
GHETTO
SUPERSTAR
HACK

who

Petar Anastasov
panastasov@secragon.com

- Everything @ Secragon
- Coach of CSCB
- \x4247 FTW

https://github.com/gbrsh

Yordan Stoychev
anatomicys@gmail.com

- Penetration Tester @ PwC
- Member of CSCB
- Kernel Hacker

https://github.com/ysanatomic

why

- Ghetto Forensics
- Ghetto Superstar
- OffSec POV
- Some fun

later?!

print(f'Thanks to {re.sub(r"a", "e", "Pras - Ghetto Superstar")[:4]}o!')

pre-how

- Rings
- Modules
- System calls

how

root

Applications

Shells

Services

Ring 3

Hey, give me info(X)

Sure, lame_root_info(X)

Ring 0

Kernel

LKMs

superstar

ok but how

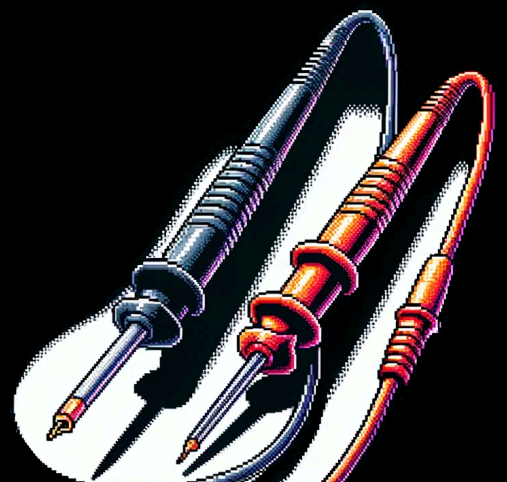
THE PAST

THE PRESENT

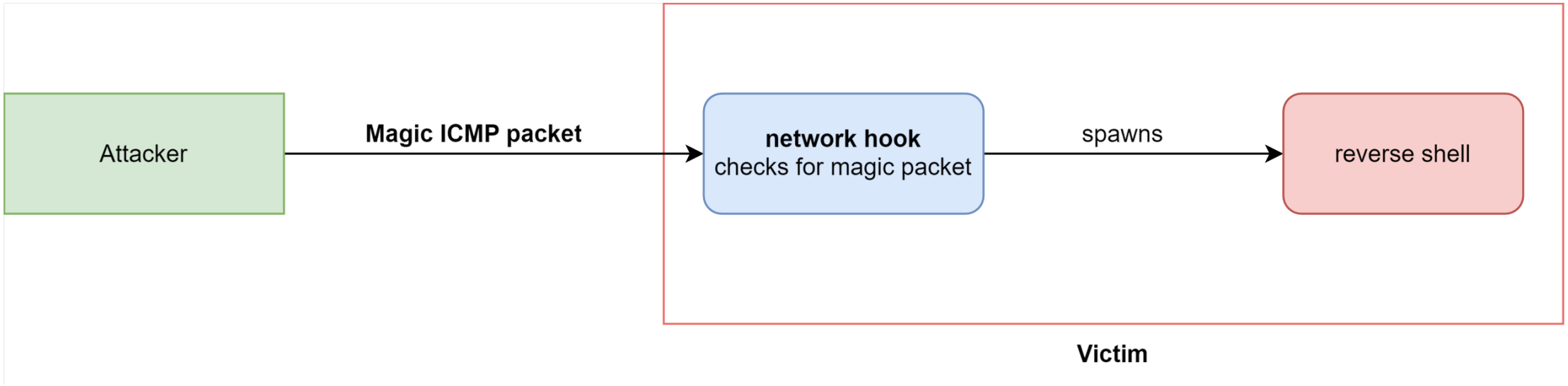
example

KProbes is a debugging mechanism for the Linux kernel which can also be used for monitoring events inside a production system.
Kprobes enables you to dynamically break into any kernel routine and collect debugging and performance information non-disruptively. *You can trap at almost any kernel code address*, specifying a handler routine to be invoked when the breakpoint is hit.

