Mandatory Assignment 1 for System Security course

This is a description for the mandatory assignment 1 in
KEA Kompetence System Security F2023

To be handed in at latest Juni 13, 2023 by email to xhek@kea.dk or hlk@zencurity.com

Note: this will be the 2nd mandatory assignment.

Overall goal

Get a formal business style report done, try out the hand-inn process.

Demonstrate knowledge about

Teacher will provide image 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

Students use forensics tools for analyzing this:

- Suggest using Sleuthkit and Autopsy browser based tool, simple and free
- 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)

The process should be possible to complete in less than 10 hours, but you are welcome to do more.

Deliverables

The assignment must be documented in a report sent to me, either on xhek@kea.dk or hlk@zencurity.com

Report must be a formal template including:

- Overview - description of the project
- Table of contents, page numbers, headlines - business report style
- Results - including method description and screenshots from the forensic tool
- Executive summary

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:

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 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