Chi Zhang & Yuyang Zhang
CS6740 Network Security

Lab Report for Host-based Intrusion Detection System

1. To configure the AIDE, we first modify the /etc/aide/aide.conf to our needs and then run aide --init to start the initialization of AIDE database, which scans all the files in folders that were included in the aide.conf file and save their hash. Then we use "aide –c /etc/aide/aide.conf --check" in our shell file to figure out the four-hour integrity check.

The aide.conf file is attached in the directory.

2. Crontab and shell file is attached in the directory. mailto executes the mailing process. You could see the email in /var/mail/root as root user.

3. Email alert received after changing the file ndiff time in/usr/local/bin

```
team@nslabu:/usr/local/bin$ sudo touch -c -m -t 201703150000 ndiff
```

And the email alert(/var/changes.txt) goes as follows: (changes.txt is included in the directory)

From root@nslabu Wed Mar 15 17:16:52 2017
Return-Path: <root@nslabu>
Received: from nslabu (localhost [127.0.0.1])
    by nslabu (8.15.2/8.15.2/Debian-3) with ESMTP id v2FLGq7u005824
    for <root@nslabu>; Wed, 15 Mar 2017 17:16:52 -0400
Received: (from root@localhost)
    by nslabu (8.15.2/8.15.2/Submit) id v2FLGqi8005805
    for root; Wed, 15 Mar 2017 17:16:52 -0400
Date: Wed, 15 Mar 2017 17:16:52 -0400
Message-Id: <201703152116.v2FLGqi8005805@nslabu>
From: root@nslabu (Cron Daemon)
To: root@nslabu
Subject: Cron <root@nslabu> /var/lab6.sh
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>

AIDE 0.16a2-19-g16ed855 found differences between database and filesystem!!
Start timestamp: 2017-03-15 17:15:01 -0400

Summary:
   Total number of entries: 32482
   Added entries: 0
   Removed entries: 0
   Changed entries: 1

Changed entries:
---

f =.... c.. : /usr/local/bin/ndiff

Detailed information about changes:

File: /usr/local/bin/ndiff
   Ctime : 2017-03-15 11:47:49 -0400 | 2017-03-15 17:13:02 -0400

The attributes of the (uncompressed) database(s):

/var/lib/aide/aide.db
   MD5 : T5xwL9q0s9llWUaHaejtlg==
   SHA1 : yA6p7FJeKuYd77drJO2i2YUbYng=
   RMD160 : M3mnOdIdVD+11217zWZMtzr959c=
   TIGER : SZMxxmHTDfG5ALoUyjdNIW/fFhUmxAnu
   SHA256 : x10VpASdeq8QscpHE1l4HCWEvW+bFxwn
     mpyC131CvAU=
   SHA512 : Yt6rukaKQdgRS0GomqSpkqwLn3gmxpuP
     I2RItODOprRj5r5jL0FnpeMtG29cu4nZ
     5nMzX7EajUXdyJ8Gltdajg==
   CRC32 : 350/Rg==
   HAVAL : J+gwAtzG9r+yqHBEtiT/dgIlJK/FHsd4
     7bLCEoiFVCs=
   GOST : ZlyiqYi1Dx3hPGKMDYAzo3RLP2OfooSW
     CSy2E5/aMa0=
   WHIRLPOOL: oNNmEUcHsEiM04jhNT9YWTTD63RzXoqU
     qKynFKcxFvOqe8y6YFZpSiNF5nbbZ2+R
     dZ0XZOaPNGHaLwb50KH8LQ==

End timestamp: 2017-03-15 17:15:52 -0400 (run time: 0m 51s)

It is easy to see that only the change time(ctime) of /user/local/ndiff is changed between the new and the old database.

4. In your Linux VM's current AIDE configuration, name one way an attacker could prevent you from being alerted about system changes. In the worst-case scenario, if an attacker can gain root on your system, will file integrity checking suffice as an intrusion detection mechanism? If not, in what scenarios might it help secure the system?

The only way that an attacker could prevent us from being alerted about system changes is to change the files and recalculate the hashes and store them into the database before the 4-hour interval of alert. In the worst case, if the attacker can gain the root of the system, file integrity checking would not be sufficient to detect the intrusion. To improve this scenario, we could secure the hash by encrypting it and compare the encrypted hash to detect intrusion.