Hacking into an virtual appliance

Pavel Růžička <ruza@ruza.eu>

Brmlab
hackerspace Prague
Lightning talks

December 2015

brmlab hackerspace prague

There is no access into virtual appliance OS. Only this virtual console (tty1) and web interface (limited)

```
> vmware-mount -f xsuite.vmdk disk/
> ls -la disk/
-rw------- 1 ruza ruza 8589934592 Nov 21 04:03 flat

> sudo fdisk -l disk/flat
Disk disk/flat: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x1cde358c

Device      Boot    Start      End  Sectors   Size Id Type
disk/flat1  *          63 16450559 16450497   7.9G 83 Linux
disk/flat2  *    16450560 16771859   321300 156.9M 83 Linux
```

```
# echo '16450560*512' |bc
8422686720
# echo '63*512'|bc
32256

# losetup -o 32256 /dev/loop1 disk/flat        ## sda1
# losetup -o 8422686720 /dev/loop2 disk/flat   ## sda2

# losetup -a
/dev/loop1: [0071]:2 (disk/flat), offset 32256
/dev/loop2: [0071]:2 (disk/flat), offset 8422686720

# mount /dev/loop2 sda2   # /boot
# mount /dev/loop1 sda1   # /(root fs)
mount: /dev/loop1: can't read superblock
```

/boot (sda2)

```
-rwxr-xr-x 1 root root  600844 Oct 23  2014 aespipe
lrwxrwxrwx 1 root root      19 Oct  9 17:02 config -> config-3.13.2+xcd01
-rw-r--r-- 1 root root   42482 Oct  9 17:02 config-2.6.36.1+xcd07
-rw-r--r-- 1 root root   68649 Oct  9 17:02 config-3.13.2+xcd01
-rw-r--r-- 1 root root   16172 Oct  3  2014 default.kmap
-rwxr-xr-x 1 root root 1577188 Oct 23  2014 gpg
drwxr-xr-x 2 root root    1024 Nov 22 22:43 grub
-rw-r--r-- 1 root root    6336 Oct  3  2014 initrd.gz
-rwxr-xr-x 1 root root    5672 Oct 23  2014 insmod
-rwxr-xr-x 1 root root  113248 Oct 23  2014 ld-linux.so.2
-rw-r--r-- 1 root root   10712 Oct  3  2014 libcfont.so.0
-rw-r--r-- 1 root root   72816 Oct  3  2014 libconsole.so.0
-rwxr-xr-x 1 root root 1413540 Oct 23  2014 libc.so.6
-rw-r--r-- 1 root root   17024 Oct  3  2014 libctutils.so.0
-rwxr-xr-x 1 root root   35048 Oct 23  2014 loadkeys
-rwxr-xr-x 1 root root   62654 Oct 23  2014 losetup
drwxr-xr-x 2 root root    1024 Oct 13 17:54 modules-3.13.2+xcd01
-rw-r--r-- 1 root root    9192 Oct  3  2014 pubring.gpg
-rw-r--r-- 1 root root    3630 Oct  3  2014 rootkey.gpg
-rw-r--r-- 1 root root    4899 Oct  3  2014 secring.gpg
lrwxrwxrwx 1 root root      23 Oct  9 17:02 System.map -> System.map-3.13.2+xcd01
-rw-r--r-- 1 root root 1639369 Oct  9 17:02 System.map-2.6.36.1+xcd07
-rw-r--r-- 1 root root 2080641 Oct  9 17:02 System.map-3.13.2+xcd01
lrwxrwxrwx 1 root root      20 Oct  9 17:02 vmlinuz -> vmlinuz-3.13.2+xcd01
-rw-r--r-- 1 root root 2946720 Oct  9 17:02 vmlinuz-2.6.36.1+xcd07
-rw-r--r-- 1 root root 3789600 Oct  9 17:02 vmlinuz-3.13.2+xcd01
```

- **pubring.gpg**: GPG key public ring
- **secring.gpg**: PGP011Secret Key 4096b created on Mon Sep 24 14:50:43 2012 RSA (Encrypt or Sign) e=65537 hashed CAST5 (128 bit key) Salted&Iterated S2K SHA-1
- **rootkey.gpg**: PGP RSA encrypted session key keyid: BABABABA EAEAEAEA RSA (Encrypt or Sign) 4096b

```
# gpg --import rootkey.gpg
gpg: key 321ABCDE: secret key imported
gpg: key 321ABCDE: public key imported
gpg: Total number processed: 1
gpg:                imported: 1  (RSA: 1)
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

brmlab hackerspace prague

GRUB

- ignores kernel parameters like rdinit=/bin/bash

