Hand-in assignment II: KEA System Security F2022 course

Assignment:
Demonstrate knowledge about forensics and system security. Focus is on disk image investigation, consider a hacked server - what happened.

Teacher will provide image which was made in this way:

- Install a Debian using a small disk size 10G
- Install a "root-kit" using the chmod +s on a copy of dash as described in Bishop book page 775. Using dash since sh is bash which prevents this!
- Create extra users not usually found on Debian, copies of root with uid 0 or new users with sudo rights

You are welcome to create your own "hacked server" using above method.

Create a report describing the following in main chapters:

- Company back story, create back story for your fictive company, half a page
- Analyze using forensics tools the hacked server
  Suggest using Sleuthkit and Autopsy browser based tool, simple and free
  Multiple other tools exist, you are free to choose
- Describe the system, what operating system is it running, maybe some more about when it was lasted updated etc.
- Search for your evidence, MAKE SURE to demonstrate how a user would find these - searching for SUID files is one method to document, looking into sudo config and user database is another
- Present a timeline of when the "hack" occurred, perhaps relate to when system was installed
- Present as much information as possible about the "malware" (the file found with SUID bit)
- Create a list of skills requirements for analyzing this environment. Consider job postings for similar jobs, and you may copy parts of that and adapt. Note down if you feel you have these skills, how much time would you require to learn these

The report should include the following sections at least:

- Title
- Confidentiality agreement – Write "Confidential" on each page
- Overview - description of the project

- Table of contents, page numbers, headlines - business report style
- Results - including method description and screenshots
- Executive summary
- Appendices

Formal requirements:
To be handed in at latest March 14, 2022 by fronter, or email to xhek@kea.dk

Teams up to 3 are allowed. Make sure to list team members in the report.

Expect PDF as A4, portrait mode around 15 pages with illustrations as needed. No more than 25 pages if 3 members.

Recommend to use a report template with table of contents, front matter, page numbers etc. You can use Word, Google Docs, LaTeX, whatever you feel most comfortable with.

You are NOT expected to spend more than 25-30 hours on this. Less is also OK.

The report is not graded, but feedback will be given.

Whats in the image:
Indeholdt i det hackede image er:

- En dash kopi med suid bitten sat
- Et par ekstra brugere
- den ene hacker har sudo rettigheder - hvordan er dette konfigureret?
- den anden hacker har vist user id `0` - hvad betyder det når vedkommende logger ind?

Check eventuelt også shadow password filen med John The Ripper - eftersom det er en fuldt opdateret Debian, så kan det være via dårlige passwords at der er foretaget indbrud?

Images:
The image files are at: https://files.kramse.org/.kea/

You can choose from:

Hand-in assignment II: KEA System Security F2022 course

1. Easiest - just the root file system, can be opened directly `debian-hacked-rootfs.img.gz`
   Same content as found in 2), but already extracted
2. Multiple files - in a Tar Gzip'ed archive `debian-hacked.tgz`
3. Another version, recreated in 2021 but essentially the same `debian-hacked-2021.img.gz`

Hints:
Consider this a proposal for your imaginary management team.

Help may be found in the Forensics Discovery book

Think about what you would like to receive if you were responsible for managing an incident and hiring people.

If you need more help contact me,

Henrik Kramselund, `xhek@kea.dk`

Hints for analyzing RAW Partition with LVM:

Dit udgangspunkt skal være en Debian med rigeligt plads.

0) Dvs lav evt en ny Debian med en 50Gb VM disk.

1) På denne Debian overfører du filen fra mig.

```
wget https://files.kramse.org/.kea/debian-hacked.tgz
```

2) Den udpakker du

```
tar zxvf debian-hacked.tgz
cd debian-hacked
```

3) Disk images Så har du et image af en disk fra en VM. Disk images indeholder typisk partitioner - dvs man har typisk op til 4 primære partioner

```
[ ---- Master Boot Record --- // starten af disken
[ Partition 1 typisk en slags boot disk      ---]
[ Partition 2 typisk en slags data partition ---]
[ Partition 3 typisk en swap - virtuel memory ]
```

Til at finde ud af denne information bruger man programmet: mmls

Den lister partitioner - herunder hvor de starter og stopper, størrelser

Med disse informationer kan man skære data ud fra filen.

Et program som "dd" kan med start og antal blokke - count skære ud.

Så derfor omregnes :

```
expr 501760 * 512
```

4) losetup

Når nu autopsy ikke forstår LVM, så må vi bruge Linux kernen til at mounte filen, og derved opnås adgang til data som et /dev device

sudo losetup -r -o 256901120 /dev/loop0 debian-hacked-root.img

Det gør at den volume group hacked-vg kan tilgås som device dm-0 og dm-1

```
user@KaliVM:~/QubesIncoming/dom0$ ls -l /dev/hacked-vg/
total 0
lrwxrwxrwx 1 root root 7 Mar  7 17:32 root -> ../dm-0
lrwxrwxrwx 1 root root 7 Mar  7 17:32 swap_1 -> ../dm-1
```

Vi skal bruge dm-0, dvs /dev/dm-0

5) Udskæring af partition

Jeg udførte testen selv for at sikre at man kan læse det endelige filsystem med autopsy, men da autopsy ikke forstår Linux Logical Volume Manager - som være data partition er, så skal denne skrælles ud.

These can now be read or used, for instance use it to create image file for the rootfs!

```
sudo dd if=/dev/dm-0 of=debian-hacked-rootfs.img
```

NU er der således en fil - root fs - fra den hackede server :-D

General feedback on the mandatory assignment

Read after doing this exercise!

One of the goals was to put you out of your comfort zone. Having to analyze a disk image, without the proper tool experience. Being in this position you had to research for yourself.

Fortunately this is an exercise, so not a real live critical system. You could relax more. Also, this mimics a normal situation, suddenly you have to do X, for the first time.

Learnings:
You probably learned that even though you could grasp the concepts, actually doing it required more. Attention to details, disks, partitions, etc. while tools might have some missing features - all modern Linux systems use LVM Logical Volume Manager, which Autopsy does NOT support.

You also learned that forensics is time consuming, and I did try to warn you. So if you did much more, then you probably should have asked for help from instructor or fellow students.

Side notes and history:
This exercise is partly inspired by the Bishop book, the "back door SUID shell", but also from a forensic challenge by The Honeynet Project.

This challenge was a Forensic Challenge: https://www.honeynet.org/challenges/forensic-challenge-2001-archive/

Take special note of the "results" http://www.all.net/journal/deception/www.honeynet.org/project.honeynet.org/challenge/results/index.html

> The average time spent in investigation turned out to be about 34 hours per person. That's a standard week's worth of work to clean up and deal with the mess left by an intruder in about a half an hour. That's about a 60:1 ratio! Using a standard upper-mid range annual salary figure of US$70,000 per investigator, that works out to be a cleanup cost of over US$2000 for a single incident. It is very likely one of dozens, if not hundreds, of intrusions just like it. As you will see when you read the analyses, this wasn't the first time this intruder did this.

They spent 60 times more analyzing the image, than the attacker spent! So your experience is not far from what others have experienced. Even though some people probably took the opportunity to learn, and used more hours.