consorzio nazionale
interuniversitario
per le telecomunicazioni

The eBPF hacker toolkit

Pasquale Caporaso & Lorenzo Valeriani

@whoami

Lorenzo Valeriani

- ~~Pasquale Caporaso,~~ phd student, security researcher for CNIT
- ~~Ex-Malware Analyst for Leonardo spa~~
- Research in cyber security, malware and operating systems
- Addicted to CTFs

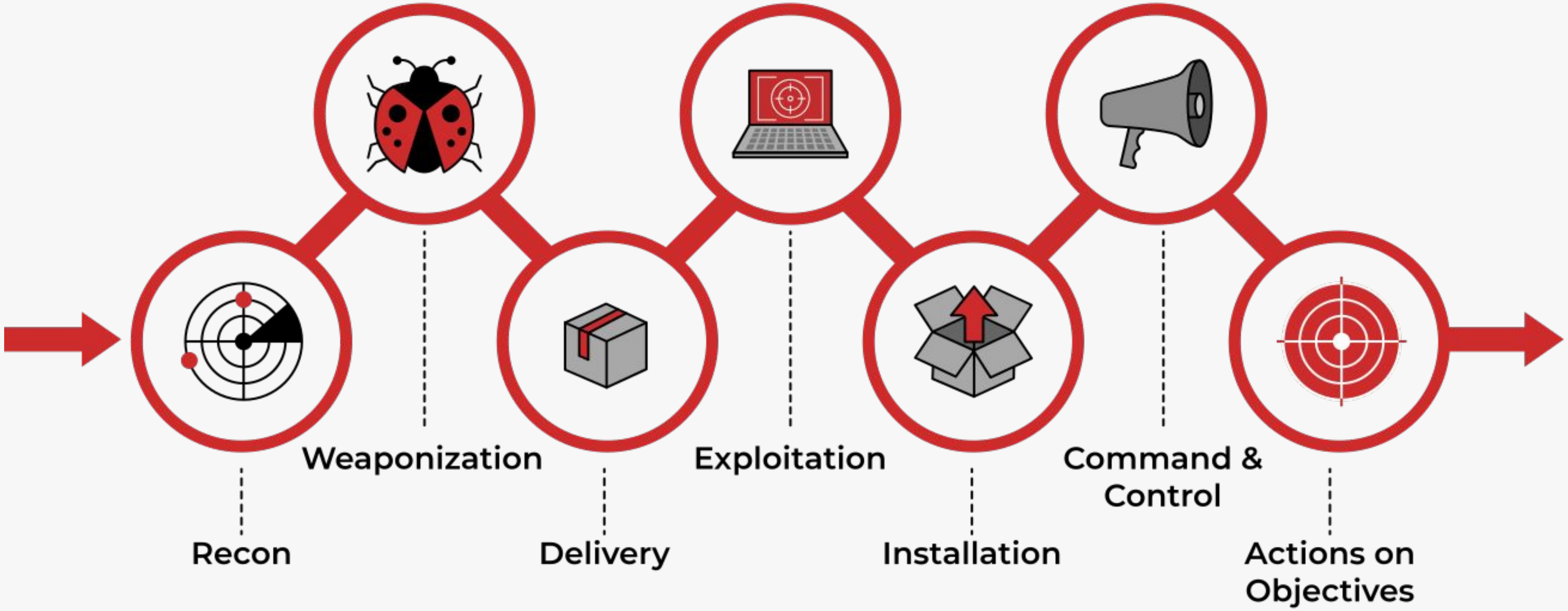
Mainly Android

mHACKeroni

- Tor Vergata CTF team? Anyone?

Attack scenario

- High privilege attacker (root - CAP_BPF)
- Main use: ROOTKITS!!



[1] https://github.com/h3xduck/TripleCross

The weapons

- Packet manipulation (already seen how)

- bpf_probe_write_user()
  - Arbitrary user memory write!

