Welcome to

Core Infrastructure and BGP Intro

Building a production network

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github
core-infrastructure.tex in the repo security-courses

Goal

Don’t Panic!

Spend some hours setting up a production network:

Use VLANs, IP subnetting, routing, BGP

Use Automated provisioning scripts Ansible

Use SNMP and introduce some debugging, monitoring tools

Discuss how to Monitor, Mirror data and start an IDS

We try to do a lot, feel free to focus on specific parts

Plan for today

- Design a robust network
- Isolation and segmentation
- (Routing Security) removed, see Running a Modern Network slide set
- Switch and access security, port security
- (Wireless security) removed

Think if you could redesign your office network!

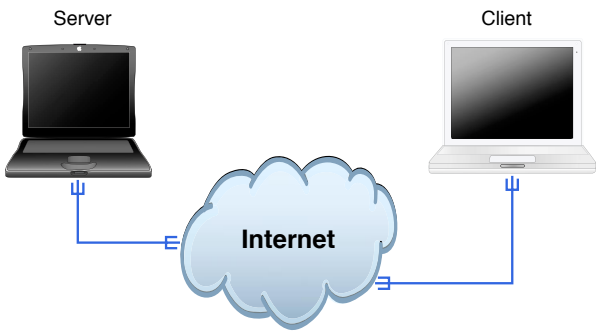
Reading Ideas

- Read
- https://nsrc.org/workshops/2018/myren-nsrc-cndo/networking/cndo/en/presentations/Campus_Security_Overview.pdf
- https://nsrc.org/workshops/2018/tenet-nsrc-cndo/networking/cndo/en/presentations/Campus_Operations_BCP.pdf
- Download, but dont read it all

  https://nsrc.org/workshops/2015/apricot2015/raw-attachment/wiki/Track1Agenda/01-ISP-Network-Design.pdf

These are good resources when you come home, and want to build networks!

