Welcome to

Network Security Basics

Learn to defend your organisation

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

Slides are available as PDF, kramse@Github

network-security-basics.tex in the repo security-courses

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen, DIKU
- Email: hlk@zencurity.dk Mobile: +45 2026 6000

You are welcome to drop me an email

Goals: Network Security Basics

- Introduce networking and related security issues
- Introduce resources, programs, people, authors, documents, sites that further your exploration into network security
- Introduce security problems that have haunted us in +35 years
- Suggest methods and ways to reduce problems, longer lasting than patching
- Create an understanding of a more paranoid mindset – take control of your networks
- Network configuration of existing equipment, mostly enterprise networks 🚩

Red flags are considered check points, actions, something I think you should investigate

Plan for Today

A blue-team introduction to Communication and Network Security

- Network information TCP/IP
- Challenges in network security
- The basic tools for countering threats
- Introduce the encryption protocols in use in networks
  Virtual Private Network (VPN) and Transport Layer Services (TLS).
- Network segmentation will be discussed
- How tools like Firewalls, Access Control Lists (ACL) and VLANs can help reduce risk for the network.
- Examples from Zeek Security Monitor for getting information about flows

Duration: 4 hours - with breaks

Keywords: Encryption, TLS, VPN, VLAN IEEE 802.1q, Wifi security, IEEE 802.1x

Time schedule

- 17:00 - 18:15 Introduction and basics
- 30min break Eat and mingle, hang around, get coffee/tea
- 18:45 - 19:30 45min Walking through the technologies and protection
- 15min break
- 19:45 -20:30 45min More about components used for building secure and robust networks
- 20:30 - 21:00 playtime, questions, demo, discussion

About Equipment and Exercises

- Bringing a laptop is not required, but welcome.
- Exercises booklets are available for many of my courses, see Github
  but it is expected that participants will do any exercises on their own later or at the scheduled hacker days
- The hacker days will be announced in various places
- Events like BornHack are excellent places to arrange hacker days in the network warrior village, or other places
- I announce mine at https://nwwc.dk

Invite a few friends, make a hacker day and work together!

Course Materials

This material is in multiple parts:

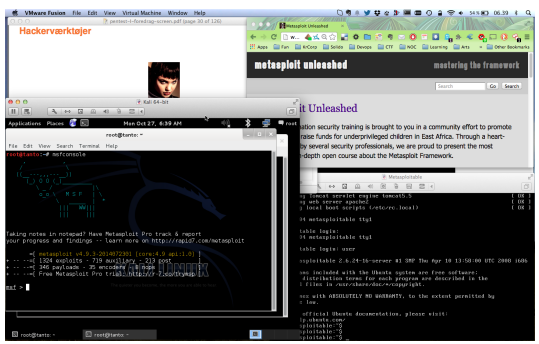
- Slide shows - presentation - this file
- Exercises - PDF files in my repository

Links

- All materials will be released as open source at:
  https://github.com/kramse/security-courses/
- Additional resources from the internet linked from lecture plans:
  https://zencurity.gitbook.io/kea-it-sikkerhed/

Note: slides and materials will mostly be in english, but presentation language will be danish

Hackerlab Setup



- Hardware: modern laptop CPU with virtualisation
  Dont forget to enable hardware virtualisation in the BIOS
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine https://www.kali.org/

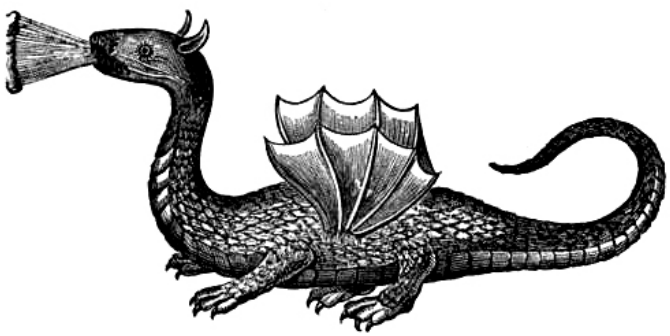
Networking Hardware

If you want to do exercises, sniffing data it
will be an advantage to have a wireless USB network card.