consorzio nazionale
interuniversitario
per le telecomunicazioni

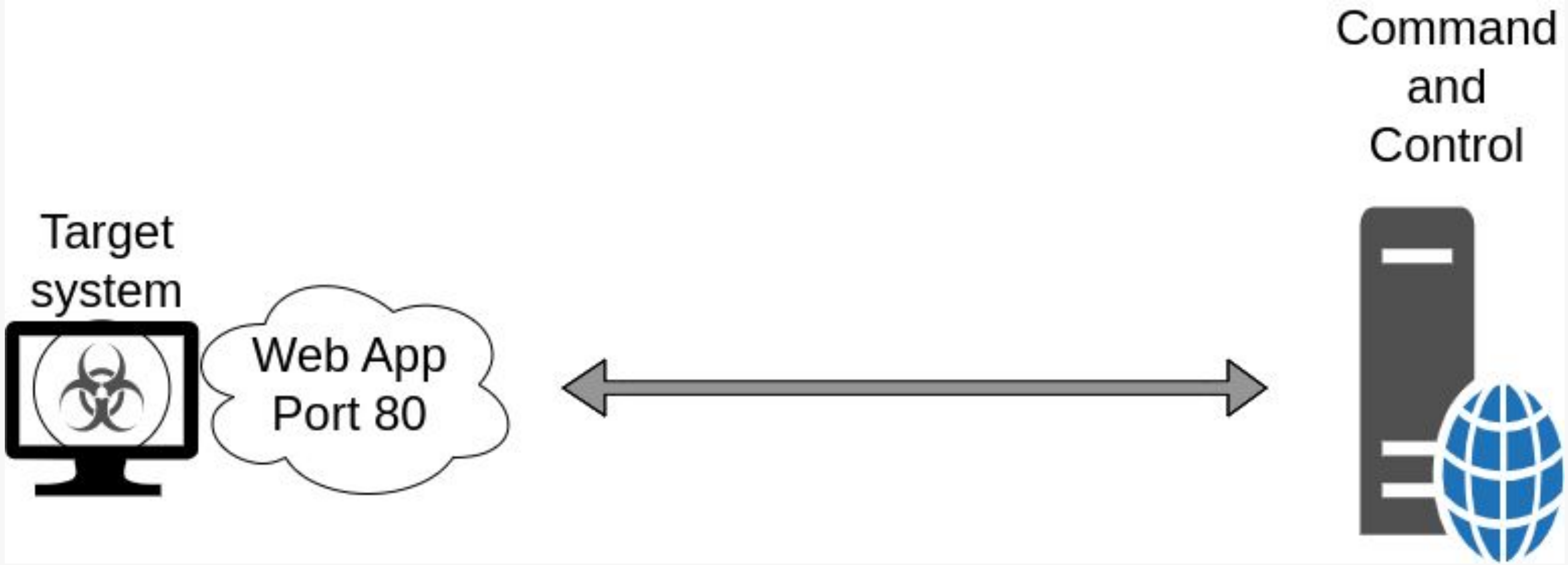
Attack 1

Stealth communication

Attack scenario

- Rootkit wants to talk to C&C

- Infected machine has a Web App installed



Choosing the type

BPF_PROG_TYPE_XDP

- Deep Packet Inspection
- Ingress only
- Can be offloaded to the NIC / driver
- Can drop, allow, modify and retransmit packets

BPF_PROG_TYPE_SCHED_CLS

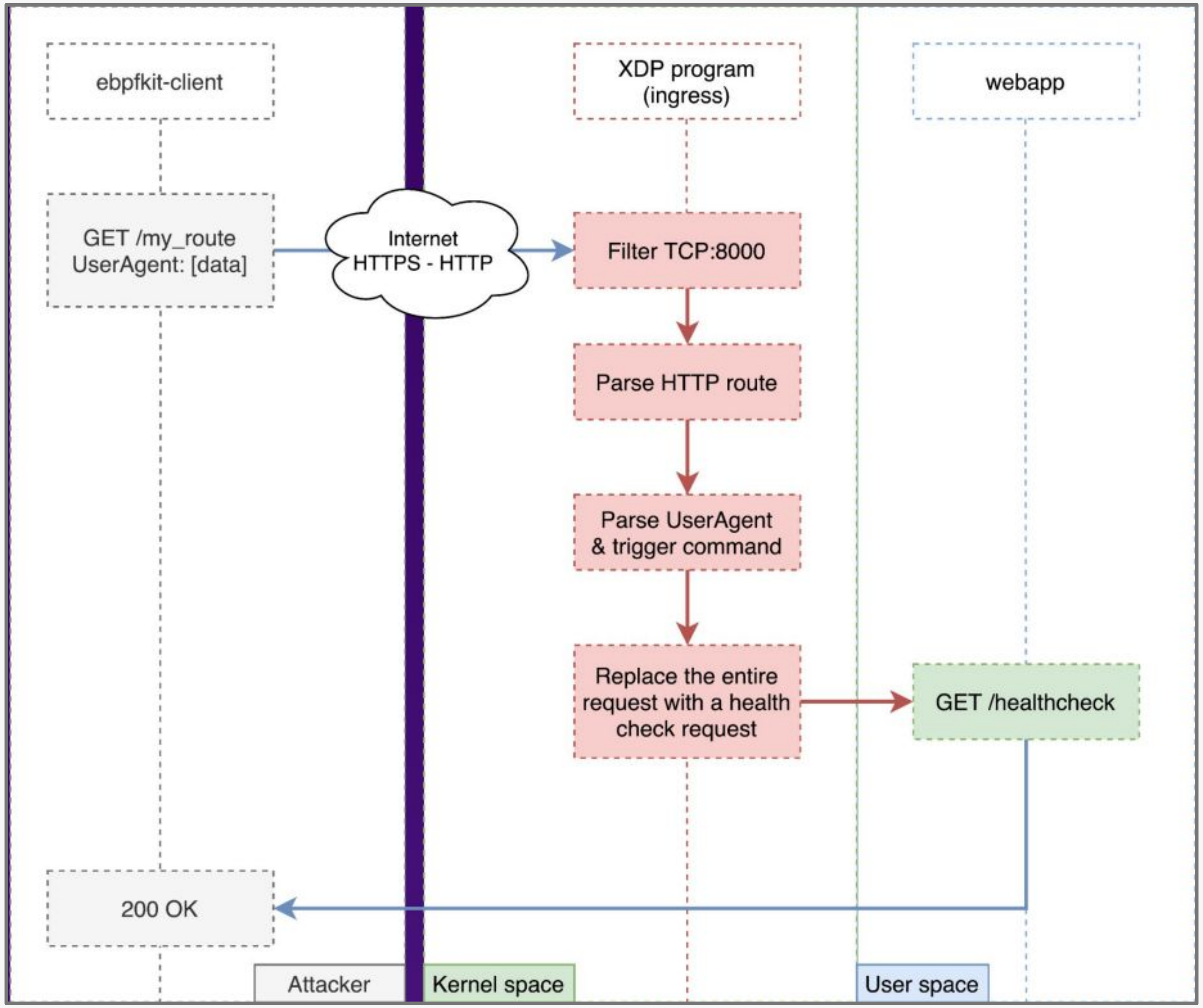
- Egress and Ingress
- Attached to a network interface
- Can drop, allow and modify packets

