SAVONIA

Cybersecurity in computer networking LAB 2 – Data gathering

Cybersecurity Fundamentals

Markku Kellomäki

Jussi Nivamo

SAVONIA

Today we will be

- Entering a network switch through management network and securing it with password.
- Comparing different hashing methods.
- Configuring a web server and configuring a firewall from a router.

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?

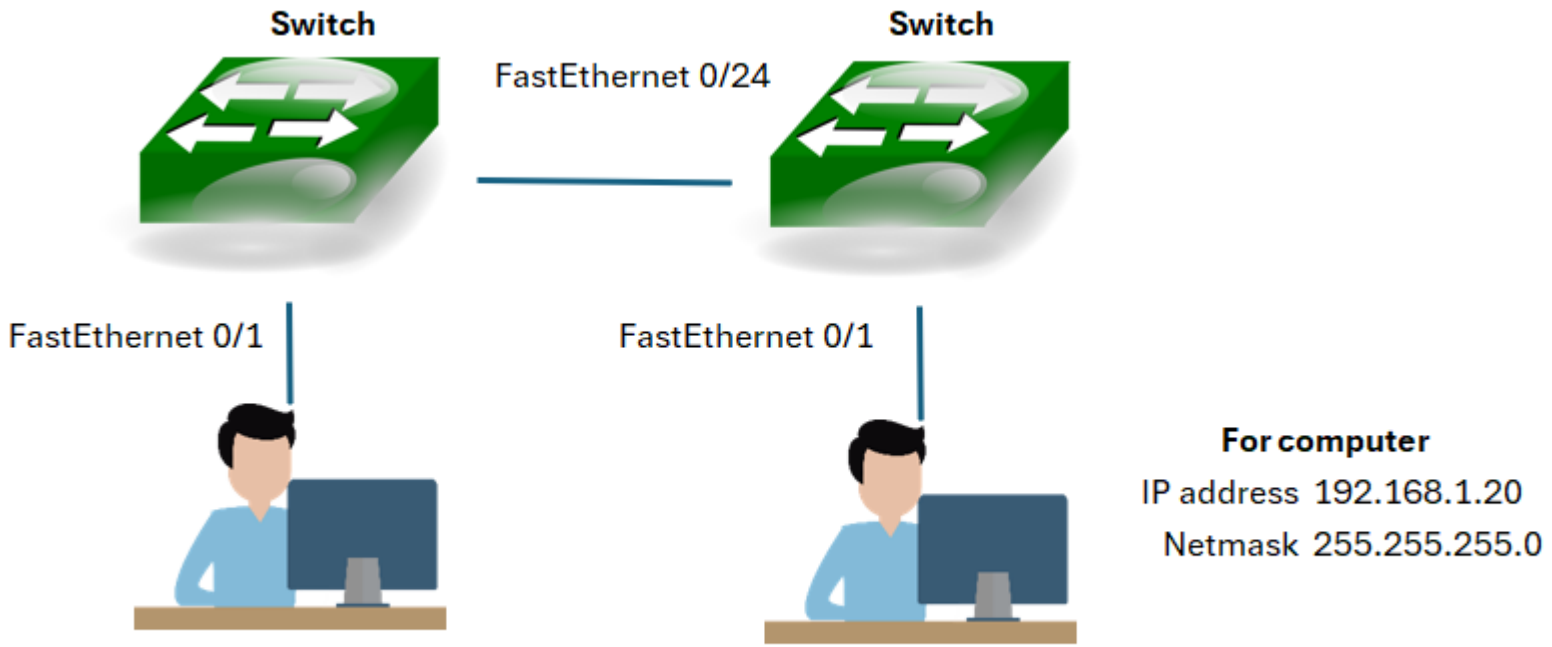
SAVONIA

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



For computer

IP address 192.168.1.20

Netmask 255.255.255.0

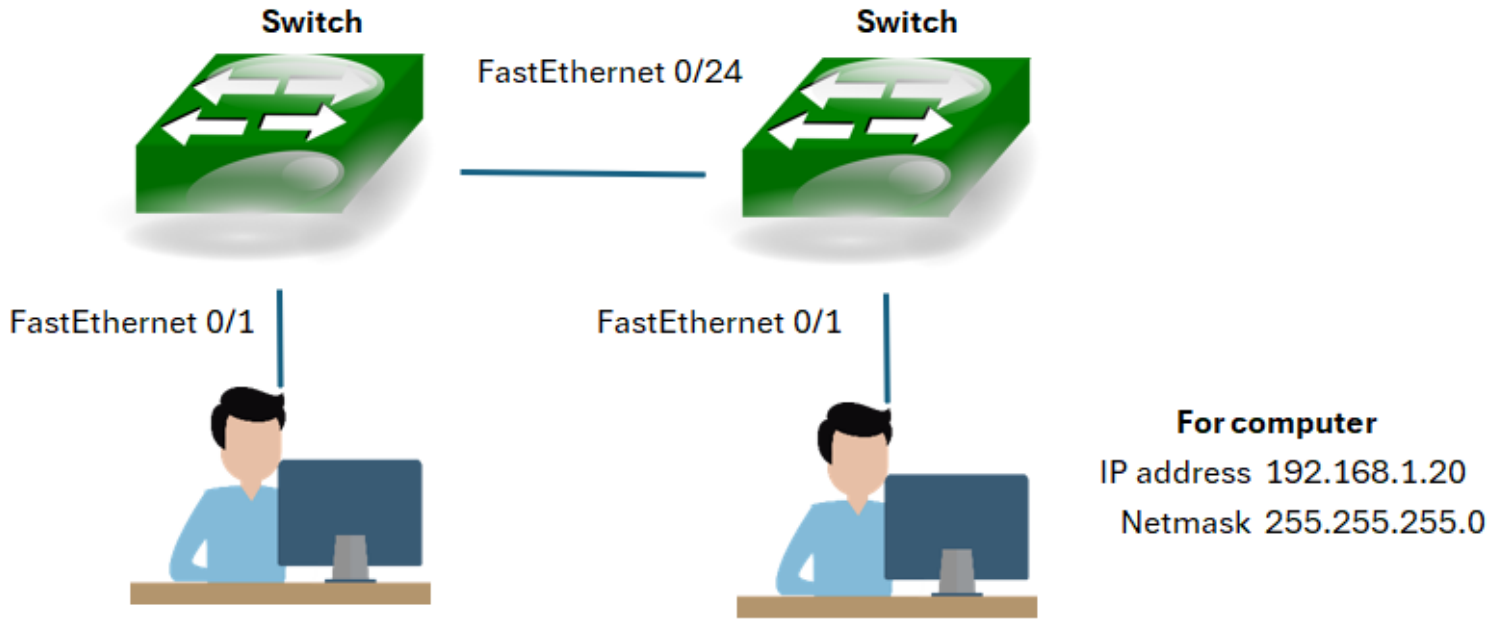
SAVONIA

Open Wireshark with commands:

sudo su

wireshark

And start listening to eth0



SAVONIA

You can connect to switches with screen-program with command

```
screen /dev/ttyS0
```

SAVONIA

On the right switch configure trunk and vlan access switchport

```
enable
configure terminal
interface fastethernet 0/24
switchport mode trunk
switchport trunk allowed vlan 42
no shutdown
exit
interface fastethernet 0/1
switchport mode access
switchport access allowed vlan 42
no shutdown
exit
```

SAVONIA

On the left switch lets configure a trunk between switches?

```
enable
configure terminal
interface fastethernet 0/24
switchport mode trunk
switchport trunk allowed vlan 42
no shutdown
end
```

SAVONIA

See from switch’s terminal

- **What kind of switchport configuration does it have?**

show interfaces switchport

- **What does switchport automated negotiation do?**

- **What does this mean for the switch if people can connect to it?**

SAVONIA

Secure switchports

interface fastEthernet 0/1

- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation restrict
- switchport port-security mac-address sticky

What this does:

- port-security # Enables port security
- maximum 1 # Only 1 MAC allowed
- violation restrict # Blocks unauthorized MACs
- mac-address sticky # Learns the first MAC seen and locks it in

