Welcome to

Creating slides using LaTeX
Using the old skool foils.cls

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

first-presentation.tex in the repo security-courses

Goals for today

Abstract

Doing slides can be very frustrating. WYSIWYG programs are often clunky and you dont need the "funny animations" anyway :-D

Using LaTeX allows you to quickly write down text and make them into slides. The power of LaTeX also allows you to link exercise booklets and reference with names, numbers across documents easily.

The talk will present my template for doing this, and link to my repository on Github with examples https://github.com/kramse/security-courses

Introduce the old skool foils.cls which is very *clean*

Introduce some of the basic tools i use in my presentations

You should be able to clone and modify repo afterwards

LaTeX can do so much by itself

Small example file

```
\documentclass[Screen16to9,17pt]{foils}
%\documentclass[16pt,landscape,a4paper,footrule]{foils}
\usepackage{zencurity-slides}
% This is an example presentation

\begin{document}

%\rm
\selectlanguage{english}

\mytitlepage
{Small \LaTeX presentation}

\LogoOn
```

```
\slide{First slide}

\begin{list1}
\item Step 1: install \TeX Live \link{https://www.tug.org/texlive/}\\
 or other \LaTeX, and Latexmk \link{https://mg.readthedocs.io/latexmk.html}
\item Step 2: git clone \link{https://github.com/kramse/security-courses}
\item Step 3: Make sure TEXINPUTS can find the texfiles, add to .bashrc or .profile:\\
\verb+export TEXINPUTS=/home/user/projects/security-courses//:+
\item Step 4: Update your \verb+~/.latexmkrc+
\vskip 5mm
\item Finally Go to \verb+security-courses/texfiles+ and run \verb+latexmk small.tex+
\item another option is to use \link{https://www.overleaf.com/}\\ The easy to use, online, c
\end{list1}

\vskip 5mm
\centerline{\LARGE You can do PDF presentations now, congratulations}
\end{document}
```

Starting out

Hey, wait! This is just small text files!

Yes, creating 100s of slides becomes easier

Power comes when integrating multiple files, cross references from slides to exercise booklets

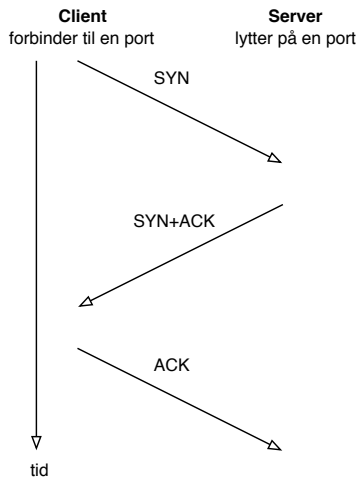
Also using `VerbatimInput` the example file was included from disk, putting code in preformatted or minted with syntaxhighlighting covers a lot of use-cases - for me

And git all the versions! ☺

Example preformatted text

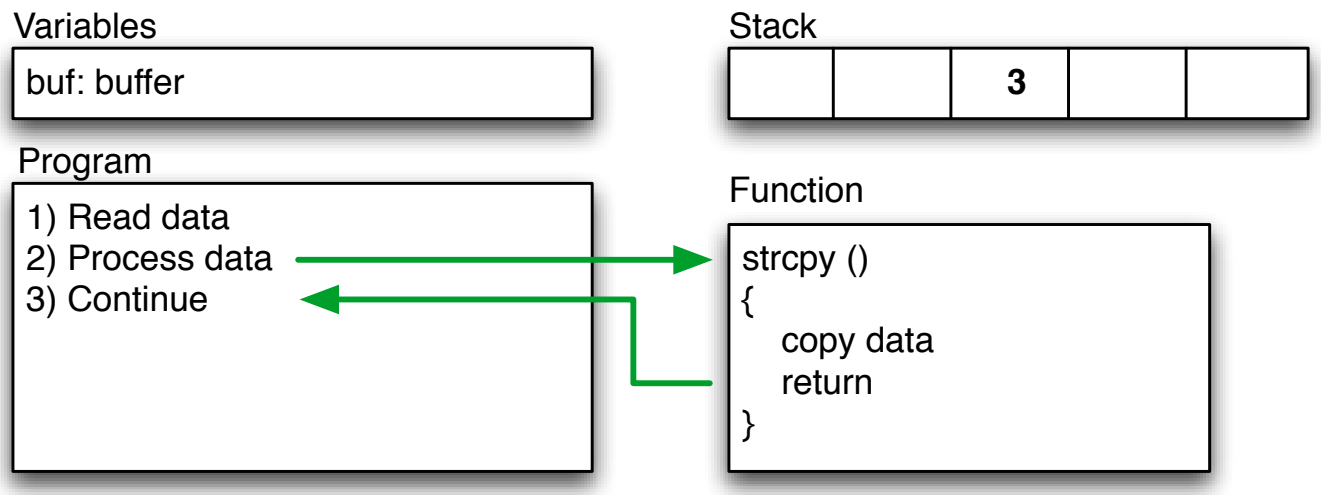
```
 #  tcpdump -i en0 host 10.20.20.129 or host 10.0.0.11
tcpdump: listening on en0
23:23:30.426342 10.0.0.200.33849 > router.33435: udp 12  [ttl 1]
23:23:30.426742 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.436069 10.0.0.200.33849 > router.33436: udp 12  [ttl 1]
23:23:30.436357 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.437117 10.0.0.200.33849 > router.33437: udp 12  [ttl 1]
23:23:30.437383 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.437574 10.0.0.200.33849 > router.33438: udp 12
23:23:30.438946 router > 10.0.0.200: icmp: router  udp port 33438 unreachable
23:23:30.451319 10.0.0.200.33849 > router.33439: udp 12
23:23:30.452569 router > 10.0.0.200: icmp: router  udp port 33439 unreachable
23:23:30.452813 10.0.0.200.33849 > router.33440: udp 12
23:23:30.454023 router > 10.0.0.200: icmp: router  udp port 33440 unreachable
23:23:31.379102 10.0.0.200.49214 > safri.domain:  6646+ PTR?
200.0.0.10.in-addr.arpa. (41)
23:23:31.380410 safri.domain > 10.0.0.200.49214:  6646 NXDomain* 0/1/0 (93)
14 packets received by filter
0 packets dropped by kernel
```