Wh BOTH! use?

[2] Guillaume Fournier Sylvain Afchain Sylvain Baubeau - eBPF, I thought we were friends.pdf

C&C to Rootkit

- Kernel and server see legitimate GET request
- Rootkit gets the message through a map

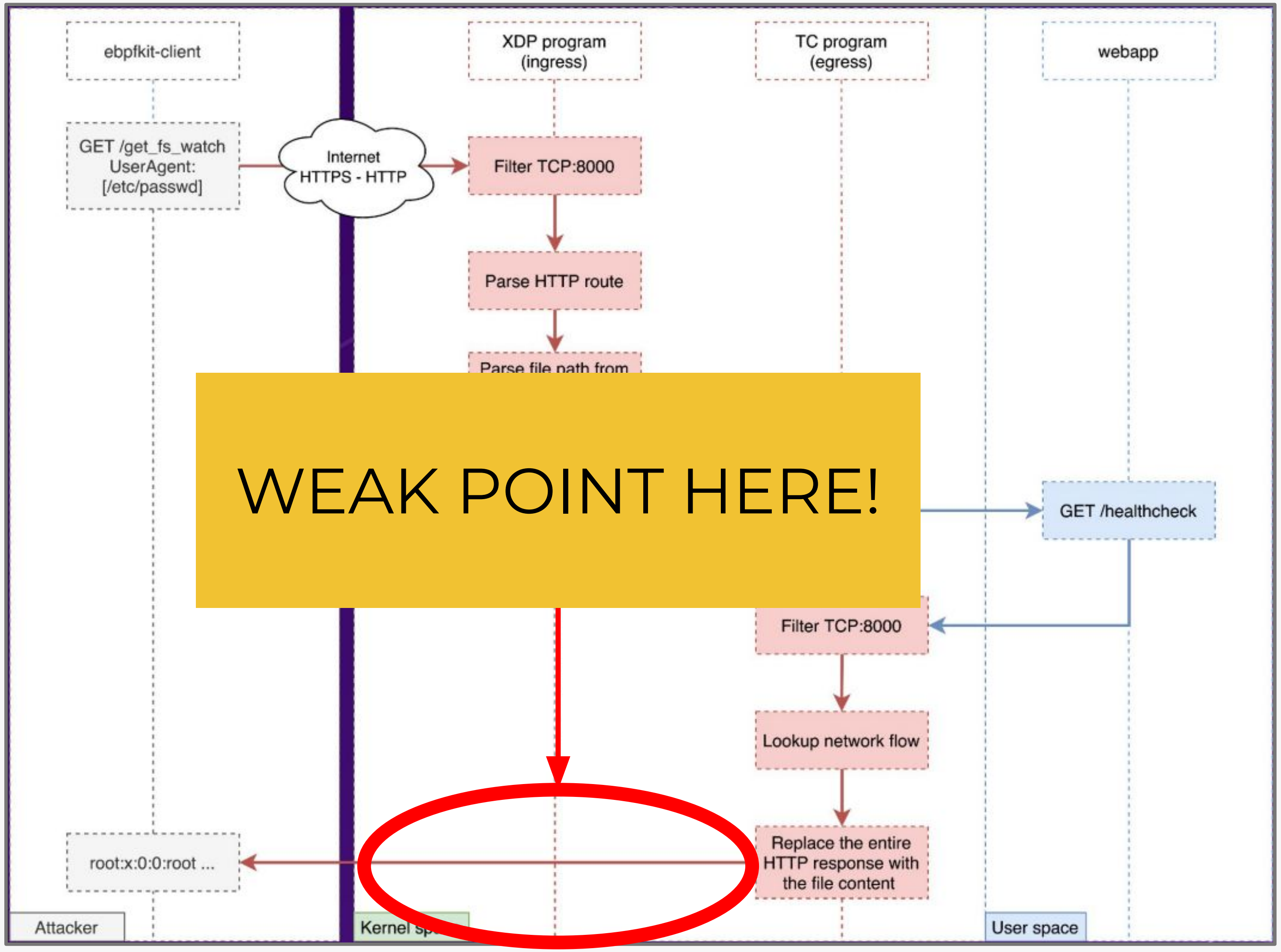


[3] https://github.com/Gui774ume/ebpfkit

Rootkit to C&C

- The CC needs to start the communication

- This time we overwrite the response too



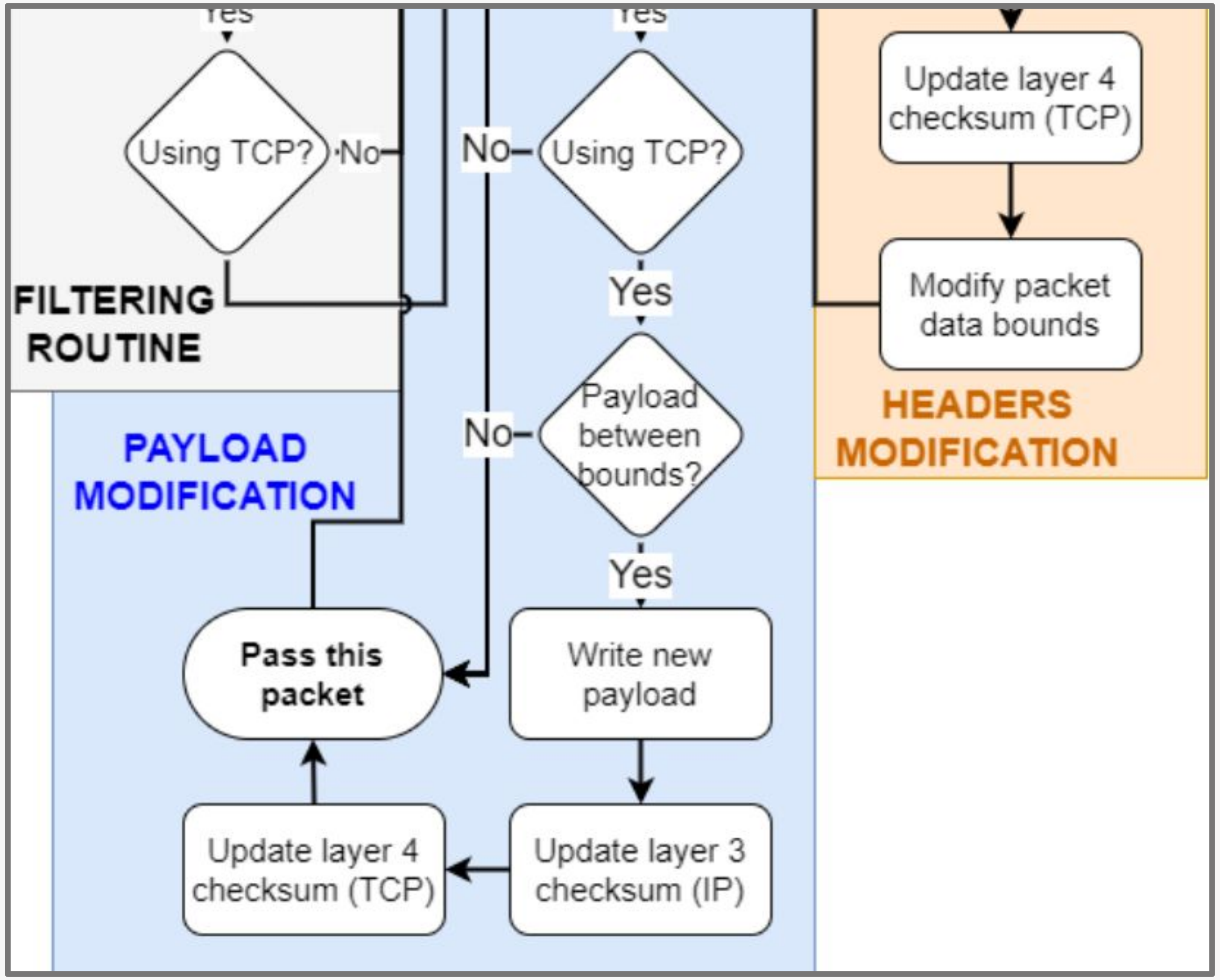
WEAK POINT HERE!

