# WAYS TO AUTOMATE TESTING LINUX KERNEL EXPLOITS

---

Mikhail Klementev

ZeroNights 2018

# $ agenda

- What’s the problem?
- Solution
- Key features
- Demo
- Future plans

# What’s the problem?

```
$ qemu-system-x86_64 \
        -kernel vmlinuz-4.18.8 \
        -hda sid.img \
        -append 'root=/dev/sda console=ttyS0 rw'

$ vagrant up
$ tail -f ubuntu-bionic-18.04-cloudimg-console.log
```

```
[  269.912918] CPU: 1 PID: 1858 Comm: bash Not tainted 4.20.0-rc2+ #1
[  269.913841] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.11.0-1.fc284
[  269.915144] RIP: 0010:sysrq_handle_crash+0xd/0x20
[  269.915818] Code: 41 5f e9 d6 6a cb ff 48 89 ef e8 fe fb ff ff e9 bd fe ff ff 90 90 9f
[  269.918416] RSP: 0018:ffffac2e805d7df8 EFLAGS: 00010286
[  269.919115] RAX: ffffffffad844410 RBX: 0000000000000063 RCX: 0000000000000000
[  269.920037] RDX: 0000000000000000 RSI: ffff9606df315418 RDI: 0000000000000063
[  269.920969] RBP: ffffffffae6a90c0 R08: 0000000000000000 R09: 0000000000000007
[  269.921885] R10: 0000000000000000 R11: ffffffffaec9b9ad R12: 0000000000000007
[  269.922803] R13: 0000000000000000 R14: 000055f33fff0f50 R15: 0000000000000000
[  269.923733] FS:  00007fbfddd78740(0000) GS:ffff9606df300000(0000) knlGS:0000000000000000
[  269.924704] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[  269.925547] CR2: 0000000000000000 CR3: 0000000d3972000 CR4: 00000000000006e0
[  269.926435] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[  269.927321] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[  269.928211] Call Trace:
[  269.928533]  __handle_sysrq+0x7f/0x130
[  269.929014]  write_sysrq_trigger+0x26/0x30
[  269.929535]  proc_reg_write+0x37/0x70
[  269.930010]  ? __cond_resched+0x10/0x40
[  269.930485]  __vfs_write+0x31/0x180
[  269.930939]  ? selinux_file_permission+0x118/0x130
[  269.931541]  ? security_file_permission+0x27/0xb0
[  269.932131]  vfs_write+0xa8/0x190
[  269.932551]  ksys_write+0x4d/0xb0
[  269.932977]  do_syscall_64+0x43/0xf0
[  269.933435]  entry_SYSCALL_64_after_hwframe+0x44/0xa9
[  269.934080] RIP: 0033:0x7fbfdde642a4
[  269.934557] Code: 89 02 48 c7 c0 ff ff ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 66 90 45
[  269.936924] RSP: 002b:00007ffca72d5448 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
[  269.937823] RAX: ffffffffffffffda RBX: 0000000000000002 RCX: 00007fbfdde642a4
[  269.938676] RDX: 0000000000000002 RSI: 000055f33fff0f50 RDI: 0000000000000001
[  269.939541] RBP: 000055f33fff0f50 R08: 0000000000000000 R09: 000055f33fffaa80
[  269.940354] R10: 0000000000000000 R11: 0000000000000246 R12: 00007fbfddf33760
[  269.941174] R13: 0000000000000002 R14: 00007fbfddf2e760 R15: 0000000000000002
[  269.941988] Modules linked in:
[  269.942335] CR2: 0000000000000000
[  269.942759] ---[ end trace 3d8985002a7d0f75 ]---
[  269.943446] RIP: 0010:sysrq_handle_crash+0xd/0x20
[  269.944151] Code: 41 5f e9 d6 6a cb ff 48 89 ef e8 fe fb ff ff e9 bd fe ff ff 90 90 9f
[  269.946735] RSP: 0018:ffffac2e805d7df8 EFLAGS: 00010286
[  269.947495] RAX: ffffffffad844410 RBX: 0000000000000063 RCX: 0000000000000000
[  269.948376] RDX: 0000000000000000 RSI: ffff9606df315418 RDI: 0000000000000063
[  269.949180] RBP: ffffffffae6a90c0 R08: 0000000000000000 R09: 0000000000000007
