

SAVONIA

1

Cybersecurity in computer networking LAB 2 – Data gathering

Cybersecurity Fundamentals

Markku Kellomäki

Jussi Nivamo





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



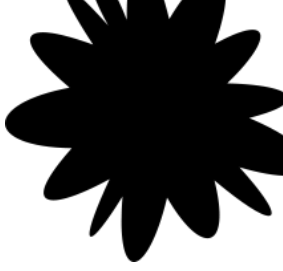
If the computer does not go to BIOS in the beginning

- In Windows-computer
 - Go to **Settings**
 - Go to **Update and Security**
 - Go to **Recovery**
 - Go to **Advanced Start-up**
 - Select **Restart Now**
 - Select **Troubleshoot**
 - Select **Advanced Options**
 - Select **Recovery**
 - Select **Start from usb stick**



Case

- Your computer is connected to a network.
- You don't know what devices are there.
- Your objective is to find a computer acting as server.
- Find out if you can get into any services of the server



Utilities to use

- **Linux terminal**
- **Wireshark** – Network monitoring tool
- **SSH** – Secure Shell
- **nmap** – Network mapping tool
- **Hydra** – Username and Password brute forcing tool



Make notes and report after the lab:

- What devices did you discover in the network?
- How did you check what kind of services they are running?
- How can you be sure if device is the device it seems to be?
- How did you utilize the tools to do what you ended up doing?



Using Wireshark

- Understand when you are looking at a frame, and when you are looking at packet.
- What kind of frames and packets give information about protocols running on devices?



Using Linux terminal in Kali

- Basic things – How to navigate the file system?
- How to see what services are in use?



Objective

- Find out the server computer.
- There might be an *admin* user. How to get in?
- After getting in. How to find out what services are running there? Maybe a database service?
- How to get into the database?
- What did you find in the database?
- Report to the teacher after finding what you found in the database.