- The following are two recommended models:
- TP-link TL-WN722N hardware version 2.0 cheap
- Alfa AWUS036ACH 2.4GHz + 5GHz Dual-Band and high performing
- Often you need to compile drivers yourself, and research a bit
- Get an USB 3.0 1Gbit Ethernet too

Getting an USB card allows you to use the regular one for the main OS, and insert the USB into the virtual machine

Networks are trouble



Internet here be dragons

- Networks are constantly evolving
- Threats are constantly increasing
- Vulnerabilities are found daily
- Even more vulnerabilities are *developed* and *installed*
  Sorry developers, but some of you don't care, and it shows!

Internet is based on Open Standards and collaboration!

> We reject kings, presidents, and voting.
> We believe in rough consensus and running code.
> – The IETF credo Dave Clark, 1992.

- Request for comments - RFC – series of documents describing internet standards
- RFC, BCP, FYI, informational
  First ones from 1969
- Never changed but status changed to Obsoleted when a never version or document superseeds it
  (Errata exist and are published though)
- Standards track:
  Proposed Standard $\rightarrow$ Draft Standard $\rightarrow$ Standard
- Open standards gurantee transparency, but not security

What is the Internet

Communication between humans - currently!

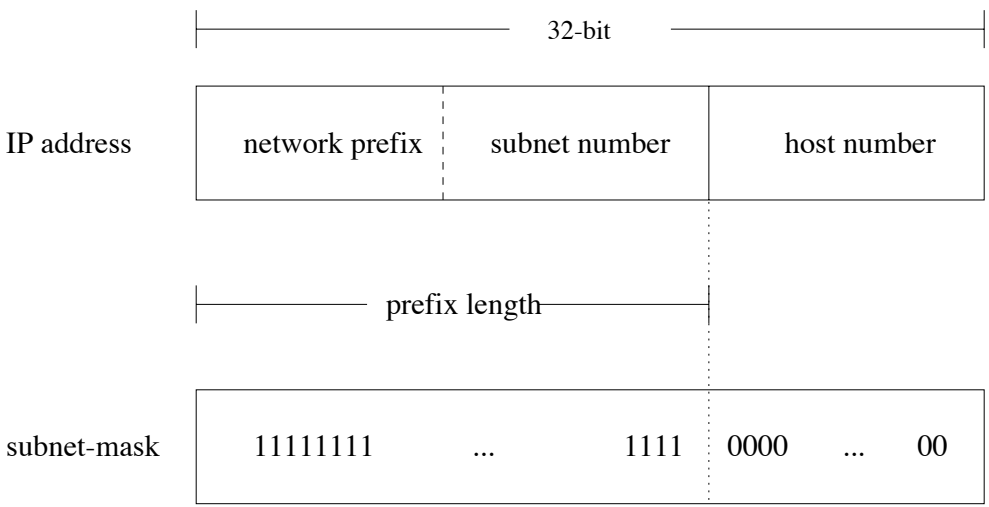
Based on TCP/IP

- best effort
- packet switching (IPv6 calls it packets, not datagram)
- *connection-oriented* TCP
- *connection-less* UDP

RFC-1958:

> A good analogy for the development of the Internet is that of constantly renewing the individual streets and buildings of a city, rather than razing the city and rebuilding it. The architectural principles therefore aim to provide a framework for creating cooperation and standards, as a small "spanning set"of rules that generates a large, varied and evolving space of technology.