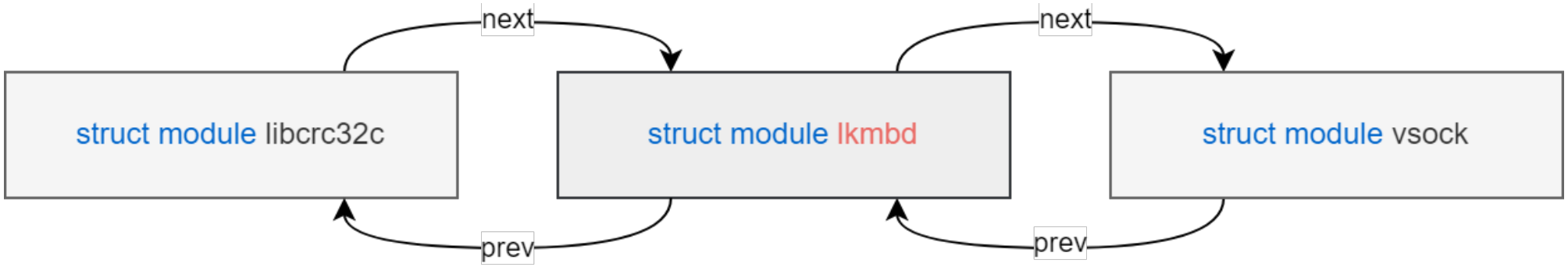
There are currently two types of probes: kprobes, and kretprobes (also called return probes). *A kprobe can be inserted on virtually any instruction in the kernel*. A return probe fires when a specified function returns.