[3] https://github.com/Gui774ume/ebpfkit

□ Upgrade! Get rid of the starter

- Just overwrite random TCP packets

- TCP will resend the packet for us



[4] https://github.com/h3xduck/TripleCross/blob/master/docs/ebpf_offensive_rootkit_tfg.pdf - page 118

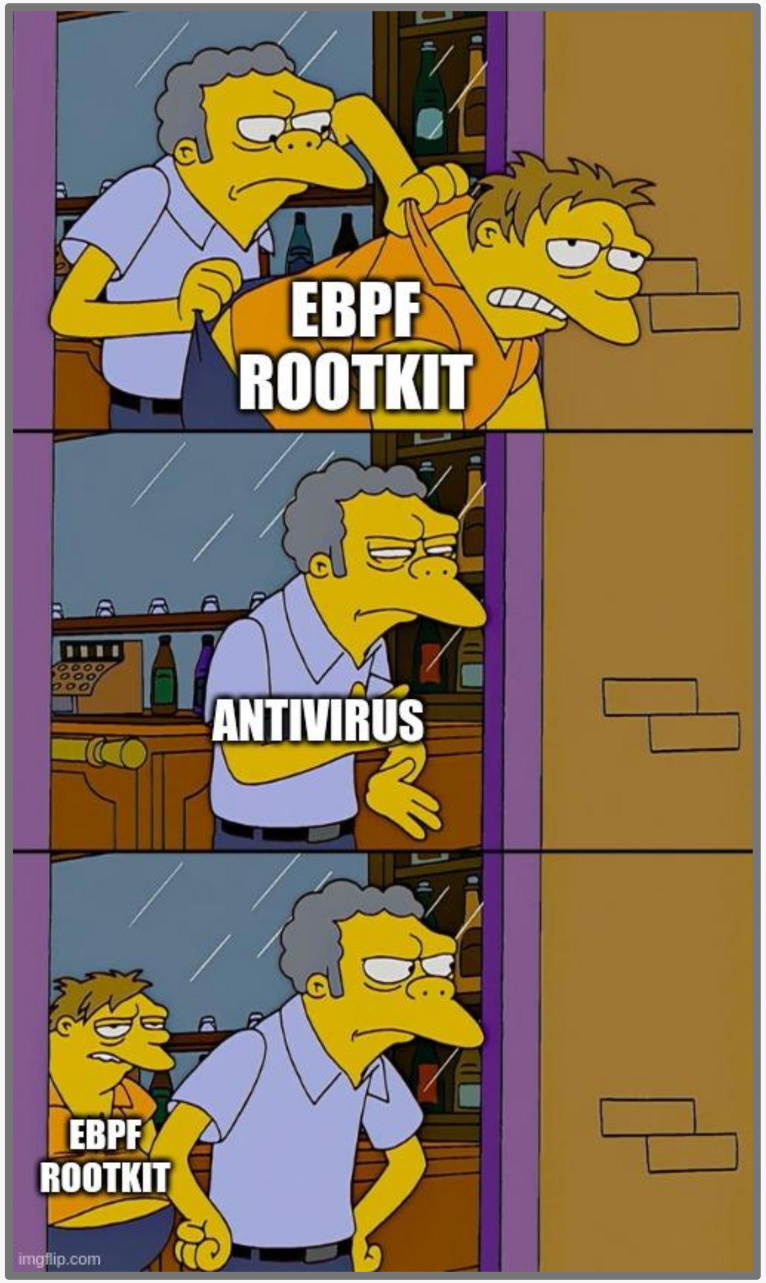
□ Demo

- Did not have time for a demo of this
- Go watch the original :)

