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
PROJECT GUIDE

MR. ROHIT PURANIK
CENTRE CO-ORDINATOR

INDEX

LIST OF ABBREVIATIONS

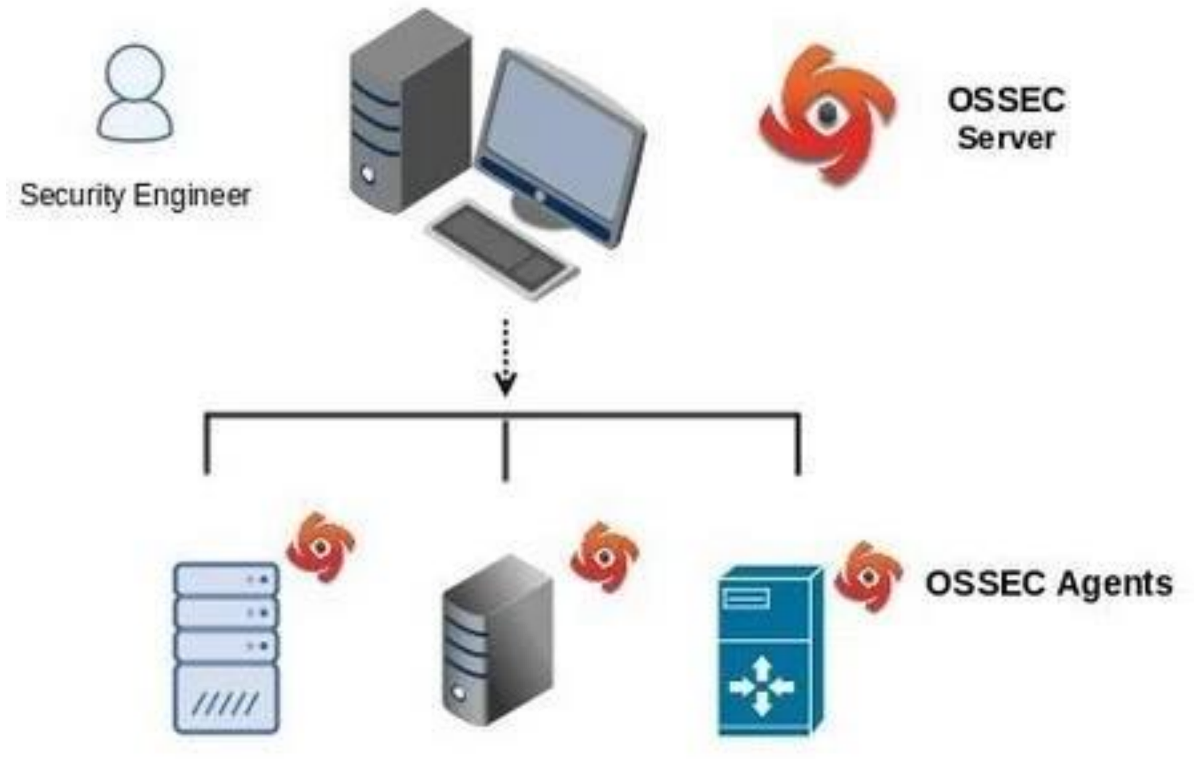
Sr no.	Abbreviation	Full-Form
1.	OSSEC	Open Source HIDS SECURITY
2.	HIDS	Host BASED INTRUSION DETECTION SYSTEM
3.	SIEM	Security Information and Event Management
4.	SIM	Security Incident Management

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.

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.

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. 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.

5. 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.

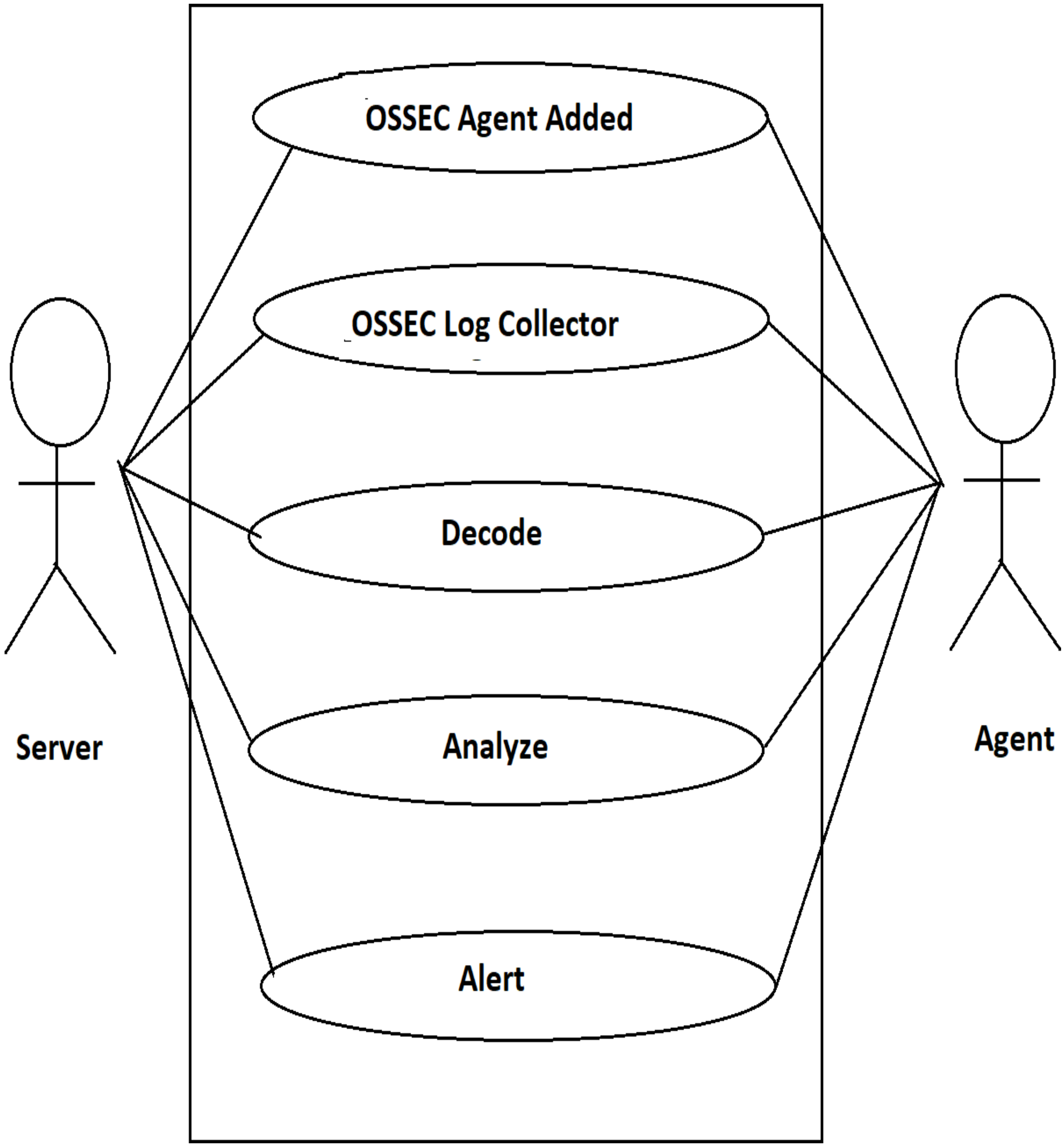
Centralized management

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.