Common Address Space



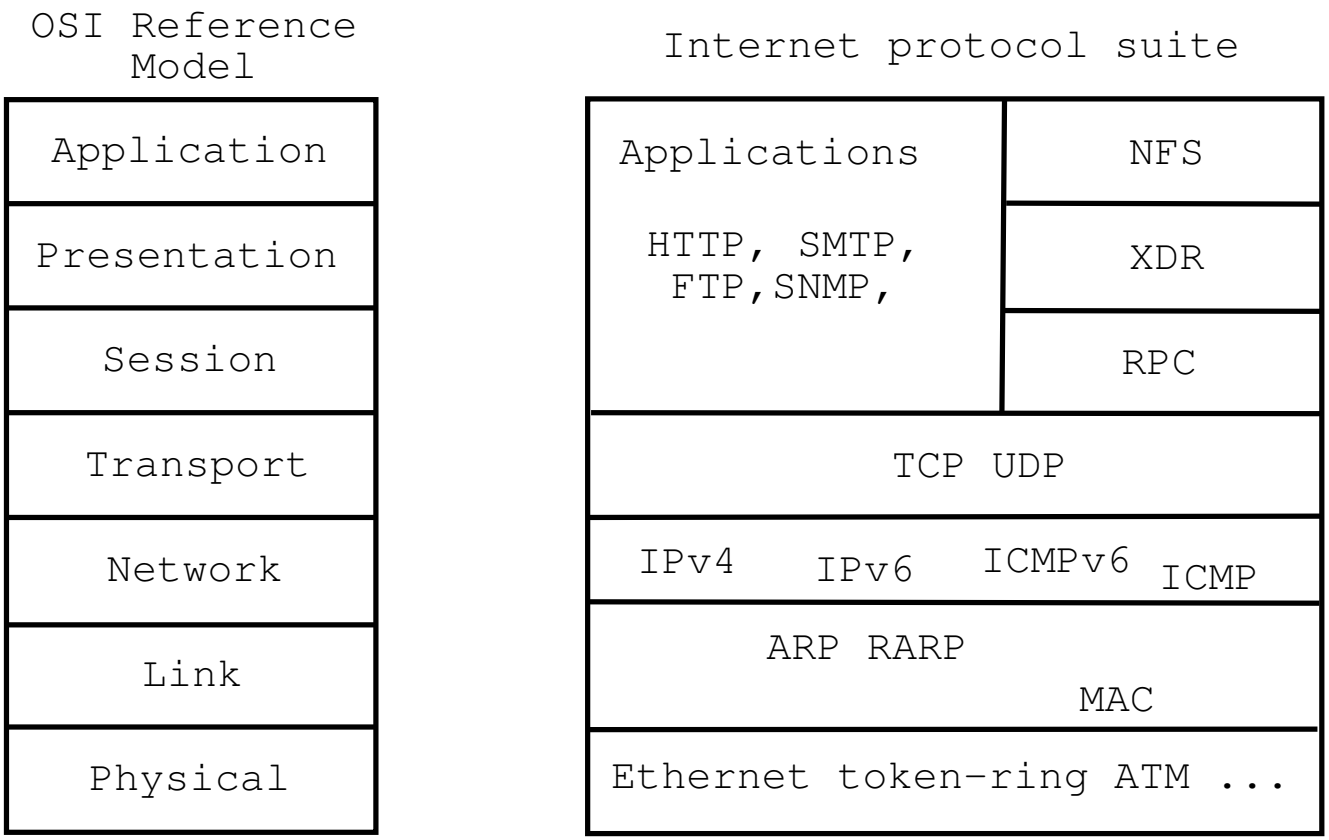
- Internet is defined by the address space
- IPv4 based on 32-bit addresses, example dotted decimal format 10.0.0.1
- IPv6 very similar to IPv4 without NAT, 128-bit addresses in hex ::1, 2a06:d380:0:101::80

CIDR Classless Inter-Domain Routing

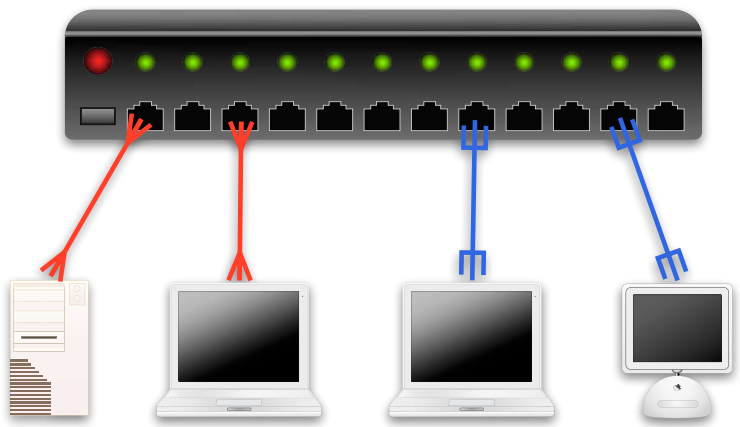
Classful routing		Classless routing CIDR	
4 class C networks	Inherent subnet mask	Supernet	Subnet mask
192.0.8.0	255.255.255.0	192.0.8.0	255.255.252.0
192.0.9.0	255.255.255.0		252d=11111100b
192.0.10.0	255.255.255.0		
192.0.11.0	255.255.255.0	Base network/prefix	
		192.10.8.0/22	