Internet today



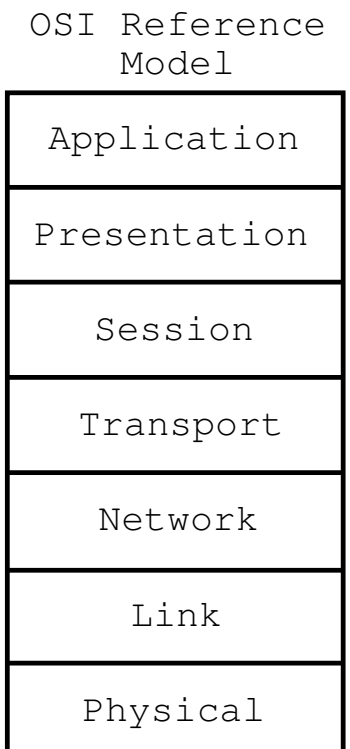
Clients and servers

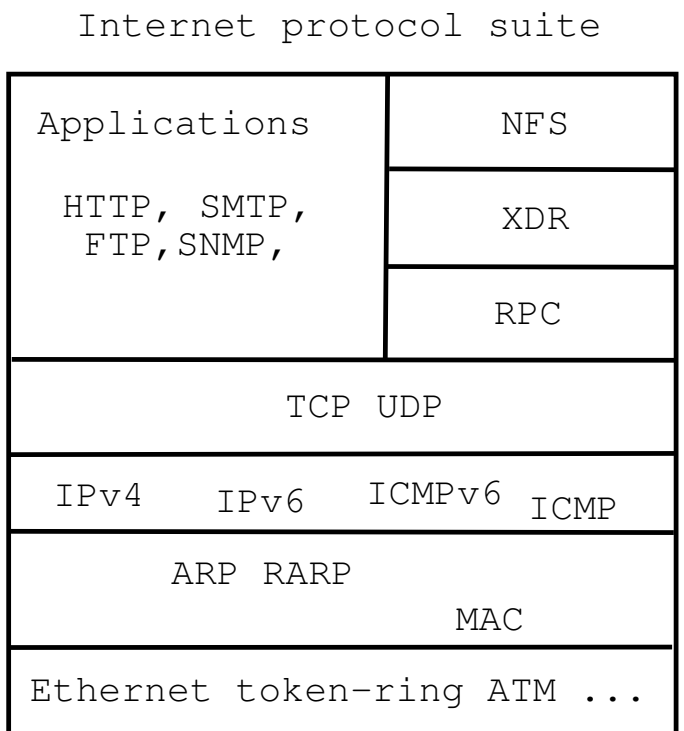
Roots in academia

Protocols more than 20 years old

HTTP is becoming encrypted, but a lot other traffic is not

OSI og Internet modellerne





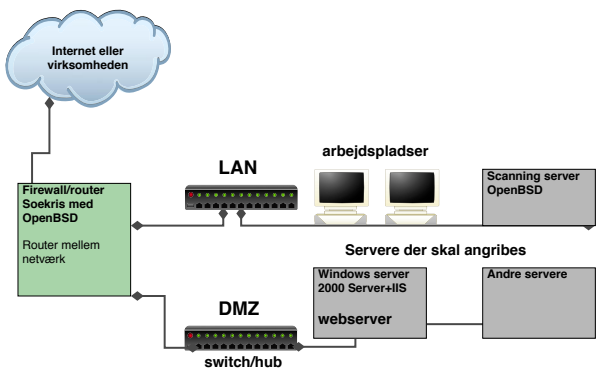
Design a robust network Isolation and segmentation

Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switche - der skal ARP spoofes og bedre performance
- Opdele med firewall til flere DMZ zoner for at holde udsatte servere adskilt fra hinanden, det interne netværk og Internet
- Overvåge, læse logs og reagere på hændelser

Husk du skal også kunne opdatere dine servere

Basic Network Security Pattern Isolate in VLANs



Du bør opdele dit netværk i segmenter efter trafik

Du bør altid holde interne og eksterne systemer adskilt!

Du bør isolere farlige services i jails og chroots

Brug port security til at sikre basale services DHCP, Spanning Tree osv.

Our Networks

We will now configure networks, using our sample switch TP-Link T1500G-10PS

Core network provides uplink through a switch / internet exchange

Each team will need:

- A switch TP-Link T1500G-10PS L2 features - default config
- USB Ethernet - or VLAN compatible virtualization network
- Ethernet cables

Exercise in networking VLANs, Routing and RPF

Each team will configure:

- Debian VM router-on-a-stick - L3 forwarding https://en.wikipedia.org/wiki/One-armed_router
- Recommended to serve DHCP service, and possibly NTP etc.
- Configure Monitoring and LibreNMS - optional
- Reconfigure uplink from static routing to BGP - optional
- Connect your IDS - optional, Configure port security - optional

Use the guides from:

https://www.tp-link.com/uk/support/download/t1500g-10ps/#Related-Documents

Packet sniffing tools

Tcpdump for capturing packets

Wireshark for dissecting packets manually with GUI

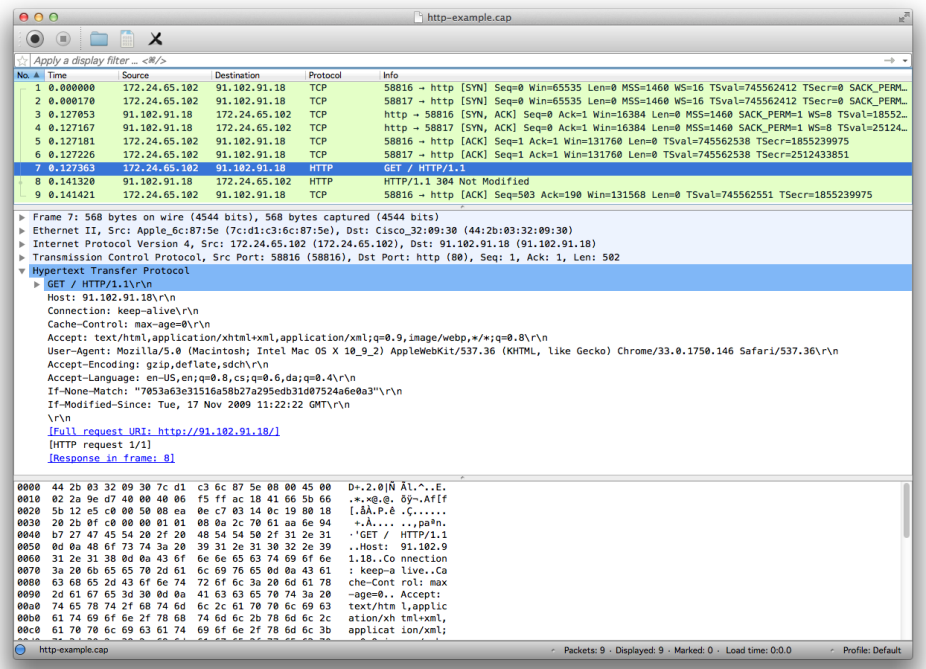
Zeek Network Security Monitor

Discuss Suricata, modern robust capable of IDS and IPS (prevention), ntopng High-speed web-based traffic analysis and Maltrail Malicious traffic detection system `https://github.com/stamparm/MalTrail`

Often a combination of tools and methods used in practice

Full packet capture big data tools also exist

Using Wireshark



https://www.wireshark.org

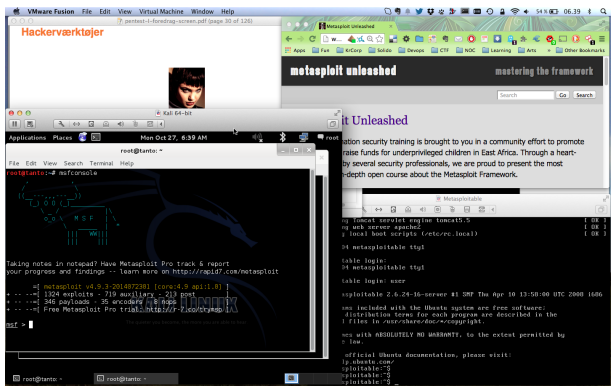
Kali Linux the pentest toolbox

Kali `http://www.kali.org/` brings together 100s of tools

100.000s of videos on youtube alone, searching for kali and $TOOL

Use this to generate bad traffic

Hackerlab setup



- Hardware: most modern laptops has CPU with virtualization
  May need to enale it in BIOS
- Software: use your favorite operating system, Windows, Mac, Linux
- Virtualization software: VMware, Virtual box, choose your poison
- Hackersoftware: Kali as a Virtual Machine `https://www.kali.org/`
- Install sniffing VM - put into *bridge mode*

What happens today?

Think like a network architect team member

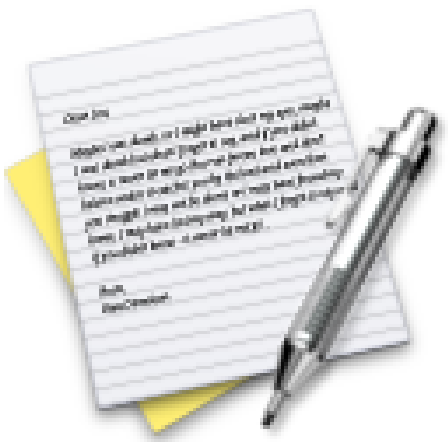
Get basic tools running

Start routing and creating a network

Improve situation, think about how to monitor while building

Today focus on the lower parts, but user interfaces are important too

Exercise

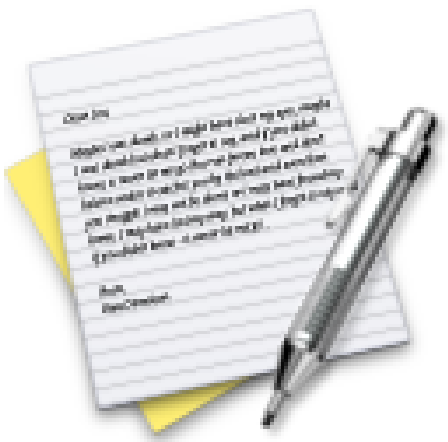


Now lets do the exercise

Bonus: Download Kali Linux Revealed (KLR) Book 10 min

which is number 1 in the exercise PDF.