7. UML DIAGRAM



Implementation of HIDS

8. 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 roleof 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.

9. 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:

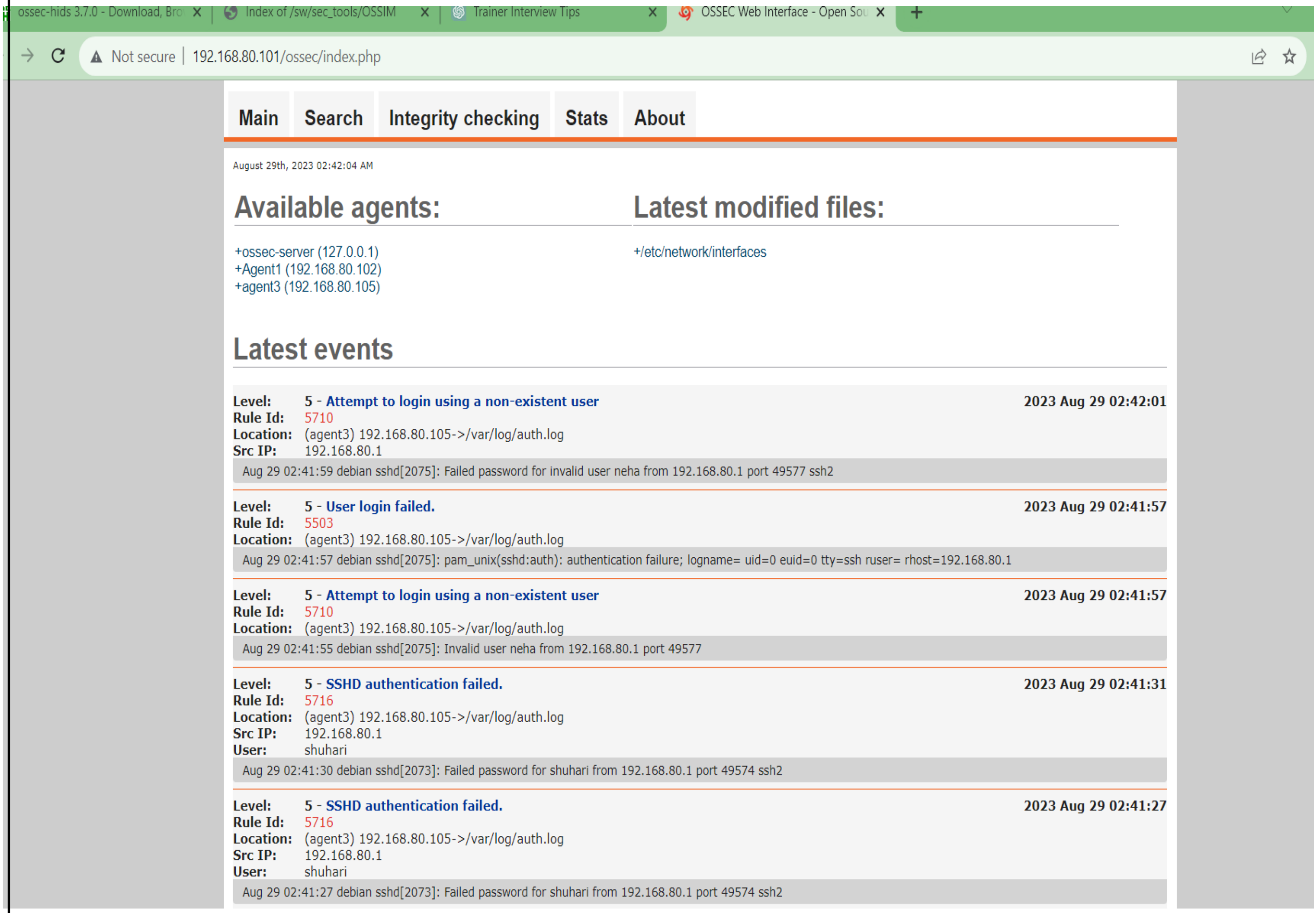
■ Available agents

■ Latest modified files

■ Latest events

10.IMPLEMENTATION SCREENSHOTS

10.1 OSSEC Server-Agent Setup:


ossec-hids 3.7.0 - Download, Bro
Index of /sw/sec_tools/OSSIM
Trainer Interview Tips
OSSEC Web Interface - Open Sou
Not secure
192.168.80.101/ossec/index.php
Main
Search
Integrity checking
Stats
About

August 29th, 2023 02:42:04 AM

Available agents:

+ossec-server (127.0.0.1)
+Agent1 (192.168.80.102)
+agent3 (192.168.80.105)

Latest modified files:

+/etc/network/interfaces

Latest events

Level: 5 - Attempt to login using a non-existent user **2023 Aug 29 02:42:01**
Rule Id: 5710
Location: (agent3) 192.168.80.105->/var/log/auth.log
Src IP: 192.168.80.1

```
Aug 29 02:41:59 debian sshd[2075]: Failed password for invalid user neha from 192.168.80.1 port 49577 ssh2
```

Level: 5 - User login failed. **2023 Aug 29 02:41:57**
Rule Id: 5503
Location: (agent3) 192.168.80.105->/var/log/auth.log

```
Aug 29 02:41:57 debian sshd[2075]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.80.1
```

Level: 5 - Attempt to login using a non-existent user **2023 Aug 29 02:41:57**
Rule Id: 5710
Location: (agent3) 192.168.80.105->/var/log/auth.log

```
Aug 29 02:41:55 debian sshd[2075]: Invalid user neha from 192.168.80.1 port 49577
```