[  269.949962] R10: 0000000000000000 R11: ffffffffaec9b9ad R12: 0000000000000007
[  269.950730] R13: 0000000000000000 R14: 000055f33fff0f50 R15: 0000000000000000
[  269.951565] FS:  00007fbfddd78740(0000) GS:ffff9606df300000(0000) knlGS:0000000000000000
[  269.952464] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[  269.953135] CR2: 0000000000000000 CR3: 0000000d3972000 CR4: 00000000000006e0
[  269.953992] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[  269.954835] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[  269.955662] Kernel panic - not syncing: Fatal exception
[  269.956464] Kernel Offset: 0x2c400000 from 0xffffffff81000000 (relocation range: 0xff)
[  269.957553] ---[ end Kernel panic - not syncing: Fatal exception ]---
```

```
loop4           tty15           tty5            vcsa5
loop5           tty16           tty50           vcsa6
loop6           tty17           tty51           vcsu
loop7           tty18           tty52           vcsu1
mapper/         tty19           tty53           vcsu2
md0             tty2            tty54           vcsu3
mem             tty20           tty55           vcsu4
memory_bandwidth  tty21         tty56           vcsu5
mqueue/         tty22           tty57           vcsu6
network_latency   tty23         tty58           vga_arbiter
network_throughput  tty24       tty59           zero
null            tty25           tty6
root@localhost:~# echo /proc/sys/kernel/
acct                            perf_event_max_contexts_per_stack
acpi_video_flags                perf_event_max_sample_rate
auto_msgmni                     perf_event_max_stack
bootloader_type                 perf_event_mlock_kb
bootloader_version              perf_event_paranoid
cad_pid                         pid_max
cap_last_cap                    poweroff_cmd
core_pattern                    print-fatal-signals
core_pipe_limit                 printk
core_uses_pid                   printk_delay
ctrl-alt-del                    printk_devkmsg
dmesg_restrict                  printk_ratelimit
domainname                      printk_ratelimit_burst
ftrace_dump_on_oops             pty/
hostname                        random/
hotplug                         randomize_va_space
io_delay_type                   real-root-dev
kexec_load_disabled             sched_child_runs_first
keys/                           sched_rr_timeslice_ms
kptr_restrict                   sched_rt_period_us
max_lock_depth                  sched_rt_runtime_us
modprobe                        seccomp/
modules_disabled                sem
msgmax                          sg-big-buff
msgmnb                          shm_rmid_forced
msgmni                          shmall
ngroups_max                     shmmax
osrelease                       shmmni
ostype                          sysctl_writes_strict
overflowgid                     sysrq
overflowuid                     tainted
panic                           threads-max
panic_on_io_nmi                 timer_migration
panic_on_oops                   traceoff_on_warning
panic_on_rcu_stall              tracepoint_printk
panic_on_stackoverflow          unknown_nmi_panic
panic_on_unrecovered_nmi        usermodehelper/
panic_on_warn                   version
perf_cpu_time_max_percent
root@localhost:~# echo 1 > /proc/sys/kernel/sysrq
