

**Department of Network and Computer Security**

**NCS 384 Network Intrusion Detection/NCS 532 Netwrk Intrusion Prev & Detect**

**Spring 2023**

**Hands-on Exercise 8**

**Host-based Intrusion Detection System (HIDS) using AIDE**

**Introduction:**

In this lab, you will use a Host-based Intrusion Detection System (HIDS) to detect compromises on your Linux machine. We will be using AIDE (Advanced Intrusion Detection Environment), a HIDS which uses techniques similar to that of the more well-known Tripwire. It attempts to detect intrusions by monitoring the filesystem and alerting administrators when suspicious changes occur.

AIDE is a small yet powerful, free open-source host-based intrusion detection tool that uses predefined rules to check file and directory integrity in Unix-like operating systems such as Linux. It is an independent static binary for simplified client/server monitoring configurations. It is feature-rich: uses plain text configuration files and database making it easy to use; supports several message digest algorithms such as but not limited to md5, sha1, rmd160, tiger; supports common file attributes; also supports powerful regular expressions to selectively include or exclude files and directories to be scanned. Also, it can be compiled with exceptional support for Gzip compression, Posix ACL, SELinux, XAttrs and Extended file system attributes. AIDE works by creating a database (which is simply a snapshot of selected parts of the file system), from the regular expression rules defined in the configuration file(s). Once this database is initialized, you can verify the integrity of the system files against it. Following section will show how to install and use aide in Linux.

**Helpful Materials (Highly recommended to explore)**

* How to Install and Configure AIDE on Ubuntu Linux

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

* Enhancing Linux security with Advanced Intrusion Detection Environment (AIDE)

<https://www.redhat.com/sysadmin/linux-security-aide>

**Software Requirements**

* Any virtual machine, e.g., the VirtualBox, VMWare Software
* Any operating system, e.g., the Ubuntu 14.04 Long Term Support (LTS) Version

<http://www.ubuntu.com/download/desktop>

* AIDE (Advanced Intrusion Detection Environment): A host-based Intrusion Detection Tool

<https://sourceforge.net/projects/aide/>

<https://github.com/aide/aide>

<https://aide.github.io/>

### AIDE Summary

* **NAME**

aide - Advanced Intrusion Detection Environment

* **SYNOPSIS**

aide [parameters] command

* **DESCRIPTION**

AIDE is an intrusion detection system for checking the integrity of files.

* **COMMANDS**

--check, -C

Checks the database for inconsistencies. You must have an initialized

database to do this. This is also the default command. Without any

command aide does a check.

--init, -i

Initialize the database. You must initialize a database and move it to the appropriate place before you can use the --check command.

--update, -u

Checks the database and updates the database non-interactively. The input and output databases must be different.

--compare, -E

Compares two databases. They must be defined in config file with database=<url> and database\_new=<url>.

--config-check, -D

Stops after reading in the configuration file. Any errors will be reported. If aide was compiled with the "--with-dbhmackey" option, a hash for the config file will be calculated. See the AIDE manual for more information.

* **PARAMETERS**

--config=configfile , -c configfile

Configuration is read from file configfile instead of "./aide.conf". Use '-'

For stdin.

--limit=REGEX , -l REGEX

Limit command to entries matching REGEX. Note that the REGEX only

matches at the first position.

Example

Only check and update the database entries matching /etc (i.e., the /etc directory) while leaving all other entries unchecked and unchanged:

aide --update --limit /etc

--before="configparameters”, -B "configparameters"

These configparameters are handled before the reading of the configuration

file. See aide.conf (5) for more details on what to put here.

--after="configparameters”, -A "configparameters"

These configparameters are handled after the reading of the configuration file. See aide.conf (5) for more details on what to put here.

--verbose=verbosity\_level,-Vverbosity\_level

Controls how verbose aide is. Value must [0-255]. The default is 5. With no argument Value is set to 20. This parameter overrides the value set in a Configuration file.

--report=reporter,-r reporter

reporter is a URL which tells aide where to send its output. See aide.conf (5) section URLS for available values.