- Subnet mask originally inferred by the class
- Started to allocate multiple C-class networks - save remaining B-class
  Resulted in routing table explosion - btw Stop using A, B, C
- A subnet mask today is a row of 1-bit
- Supernet, supernetting
- 10.0.0.0/24 means the network 10.0.0.0 with 24 subnet bits (mask 255.255.255.0)
- 2a06:d380:0:101::80/64 means the network with 64-bit prefix length

Protocols: OSI and Internet models



A switch



Today we use switches, Don't buy a hub, not even for experimenting or sniffing

A switch can receive and send data on multiple ports at the same time

Performance only limited by the backplane and switching chips

Can also often route with the same speed and mirror packets

MAC address

```
00-03-93    (hex)        Apple Computer, Inc.
000393      (base 16)    Apple Computer, Inc.
                         20650 Valley Green Dr.
                         Cupertino CA 95014
                         UNITED STATES
```

Network technologies use a layer 2 hardware address

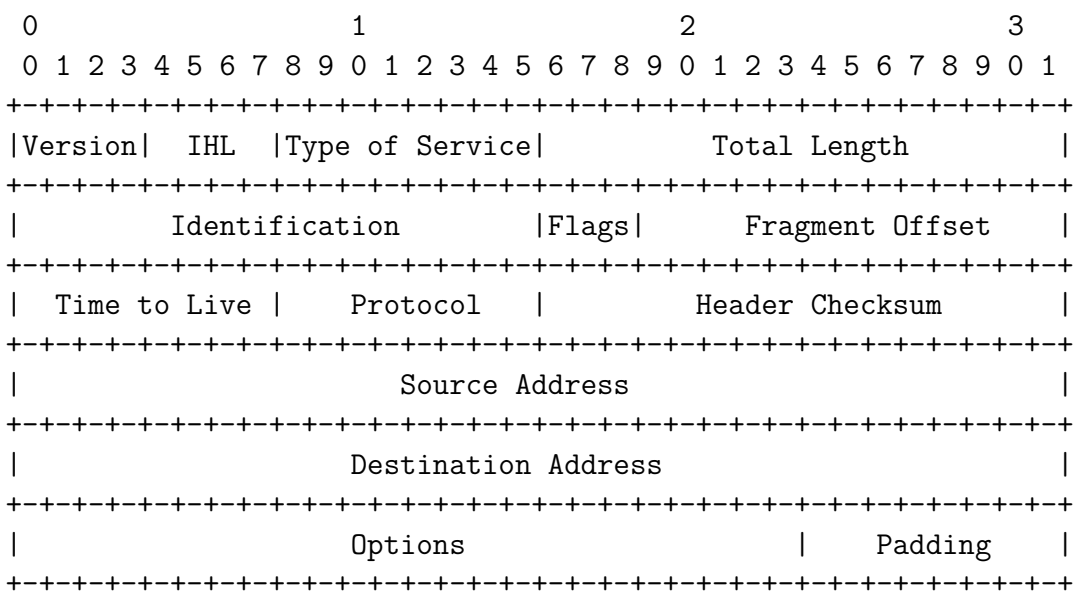
Typically using 48-bit MAC addresses known from Ethernet MAC-48/EUI-48

First half is assigned to companies – Organizationally Unique Identifier (OUI)

