Practical : 7

Aim: Install OSSEC, a host-based IDS/IPS. Configure OSSEC to monitor system logs and file integrity. Trigger and analyze alerts on the test system.

OSSEC Installation

1. **Update Your System**

   Run the package manager update command on your server:

```
sudo apt update    # For Ubuntu/Debian
sudo yum update    # For CentOS/RHEL
```

2. **Install Required Dependencies**

   OSSEC requires some utilities for compilation. Install them:

```
sudo apt install build-essential make gcc zlib1g-dev libpcre2-dev libevent-dev
libssl-dev libsqlite3-dev -y   # Ubuntu/Debian
sudo yum install gcc make libc-dev   # CentOS/RHEL
```

3. **Download and Install OSSEC**

   Download the latest OSSEC release:

```
wget https://github.com/ossec/ossec-hids/archive/master.zip
unzip master.zip
cd ossec-hids-master
sudo ./install.sh
```

   - Follow the installation prompts: select language, choose 'server' or 'local' install, and enable active response as needed.[1][2]

OSSEC Configuration

Monitor System Logs

1. **Add Log Files to Monitor**

   Edit `/var/ossec/etc/ossec.conf` and locate the `<ossec_config>` section. Add entries for the logs:

   ```
   <localfile>
     <location>/var/log/auth.log</location>
     <log_format>syslog</log_format>
   </localfile>
   <localfile>
     <location>/var/log/syslog</location>
     <log_format>syslog</log_format>
   </localfile>
   ```

   - For other critical logs, repeat with their paths and appropriate format.[3][4][5]

2. **Restart OSSEC to Apply Changes**

   ```
   sudo systemctl restart ossec
   # or
   sudo /var/ossec/bin/ossec-control restart
   ```

Configure File Integrity Monitoring

1. **Edit Syscheck Configuration**

   In the same `ossec.conf`, find or create the `<syscheck>` section:

   ```
   <syscheck>
     <frequency>14400</frequency> <!-- Every 4 hours -->
     <directories realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
     <directories realtime="yes" check_all="yes">/bin,/sbin</directories>
   </syscheck>
   ```

   - For web servers, add:

```
<directories realtime="yes" report_changes="yes"
restrict=".php|.html|.js|.htaccess">/var/www/html</directories>
```

2. **Restart OSSEC**

   ```
   sudo systemctl restart ossec
   # or
   sudo /var/ossec/bin/ossec-control restart
   ```

   - Confirm syscheck is running by tailing the OSSEC log:

```
tail -f /var/ossec/log/ossec.log
```

3. Look for “Starting real time file monitoring” or alert messages.[6][7][3]

Trigger and Analyze Alerts

1. **Test Log Alert**

   - Generate a suspicious log entry in `auth.log`, for example:

```
sudo su -    # triggers a session start in logs
```

   - OSSEC should alert on unusual or failed authentication attempts.

2. **Test File Integrity Alert**

   - Modify a file monitored by syscheck:

```
sudo echo "test" >> /etc/hosts
```

   - OSSEC should alert on unexpected changes.[8][3]

3. **Analyze Alerts**

   - OSSEC alerts are available in:

```
/var/ossec/logs/alerts/alerts.log
```

   - Look for entries corresponding to your test actions, noting alert severity and description.

Summary Table

Step	Command/Action	Config File/Path	Expected Result
Install OSSEC	`wget, unzip, ./install.sh`	-	Installer prompts complete[2]
Monitor system logs	Edit `<localfile>` blocks	`/var/ossec/etc/ossec.conf`	Logs monitored[4][3]
Configure file integrity	Edit `<syscheck>` section	`/var/ossec/etc/ossec.conf`	Files/dirs monitored[7][3]
Restart OSSEC	`systemctl restart ossec` or `/var/ossec/bin/ossec-control restart`	-	Changes applied
Trigger alerts	Edit files/logs	Targeted files/logs	Alerts generated[3]
Analyze alerts	Check `/var/ossec/logs/alerts/alerts.log`	-	Alerts visible

This document guides through a full OSSEC HIDS installation, configuration for monitoring logs and file integrity, and verification by triggering and analyzing alerts.[9][2][4][7][5][1][3][6][8]

⁂

1. https://dcid.me/notes/my-ossec-setup-guide
2. https://trunc.org/ossec/ossec-linux
3. https://trunc.org/ossec/ossec-for-website-security-logs-integritychecking
4. https://www.ossec.net/docs/docs/manual/monitoring/file-log-monitoring.html

5. https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/monitoring-log-files.html

6. https://www.ibm.com/docs/en/safer-payments/6.7.0?topic=configuration-implementing-integrity-monitoring-critical-files

7. https://www.ossec.net/docs/manual/syscheck/index.html

8. https://www.ossec.net/docs/manual/non-technical-overview.html

9. https://www.rapid7.com/blog/post/2017/06/30/how-to-install-and-configure-ossec-on-ubuntu-linux/

10. https://www.ossec.net/docs/docs/manual/installation/index.html

11. https://www.youtube.com/watch?v=7RhTJtF6Ab0

12. https://community.hetzner.com/tutorials/ossec-server-and-agent-setup/

13. https://www.ossec.net/finish-ossec-plus-install/

14. https://www.ossec.net/ossec-fim-file-integrity-monitoring/

15. https://www.hostmycode.in/tutorials/install-and-use-ossec-hids-on-ubuntu-2404

16. https://www.ossec.net/docs/docs/manual/monitoring/index.html

17. https://documentation.wazuh.com/current/proof-of-concept-guide/poc-file-integrity-monitoring.html

18. https://dyindia.weebly.com/linux/how-to-install-and-setup-ossec-agent-on-rhelcentos-7

19. https://ossec-docs.readthedocs.io/en/pr_314/docs/manual/monitoring/

20. https://cloud.google.com/chronicle/docs/ingestion/default-parsers/ossec