```
root (hd0,1)
kernel /vmlinuz ro console=ttyS0,115200n1 acpi=force fips=1
initrd /initrd.gz
```

- but we can read serial console output (add serial in Vmware, or using ”qemu -serial stdio”)

```
qemu-system-x86_64 -kernel vmlinuz -initrd initrd.gz
 -append "ro console=ttyS0,115200n1 acpi=force fips=1"
 -serial stdio -hda ../disk/flat

EXT3-fs (sda2): mounted filesystem with ordered data mode
loadkeys: error reading keyboard mode
Command "/lib/loadkeys /lib/default.kmap" returned error
loop: loaded (max 8 devices)
```

Encrypted file system, please supply correct password to continue

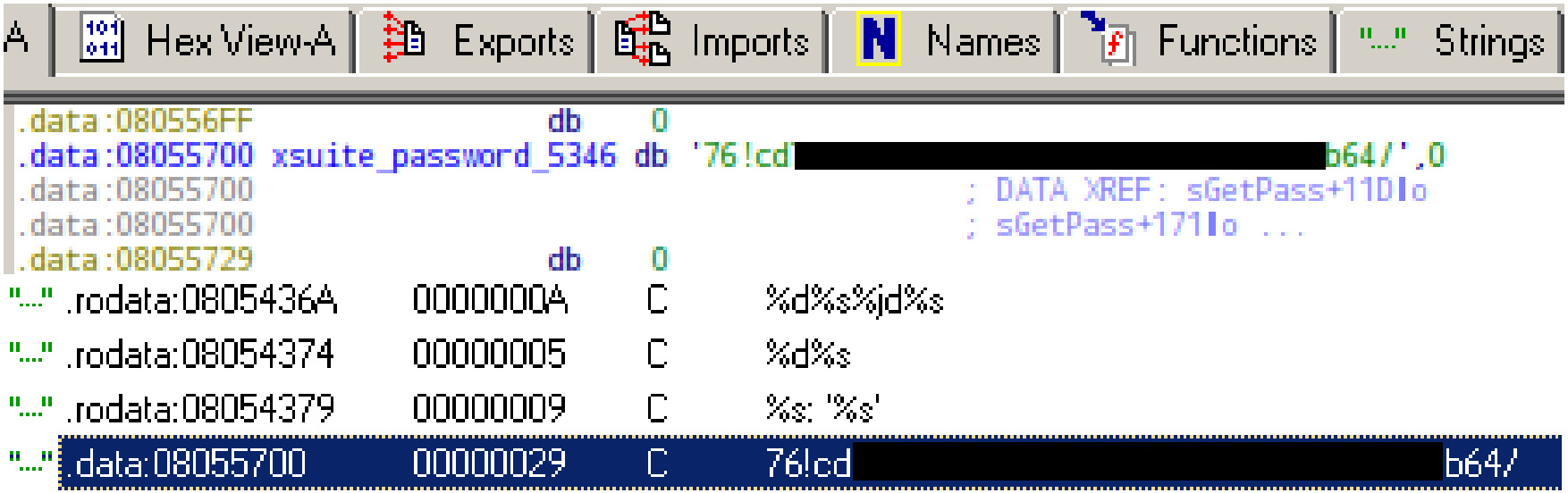
```
kjournald starting.  Commit interval 5 seconds
EXT3-fs (loop5): mounted filesystem with ordered data mode
Switching to encrypted root completed successfully
^MINIT: version 2.86 booting^M
EXT3-fs (loop5): using internal journal
```

