Kickstart: Hacker Workshop PROSA Wednesday Nov 29, 2023 from 17:00 - 20:00

This material is prepared for use in *Hacker Workshop PROSA* It contains the very basic information to get started!

This workshop and exercises are expected to be performed in a training setting with network connected systems. The exercises use a number of open source tools which can be copied and reused after training.

To get kickstarted in this workshop it is recommended to perform the following:

- ☐ **Download and install Nmap**
  We will use Nmap as the main tool https://nmap.org/download.html this package is easily installed on Windows, Mac OS X and Linux.
  Note: The tool Nmap is an advanced portscanner and *may* be flagged by your anti-virus program. Usually that is a good thing, we don't want anyone inside an organisation to do port scans, only authorized administrators. The tool itself is NOT malware.
- ☐ **Download slides and exercises booklet**
  Recommend downloading latest version at the beginning of the workshop. Get main slides and exercises PDF from
  https://github.com/kramse/security-courses/tree/master/presentations/pentest/hackerworkshop-prosa
- ☐ **Join the Pentest Wi-Fi network: SSID pentest**
  I brought my own network for this workshop, where we can scan and perform things which are not recommended on the PROSA Wi-Fi

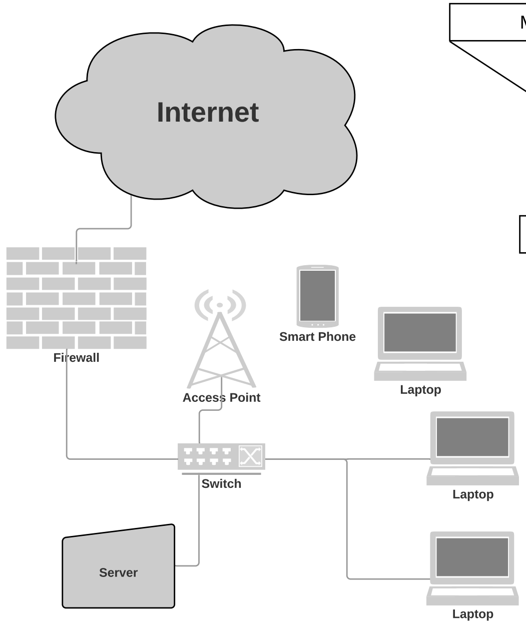
You don't **need** a virtual machine for the workshop, but if you want to do more advanced pentesting after the workshop it is recommended to install a Kali virtual machine:

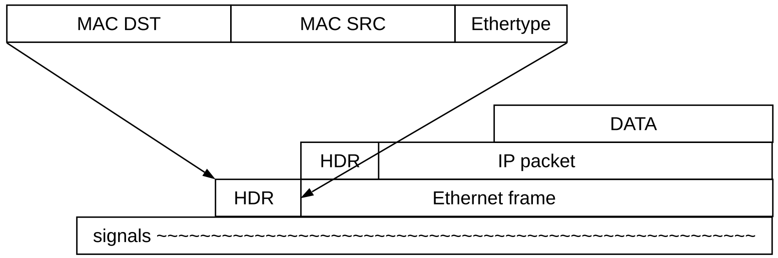
- ☐ Read my recommendations about setup of virtual systems here
  https://github.com/kramse/kramse-labs

I hope we will have a fun and enjoyable time in this workshop.

Henrik Kramselund, `hlk@zencurity.com` `xhek@kea.dk`.

Sample IP network





Ethernet frames contain packets

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet IPv4 Packet Header

- Network addresses 10.0.45.0/24 – 10.0.45.0 - 10.0.45.255
- The router is typically the first 10.0.45.1 or last usable address 10.0.45.254
- Check you own address using the command line, or some control panel: Linux terminal: `ip address` , Mac OS X terminal: `ifconfig` , Windows `ipconfig`
- The network configuration you get from DHCP will include name servers and router
- You may port scan the whole network, using Nmap is fine
- **You are allowed to attack the router and servers provided by the instructor!** (Metasploit/exploits etc.)