INSTITUTE FOR ADVANCED COMPUTING AND

SOFTWARE DEVELOPMENT AKURDI, PUNE

DOCUMENTATION ON

## “Implementation of HIDS Using OSSEC ”

PG-DITISS March-2023

*SUBMITTED BY:*

**GROUP NO: 12**

**NEHA KULKARNI (233422)**

**PRATIKSHA GIRNALE (233434)**

**MR. KARTIK AWARI MR. ROHIT PURANIK**

**PROJECT GUIDE CENTRE CO-ORDINATOR**

**INDEX**

|  |  |  |
| --- | --- | --- |
| **Chapter No.** | **Title of the chapter** | **Page No.** |
| Chapter I | Introduction. | 1 |
| Chapter II | Architecture | 2-3 |
| Chapter III | Key Features | 4 |
| Chapter IV | Why OSSEC? | 5 |
| Chapter V | Technology Used | 6 |
| Chapter VI | Key Benefits | 7 |
| Chapter VII | Use Case Diagram | 9 |
| Chapter VIII | Installation   * 1. OSSEC-Server   2. OSSEC-agent | 10 |
| Chapter IX | Description of WUI Components | 11 |
| Chapter X | Implementation Screenshots   * 1. OSSEC-server-agent setup   2. Authentication logs      1. Fail login 10.2.2. IP blocked   3. File integrity checking      1. /etc/timezone file   4. Rootkit Installed      1. Rootkit detection alert generated | 12-19 |
| Chapter XI | Advantages of HIDS | 20 |
| Chapter XII | Future Development | 21 |
| Chapter XIII | Conclusion | 22 |
| Chapter XIV | References | 23 |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Sr no.** | **Abbreviation** | **Full-Form** |
| 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 |

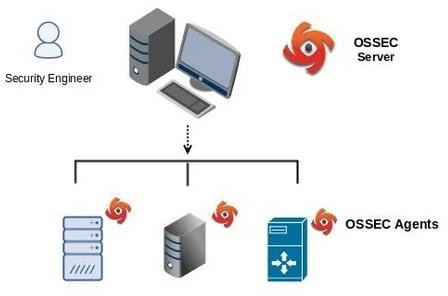
# Introduction

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.