root@localhost:~# echo c > /proc/sysrq-trigger
```

```
user@localhost /tmp/test $ vagrant ssh
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-34-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Nov 14 22:31:51 UTC 2018

  System load:  0.58                Processes:             109
  Usage of /:   14.1% of 9.63GB   Users logged in:       0
  Memory usage: 16%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%


  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

101 packages can be updated.
41 updates are security updates.


vagrant@ubuntu-bionic:~$ sudo -i
root@ubuntu-bionic:~# echo 10 > /proc/sys/kernel/printk
root@ubuntu-bionic:~# echo c > /proc/sysrq-trigger
root@ubuntu-bionic:~# echo 1 > /proc/sys/kernel/sysrq
root@ubuntu-bionic:~# echo c > /proc/sysrq-trigger
```

```
[  256.510789] sysrq: SysRq : Trigger a crash
[  256.563064] BUG: unable to handle kernel NULL pointer dereference at 0000000000000000
[  256.673584] IP: sysrq_handle_crash+0x16/0x20
[  256.798049] PGD 0 P4D 0
[  256.879353] Oops: 0002 [#1] SMP PTI
[  256.949456] Modules linked in: vboxvideo(OE) drm_kms_helper ttm drm fb_sys_fops syscopyarea sysfillrect sysimgblt vboxsf(OE) vboxguest(OE) lsofs crct10dif_pclmul crc32_pclmul ghash_clmulni_intel input_leds serio_raw video sch_fq_codel ib_iser rdma_cm iw_cm ib_cm ib_core iscsi_tcp libiscsi_tcp libiscsi scsi_transport_iscsi ip_tables x_tables autofs4 btrfs zstd_compress raid10 raid456 async_raid6_recov async_memcpy async_pq async_xor async_tx xor raid6_pq libcrc32c raid1 raid0 multipath linear nptspi scsi_transport_spi mptscsih aesni_intel aes_x86_64 crypto_simd cryptd glue_helper psmouse e1000 mptbase [last unloaded: vboxguest]
[  257.577693] CPU: 1 PID: 13488 Comm: bash Tainted: G           OE    4.15.0-34-generic #37-Ubuntu
[  257.779883] Hardware name: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[  258.029723] RIP: 0010:sysrq_handle_crash+0x16/0x20
[  258.145386] RSP: 0018:ffffa686c06ebe30 EFLAGS: 00010286
[  258.270143] RAX: ffffffff8ebe7710 RBX: ffffffff8f873a0 RCX: 0000000000000000
[  258.479599] RDX: 0000000000000000 RSI: ffff90d7bfd16498 RDI: 0000000000000063
[  258.681489] RBP: ffffa686c06ebe30 R08: 0000000000000000 R09: 00000000000001f8
[  258.865382] R10: 0000000000000001 R11: 00000000ffffffff R12: 0000000000000007
[  259.109868] R13: 0000000000000063 R14: 0000000000000002 R15: ffff90d7b9dad400
[  259.319693] FS:  00007ff77af4b740(0000) GS:ffff90d7bfd00000(0000) knlGS:0000000000000000
[  259.599403] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[  259.686753] CR2: 0000000000000000 CR3: 000000003b374003 CR4: 00000000000606e0
[  259.860379] Call Trace:
[  259.860951]  __handle_sysrq+0x9f/0x170
[  259.861809]  write_sysrq_trigger+0x34/0x40
[  259.862657]  proc_reg_write+0x45/0x70
[  259.867033]  __vfs_write+0x1b/0x40
[  259.867744]  vfs_write+0xb1/0x1a0
[  259.868426]  SyS_write+0x55/0xc0
[  259.869106]  do_syscall_64+0x73/0x130
[  259.869861]  entry_SYSCALL_64_after_hwframe+0x3d/0xa2
[  259.871228] RIP: 0033:0x7ff77a621154
[  259.872312] RSP: 002b:00007ffe52e408a8 EFLAGS: 00000246 ORIG_RAX: 0000000000000001
[  259.874194] RAX: ffffffffffffffda RBX: 0000000000000002 RCX: 00007ff77a6211540
[  260.060439] RDX: 0000000000000002 RSI: 000055f763b39d10 RDI: 0000000000000001