--version,-v

aide prints out its version number

--help,-h

Prints out the standard help message.

* **DIAGNOSTICS**

Normally, the exit status is 0 if no errors occurred. Except when the --check, --compare or --update command was requested, in which case the exit status is defined as:

1 \* (new files detected?) +

2 \* (removed files detected?) +

4 \* (changed files detected?)

Additionally, the following exit codes are defined for generic error conditions:

14 Error writing error

15 Invalid argument error

16 Unimplemented function error

17 Invalid configureline error

18 IO error

19 Version mismatch error

* **NOTES**

Please note that due to mmap issues, aide cannot be terminated with SIGTERM. Use

SIGKILL to terminate.

The checksums in the database and in the output are by default base64 encoded (see also report\_base16 option). To decode them you can use the following shell command:

echo <encoded\_checksum> | base64 -d | hexdump -v -e '32/1 "%02x" "\n" '

* **FILES**

/etc/aide/aide.conf

Default aide configuration file.

/etc/aide/aide.conf.d

Config snippets which are automatically concatenated to the configuration

file by update-aide.conf. This is a Debian extension.

aide.db

Default aide database.

aide.db.new

Default aide output database.

### Section I: How to Install AIDE in Linux

### Note:

### All commands for AIDE require root privileges

### If not root, use ‘sudo’ or ‘sudo -i’ for root shell

### AIDE is packaged in official repositories of mainstream Linux distributions, to install it run the command for your distribution using a package manager.

### 

### After installing it, the main configuration file is /etc/aide.conf. To view the installed version as well as compile time parameters, run the command below on your terminal:

### 

### Sample output

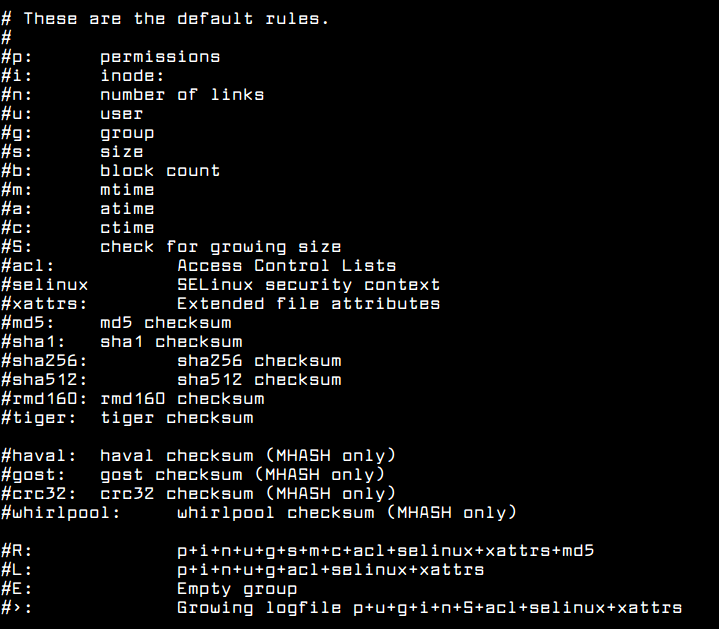
### 

**Section II: Understanding Default Aide Rules**

You can open the configuration using your favorite editor.

### # sudo gedit /etc/aide/aide.conf

It has directives that define the database location, report location, default rules, the directories/files to be included in the database.

****

* **Explanations:**

Using the above default rules, you can define new custom rules in the **aide.conf** file for example.

The following **PERMS** rule is used for access control only, it will detect any changes to file or directories based on file/directory permissions, user, group, access control permissions, SELinux context and file attributes.

PERMS = p+u+g+acl+selinux+xattrs

Following **CONTENT** will only check file content and file type.