Exercise

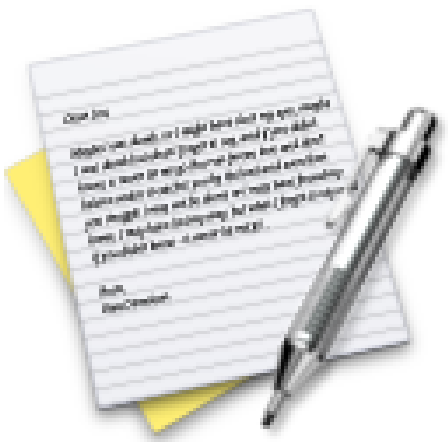


Now lets do the exercise

Bonus: Check your Kali VM, run Kali Linux 30 min

which is number 2 in the exercise PDF.

Exercise

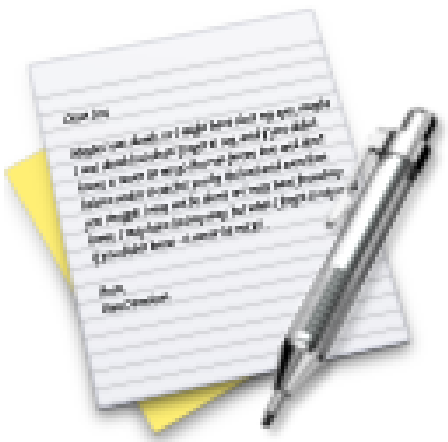


Now lets do the exercise

Bonus: Wireshark and Tcpdump 15 min

which is number 3 in the exercise PDF.

Exercise

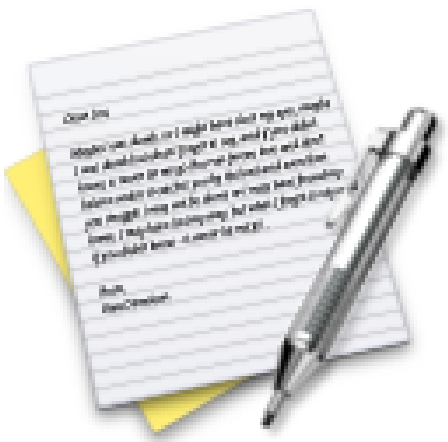


Now lets do the exercise

Bonus: Capturing TCP Session packets 10 min

which is number 4 in the exercise PDF.

Exercise

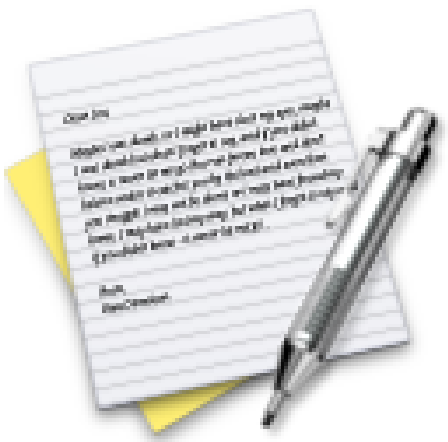


Now lets do the exercise

Bonus: Using ping and traceroute 10 min

which is number 5 in the exercise PDF.

Exercise

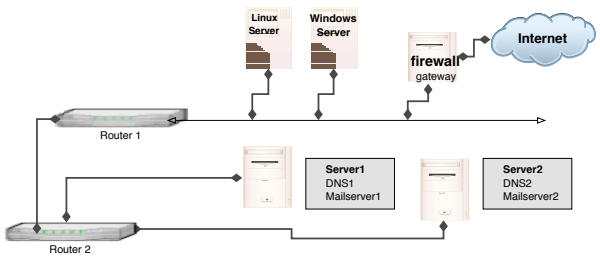


Now lets do the exercise

Bonus: DNS and Name Lookups 10 min

which is number 6 in the exercise PDF.