[  260.216246] RBP: 000055f763b39d10 R08: 000000000000000a R09: 0000000000000001
[  260.397720] R10: 000000000000000a R11: 0000000000000246 R12: 00007ff77a8fd760
[  260.630070] R13: 0000000000000002 R14: 00007ff77a8f92a0 R15: 00007ff77a8fd760
[  260.829581] Code: e7 e8 9f fb ff ff e9 c0 fe ff ff 90 90 90 90 90 90 90 90 90 0f 1f 44 00 00 55 c7 05 e8 49 36 01 01 00 00 00 48 89 e5 0f ae f8 <c6> 04 25 00 00 00 00 01 5d c3 0f 1f 44 00 00 55 c7 05 c0 af e7
[  260.983510] RIP: sysrq_handle_crash+0x16/0x20 RSP: ffffa686c06ebe30
[  260.985137] CR2: 0000000000000000
[  260.986312] ---[ end trace a7bd8af3e6d95b02 ]---
[  260.987649] Kernel panic - not syncing: Fatal exception
[  260.989783] Kernel Offset: 0xd600000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[  260.992584] ---[ end Kernel panic - not syncing: Fatal exception
```

```
System.map-4.4.0-45-generic   abi-4.4.0-134-generic        config-4.4.0-104-generic  initrd.img-4.15.0-13-generic  retpoline-4.4.0-116-generic   vmlinuz-4.4.0-77-generic
System.map-4.4.0-47-generic   abi-4.4.0-135-generic        config-4.4.0-108-generic  initrd.img-4.15.0-15-generic  retpoline-4.4.0-119-generic   vmlinuz-4.4.0-78-generic
System.map-4.4.0-51-generic   abi-4.4.0-137-generic        config-4.4.0-109-generic  initrd.img-4.15.0-20-generic  retpoline-4.4.0-121-generic   vmlinuz-4.4.0-79-generic
System.map-4.4.0-53-generic   abi-4.4.0-138-generic        config-4.4.0-112-generic  initrd.img-4.15.0-22-generic  retpoline-4.4.0-122-generic   vmlinuz-4.4.0-81-generic
System.map-4.4.0-57-generic   abi-4.4.0-21-generic         config-4.4.0-116-generic  initrd.img-4.15.0-23-generic  retpoline-4.4.0-124-generic   vmlinuz-4.4.0-83-generic
System.map-4.4.0-59-generic   abi-4.4.0-22-generic         config-4.4.0-119-generic  initrd.img-4.15.0-24-generic  retpoline-4.4.0-127-generic   vmlinuz-4.4.0-87-generic
System.map-4.4.0-62-generic   abi-4.4.0-24-generic         config-4.4.0-121-generic  initrd.img-4.15.0-29-generic  retpoline-4.4.0-128-generic   vmlinuz-4.4.0-89-generic
System.map-4.4.0-63-generic   abi-4.4.0-28-generic         config-4.4.0-122-generic  initrd.img-4.15.0-30-generic  retpoline-4.4.0-130-generic   vmlinuz-4.4.0-91-generic
System.map-4.4.0-64-generic   abi-4.4.0-31-generic         config-4.4.0-124-generic  initrd.img-4.15.0-32-generic  retpoline-4.4.0-131-generic   vmlinuz-4.4.0-92-generic
System.map-4.4.0-66-generic   abi-4.4.0-34-generic         config-4.4.0-127-generic  initrd.img-4.15.0-33-generic  retpoline-4.4.0-133-generic   vmlinuz-4.4.0-93-generic
System.map-4.4.0-67-generic   abi-4.4.0-36-generic         config-4.4.0-128-generic  initrd.img-4.15.0-34-generic  retpoline-4.4.0-134-generic   vmlinuz-4.4.0-96-generic
System.map-4.4.0-70-generic   abi-4.4.0-38-generic         config-4.4.0-130-generic  initrd.img-4.15.0-36-generic  retpoline-4.4.0-135-generic   vmlinuz-4.4.0-97-generic
System.map-4.4.0-71-generic   abi-4.4.0-42-generic         config-4.4.0-131-generic  initrd.img-4.15.0-38-generic  retpoline-4.4.0-137-generic   vmlinuz-4.4.0-98-generic
System.map-4.4.0-72-generic   abi-4.4.0-43-generic         config-4.4.0-133-generic  initrd.img-4.4.0-101-generic  retpoline-4.4.0-138-generic   vmlinuz-4.8.0-34-generic