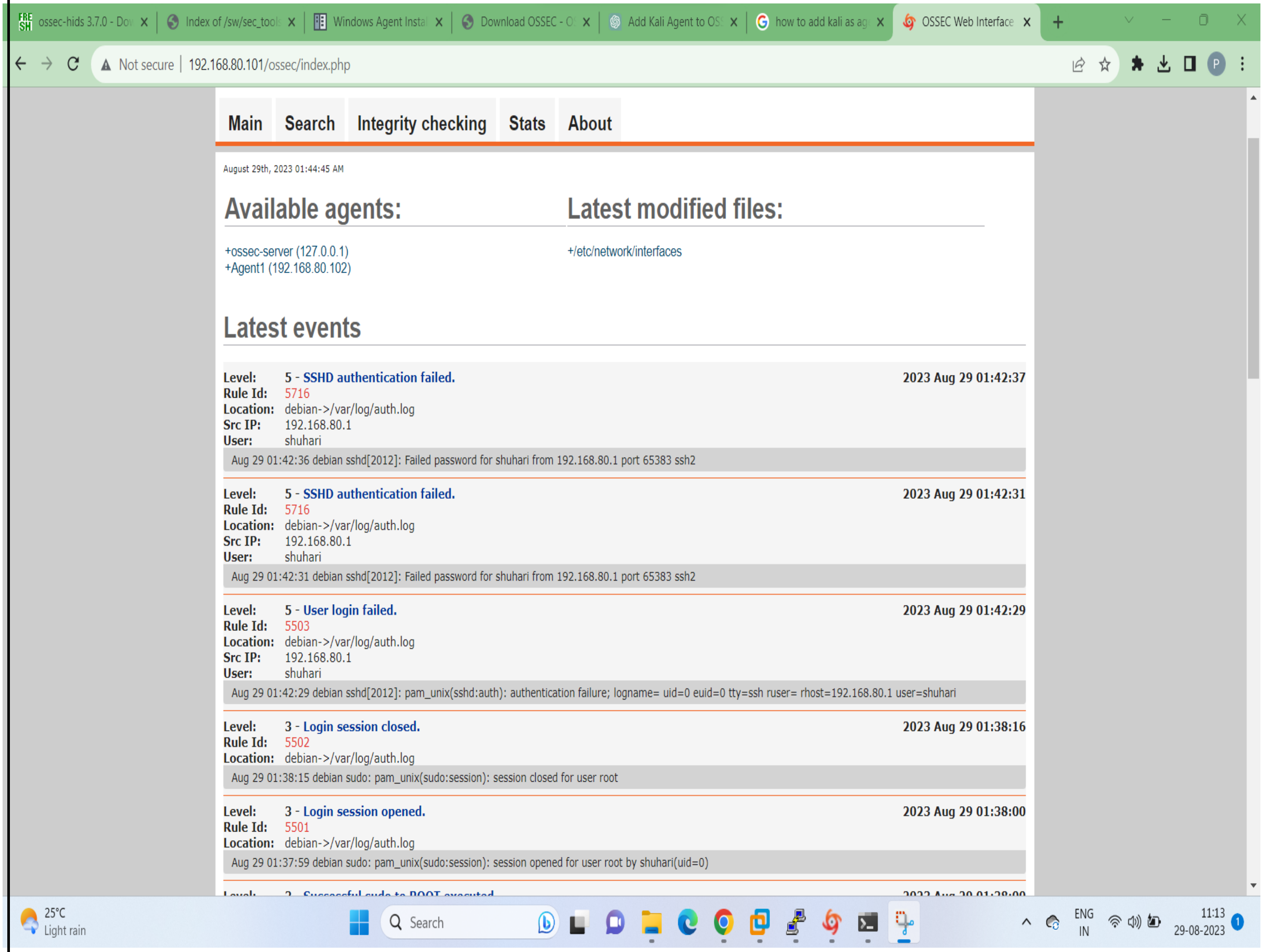
Level: 5 - SSHD authentication failed. **2023 Aug 29 02:41:31**
Rule Id: 5716
Location: (agent3) 192.168.80.105->/var/log/auth.log
Src IP: 192.168.80.1
User: shuhari

```
Aug 29 02:41:30 debian sshd[2073]: Failed password for shuhari from 192.168.80.1 port 49574 ssh2
```

Level: 5 - SSHD authentication failed. **2023 Aug 29 02:41:27**
Rule Id: 5716
Location: (agent3) 192.168.80.105->/var/log/auth.log
Src IP: 192.168.80.1
User: shuhari

```
Aug 29 02:41:27 debian sshd[2073]: Failed password for shuhari from 192.168.80.1 port 49574 ssh2
```

10.2 Authentication Logs:



August 29th, 2023 01:44:45 AM

Available agents:

+ossec-server (127.0.0.1)
+Agent1 (192.168.80.102)

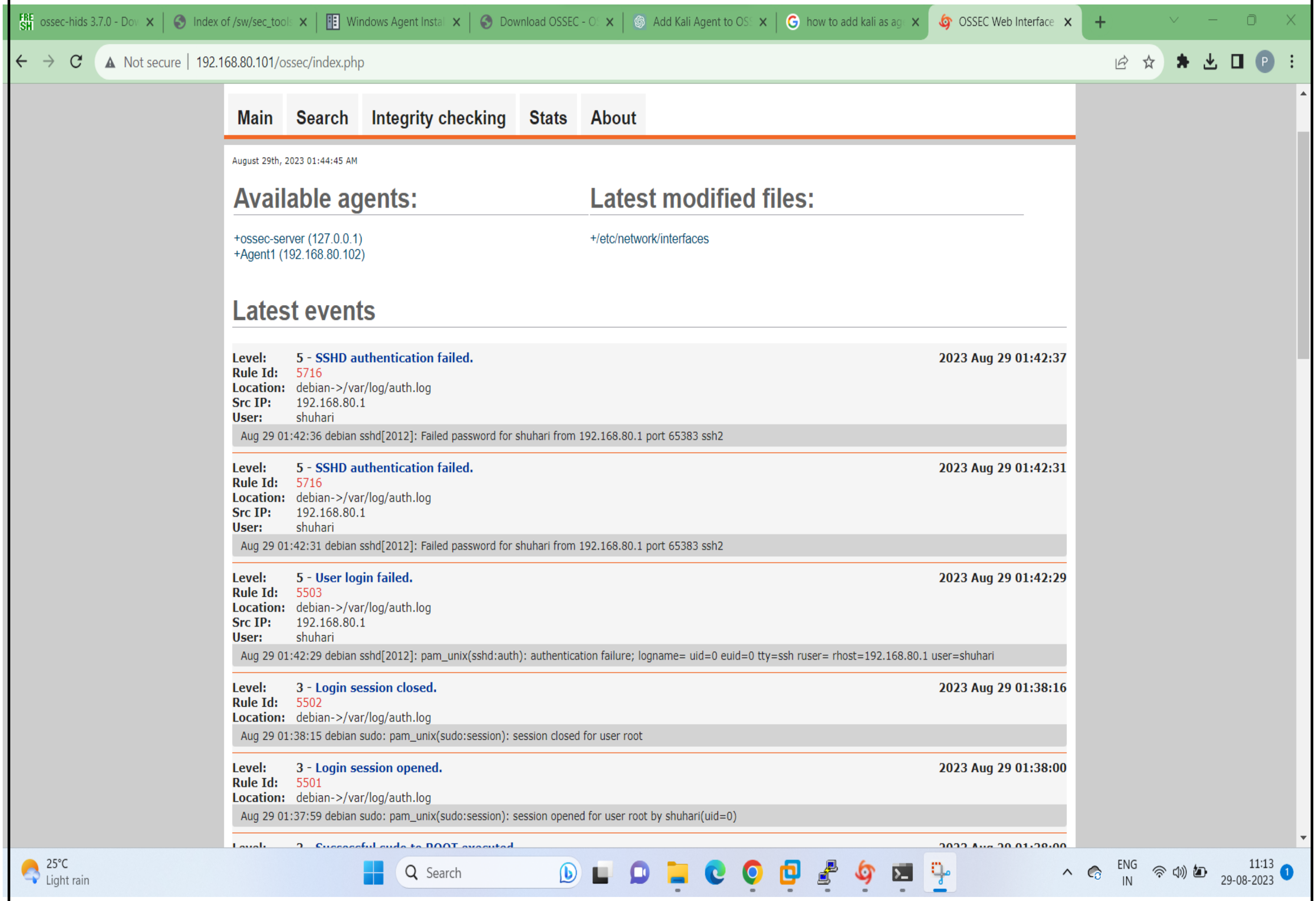
Latest modified files:

+/etc/network/interfaces

Latest events

```
Level:     5 - SSHD authentication failed.                          2023 Aug 29 01:42:37
Rule Id:   5716
Location:  debian->/var/log/auth.log
Src IP:    192.168.80.1
User:      shuhari
  Aug 29 01:42:36 debian sshd[2012]: Failed password for shuhari from 192.168.80.1 port 65383 ssh2

Level:     5 - SSHD authentication failed.                          2023 Aug 29 01:42:31
Rule Id:   5716
Location:  debian->/var/log/auth.log
Src IP:    192.168.80.1
User:      shuhari
  Aug 29 01:42:31 debian sshd[2012]: Failed password for shuhari from 192.168.80.1 port 65383 ssh2

Level:     5 - User login failed.                                   2023 Aug 29 01:42:29
Rule Id:   5503
Location:  debian->/var/log/auth.log
Src IP:    192.168.80.1
User:      shuhari
  Aug 29 01:42:29 debian sshd[2012]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.80.1 user=shuhari

Level:     3 - Login session closed.                                2023 Aug 29 01:38:16
Rule Id:   5502
Location:  debian->/var/log/auth.log
  Aug 29 01:38:15 debian sudo: pam_unix(sudo:session): session closed for user root

Level:     3 - Login session opened.                                2023 Aug 29 01:38:00
Rule Id:   5501
Location:  debian->/var/log/auth.log
  Aug 29 01:37:59 debian sudo: pam_unix(sudo:session): session opened for user root by shuhari(uid=0)

Level:     3 - Successful sudo to ROOT executed.                    2023 Aug 29 01:38:00
```

10.2.1 Login Failed Attempts:



August 29th, 2023 01:44:45 AM

Available agents:

+ossec-server (127.0.0.1)
+Agent1 (192.168.80.102)

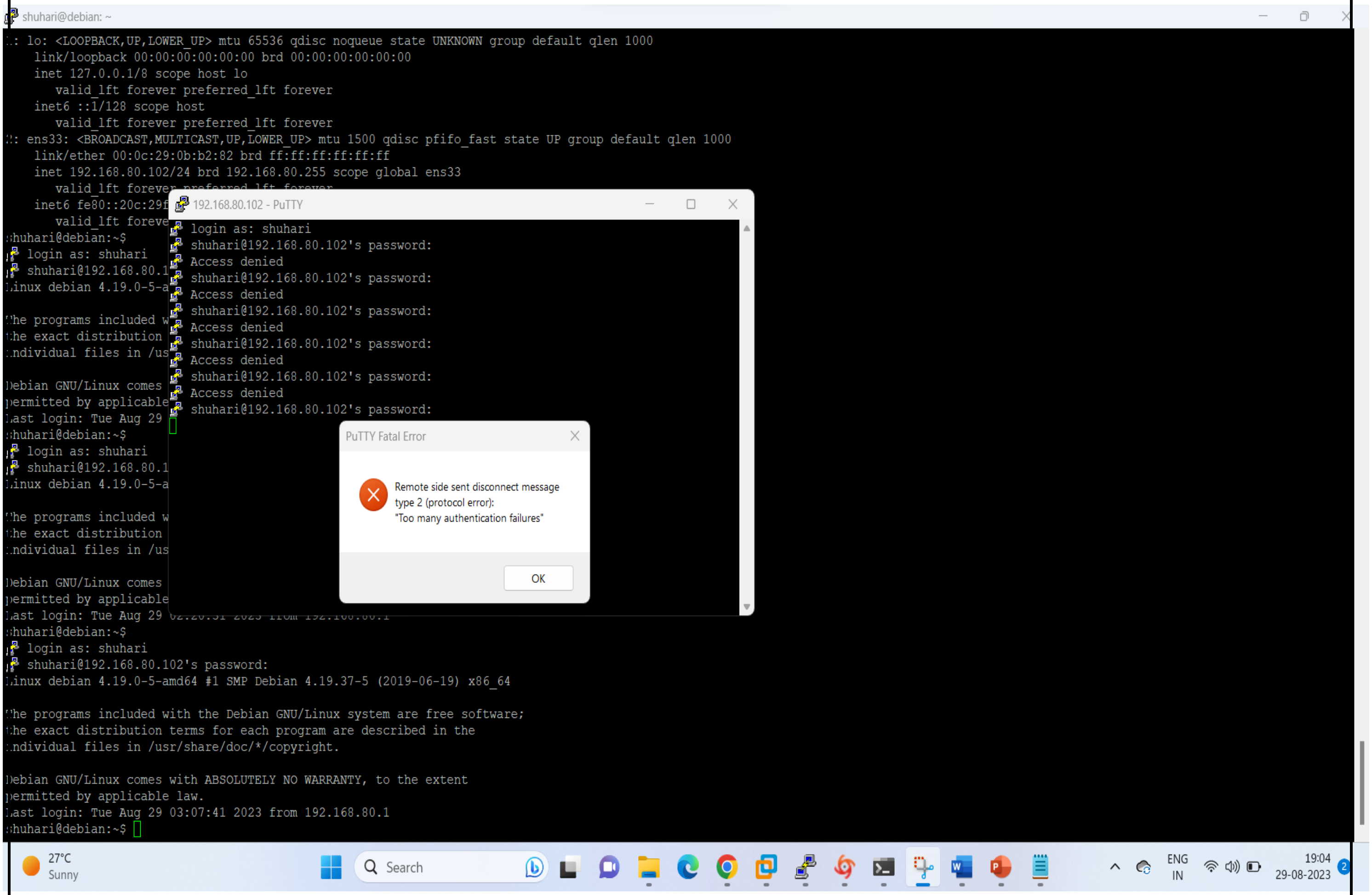
Latest modified files:

+/etc/network/interfaces

Latest events

```
Level:     5 - SSHD authentication failed.                2023 Aug 29 01:42:37
Rule Id:   5716
Location:  debian->/var/log/auth.log
Src IP:    192.168.80.1
User:      shuhari
 Aug 29 01:42:36 debian sshd[2012]: Failed password for shuhari from 192.168.80.1 port 65383 ssh2

Level:     5 - SSHD authentication failed.                2023 Aug 29 01:42:31
Rule Id:   5716
Location:  debian->/var/log/auth.log
Src IP:    192.168.80.1
User:      shuhari
 Aug 29 01:42:31 debian sshd[2012]: Failed password for shuhari from 192.168.80.1 port 65383 ssh2

Level:     5 - User login failed.                         2023 Aug 29 01:42:29
Rule Id:   5503
Location:  debian->/var/log/auth.log
Src IP:    192.168.80.1
User:      shuhari
 Aug 29 01:42:29 debian sshd[2012]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.80.1 user=shuhari

Level:     3 - Login session closed.                      2023 Aug 29 01:38:16
Rule Id:   5502
Location:  debian->/var/log/auth.log
 Aug 29 01:38:15 debian sudo: pam_unix(sudo:session): session closed for user root

Level:     3 - Login session opened.                      2023 Aug 29 01:38:00
Rule Id:   5501
Location:  debian->/var/log/auth.log
 Aug 29 01:37:59 debian sudo: pam_unix(sudo:session): session opened for user root by shuhari(uid=0)

Level:     3 - Successful sudo to ROOT executed.          2023 Aug 29 01:38:00
```

10.2.2 IP Blocked:



```
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:0b:b2:82 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.102/24 brd 192.168.80.255 scope global ens33
       valid_lft forever
    inet6 fe80::20c:29f
       valid_lft foreve
huhari@debian:~$
 login as: shuhari
 shuhari@192.168.80.1
inux debian 4.19.0-5-a

he programs included w
he exact distribution
ndividual files in /us

ebian GNU/Linux comes
ermitted by applicable
ast login: Tue Aug 29
huhari@debian:~$
 login as: shuhari
 shuhari@192.168.80.1
inux debian 4.19.0-5-a

he programs included w
he exact distribution
ndividual files in /us

ebian GNU/Linux comes
ermitted by applicable
ast login: Tue Aug 29
huhari@debian:~$
 login as: shuhari
 shuhari@192.168.80.102's password:
inux debian 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

he programs included with the Debian GNU/Linux system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*/copyright.

ebian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
ermitted by applicable law.
ast login: Tue Aug 29 03:07:41 2023 from 192.168.80.1
huhari@debian:~$
```

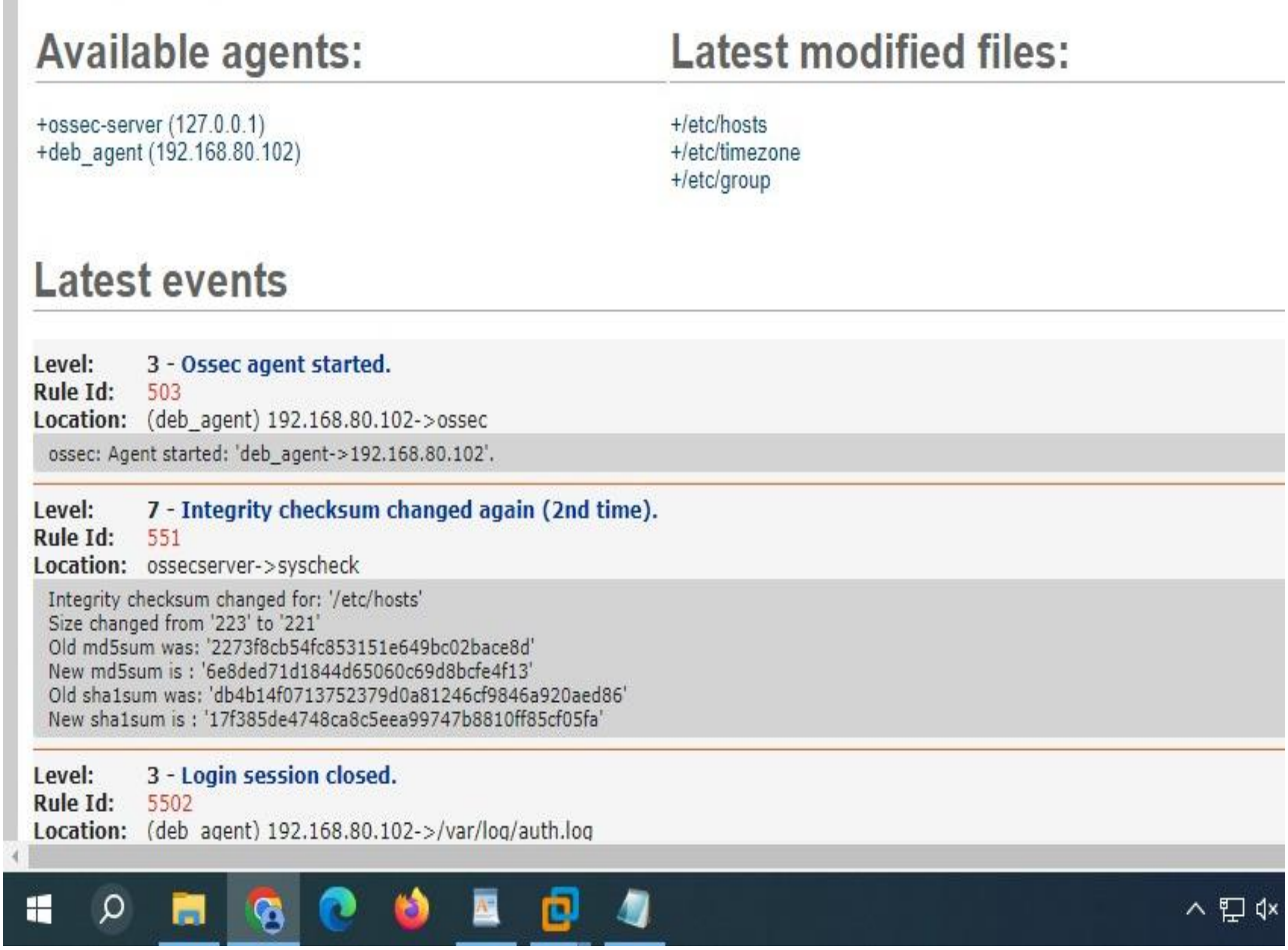
```
login as: shuhari
shuhari@192.168.80.102's password:
Access denied
shuhari@192.168.80.102's password:
Access denied
shuhari@192.168.80.102's password:
Access denied
shuhari@192.168.80.102's password:
Access denied
shuhari@192.168.80.102's password:
Access denied
shuhari@192.168.80.102's password:
```

PuTTY Fatal Error

Remote side sent disconnect message type 2 (protocol error): "Too many authentication failures"

OK

10.3 File Integrity



Available agents:

+ossec-server (127.0.0.1)
+deb_agent (192.168.80.102)

Latest modified files:

+/etc/hosts
+/etc/timezone
+/etc/group

Latest events

Level: 3 - Ossec agent started.
Rule Id: 503
Location: (deb_agent) 192.168.80.102->ossec

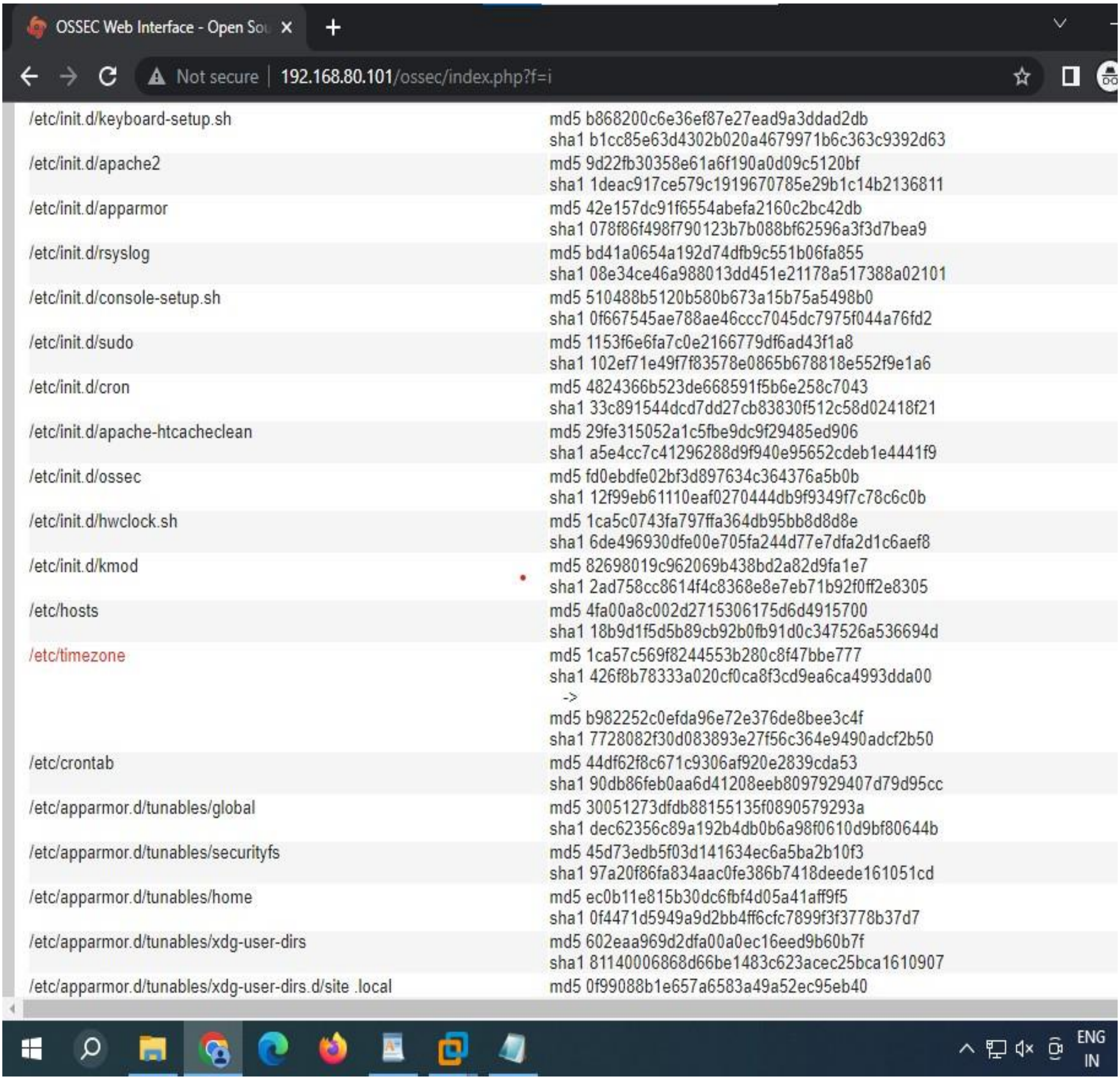
```
ossec: Agent started: 'deb_agent->192.168.80.102'.
```

Level: 7 - Integrity checksum changed again (2nd time).
Rule Id: 551
Location: ossecserver->syscheck

```
Integrity checksum changed for: '/etc/hosts'
Size changed from '223' to '221'
Old md5sum was: '2273f8cb54fc853151e649bc02bace8d'
New md5sum is : '6e8ded71d1844d65060c69d8bcfe4f13'
Old sha1sum was: 'db4b14f0713752379d0a81246cf9846a920aed86'
New sha1sum is : '17f385de4748ca8c5eea99747b8810ff85cf05fa'
```

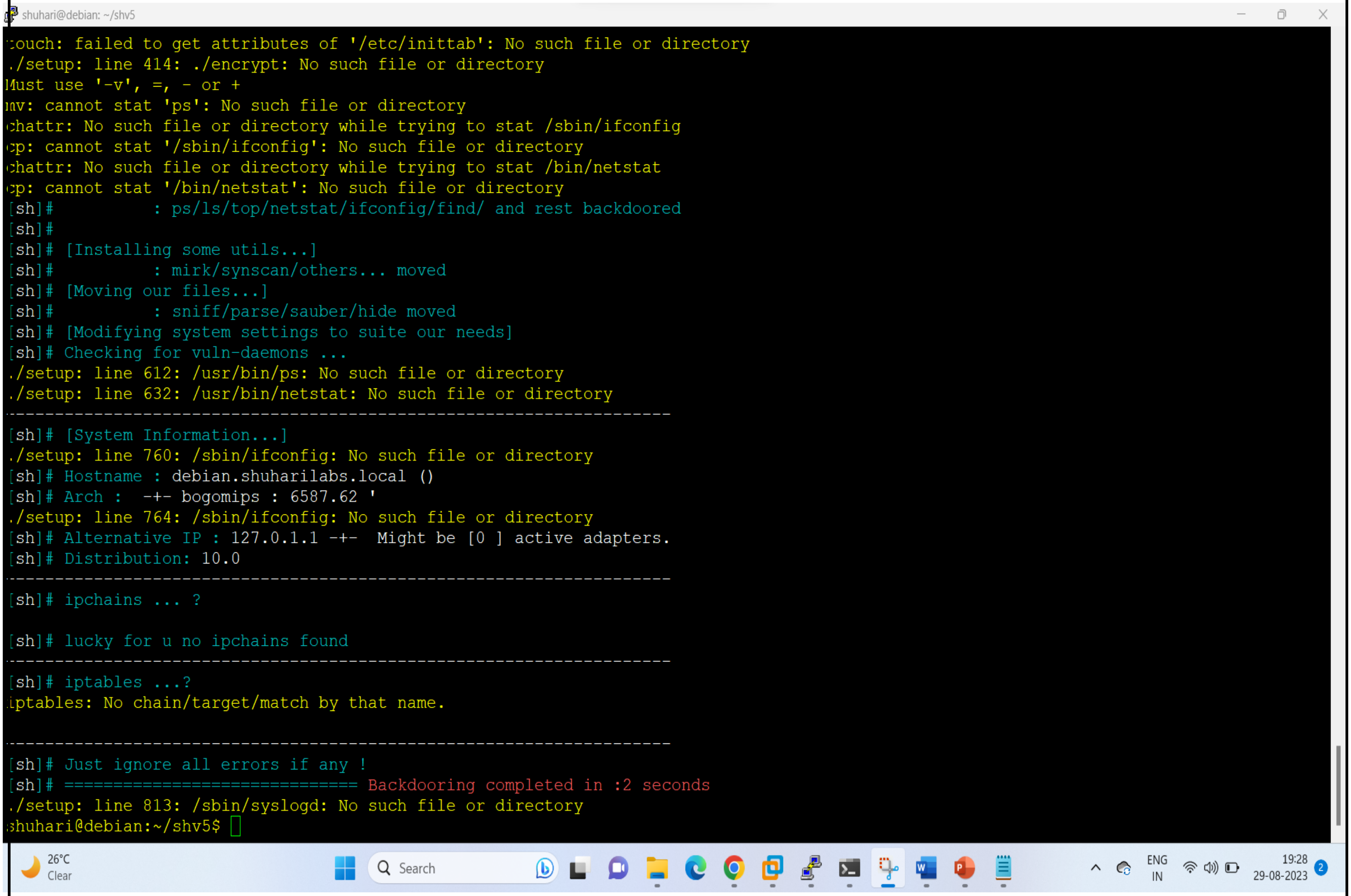
Level: 3 - Login session closed.
Rule Id: 5502
Location: (deb_agent) 192.168.80.102->/var/log/auth.log