SAVONIA

On the left switch configure remote access with following commands

enable
configure terminal
line vty 0 4
password salasana login
exit
enable secret cat

SAVONIA

Download and configure a DHCP-server

In left computer open up a terminal in Kali

- Confirm the computer is connected to Savonia network
  (Cable slot marked with X)
- ***Write commands:***
  sudo apt update
  sudo apt install dnsmasq
  sudo cp /etc/dnsmasq.conf /etc/dnsmasq.d
  sudo nano /etc/dnsmasq.d/dnsmasq.conf
- **Find a line with text**
  dhcp-range=
- **Uncomment the line, and set it up so it reads:**
  dhcp-range=10.0.0.30,10.0.0.254,12h
- **Save with Control+O**

SAVONIA

Starting a DHCP-server

In left computer open up a terminal in Kali

- **Start dnsmasq-service:**

  sudo systemctl start dnsmasq.service

- **Confirm that the service is running with**

  sudo systemctl status dnsmasq.service

SAVONIA

In kali open up a terminal on other computer

- **Write commands**

sudo ifconfig eth0 10.0.0.5 netmask 255.255.255.0 up

- **And on other computer**

sudo ifconfig eth0 10.0.0.6 netmask 255.255.255.0 up

SAVONIA

In wireshark

- What kind of traffic do you see?
- If you see ip addresses… would you be able to
- Check how *nmap* works with

  man nmap

  or

  nmap –help
- Would you find a service which you could connect?

SAVONIA

Switches by default want to get a management address by DHCP

- We can see what address a switch gets through network monitoring.
- Connect to the switch through telnet with command

  telnet 10.0.0.x
- See if you can get in!
- How would you configure the connection better?

SAVONIA

Password hashing

- Previously we gave the switch a password. What is the hashing method for the password, or is there any?
- How does the password look in

  show running-config
- How would you configure the password on switch to be encrypted better?

SAVONIA

Password hashing

- **Hash the password better with**

  enable secret 5 yourpassword

- **Where 5 means the hashing method.**

- **Save the configuration with**

  copy running-config startup-config

- **And reboot the device. How does the running-config look like now?**

- **What would be this hashing method? What others are available?**

SAVONIA

Disable all services you don’t need. What services these are?

```
no cdp enable
no lldp transmit
no lldp receive
no ip http server
no ip http secure-server
no service pad
ip dhcp snooping
ip dhcp snooping vlan 10
ip dhcp snooping untrust     ! For end-user ports
```

SAVONIA

Power up a router and connect the computers to it like this:

SAVONIA

Set up ip addresses for the computers and router interfaces

sudo ifconfig eth0 192.168.x.10 netmask 255.255.255.0 up
sudo route add default gw 192.168.x.1 eth0

set up ip addresses for router interfaces

interface gigabitethernet 0/0/0
ip address 192.168.x.1 255.255.255.0
no shutdown

SAVONIA

Set up simple web server on other Kali linux

sudo systemctl start nginx

- Check that service is running with

firefox localhost

- Confirm connectivity from other computer also

SAVONIA

Connect to the router through screen (console port) and

```
screen /dev/ttyS0
```

SAVONIA

On the router configure an role based Access Control List

Router# configure terminal

Router(config)# ip access-list extended nameofyourlist

SAVONIA

You will be applying different Access Control lists for ingress and egress traffic

For ingress traffic:

```
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ip access-group nameofyouracl in
Router(config-if)# end
```

For Egress traffic

```
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ip access-group nameofyouracl in
Router(config-if)# end
```

SAVONIA

On the router configure an role based Access Control List

Utilize the question mark (?) on command line to find out how to make a list where

- Make ACLs which
  - Will let HTTP traffic go through.
  - Will not let ping to go through.
- Apply said ACL’s to ports and confirm that they work as in

SAVONIA

On the router configure an role based Access Control List

Utilize the question mark (?) on command line to find out how to make a list where

- Make ACLs which
  - Will let HTTP traffic go through.
  - Will not let ping to go through.
- Apply said ACL’s to ports and confirm that they work as in