System.map-4.4.0-75-generic   abi-4.4.0-45-generic         config-4.4.0-134-generic  initrd.img-4.4.0-103-generic  vmlinuz-4.10.0-14-generic     vmlinuz-4.8.0-36-generic
System.map-4.4.0-77-generic   abi-4.4.0-47-generic         config-4.4.0-135-generic  initrd.img-4.4.0-104-generic  vmlinuz-4.10.0-19-generic     vmlinuz-4.8.0-39-generic
System.map-4.4.0-78-generic   abi-4.4.0-51-generic         config-4.4.0-137-generic  initrd.img-4.4.0-108-generic  vmlinuz-4.10.0-20-generic     vmlinuz-4.8.0-41-generic
System.map-4.4.0-79-generic   abi-4.4.0-53-generic         config-4.4.0-138-generic  initrd.img-4.4.0-109-generic  vmlinuz-4.10.0-21-generic     vmlinuz-4.8.0-42-generic
System.map-4.4.0-81-generic   abi-4.4.0-57-generic         config-4.4.0-21-generic   initrd.img-4.4.0-112-generic  vmlinuz-4.10.0-22-generic     vmlinuz-4.8.0-44-generic
System.map-4.4.0-83-generic   abi-4.4.0-59-generic         config-4.4.0-22-generic   initrd.img-4.4.0-116-generic  vmlinuz-4.10.0-24-generic     vmlinuz-4.8.0-45-generic
System.map-4.4.0-87-generic   abi-4.4.0-62-generic         config-4.4.0-24-generic   initrd.img-4.4.0-119-generic  vmlinuz-4.10.0-26-generic     vmlinuz-4.8.0-46-generic
System.map-4.4.0-89-generic   abi-4.4.0-63-generic         config-4.4.0-28-generic   initrd.img-4.4.0-121-generic  vmlinuz-4.10.0-27-generic     vmlinuz-4.8.0-49-generic
System.map-4.4.0-91-generic   abi-4.4.0-64-generic         config-4.4.0-31-generic   initrd.img-4.4.0-122-generic  vmlinuz-4.10.0-28-generic     vmlinuz-4.8.0-51-generic
System.map-4.4.0-92-generic   abi-4.4.0-66-generic         config-4.4.0-34-generic   initrd.img-4.4.0-124-generic  vmlinuz-4.10.0-30-generic     vmlinuz-4.8.0-52-generic
System.map-4.4.0-93-generic   abi-4.4.0-67-generic         config-4.4.0-36-generic   initrd.img-4.4.0-127-generic  vmlinuz-4.10.0-32-generic     vmlinuz-4.8.0-53-generic
System.map-4.4.0-96-generic   abi-4.4.0-70-generic         config-4.4.0-38-generic   initrd.img-4.4.0-128-generic  vmlinuz-4.10.0-33-generic     vmlinuz-4.8.0-54-generic
System.map-4.4.0-97-generic   abi-4.4.0-71-generic         config-4.4.0-42-generic   initrd.img-4.4.0-130-generic  vmlinuz-4.10.0-35-generic     vmlinuz-4.8.0-56-generic
System.map-4.4.0-98-generic   abi-4.4.0-72-generic         config-4.4.0-43-generic   initrd.img-4.4.0-131-generic  vmlinuz-4.10.0-37-generic     vmlinuz-4.8.0-58-generic
System.map-4.8.0-34-generic   abi-4.4.0-75-generic         config-4.4.0-45-generic   initrd.img-4.4.0-133-generic  vmlinuz-4.10.0-38-generic
root@e3ffc816a4ae:/# ls /boot/vmlinuz-4.*
/boot/vmlinuz-4.10.0-14-generic  /boot/vmlinuz-4.13.0-26-generic  /boot/vmlinuz-4.4.0-103-generic  /boot/vmlinuz-4.4.0-34-generic  /boot/vmlinuz-4.4.0-83-generic
/boot/vmlinuz-4.10.0-19-generic  /boot/vmlinuz-4.13.0-31-generic  /boot/vmlinuz-4.4.0-104-generic  /boot/vmlinuz-4.4.0-36-generic  /boot/vmlinuz-4.4.0-87-generic
/boot/vmlinuz-4.10.0-20-generic  /boot/vmlinuz-4.13.0-32-generic  /boot/vmlinuz-4.4.0-108-generic  /boot/vmlinuz-4.4.0-38-generic  /boot/vmlinuz-4.4.0-89-generic
/boot/vmlinuz-4.10.0-21-generic  /boot/vmlinuz-4.13.0-36-generic  /boot/vmlinuz-4.4.0-109-generic  /boot/vmlinuz-4.4.0-42-generic  /boot/vmlinuz-4.4.0-91-generic
/boot/vmlinuz-4.10.0-22-generic  /boot/vmlinuz-4.13.0-37-generic  /boot/vmlinuz-4.4.0-112-generic  /boot/vmlinuz-4.4.0-43-generic  /boot/vmlinuz-4.4.0-92-generic