10.3.1 File Integrity Testing of /etc/timezone file


OSSEC Web Interface - Open Sou
Not secure
192.168.80.101/ossec/index.php?f=i
ENG
IN

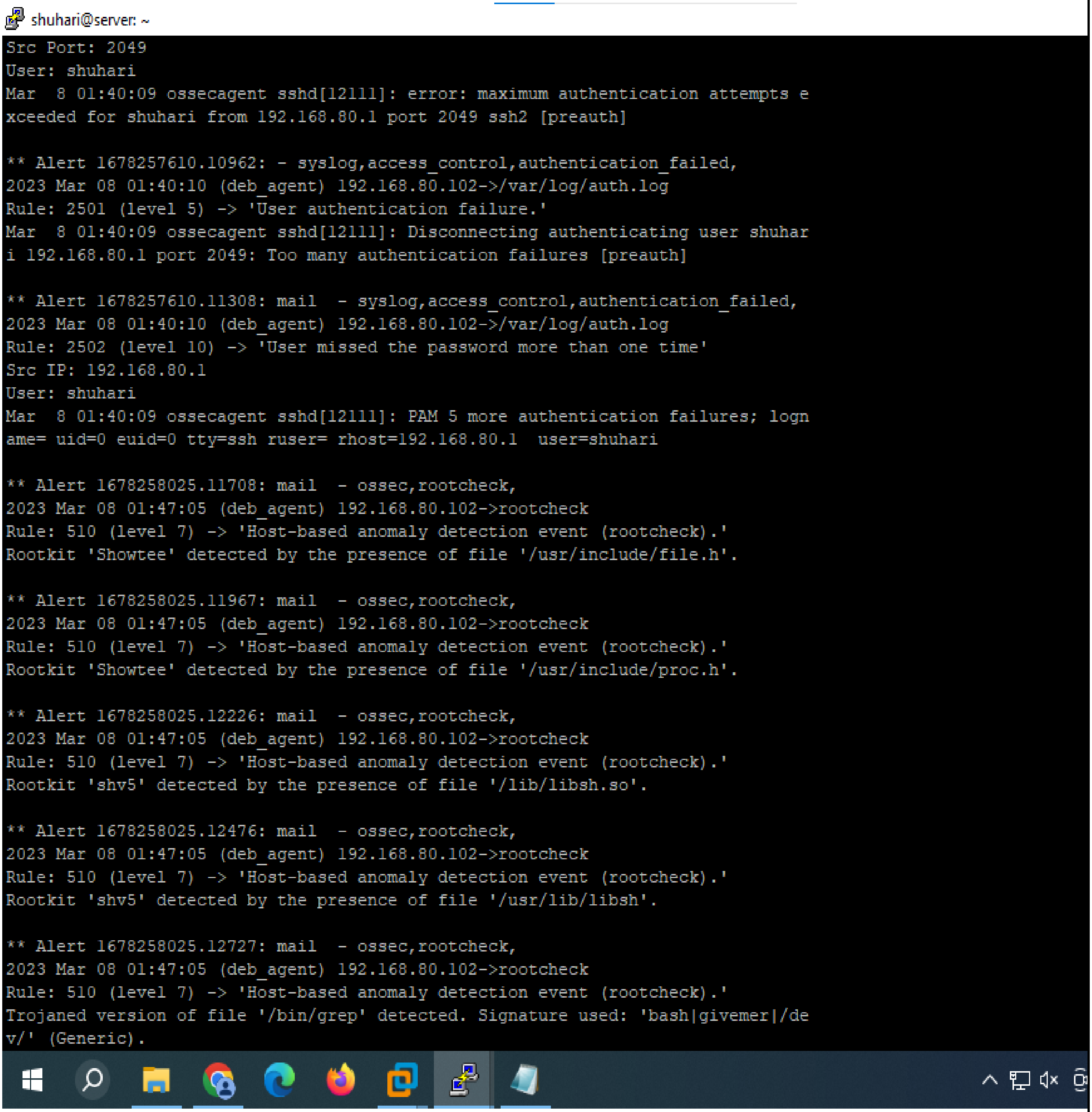
/etc/init.d/keyboard-setup.sh	md5 b868200c6e36ef87e27ead9a3ddad2db sha1 b1cc85e63d4302b020a4679971b6c363c9392d63
/etc/init.d/apache2	md5 9d22fb30358e61a6f190a0d09c5120bf sha1 1deac917ce579c1919670785e29b1c14b2136811
/etc/init.d/apparmor	md5 42e157dc91f6554abefa2160c2bc42db sha1 078f86f498f790123b7b088bf62596a3f3d7bea9
/etc/init.d/rsyslog	md5 bd41a0654a192d74dfb9c551b06fa855 sha1 08e34ce46a988013dd451e21178a517388a02101
/etc/init.d/console-setup.sh	md5 510488b5120b580b673a15b75a5498b0 sha1 0f667545ae788ae46ccc7045dc7975f044a76fd2
/etc/init.d/sudo	md5 1153f6e6fa7c0e2166779df6ad43f1a8 sha1 102ef71e49f7f83578e0865b678818e552f9e1a6
/etc/init.d/cron	md5 4824366b523de668591f5b6e258c7043 sha1 33c891544dcd7dd27cb83830f512c58d02418f21
/etc/init.d/apache-htcacheclean	md5 29fe315052a1c5fbe9dc9f29485ed906 sha1 a5e4cc7c41296288d9f940e95652cdeb1e4441f9
/etc/init.d/ossec	md5 fd0ebdfe02bf3d897634c364376a5b0b sha1 12f99eb61110eaf0270444db9f9349f7c78c6c0b
/etc/init.d/hwclock.sh	md5 1ca5c0743fa797ffa364db95bb8d8d8e sha1 6de496930dfe00e705fa244d77e7dfa2d1c6aef8
/etc/init.d/kmod	md5 82698019c962069b438bd2a82d9fa1e7 sha1 2ad758cc8614f4c8368e8e7eb71b92f0ff2e8305
/etc/hosts	md5 4fa00a8c002d2715306175d6d4915700 sha1 18b9d1f5d5b89cb92b0fb91d0c347526a536694d
/etc/timezone	md5 1ca57c569f8244553b280c8f47bbe777 sha1 426f8b78333a020cf0ca8f3cd9ea6ca4993dda00 -> md5 b982252c0efda96e72e376de8bee3c4f sha1 7728082f30d083893e27f56c364e9490adcf2b50
/etc/crontab	md5 44df62f8c671c9306af920e2839cda53 sha1 90db86feb0aa6d41208eeb8097929407d79d95cc
/etc/apparmor.d/tunables/global	md5 30051273dfdb88155135f0890579293a sha1 dec62356c89a192b4db0b6a98f0610d9bf80644b
/etc/apparmor.d/tunables/securityfs	md5 45d73edb5f03d141634ec6a5ba2b10f3 sha1 97a20f86fa834aac0fe386b7418deede161051cd
/etc/apparmor.d/tunables/home	md5 ec0b11e815b30dc6fbf4d05a41aff9f5 sha1 0f4471d5949a9d2bb4ff6cfc7899f3f3778b37d7
/etc/apparmor.d/tunables/xdg-user-dirs	md5 602eaa969d2dfa00a0ec16eed9b60b7f sha1 81140006868d66be1483c623acec25bca1610907
/etc/apparmor.d/tunables/xdg-user-dirs.d/site .local	md5 0f99088b1e657a6583a49a52ec95eb40