Example pictures in slide - TCP three-way handshake



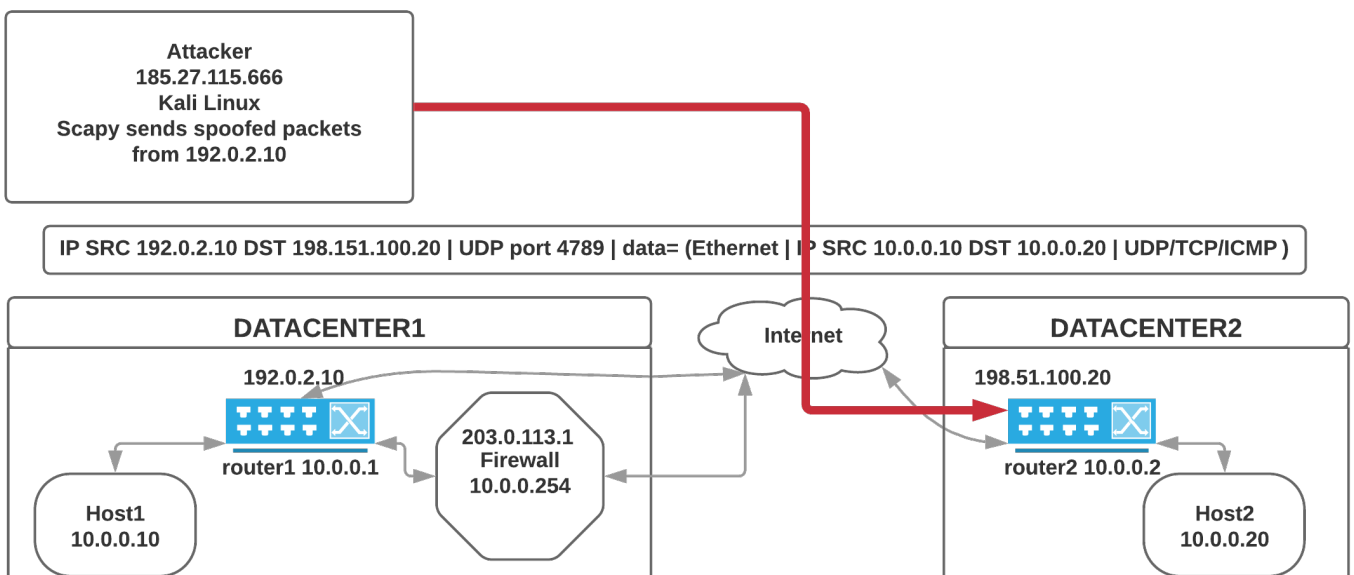
- **TCP SYN half-open** scans
- Tidligere loggede systemer kun når der var etableret en fuld TCP forbindelse
  – dette kan/kunne udnyttes til *stealth*-scans
- Hvis en maskine modtager mange SYN pakker kan dette fylde tabellen over connections op – og derved afholde nye forbindelser fra at blive oprette – **SYN-flooding**

Example: Picture and code




```
main(int argc, char **argv)
{       char buf[200];
         strcpy(buf, argv[1]);
         printf("%s\textbackslash{}n",buf);
}
```

VXLAN injection



I tested using my pentest server in one AS, sending across an internet exchange into a production network, towards Arista testing devices - no problems, it's just routed layer 3 IP+UDP packets

Example attacks, What is possible VXLAN Header

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R|R|R|R|I|R|R|R|            Reserved                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                VXLAN Network Identifier (VNI) |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Inner Ethernet Header:
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Inner Destination MAC Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Inner Destination MAC Address | Inner Source MAC Address      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Inner Source MAC Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|OptnlEthtype = C-Tag 802.1Q    | Inner.VLAN Tag Information    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Above protocol header is copied from RFC text document, and in `alltt` environment

Example: Snippets of code with minted Scapy

First create VXLAN header and inside packet

```
vxlanport=4789      # RFC 7384 port 4789, Linux kernel default 8472
vni=37              # Usually VNI == destination VLAN
vxlan=Ether(dst=routermac)/IP(src=vtepsrc,dst=vtepdst)/
   UDP(sport=vxlanport,dport=vxlanport)/VXLAN(vni=vni,flags="Instance")
broadcastmac="ff:ff:ff:ff:ff:ff"
randommac="00:51:52:01:02:03"
attacker="185.27.115.666"
destination="10.0.0.10"
# port is the one we want to contact inside the firewall
insideport=53
testport=54040
packet=vxlan/Ether(dst=broadcastmac,src=randommac)/IP(src=attacker,
    dst=destination)/UDP(sport=testport,dport=insideport)/
    DNS(rd=1,id=0xdead,qd=DNSQR(qname="www.wikipedia.org"))
```

Fun fact, Unbound on OpenBSD reply to DNS requests received in Ethernet packets with broadcast destination and IP destination being the IP of the server

Questions?

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

Email: hlk@zencurity.com