/boot/vmlinuz-4.10.0-24-generic  /boot/vmlinuz-4.13.0-38-generic  /boot/vmlinuz-4.4.0-116-generic  /boot/vmlinuz-4.4.0-45-generic  /boot/vmlinuz-4.4.0-93-generic
/boot/vmlinuz-4.10.0-26-generic  /boot/vmlinuz-4.13.0-39-generic  /boot/vmlinuz-4.4.0-119-generic  /boot/vmlinuz-4.4.0-47-generic  /boot/vmlinuz-4.4.0-96-generic
/boot/vmlinuz-4.10.0-27-generic  /boot/vmlinuz-4.13.0-41-generic  /boot/vmlinuz-4.4.0-121-generic  /boot/vmlinuz-4.4.0-51-generic  /boot/vmlinuz-4.4.0-97-generic
/boot/vmlinuz-4.10.0-28-generic  /boot/vmlinuz-4.13.0-43-generic  /boot/vmlinuz-4.4.0-122-generic  /boot/vmlinuz-4.4.0-53-generic  /boot/vmlinuz-4.4.0-98-generic
/boot/vmlinuz-4.10.0-30-generic  /boot/vmlinuz-4.13.0-45-generic  /boot/vmlinuz-4.4.0-124-generic  /boot/vmlinuz-4.4.0-57-generic  /boot/vmlinuz-4.8.0-34-generic
/boot/vmlinuz-4.10.0-32-generic  /boot/vmlinuz-4.15.0-13-generic  /boot/vmlinuz-4.4.0-127-generic  /boot/vmlinuz-4.4.0-59-generic  /boot/vmlinuz-4.8.0-36-generic
/boot/vmlinuz-4.10.0-33-generic  /boot/vmlinuz-4.15.0-15-generic  /boot/vmlinuz-4.4.0-128-generic  /boot/vmlinuz-4.4.0-62-generic  /boot/vmlinuz-4.8.0-39-generic
/boot/vmlinuz-4.10.0-35-generic  /boot/vmlinuz-4.15.0-20-generic  /boot/vmlinuz-4.4.0-130-generic  /boot/vmlinuz-4.4.0-63-generic  /boot/vmlinuz-4.8.0-41-generic
/boot/vmlinuz-4.10.0-37-generic  /boot/vmlinuz-4.15.0-22-generic  /boot/vmlinuz-4.4.0-131-generic  /boot/vmlinuz-4.4.0-64-generic  /boot/vmlinuz-4.8.0-42-generic
/boot/vmlinuz-4.10.0-38-generic  /boot/vmlinuz-4.15.0-23-generic  /boot/vmlinuz-4.4.0-133-generic  /boot/vmlinuz-4.4.0-66-generic  /boot/vmlinuz-4.8.0-44-generic
/boot/vmlinuz-4.10.0-40-generic  /boot/vmlinuz-4.15.0-24-generic  /boot/vmlinuz-4.4.0-134-generic  /boot/vmlinuz-4.4.0-67-generic  /boot/vmlinuz-4.8.0-45-generic
/boot/vmlinuz-4.10.0-42-generic  /boot/vmlinuz-4.15.0-29-generic  /boot/vmlinuz-4.4.0-135-generic  /boot/vmlinuz-4.4.0-70-generic  /boot/vmlinuz-4.8.0-46-generic
/boot/vmlinuz-4.11.0-13-generic  /boot/vmlinuz-4.15.0-30-generic  /boot/vmlinuz-4.4.0-137-generic  /boot/vmlinuz-4.4.0-71-generic  /boot/vmlinuz-4.8.0-49-generic
/boot/vmlinuz-4.11.0-14-generic  /boot/vmlinuz-4.15.0-32-generic  /boot/vmlinuz-4.4.0-138-generic  /boot/vmlinuz-4.4.0-72-generic  /boot/vmlinuz-4.8.0-51-generic
/boot/vmlinuz-4.13.0-16-generic  /boot/vmlinuz-4.15.0-33-generic  /boot/vmlinuz-4.4.0-21-generic  /boot/vmlinuz-4.4.0-75-generic  /boot/vmlinuz-4.8.0-52-generic
/boot/vmlinuz-4.13.0-17-generic  /boot/vmlinuz-4.15.0-34-generic  /boot/vmlinuz-4.4.0-22-generic  /boot/vmlinuz-4.4.0-77-generic  /boot/vmlinuz-4.8.0-53-generic
/boot/vmlinuz-4.13.0-19-generic  /boot/vmlinuz-4.15.0-36-generic  /boot/vmlinuz-4.4.0-24-generic  /boot/vmlinuz-4.4.0-78-generic  /boot/vmlinuz-4.8.0-54-generic
/boot/vmlinuz-4.13.0-21-generic  /boot/vmlinuz-4.15.0-38-generic  /boot/vmlinuz-4.4.0-28-generic  /boot/vmlinuz-4.4.0-79-generic  /boot/vmlinuz-4.8.0-56-generic
/boot/vmlinuz-4.13.0-25-generic  /boot/vmlinuz-4.4.0-101-generic  /boot/vmlinuz-4.4.0-31-generic  /boot/vmlinuz-4.4.0-81-generic  /boot/vmlinuz-4.8.0-58-generic
root@e3ffc816a4ae:/#
[0] 1:ssh  2:ssh- 3:zsh  4:docker* 5:zsh                                    "root@e3ffc816a4ae: /" 23:00 14-Nov-18
```