1. | P a g e

# 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.

2 | P a g e

## 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.

# 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.

# 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.

# TECHNOLOGY USED

## Hardware Requirements:

* RAM: 16 GB
* HDD: 512GB

## Software Requirements:

* Operating System: Linux (Debian)
* Tool: VMWare

# 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.

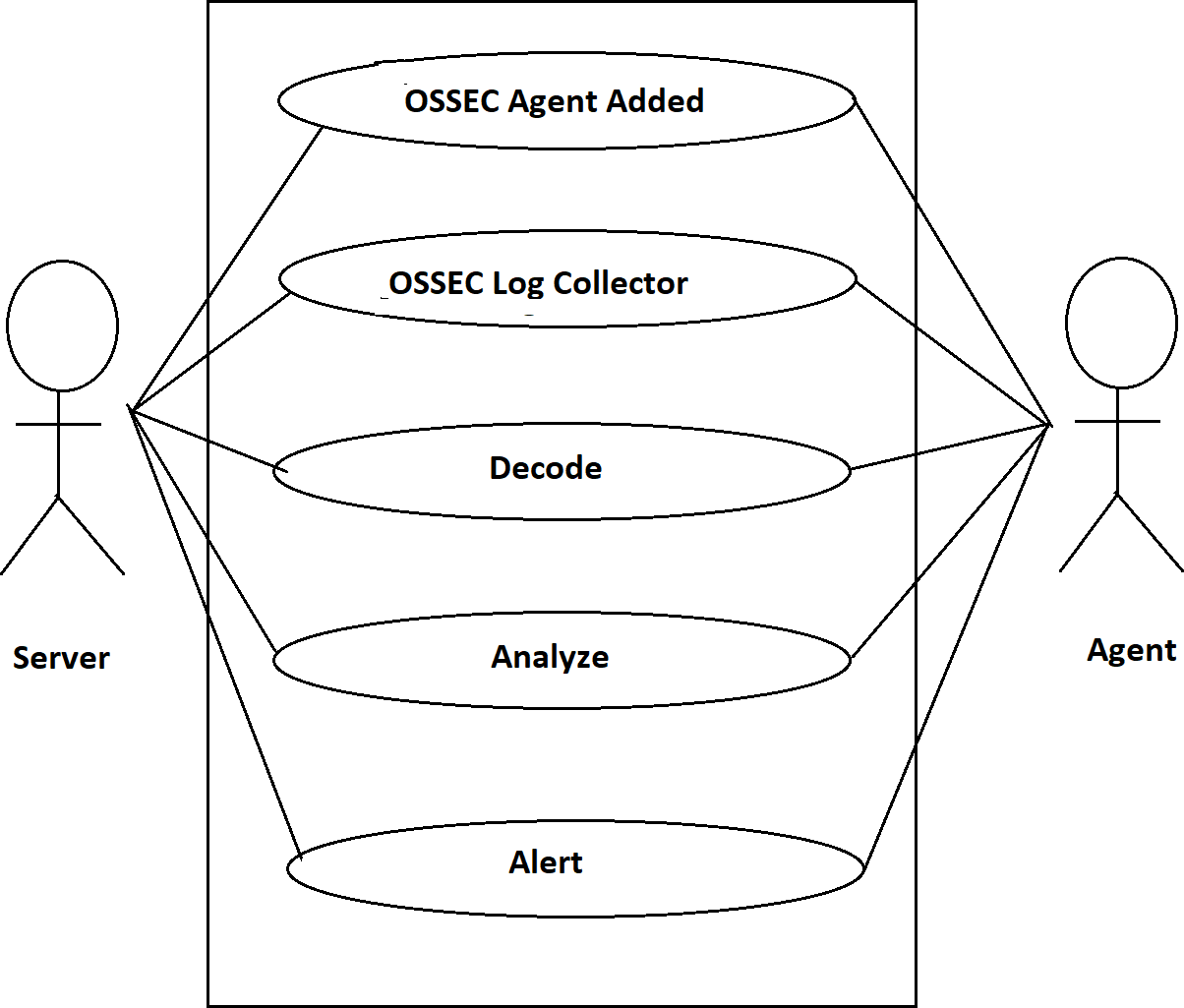
## Centralized management

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.

# UML DIAGRAM



**Implementation of HIDS**

# INSTALLATION

## Server Installation

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.

## Agent Installation

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.