```
# unpack initrd.gz and investigating init binary
# it is not possible to strace init easily
strings init |less
...
/lib/insmod /lib/modules-
/loop
/lib/losetup -e AES128   -I 0
 -K /lib/rootkey.gpg -G /lib
 /dev/loop5 /dev/sda1
/new-root
Mounting /dev/loop5 failed
/lib/losetup -d /dev/loop5
chdir() to /new-root failed
Overmounting root failed
chroot() to new root failed
..
```

- so we would like to probably run something like ”./losetup -e AES128 -I 0 -K rootkey.gpg -G ./dev/loop2 /dev/loop0” ioctl: LOOP_SET_STATUS: Invalid argument, requested cipher or key length (128 bits) not supported by kernel
- having newer Linux OS we could be able do the similar like this ”gpg –decrypt ./rootkey.gpg|cryptsetup loopaesOpen /dev/loop2 xsuit –key-size 128 **–key-file=-**” You need a passphrase to unlock the secret key for user: 4096-bit RSA key, ID 2223334E, created 2012-01-24 (main key ID 321ABCDE) gpg: gpg-agent is not available in this session Enter passphrase:
- but we dont know the passphrase needed

Staring at bits

- observing /boot/losetup as an ELF binary file in ”IDA Free”for few hours, we can see passphrase is saved as an symbol table object of the length 41 chars at the address 0x8055700!



- readelf –symbols /tmp/losetup
  Symbol table '.symtab' contains 268 entries:
  Num: Value Size Type Bind Vis Ndx Name
  65:**08055700** 41 OBJECT LOCAL DEFAULT 24 xsuite_password.5346
- gdb -q -ex 'x/s **0x8055700**' losetup -ex quit
  Reading symbols from losetup...done.
  0x8055700 xsuite_password.5346:
  '76acd758bbiqqpoiew2932ad-e7ed3289bd23642'
- echo '76acd758bbiqqpoiew2932ad-e7ed3289bd23642' | gpg **–passphrase-fd 0 -d rootkey.gpg**| tail -n 2
  vg1zYE2MDelq9UeKx3GXdtk/osBHIVhTlnD+4wrturmaNE91RII
  sZG8OXwAOZRm9n5STzc2ouyY0GglyuLZi/TLD+x5siATwB2FYF
  .. looks like a valid output

```
echo '76acd758bbiqqpoiew2932ad-e7ed3289bd23642'|gpg --passphrase-fd 0 -d /tmp/rootkey.gpg | cryptsetup loopaesOpen /dev/loop1 xsuite –key-size 128 –key-file=-
Reading passphrase from file descriptor 0

You need a passphrase to unlock the secret key for user:
4096-bit RSA key, ID 2223334E, created 2012-01-24 (main key ID 321ABCDE)

gpg: encrypted with 4096-bit RSA key, ID 2223334E, created 2012-01-24

mount /dev/mapper/xsuite /mnt/xsuite && ls -la /mnt/xsuite
drwxr-xr-x 2 root root 2048 Sep 22 2010 bin
drwxr-xr-x 2 root root 2048 Oct 9 17:02 boot
... SUCCESS! (root fs decrypted)
```

so we are able to remove password for root by editing /etc/shadow:
root:1CK2e0SmU$AO/cLzBOXqMRRNXv.rvHx/:14330:0:99999:7:::
root::14330:0:99999:7:::

and the whole process can be automated
https://github.com/ruzaq/decrypt-gpg-encrypted-rootfs

```
# ./mount-xsuite-disk.sh
## VMware FLAT disk mount..                                    [ OK ]
Disks with mounted partitions:
       xsuite.vmdk /data/virtuals/xsuite/disk/flat

## creating nodes..   sda1                                     [ OK ]
                      sda2                                     [ OK ]
/dev/loop1: [0074]:2 (xsuite/disk/flat), offset 32256
/dev/loop2: [0074]:2 (xsuite/disk/flat), offset 8422686720

## Mounting /boot..                                           [ OK ]
/dev/loop2 on xsuite/BOOT type ext3 (rw,relatime,data=ordered)
```

```
## Opening ELF binary xsuite/BOOT/losetup symbol table
## looking up for .data.08055700:.symtab.xsuite_password[ OK ]
Passphrase to decrypt key xsuite/BOOT/rootkey.gpg
is .. 76acd758bbiqqpoiew2932ad-e7ed3289bd23642
## Decrypting ROOTFS..                                    [ OK ]
/dev/mapper/xsuite-root is active.
  type:    LOOPAES
  cipher:  aes:64-cbc-lmk
  keysize: 128 bits
  device:  /dev/loop1
  loop:    /data/virtuals/xsuite/disk/flat
  offset:  0 sectors
  size:    16777153 sectors
  mode:    read/write
## Mounting rootfs..                                      [ OK ]
/dev/mapper/xsuite-root on xsuite/ROOT type ext3
Install busybox TELNETD backdoor? [Y/n]  [Enter] means No
```

busybox, multi-call binary

ldd $which busybox
not a dynamic executable

- busybox has applets, shitload of features

```
/sbin/busybox telnetd

netstat -ntalp|grep :23
tcp6 0 0 :::23 :::* LISTEN 18605/busybox

killall busybox
```

brmlab hackerspace prague

Summary

- init/rdinit kernel parameter hack ignored
- loopAES incompatibilities, AES128 bit
- hard to strace init process
- keyfile to decrypt rootfs GnuPG encrypted, passphrase hardcoded in losetup binary
- deamons defaults to bind to localhost

brmlab hackerspace prague