- Ubuntu kernels
  - 4.4.0-*-generic
  - 4.8.0-*-generic
- CentOS kernels
  - 3.10.0-862.2.3.el7
  - 3.10.0-862.11.6.el7
- Upstream kernels
  - 4.18.19
  - 4.14.81

# So, which versions are affected?

- security-tracker.debian.org
- access.redhat.com/security
- usn.ubuntu.com
- …

# What about 0-day?

# Solution

# What should it look like?

- Must work without any “non-desktop software”
- Must be easily integrateable in exploit dev workflow
- Less code is better
- …
- KISS

# Base layer

```
qemu-system-x86_64 -snapshot -nographic \
  -accel hvf -cpu host \
  -hda ubuntu1604.img \
  -kernel 4.10.0-40-generic \
  -append 'root=/dev/sda console=ttyS0 rw' \
  -smp 1 -m 512 -device e1000,netdev=n1 \
  -netdev user,id=n1,hostfwd=tcp:127.0.0.1:25178-:22 \
  -initrd initrd.img-4.10.0-40-generic
```

# *bootstrap

- debootstrap
- febootstrap
- supermin
- …

All these doesn’t work well outside of “home distro”

# Get kernels$_1$

```
FROM ubuntu:16.04
RUN apt-get update
RUN DEBIAN_FRONTEND=noninteractive \
        apt-get install -y \
        linux-image-4*-generic \
        linux-headers-*-generic \
        build-essential wget git
```

# Get kernels$_2$

```
docker build -t ${CONTAINER_NAME} ${DOCKER}

docker cp ${CONTAINER_ID}:/boot/. output/
```

# Get kernels$_3$

```
[[Kernels]]
distro_type = "Ubuntu"
distro_release = "16.04"
kernel_release = "4.10.0-14-generic"
container_name = "ubuntu1604"
kernel_path = "vmlinuz-4.10.0-14-generic"
initrd_path = "initrd.img-4.10.0-14-generic"
root_f_s = "ubuntu1604.img"
```