https://youtu.be/5zixNDolLrg?si=GQTql6JXrouFI9HX

Attack 2

Program Hiding And Persistence



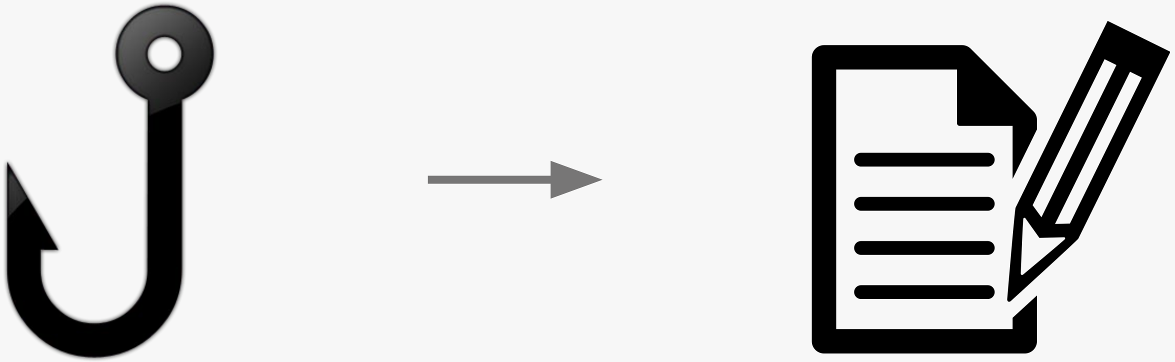
□ Attack scenario

- Rootkit client program

- We want to protect and hide the program using Ebpf

□ Key Idea

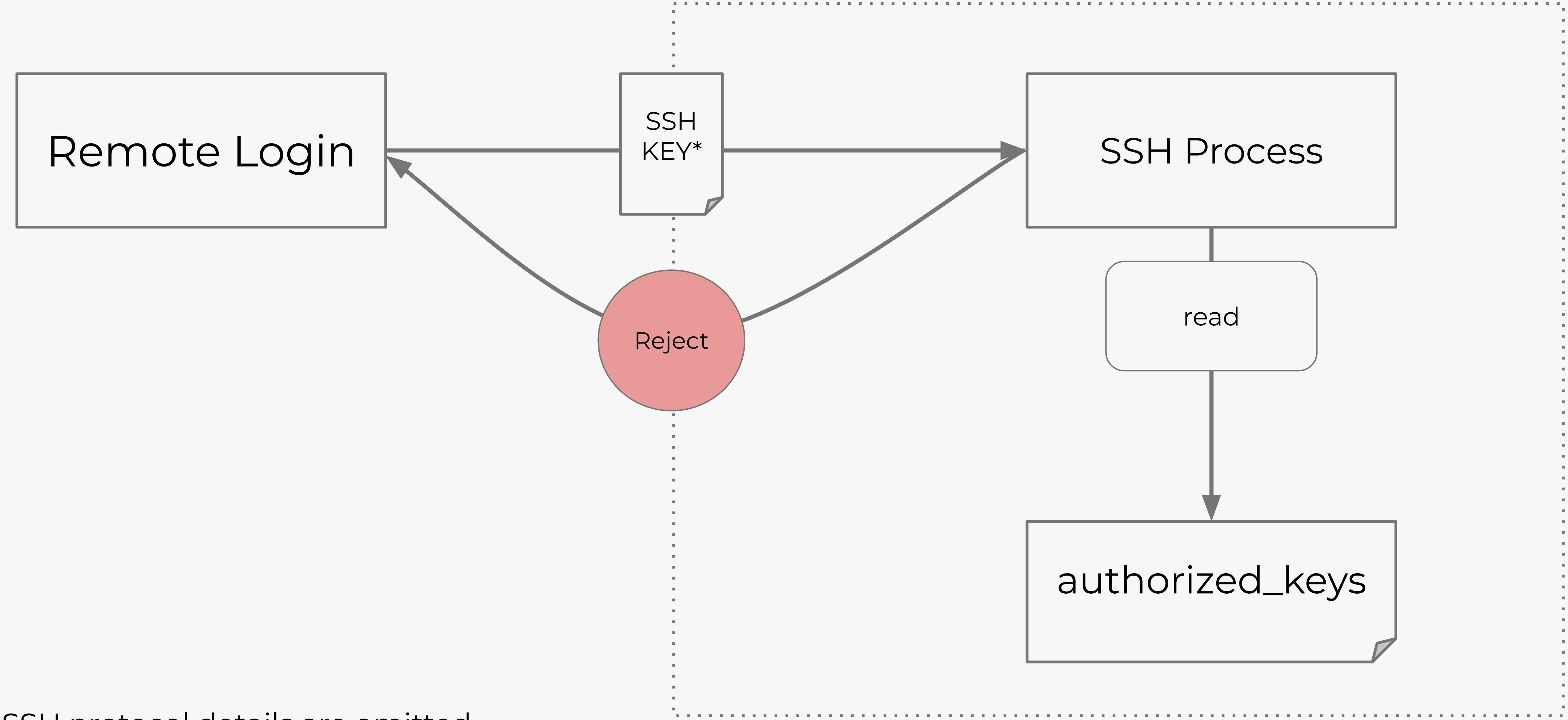
- Hook interesting syscall with eBPF
- Overwrite something with bpf_probe_write_user() to do evil