Network mapping



Using traceroute and similar programs it is often possible to make educated guess to network topology

Time to live (TTL) for packets are decreased when crossing a router

when it reaches zero the packet is timed out, and ICMP message sent back to source

Default Unix traceroute uses UDP, Windows tracert use ICMP

traceroute – UDP

```
 #  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
```

Low TTL, UDP, high ports above 33000 = Unix traceroute signature

Experiences gathered

Lots of information

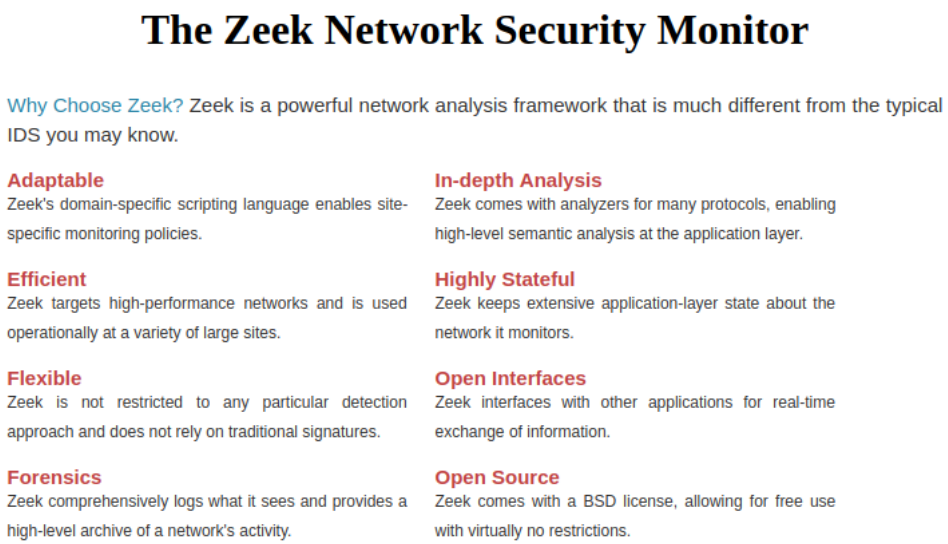
Reveals a lot about the network, operating systems, services etc.

I use a template when getting data

- Respond to ICMP: □ echo, □ mask, □ time
- Respond to traceroute: □ ICMP, □ UDP
- Open ports TCP og UDP:
- Operating system:
- … (banner information)

Beware when doing scans it is possible to make routers, firewalls and devices perform badly or even crash!

The Zeek Network Security Monitor



The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework (former name Bro)

Source `https://www.zeek.org/`, redirects to `https://www.bro.org/zeek.html`

Zeek scripts

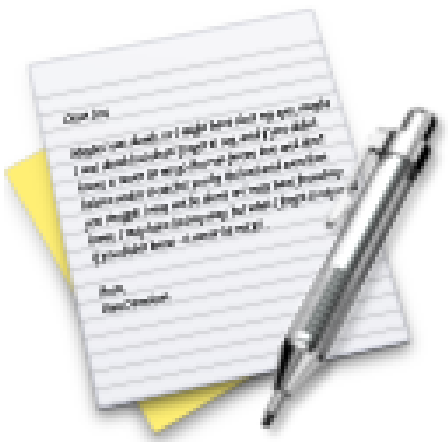
```
global dns_A_reply_count=0;
global dns_AAAA_reply_count=0;
...
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
        {
        ++dns_A_reply_count;
        }

event dns_AAAA_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
        {
        ++dns_AAAA_reply_count;
        }
```

source: dns-fire-count.bro from

https://github.com/LiamRandall/bro-scripts/tree/master/fire-scripts https://www.bro.org/sphinx-git/script-refe

scripts.html

Exercise



Now lets do the exercise

Bonus: Zeek on the web 10min

which is number 7 in the exercise PDF.

Exercise setup

We will use a combination of your virtual servers, my switch hardware and my virtual systems.