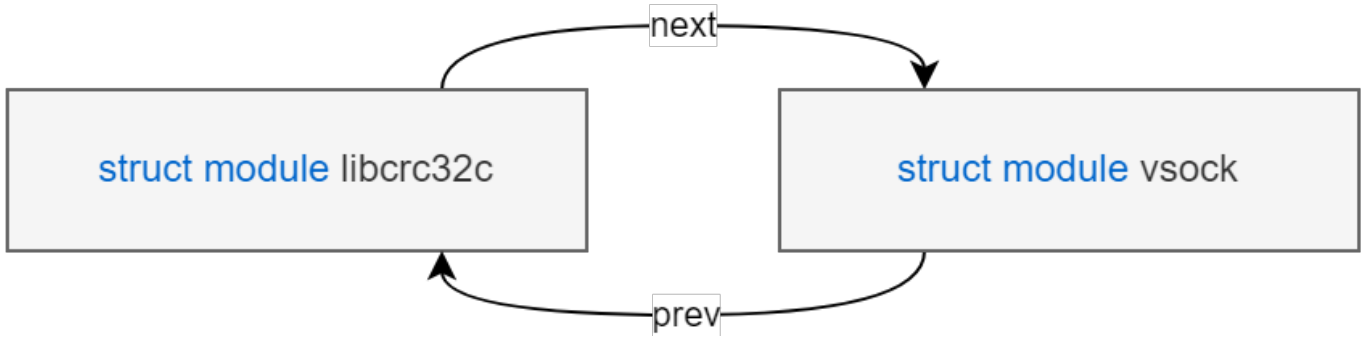


Establishing a reverse shell

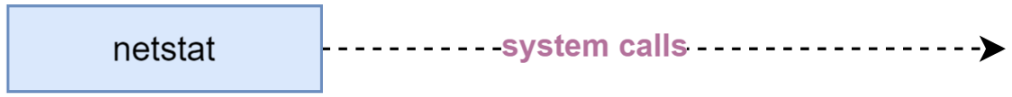


Making the kernel forget





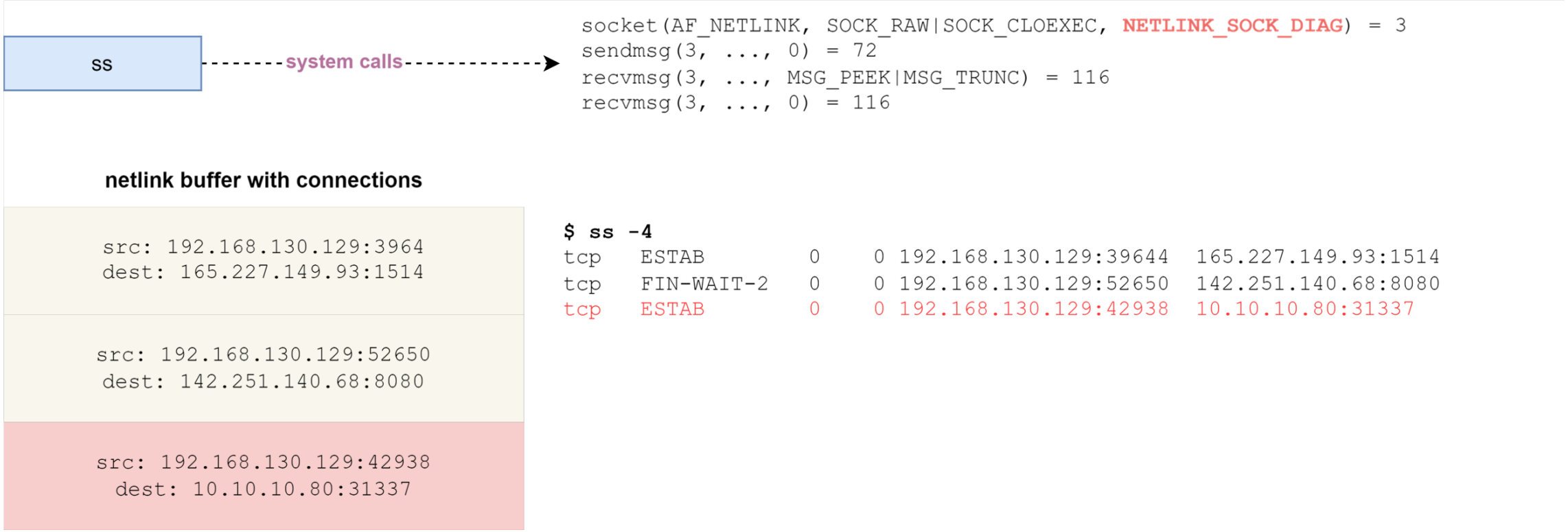
Hiding connections: netstat



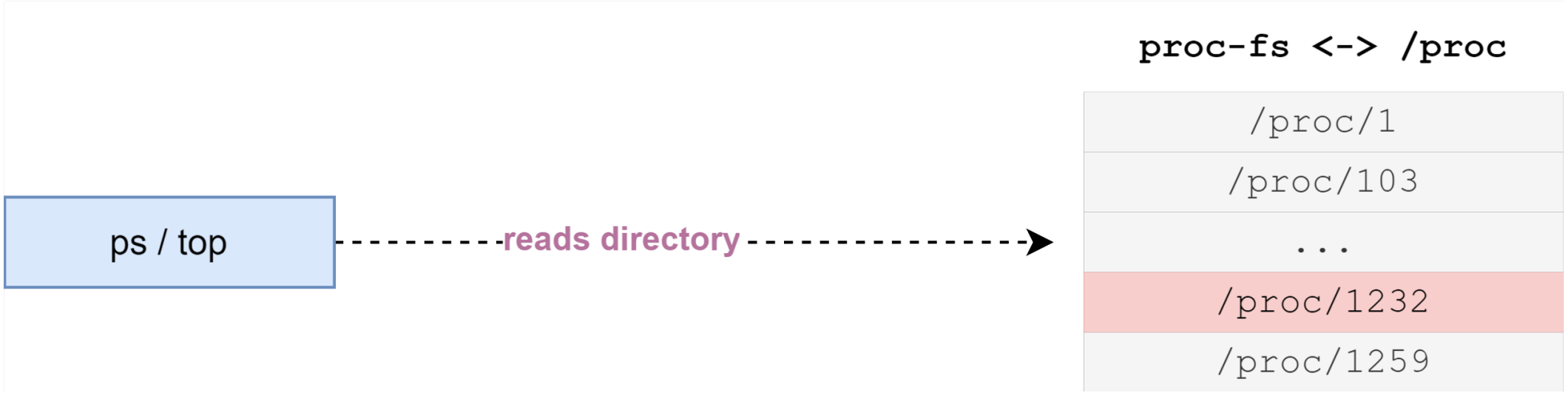

```
openat(AT_FDCWD, "/proc/net/tcp6", O_RDONLY) = 3
openat(AT_FDCWD, "/proc/net/udp", O_RDONLY) = 3
openat(AT_FDCWD, "/etc/hosts", O_RDONLY|O_CLOEXEC) = 4
openat(AT_FDCWD, "/proc/net/udp6", O_RDONLY) = 3
openat(AT_FDCWD, "/proc/net/raw", O_RDONLY) = 3
openat(AT_FDCWD, "/proc/net/unix", O_RDONLY) = 3
```

```
$ cat /proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   101        0 24758 ...
   1: 00000000:053A 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 24111 ...
   2: 00000000:053B 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 31066 ...
   3: 00000000:0538 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 27036 ...
```