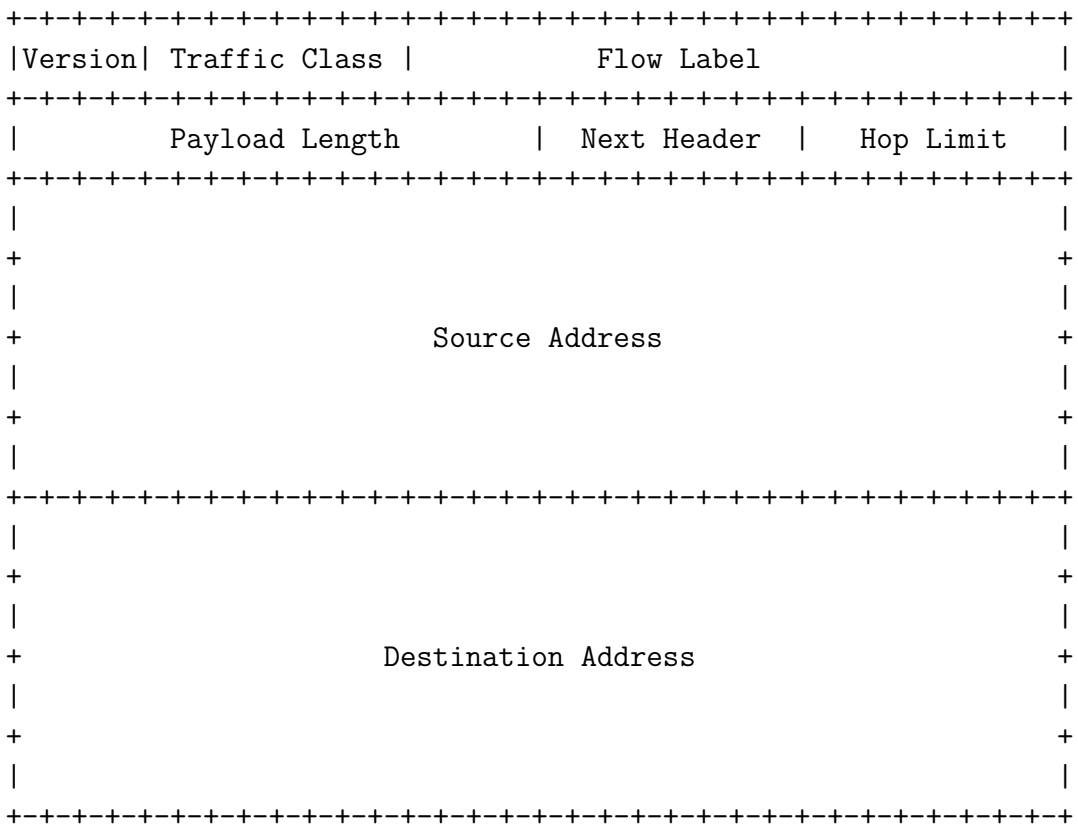
Using the OUI you can see which producer and roughly when a network chip was produced

http://standards.ieee.org/regauth/oui/index.shtml

IPv4 packets – header - RFC-791



IPv6 packets – header - RFC-2460



TCP/IP Protocol Suite

Security Problems in the TCP/IP Protocol Suite

*S.M. Bellovin**
smb@ulysses.att.com

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

- *Security problems in the TCP/IP protocol suite*, S. M. Bellovin April 1989, https://www.cs.columbia.edu/~smb/papers/ipext.pdf
- *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* 2004, https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf

Security problems in the TCP/IP Suite

> The paper "Security Problems in the TCP/IP Protocol Suite" was originally pub- lished in Computer Communication Review, Vol. 19, No. 2, in April, 1989

Some problems described in the original:

sequence number spoofing

routing attacks,

source address spoofing

authentication attacks

Should have been fixed by now!

But really, our networks are NOT secure today

Routing attacks

Problems described in the original from 1989:

- IP Source routing attacks - use a specific source
  Usually not a problem today, ICMP redirect not used much, but layer 2 with ARP spoofing IS a problem
- Routing Information Protocol Attacks
  The Routing Information Protocol [15] (RIP) - RIP is outdated, but using STP, OSPF etc. without authentication is similar
- Border Gateway Protocol (BGP) still used today, still problems
- Domain Name System (DNS) problems
- Simple Network Management Protocol (SNMP) problems

Fun packets with Yersinia could still break a lot of networks https://github.com/tomac/yersinia

So we still have problems on all layers

Still TCP/IP Problems?