# DESCRIBING THE 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

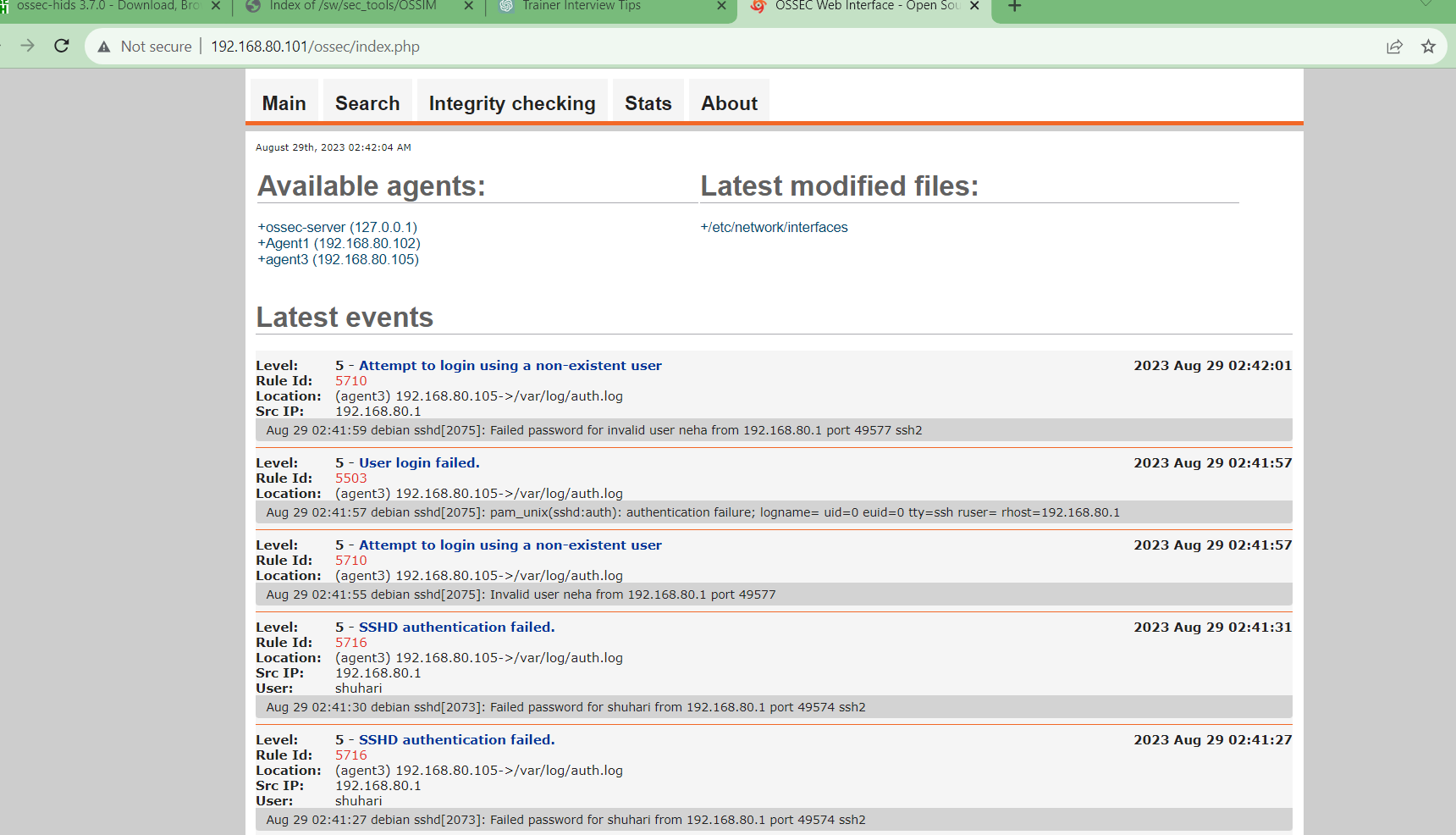
## Main

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:

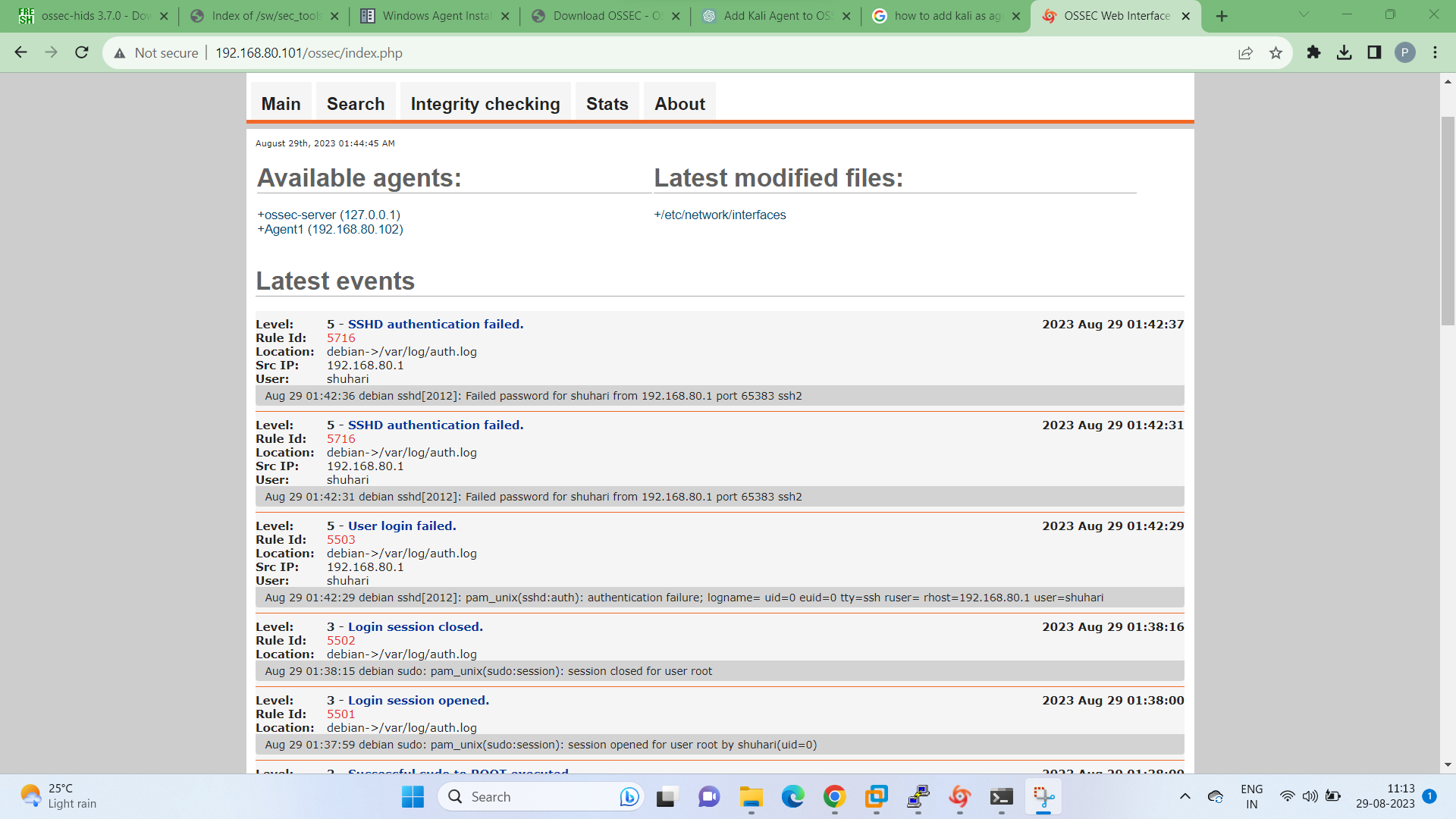
* Available agents
* Latest modified files
* Latest events