HOOK

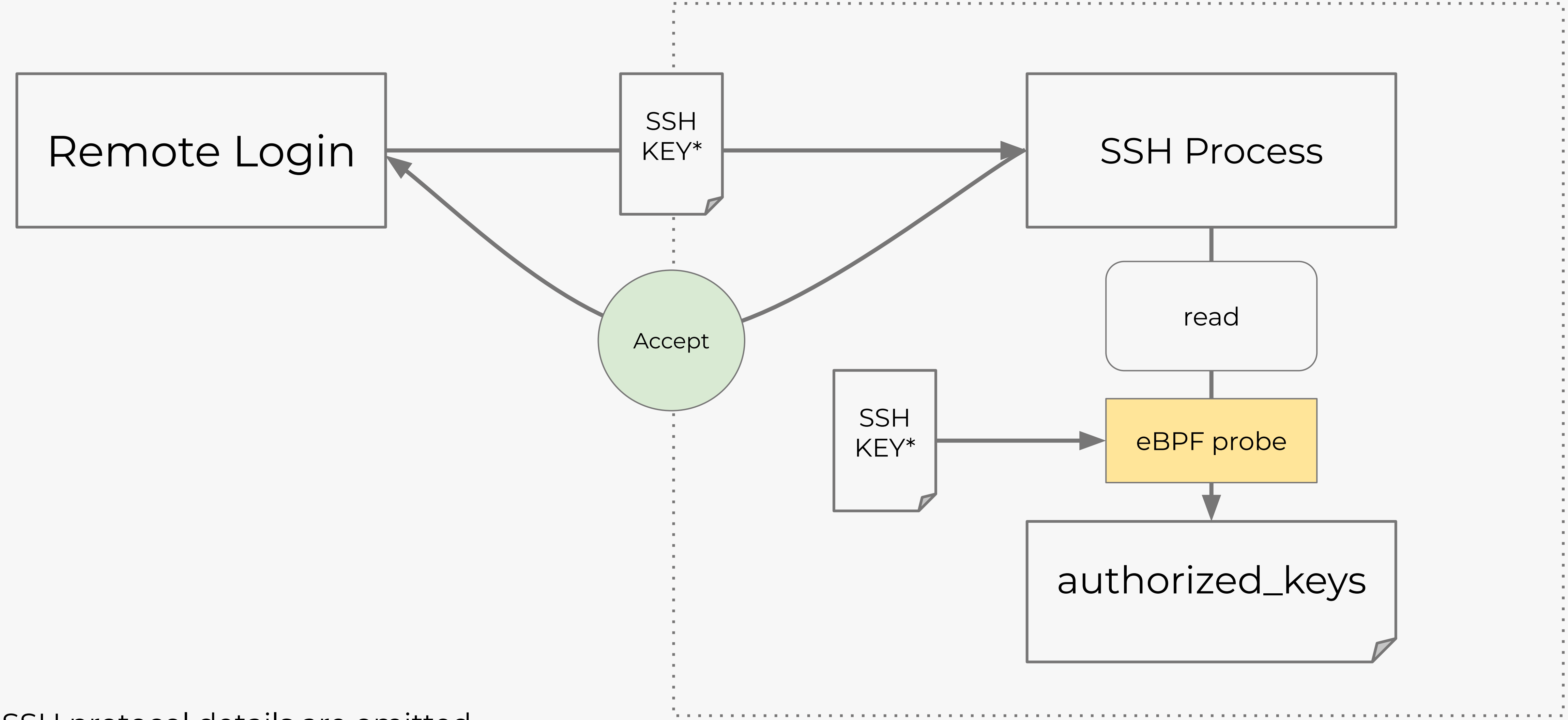
WRITE

Example 1 - ssh connection



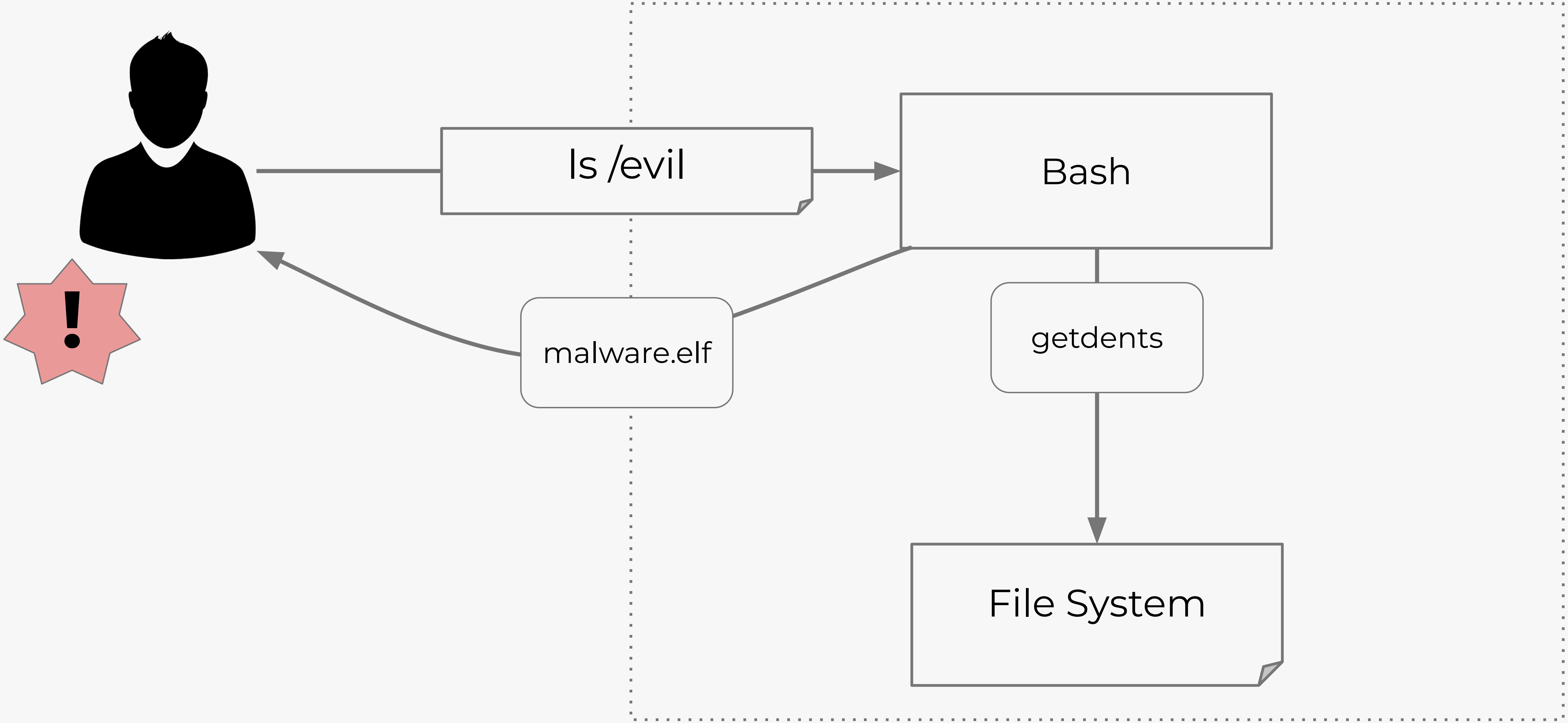
*Some SSH protocol details are omitted

Example 1 - ssh connection

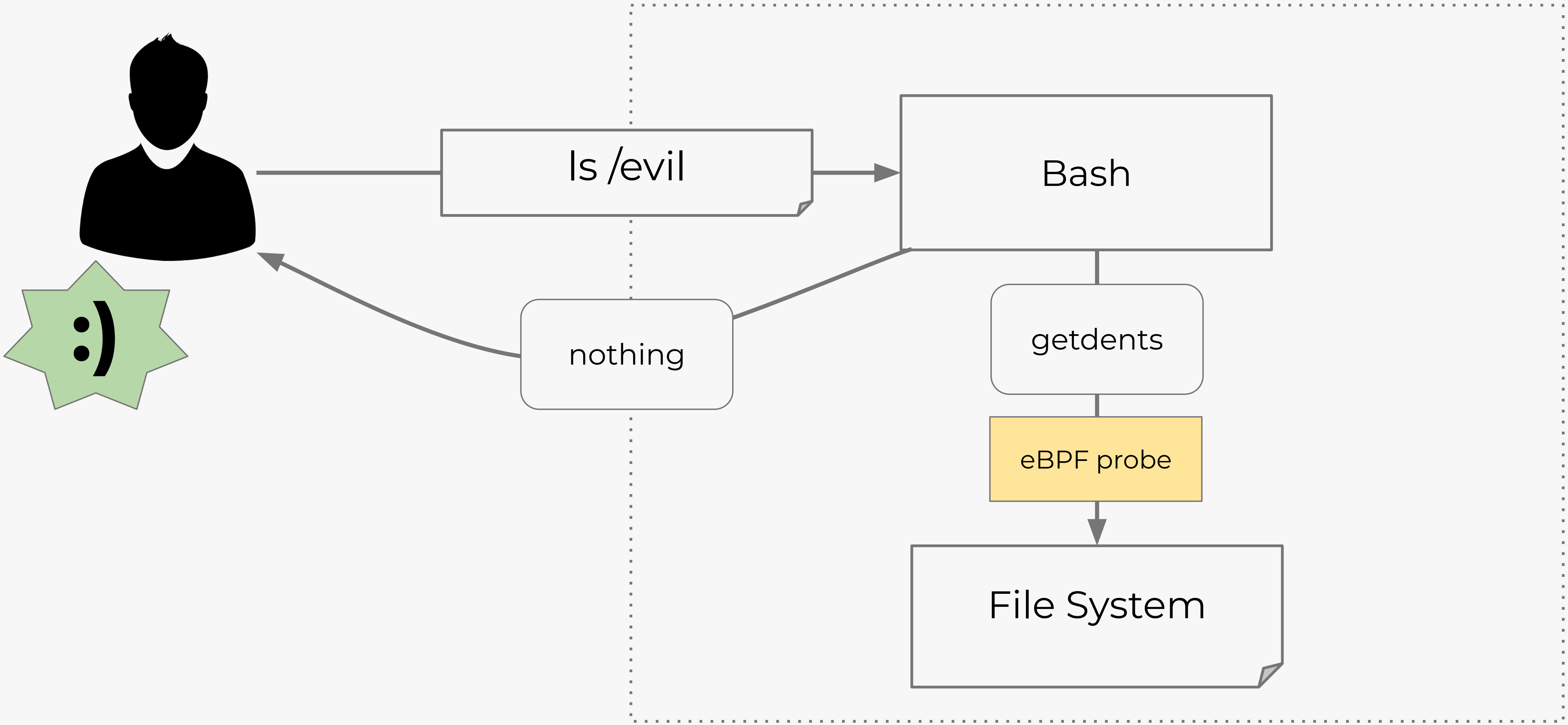


*Some SSH protocol details are omitted

Example 2 - File Hiding



Example 2 - File Hiding



Sources & Contacts

[1] https://github.com/h3xduck/TripleCross

[2] Guillaume Fournier Sylvain Afchain Sylvain Baubeau - eBPF, I thought we were friends.pdf

[3] https://github.com/Gui774ume/ebpfkit

[4] https://github.com/h3xduck/TripleCross/blob/master/docs/ebpf_offensive_rootkit_tfg.pdf

Thanks for the attention!

Mail: lorenzo.valeriani@cnit.it

Linkedin: Lorenzo Valeriani