There will be sniffing done on traffic!
Don't abuse information gathered

We try to mimic what you would do in your own networks during the exercises.

Get Started with Zeek

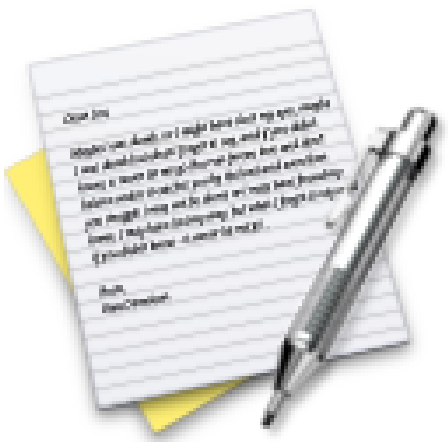
To run in “base” mode: `bro -r traffic.pcap`

To run in a “near broctl” mode: `bro -r traffic.pcap local`

To add extra scripts: `bro -r traffic.pcap myscript.bro`

Note: the project was renamed from Bro to Zeek in Oct 2018

Exercise

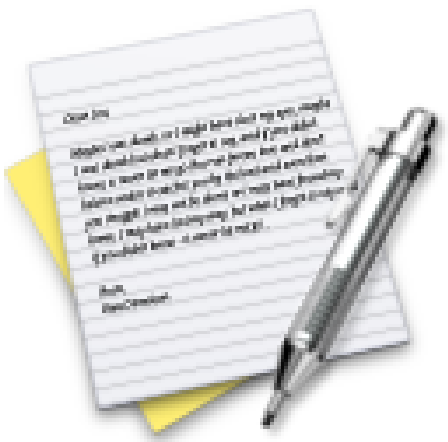


Now lets do the exercise

Bonus: Zeek DNS capturing domain names 10min

which is number 8 in the exercise PDF.

Exercise



Now lets do the exercise

Bonus: Zeek TLS capturing certificates 10min

which is number 9 in the exercise PDF.

DNS is important

Another tool that provides a basic SQL-frontend to PCAP-files

`https://www.dns-oarc.net/tools/packetq`

`https://github.com/DNS-OARC/PacketQ`

Going back in time and finding systems that visited a specific domain can explain when and where an infection started.

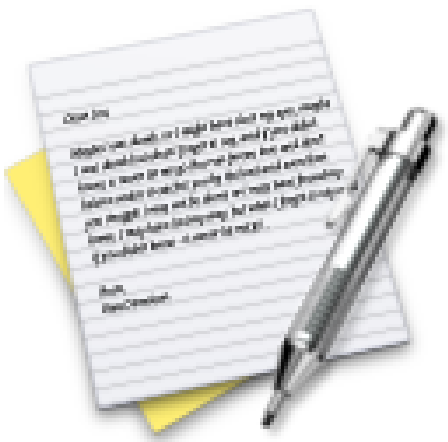
Deciding on which tool to use, Zeek or PacketQ depends on the situation.

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by th e OISF and its supporting vendors.

http://suricata-ids.org/ http://openinfosecfoundation.org

Exercise

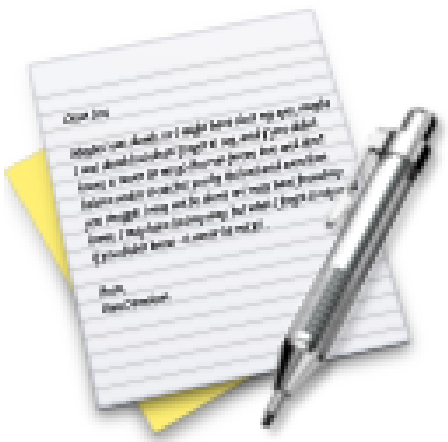


Now lets do the exercise

Check your Debian VM 10 min

which is number 10 in the exercise PDF.

