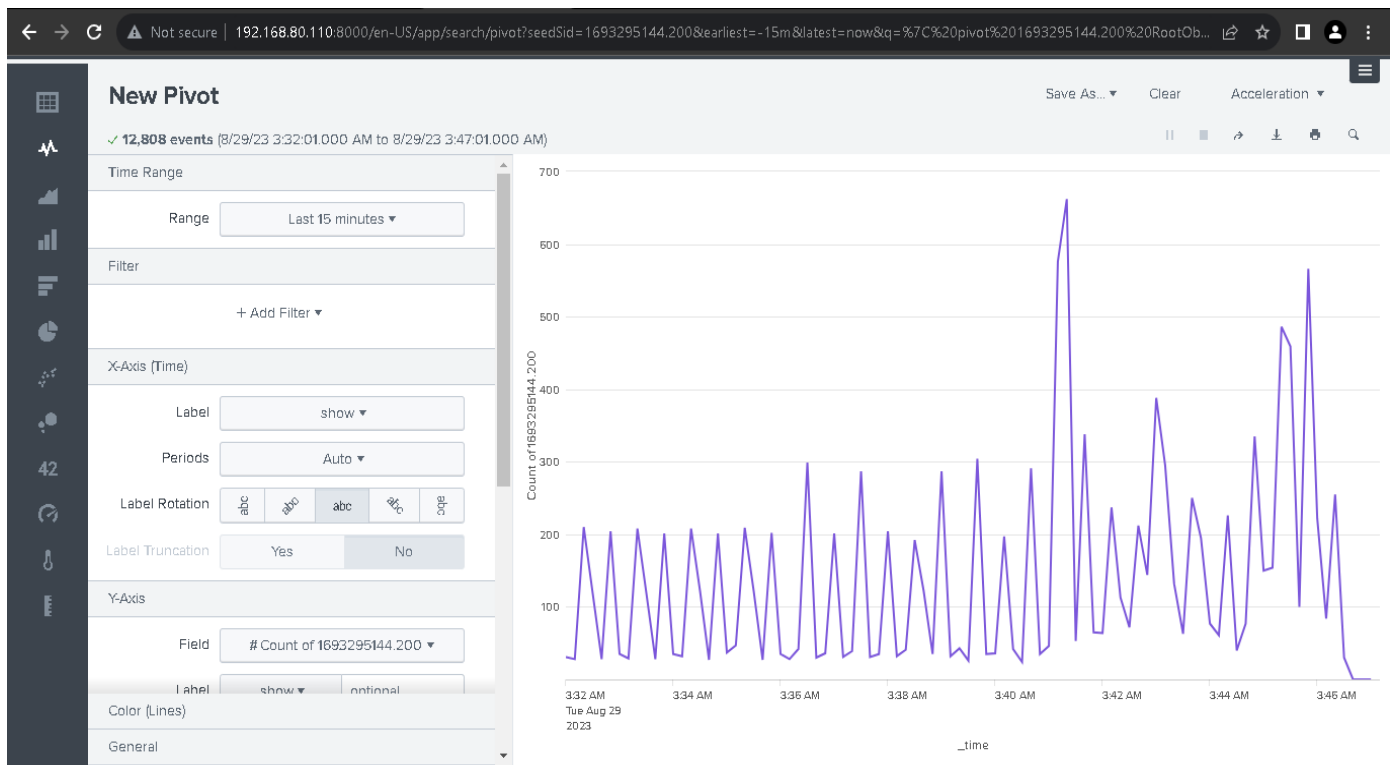
Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Last 24 hours

Smart Mode

Create Table View

## 10.6.4 Graphical Representation



## 11. HIDS Advantages

The advantage of implementing a HIDS is the ability to detect an attack to a system within our perimeter. A HIDS gives security operators the ability to spot and stop an attack on any host early, which can potentially save lots of effort down the road on cleanup and damage recovery. A HIDS also has the capability to detect attacks outside your network perimeter. HIDS installed on corporate laptops can protect those systems while they are on the road at customer locations. If someone attempts to compromise the machine external to our network, a HIDS will be able to notify us before internal resources damage occurs. Because a HIDS has the capability to see what is happening on the host operating system, it can be used to detect breaches in software policy. If a HIDS sees installed software that is not part of the corporate standard, it can notify an administrator. This notification can prevent users from installing unlicensed software, and stop developers from installing tools in production servers that could weaken the security posture of the host. A HIDS agent has the capability to monitor all network traffic destined for it on all interfaces on the system. For example, most laptops now include a NIC card, wireless card, and a modem. A HIDS agent has the capability to protect your laptop from network traffic that may try to compromise your system through a wireless card. To optimize the benefit of a HIDS, a central server is deployed for reporting. The central server acts as the eyes and ears for security officers when it comes to internal hosts on the network. Having multiple IDS sensors in an environment will give greater insight on systems that do not have IDS installed. The more systems with a HIDS installed increases the resolution of the overall security picture.

## 12. Future Scope

A HIDS is definitely beneficial in detecting rootkits, but newer developments in this area are becoming slightly more attractive. Host-based intrusion prevention (HIPS) technology is becoming more commonplace because it has the capability to prevent an attack from happening versus detecting the event with a HIDS and having a minimal amount of time to respond. If a HIPS is more attractive, but not in the budget, remember there are open source HIDS options you can use. Prevention is ideal, but detection is a must. By encapsulating OSSEC's expertise in host-based monitoring and Splunk's prowess in data analysis, the integration culminates in a fortified security monitoring framework. This framework not only bolsters incident detection and response but also streamlines the forensic analysis of security incidents, enabling organizations to navigate the complex threat landscape with confidence and agility.

## 13. Conclusion

The OSSEC Web User Interface (WUI) was created to provide a visual representation of our collected OSSEC HIDS alerts in an easy-to-use Web page. From the WUI, an analyst can view all alerts and individual events related to an incident, review data to see if there are any similarities from previous incidents, and present management with recommendations on how to address the incident and prevent it from happening again in the future. The WUI allows us to look into all aspects of the OSSEC HIDS. The Main page, which acts as a dashboard for your entire deployment, provides a listing of the latest modified files, latest events, and the current status of all OSSEC HIDS agents in our deployment. The integration of Splunk with the OSSEC server proves to be a robust and synergistic approach to security monitoring and threat detection. By combining OSSEC's host-based intrusion detection capabilities with Splunk's powerful data analysis and visualization tools, organizations can elevate their security posture to new heights. Through this integration, security teams gain centralized visibility into their environment's security events, enabling them to swiftly identify anomalies, detect potential threats, and respond proactively. The seamless forwarding of OSSEC logs and alerts to Splunk ensures that no critical information is overlooked, providing a comprehensive overview of the security landscape.

## 14. References

### Links

<https://computingforgeeks.com/how-to-install-ossec-hids-on-ubuntu-debian/>

<https://youtu.be/c1t1QFTIGBg?si=F4D5NTTLexWUONJr>

<https://theseccmaster.com/step-by-step-procedure-to-install-splunk-on-linux-server/>