10.4 Rootkit Installed



```
touch: failed to get attributes of '/etc/inittab': No such file or directory
./setup: line 414: ./encrypt: No such file or directory
Must use '-v', =, - or +
mv: cannot stat 'ps': No such file or directory
chattr: No such file or directory while trying to stat /sbin/ifconfig
cp: cannot stat '/sbin/ifconfig': No such file or directory
chattr: No such file or directory while trying to stat /bin/netstat
cp: cannot stat '/bin/netstat': No such file or directory
[sh]#          : ps/ls/top/netstat/ifconfig/find/ and rest backdoored
[sh]#
[sh]# [Installing some utils...]
[sh]#          : mirk/synscan/others... moved
[sh]# [Moving our files...]
[sh]#          : sniff/parse/sauber/hide moved
[sh]# [Modifying system settings to suite our needs]
[sh]# Checking for vuln-daemons ...
./setup: line 612: /usr/bin/ps: No such file or directory
./setup: line 632: /usr/bin/netstat: No such file or directory
--------------------------------------------------------------------
[sh]# [System Information...]
./setup: line 760: /sbin/ifconfig: No such file or directory
[sh]# Hostname : debian.shuharilabs.local  ()
[sh]# Arch :  -+- bogomips : 6587.62 '
./setup: line 764: /sbin/ifconfig: No such file or directory
[sh]# Alternative IP : 127.0.1.1 -+-  Might be [0 ] active adapters.
[sh]# Distribution: 10.0
--------------------------------------------------------------------
[sh]# ipchains ... ?

[sh]# lucky for u no ipchains found
--------------------------------------------------------------------
[sh]# iptables ...?
iptables: No chain/target/match by that name.

--------------------------------------------------------------------
[sh]# Just ignore all errors if any !
[sh]# ============================== Backdooring completed in :2 seconds
./setup: line 813: /sbin/syslogd: No such file or directory
shuhari@debian:~/shv5$
```

10.4.1 Rootkit detection alert generated



```
Src Port: 2049
User: shuhari
Mar  8 01:40:09 ossecagent sshd[12111]: error: maximum authentication attempts e
xceeded for shuhari from 192.168.80.1 port 2049 ssh2 [preauth]

** Alert 1678257610.10962: - syslog,access_control,authentication_failed,
2023 Mar 08 01:40:10 (deb_agent) 192.168.80.102->/var/log/auth.log
Rule: 2501 (level 5) -> 'User authentication failure.'
Mar  8 01:40:09 ossecagent sshd[12111]: Disconnecting authenticating user shuhar
i 192.168.80.1 port 2049: Too many authentication failures [preauth]

** Alert 1678257610.11308: mail  - syslog,access_control,authentication_failed,
2023 Mar 08 01:40:10 (deb_agent) 192.168.80.102->/var/log/auth.log
Rule: 2502 (level 10) -> 'User missed the password more than one time'
Src IP: 192.168.80.1
User: shuhari
Mar  8 01:40:09 ossecagent sshd[12111]: PAM 5 more authentication failures; logn
ame= uid=0 euid=0 tty=ssh ruser= rhost=192.168.80.1  user=shuhari

** Alert 1678258025.11708: mail  - ossec,rootcheck,
2023 Mar 08 01:47:05 (deb_agent) 192.168.80.102->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Rootkit 'Showtee' detected by the presence of file '/usr/include/file.h'.

** Alert 1678258025.11967: mail  - ossec,rootcheck,
2023 Mar 08 01:47:05 (deb_agent) 192.168.80.102->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Rootkit 'Showtee' detected by the presence of file '/usr/include/proc.h'.

** Alert 1678258025.12226: mail  - ossec,rootcheck,
2023 Mar 08 01:47:05 (deb_agent) 192.168.80.102->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Rootkit 'shv5' detected by the presence of file '/lib/libsh.so'.

** Alert 1678258025.12476: mail  - ossec,rootcheck,
2023 Mar 08 01:47:05 (deb_agent) 192.168.80.102->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Rootkit 'shv5' detected by the presence of file '/usr/lib/libsh'.

** Alert 1678258025.12727: mail  - ossec,rootcheck,
2023 Mar 08 01:47:05 (deb_agent) 192.168.80.102->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Trojaned version of file '/bin/grep' detected. Signature used: 'bash|givemer|/de
v/' (Generic).
```

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 networktraffic 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 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.

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. 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.

14. 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/