Exercise

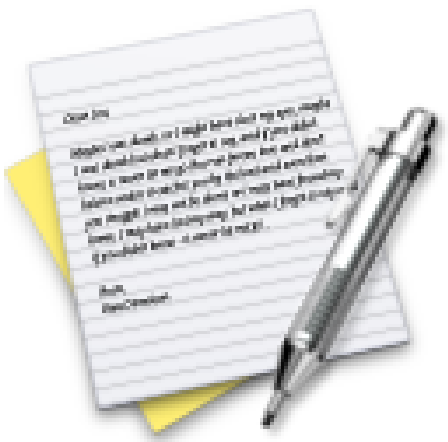


Now lets do the exercise

VLANs, Routing and RPF - 2h

which is number 11 in the exercise PDF.

Exercise

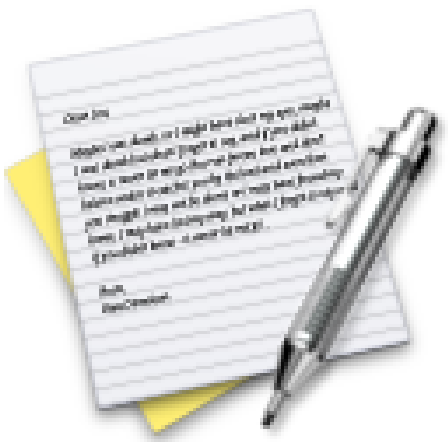


Now lets do the exercise

Configuration of DHCP server 30min

which is number 12 in the exercise PDF.

Exercise

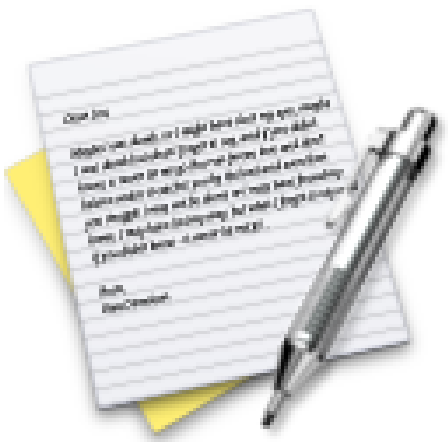


Now lets do the exercise

Bonus: Configuration of Ubound DNS server 20min

which is number 13 in the exercise PDF.

Exercise

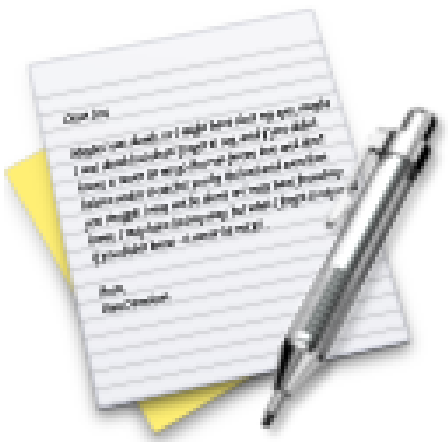


Now lets do the exercise

Bonus: Configuration of BIRD BGP daemon 40min

which is number 14 in the exercise PDF.

Exercise

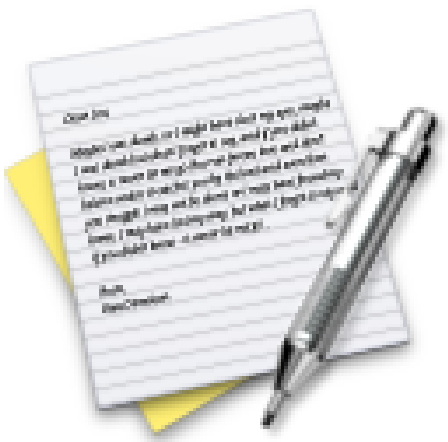


Now lets do the exercise

How to Configure Mirror Port 10min

which is number 15 in the exercise PDF.

Exercise



Now lets do the exercise

Learn about port security - 10 min

which is number 16 in the exercise PDF.

Summary

We started from a basic Ubuntu/Debian server, and we now know more about our network.

We know it is possible to create dashboards and visualizing the data.

What are the next steps?

Questions?

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Need help with infrastructure security or pentesting, ask me!

You are always welcome to send me questions later via email