SAVONIA

Cybersecurity in computer networking LAB 4 – Data gathering

Cybersecurity Fundamentals

Markku Kellomäki

Jussi Nivamo

SAVONIA

Today we will be

- Sending a bruteforce attack through a network router.
- Inspecting the attack.
- Mitigating the attack from the router configuration.
- Mitigating the attack from the receiving end.

SAVONIA

Make notes and report after the lab:

- What did you do?
- What kind of devices did you use?
- What kind of vulnerabilites did you notice?
- How would you try to fix them?

SAVONIA

Starting Live Kali-

- Don’t start the computer yet.
- Plug in the Kali live USB stick
- Start the computer and start repeatedly pushing F2-button
- You will enter UEFI/BIOS screen
- Here you need to change the boot order of the computer so that USB-stick will start first
- Also disable Secure Boot-option.
- Apply changes and exit

SAVONIA

Cable a setup according to the diagram

SAVONIA

Give ip addresses to the devices

- Command on computer 1:

  sudo ifconfig eth0 192.168.1.10 netmask 255.255.255.0 up

- Command on computer 2:

  sudo ifconfig eth0 192.168.2.10 netmask 255.255.255.0 up

- And default gateway with

  sudo route add default gw 192.168.x.1 eth0

SAVONIA

Give ip addresses to the devices

- Commands on router:

```
enable
configure terminal
interface gigabitethernet 0/0/0
ip address 192.168.1.1 255.255.255.0   ## connected to 192.168.1.10
no shutdown
exit
interface gigabitethernet 0/0/1
ip address 192.168.2.1 255.255.255.0   ## connected to 192.168.2.10
no shutdown
```

SAVONIA

Set up http server on the receiving end

- Commands on the computer

  sudo systemctl start nginx

- Confirm that the service is running with

  firefox localhost

- Also start wireshark with commands:

  sudo su
  wireshark

SAVONIA

Now let’s try flooding the server with meaningless queries

- Utilize hping3

  sudo hping3 -c 1 –S -p 80 192.168.2.10

- What the parameters mean:
  - –c 1 sending only one packet
  - -S setting SYN flag.
  - -p 80 target port (unencrypted HTTP)
  - 192.168.2.10 ip address of the target

- Inspect the packet in wireshark. You will see that

SAVONIA

Now let’s try flooding the server with meaningless queries

- Utilize hping3

  sudo hping3 --flood 1 -S -F -P -U -p 80 192.168.2.10

- What the parameters mean:
  - --flood flooding as much packets as possible
  - -S -F -P –U setting SYN, FIN, PSH, URG flags respectively.
  - -p 80 target port (unencrypted HTTP)
  - 192.168.2.10 ip address of the target

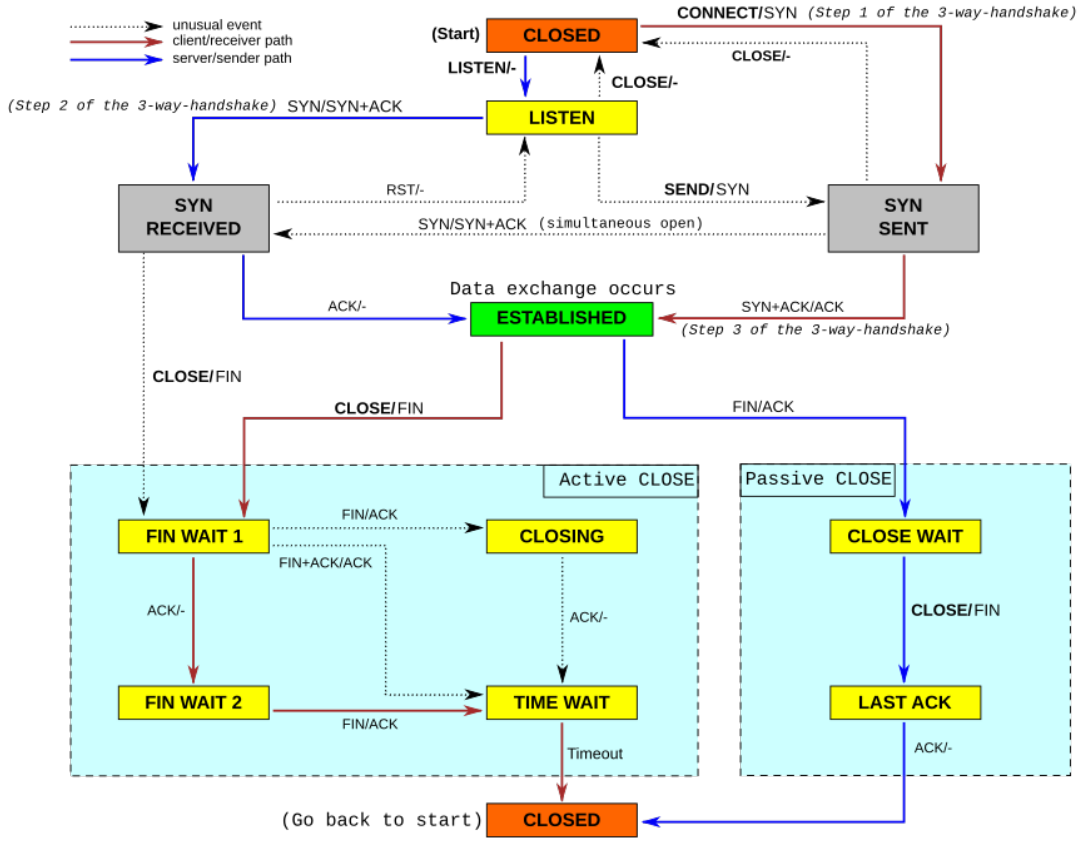
- Flood only for few seconds! Wireshark cannot process that much packets and computer might crash!
- Inspect the packets in wireshark. You will see that it matches all states of TCP IP negotiation

SAVONIA

Understand XMAS-attack

- All flags in TCP packet set to 1 means that it will mean anything in TCP state diagram.

- Improperly configured or old implementations will break and reveal vulnerabilities from systems.



Picture: https://commons.wikimedia.org/wiki/File:Tcp_state_diagram_fixed_new.svg Sergiodc2