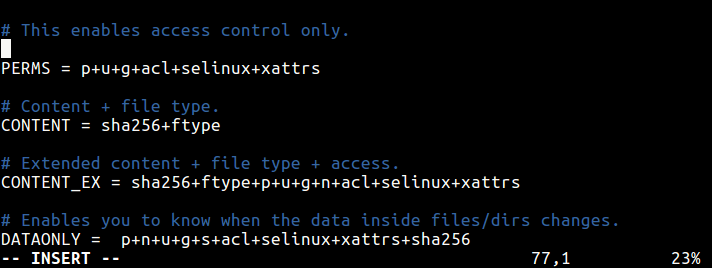
CONTENT = sha256+ftype

Following is an extended version of the previous rule, it checks extended content, file type and access.

CONTENT\_EX = sha256+ftype+p+u+g+n+acl+selinux+xattrs

The **DATAONLY** rule below will help detect any changes in data inside all files/directory.

DATAONLY = p+n+u+g+s+acl+selinux+xattrs+sha256



* Defining Rules to Watch Files and Directories

Once you have defined rules, you can specify the file and directories to watch. Considering the PERMS rule above, this definition will check permissions for all files in root directory.

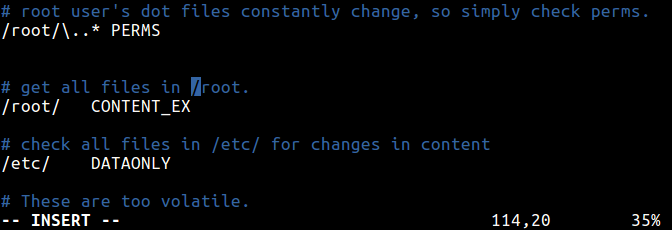
/root/\..\* PERMS

This will check all files in the /root directory for any changes.

/root/ CONTENT\_EX

To help you detect any changes in data inside all files/directory under /**etc**/, use this.

/etc/ DATAONLY

****

**Now you can close the file you opened.**

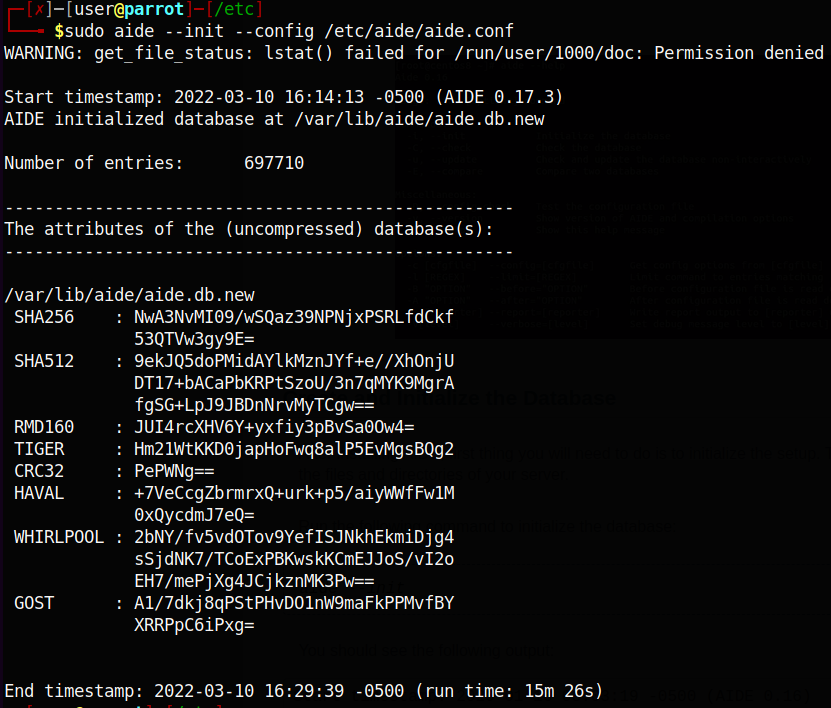
**Section III: Using AIDE to Check File and Directory Integrity in Linux**

Start by constructing a database against the checks that will be performed using --init flag. This is expected to be done before your system is connected to a network. The command below will create a database that contains all of the files that you selected in your configuration file.

# aideinit

**Note**:

* Even if you use ‘sudo’, you may get a permission warning but it will still work okay.
* It may take some time, e.g., 15 minutes.



Then rename the database to **/var/lib/aide/aide.db** before proceeding, using this command.