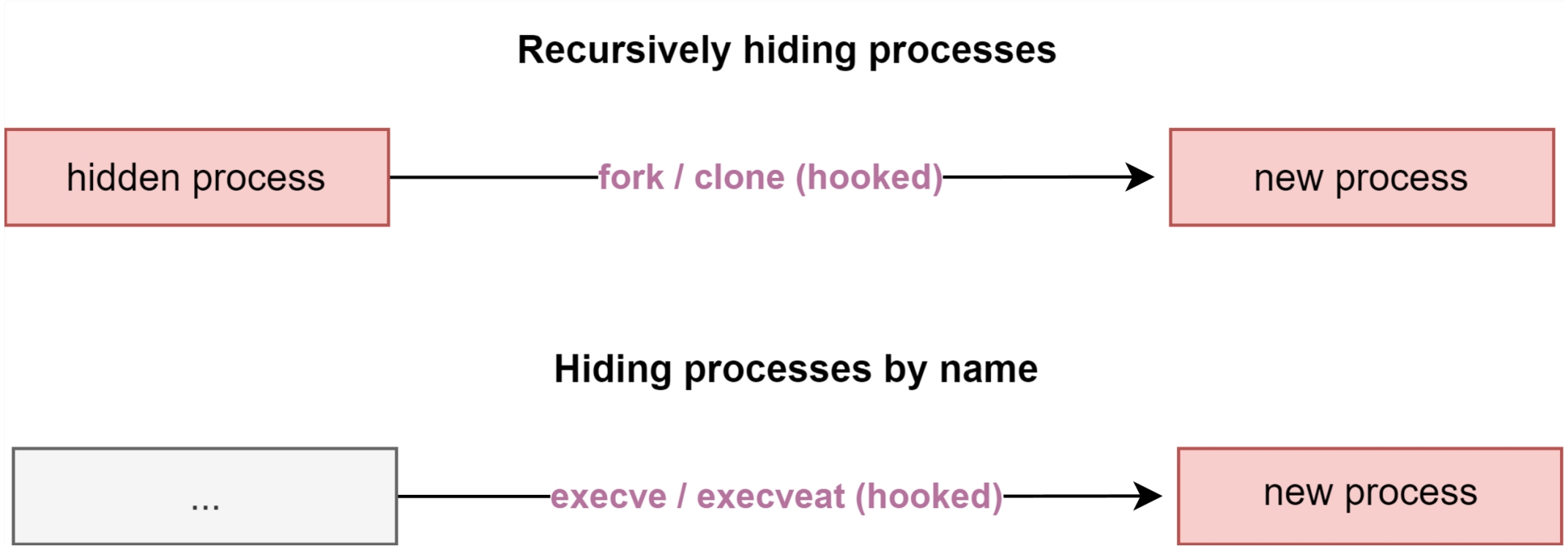
Hiding connections: ss



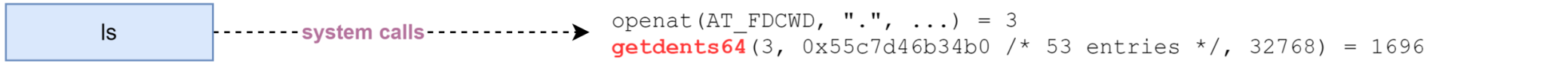
Hiding processes: ps / top



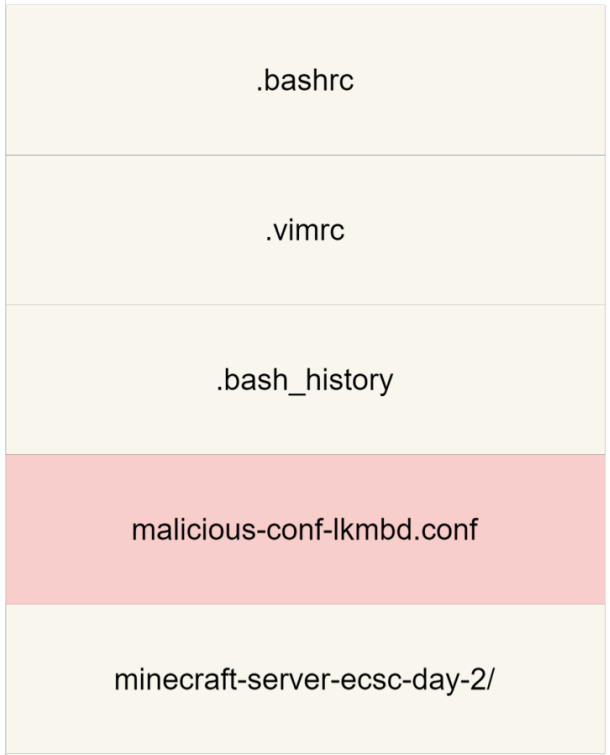
Hiding processes: ps / top



Hiding files: ls



Array of linux_dirent64(s)




```
struct linux_dirent64 {
    ino64_t        d_ino;    /* 64-bit inode number */
    off64_t        d_off;    /* 64-bit offset to next structure */
    unsigned short d_reclen; /* Size of this dirent */
    unsigned char  d_type;   /* File type */
    char           d_name[]; /* Filename (null-terminated) */
};
```

```
$ ls -a
.   .bash_history  .vimrc   minecraft-serer-ecsc-day-2/
..  .bashrc        malicious-conf-lkmbd.conf
```

Evasion: chkrootkit

```
Checking `bindshell'...                                    not infected
Checking `lkm'...                                          chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'...                                      not found
```

Evasion: rkhunter

```
Performing Linux specific checks
    Checking loaded kernel modules                 [ OK ]
    Checking kernel module names                   [ OK ]


Checking the network...


  Performing checks on the network ports
    Checking for backdoor ports                    [ None found ]


  Performing checks on the network interfaces
    Checking for promiscuous interfaces            [ None found ]


Checking the local host...


  Performing system boot checks
    Checking for local host name                   [ Found ]
    Checking for system startup files              [ Found ]
    Checking system startup files for malware      [ None found ]

Rootkit checks...
    Rootkits checked : 477
    Possible rootkits: 0
```

I’m monitoring…

thank you

Q & A

*first blood == free drink