# 10.IMPLEMENTATION SCREENSHOTS

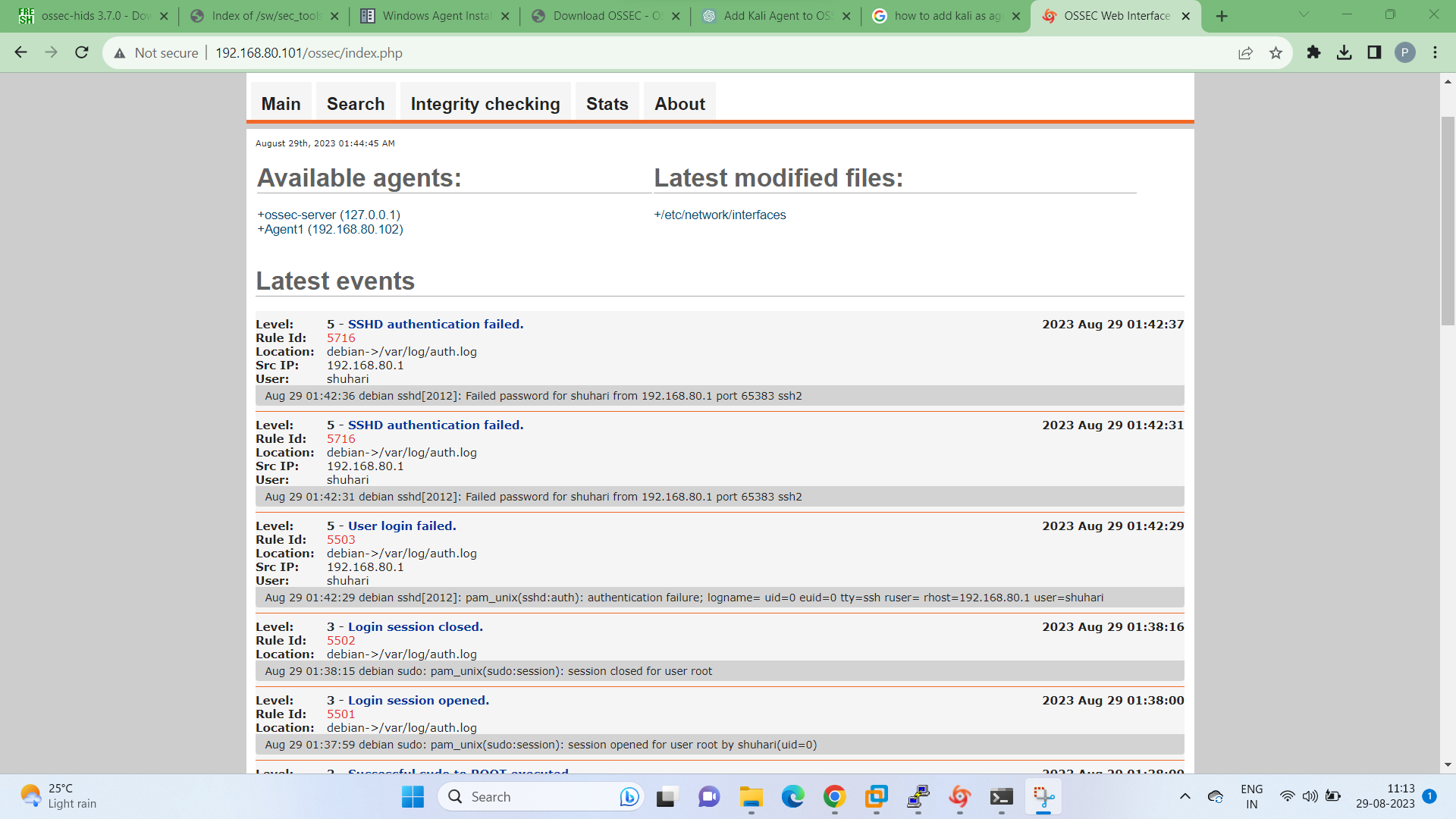
## OSSEC Server-Agent Setup:



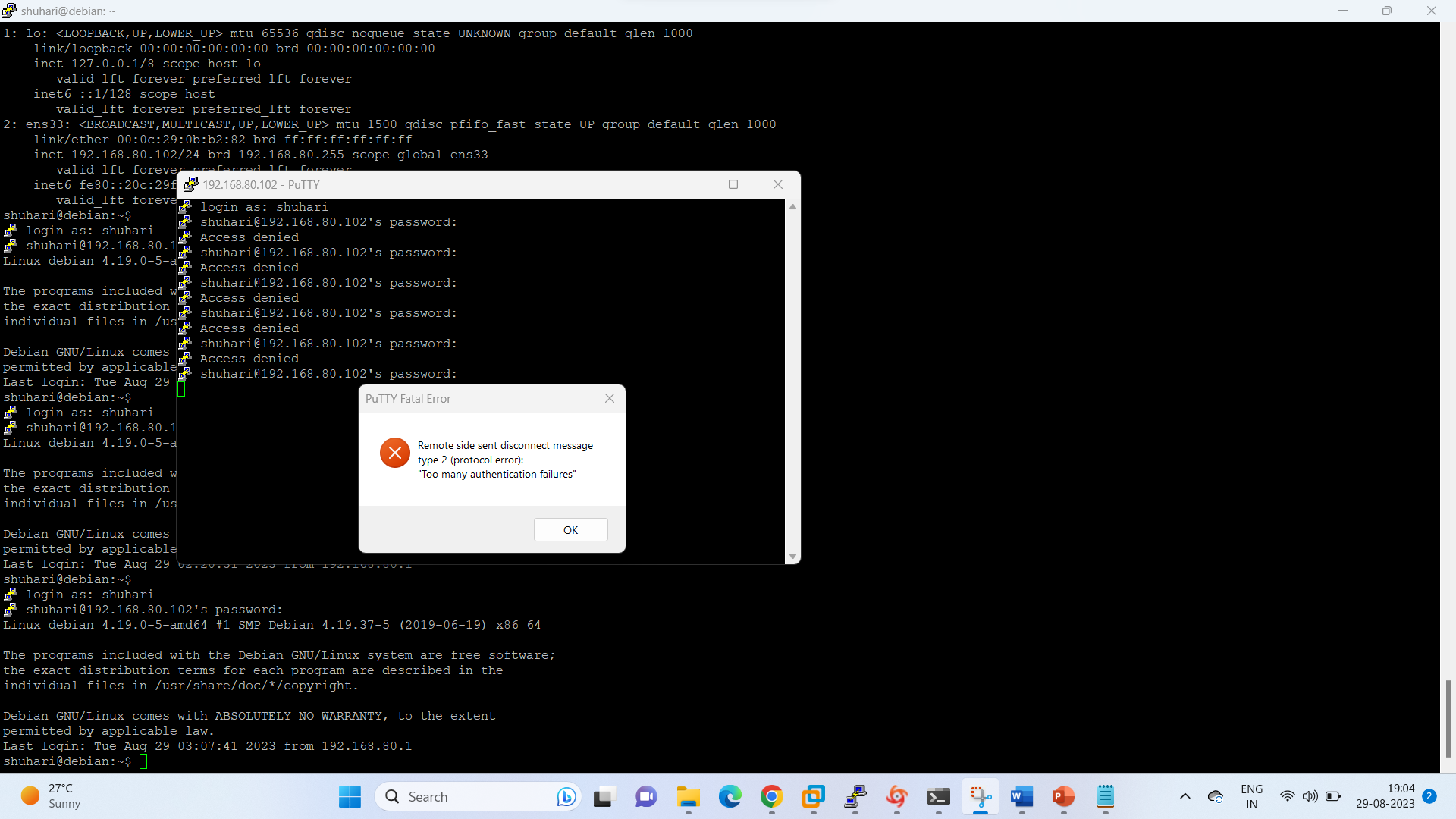
* 1. **Authentication Logs:**



* + 1. **Login Failed Attempts:**

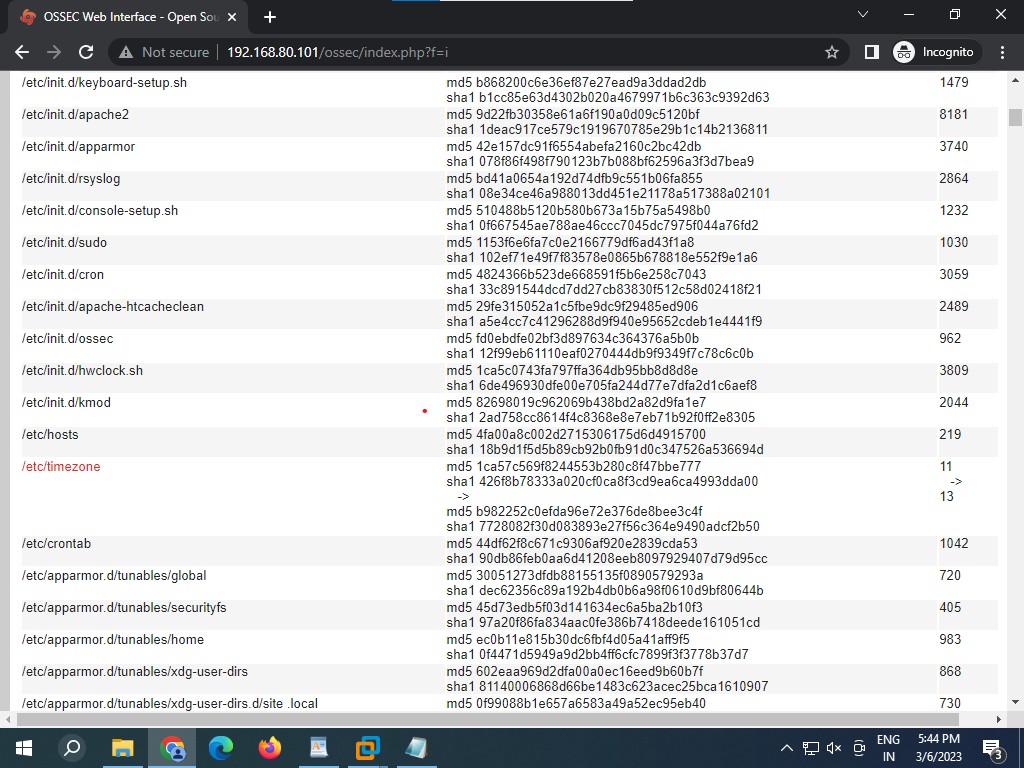


* + 1. **IP Blocked:**

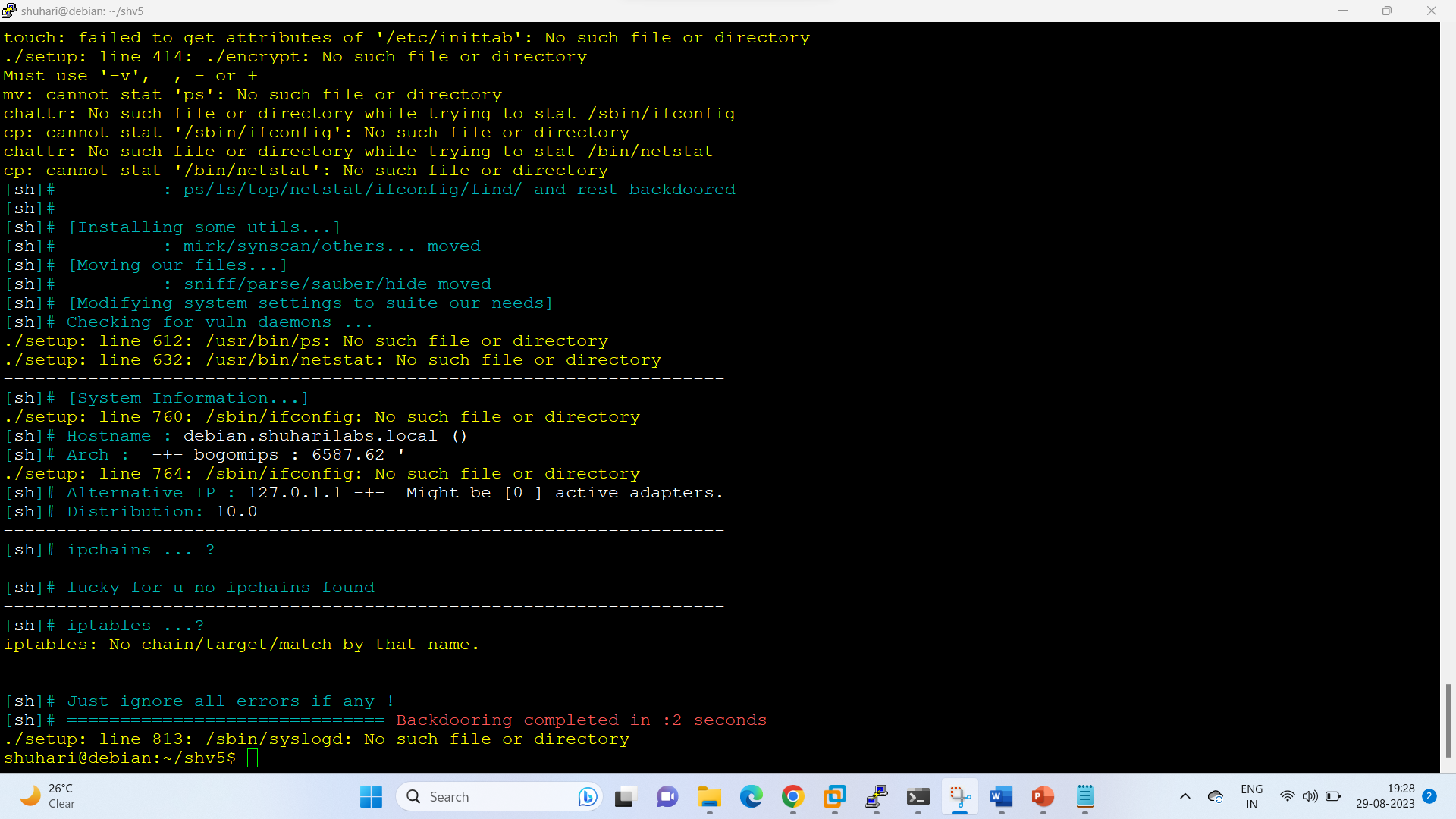


## I:\snapshots\5.pngFile Integrity

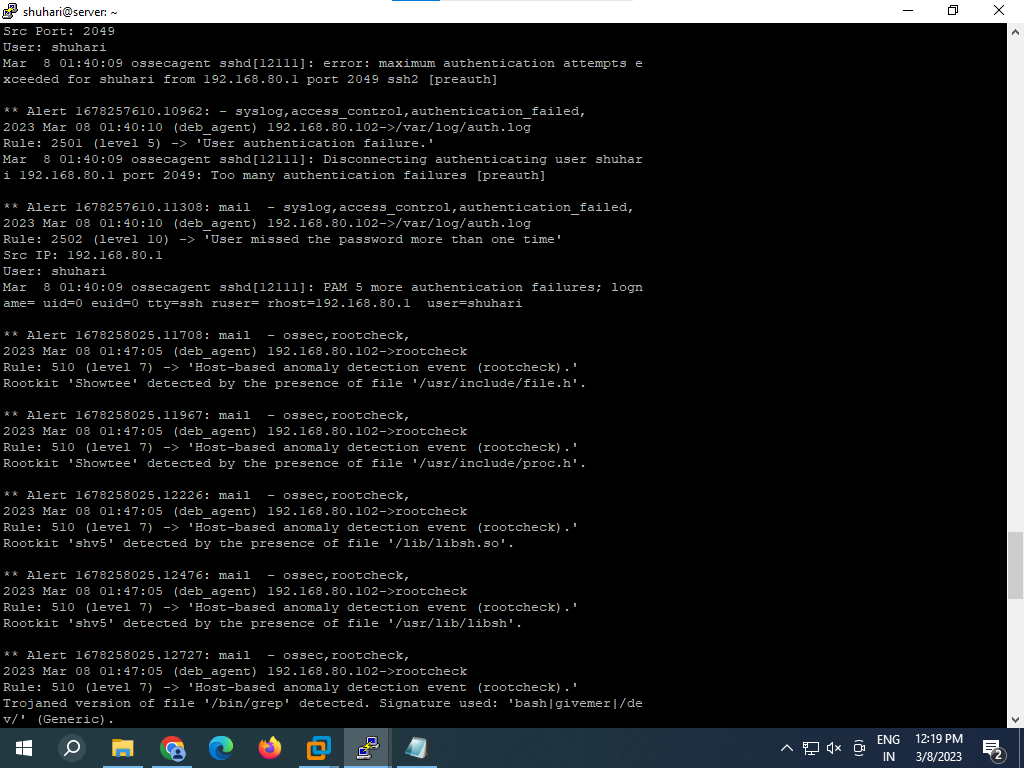
**10.3.1 File Integrity Testing of /etc/timezone file**



**10.4 Rootkit Installed**



## 10.4.1 Rootkit detection alert generated



# 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.

# FUTURE DEVELOPMENTS

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.

# 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. Collected events and alerts are readily accessible using the powerful search capabilities of the tool. Scripts to get at the data you need to address incidents. This provides a window into the integrity of key files on all of your deployed OSSEC HIDS agents and allows us to see if a rootkit or malicious application has altered key system files without the user’s knowledge. OSSEC HIDS statistics can be viewed and aggregated by severity, rule numbers, and even the hour they occur to help us visualize what is happening on your network. This information can be used to determine our event rate and help us decide when to add additional hardware to our OSSEC HIDS deployment to help with the collection and processing of events.

# REFEFRENCES

## Book:

OSSECHIDS host based intrusion detection guide by Andrew Hay, Daniel Cid (Creator of OSSEC), Rory Bray

## Links:

1. <http://www.ossec.net/wiki/index.p>
2. hp/OSSECWUI:Install
3. <http://ossec.github.io/>