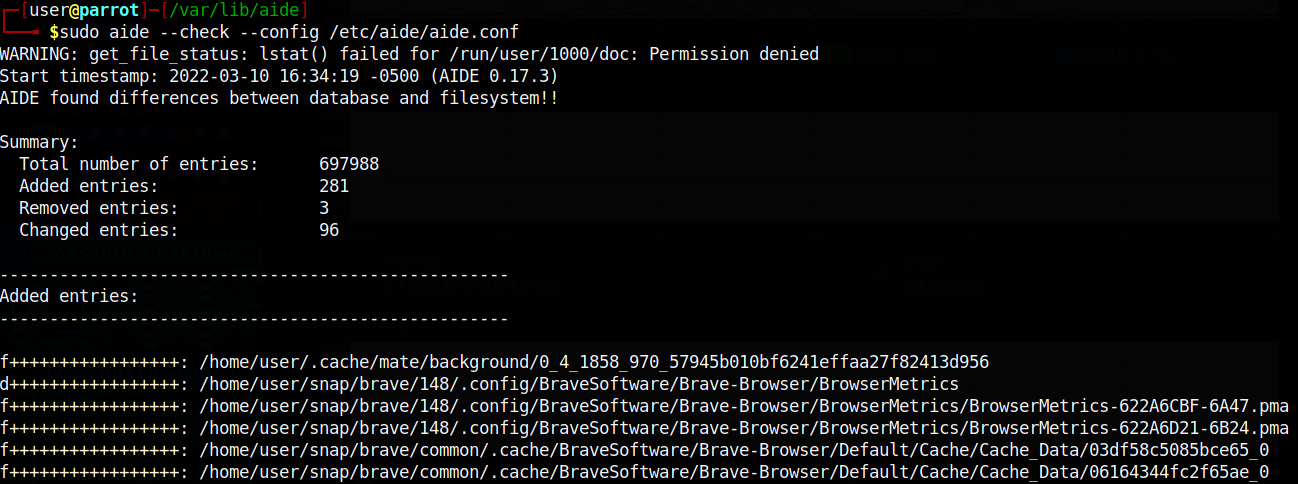
# mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db

It is recommended to move the database to a secure location possibly in a read-only media or on another machines, but ensure that you update the configuration file to read it from there.

After the database is created, you can now check the integrity of the files and directories using the --check flag.

# aide --check --config /etc/aide/aide.conf

It will read the snapshot in the database and compares it to the files/directories found you system disk. If it finds changes in places that you might not expect, it generates a report which you can then review.



Since no changes have been made to the file system, you will only get an output similar to the one above. Now try to create some files in the file system, in areas defined in the configuration file.

# vi /etc/script.sh

# touch all.txt

Then run a check once more, which should report the files added above. The output of this command depends on the parts of the file system you configured for checking; it can be lengthy overtime.

# aide --check --config /etc/aide/aide.conf

You need to run aide checks regularly, and in case of any changes to already selected files or addition of new file definitions in the configuration file, always update the database using the --update option:

# aide --update

After running a database update, to use the new database for future scans, always rename it to **/var/lib/aide/aide.db**:

# mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db

**Summary/Conclusions**

* One characteristic of most intrusion detection systems AIDE inclusive, is that they will not provide solutions to most security loop holes on a system. They however, assist in easing the intrusion response process by helping system administrators examine any changes to system files/directories. So, you should always be vigilant and keep updating your current security measures.
* It is highly recommended to keep the newly created database, the configuration file and the AIDE binary in a secure location such as read-only media (possible if you install from source).
* For additional security, consider signing the configuration and/or database.

**Hands-on exercise assignments to be submitted for grade:** [Total = 10 Points]

1. Configure **aide.conf** file with your own custom rules.
2. Initialize the database with your rule file.
3. Do any/suspicious modification, check for that/suspicious modifications after some time, e.g., a few hours/days.
4. Write a detailed lab report by adding screenshots of your experiment with AIDE. You may also include details, if you found any possible unwanted modifications found in the host file system.