# build

```
docker run -v \
   /tmp/out-of-tree_096015149/source:/work \
   ubuntu1604 \
  "bash -c cd /work && \
   make KERNEL=/lib/modules/4.10.0-19-generic/build \
   TARGET=17473511124516436O2_4.10.0-19-generic"
```

# Configuration file

```
name = "out-of-tree exploit example"
type = "exploit"

[[supported_kernels]]
distro_type = "Ubuntu"
release_mask = "4.11.0-(1|2|3|4|5|6|7|8)-.*"
```

# Key features

# Testing kernel modules

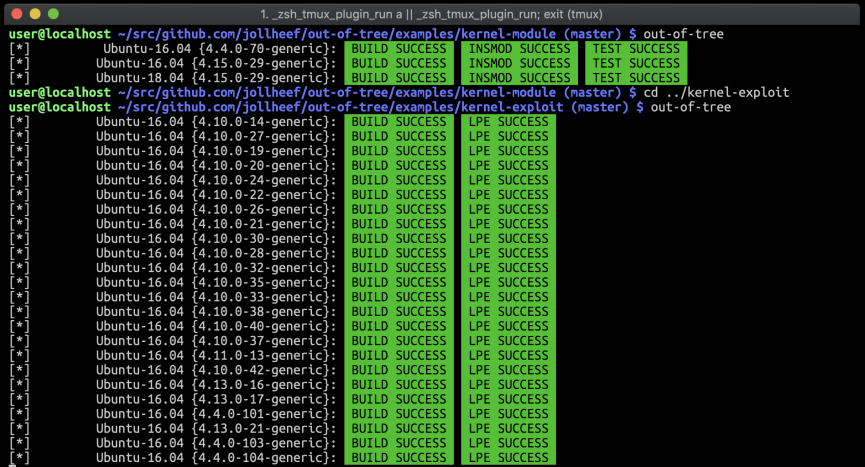
- build in docker
- run qemu -kernel …
- dmesg | grep …

# Testing kernel exploits

- build in docker
- run qemu -kernel …
- echo touch RANDOM_FILE | EXPLOIT

# Identifying vulnerable kernel version

- define “exploit” type in .out-of-tree.toml
- run “out-of-tree pew –guess”
- wait …
- wait …
- PROFIT!


1. _zsh_tmux_plugin_run a || _zsh_tmux_plugin_run; exit (tmux)
user@localhost ~/src/github.com/jollheef/out-of-tree/examples/kernel-module (master) $ out-of-tree
[*] Ubuntu-16.04 {4.4.0-70-generic}: BUILD SUCCESS INSMOD SUCCESS TEST SUCCESS
[*] Ubuntu-16.04 {4.15.0-29-generic}: BUILD SUCCESS INSMOD SUCCESS TEST SUCCESS
[*] Ubuntu-18.04 {4.15.0-29-generic}: BUILD SUCCESS INSMOD SUCCESS TEST SUCCESS
user@localhost ~/src/github.com/jollheef/out-of-tree/examples/kernel-module (master) $ cd ../kernel-exploit
user@localhost ~/src/github.com/jollheef/out-of-tree/examples/kernel-exploit (master) $ out-of-tree
[*] Ubuntu-16.04 {4.10.0-14-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-27-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-19-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-20-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-24-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-22-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-26-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-21-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-30-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-28-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-32-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-35-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-33-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-38-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-40-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-37-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.11.0-13-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.10.0-42-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.13.0-16-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.13.0-17-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.4.0-101-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.13.0-21-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.4.0-103-generic}: BUILD SUCCESS LPE SUCCESS
[*] Ubuntu-16.04 {4.4.0-104-generic}: BUILD SUCCESS LPE SUCCESS
[0] 1:out-of-tree* 2:zsh- "localhost.local" 19:39 08-Oct-18

# Demo

# Future plans

- Add some generic tests
- Auto-analysis of kernel crash
- OpenSTF support
- Continious Integration
- fastboot support
- Exploit pack coverage

# Questions?

jollheef@riseup.net
out-of-tree.io