Recent example from 2020:

> The JSOF research lab has discovered a series of zero-day vulnerabilities in a widely used low-level TCP/IP software library developed by Treck, Inc. The 19 vulnerabilities, given the name Ripple20, affect hundreds of millions of devices (or more) and include multiple remote code execution vulnerabilities.
>
> **Pre-emptive traffic filtering is an effective technique that can be applied as appropriate to your network environment.**

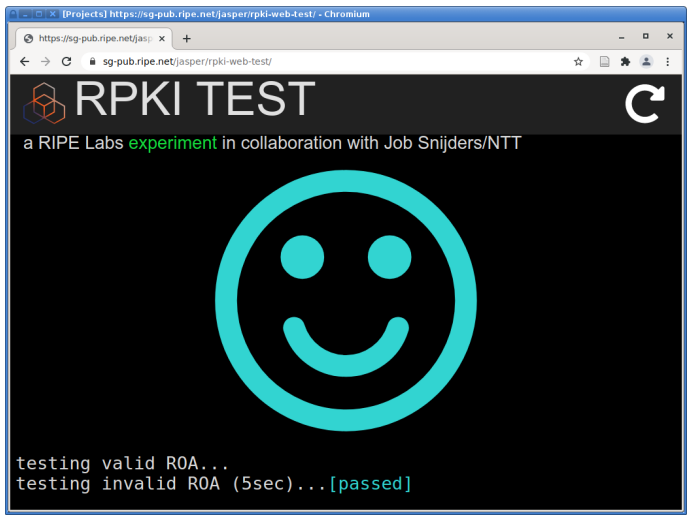
Source: https://www.jsof-tech.com/ripple20/

- I highly recommend old and known technologies like firewalls – both network and hosts
- Isolation into different VLANs and zones
- Layer 2 attacks only work if you are in the same L2 zone!

Routing and BGP Solutions

- Filtrering, ingress / egress:
  "reject external packets that claim to be from the local net"
- See also Reverse Path forwarding https://en.wikipedia.org/wiki/Reverse-path_forwarding
- Routers and routing protocols must be more skeptical
  Routing filters implemented everywhere, auth on routing protocols OSPF/BGP etc.
- Has been recommended for some years, but not done in all organisations
- BGP routing Resource Public Key Infrastructure RPKI
- BCP38 is RFC2827: *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
  http://www.bcp38.info/
- *Mutually Agreed Norms for Routing Security*, https://www.manrs.org/

RPKI Testing



- Check your own networks! Ask your ISP to check RPKI
  https://sg-pub.ripe.net/jasper/rpki-web-test/
- Read more about RPKI at:
  https://www.ripe.net/manage-ips-and-asns/resource-management/rpki

DNS Problems

5.3 The Domain Name System

The Domain Name System (DNS) [32][33] provides for a distributed database mapping host names to IP addresses. An intruder who interferes with the proper operation of the DNS can mount a variety of attacks, including denial of service and password collection. There are a number of vulnerabilities.

Source: *Security Problems in the TCP/IP Protocol Suite*, S.M. Bellovin 1989
https://www.cs.columbia.edu/~smb/papers/ipext.pdf

We have a lot of the same problems in DNS today

Plus some more caused by middle-boxes, NAT, DNS size, DNS inspection

- DNS must allow both UDP and TCP port 53
- **Your DNS servers must have updated software, see DNS flag days**
  https://dnsflagday.net/ after which kludges will be REMOVED!
- **Use DNSSEC now!**

SNMP Problems

5.5 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) [37] has recently been defined to aid in network management. Clearly, access to such a resource must be heavily protected. The RFC states this, but also allows for a null authentication service; this is a bad idea. **Even a "read-only" mode is dangerous;** it may expose the target host to netstat-type attacks if the particular Management Information Base (MIB) [38] used includes sequence numbers. (The current standardized version does not; however, the MIB is explicitly declared to be extensible.)

Source: *Security Problems in the TCP/IP Protocol Suite*, S.M. Bellovin 1989
https://www.cs.columbia.edu/~smb/papers/ipext.pdf

True - still there, still useful, still dangerous – use SNMPv3!

If you must use SNMPv2 then at least put it into separate VLAN! 🚩

Local Networks – LAN problems

6.1 Vulnerability of the Local Network

Some local-area networks, notably the Ethernet networks, are extremely vulnerable to eavesdropping and host-spoofing. If such networks are used, physical access must be strictly controlled. It is also unwise to trust any hosts on such networks if any machine on the network is accessible to untrusted personnel, unless authentication servers are used. If the local network uses the Address Resolution Protocol (ARP) [42] more subtle forms of host-spoofing are possible. In particular, it becomes trivial to intercept, modify, and forward packets, rather than just taking over the host's role or simply spying on all traffic.

Today we can send MPLS or VXLAN spoofed packets across the internet/layer 3 and inject ARP behind firewalls, in some cloud infrastructure cases ...

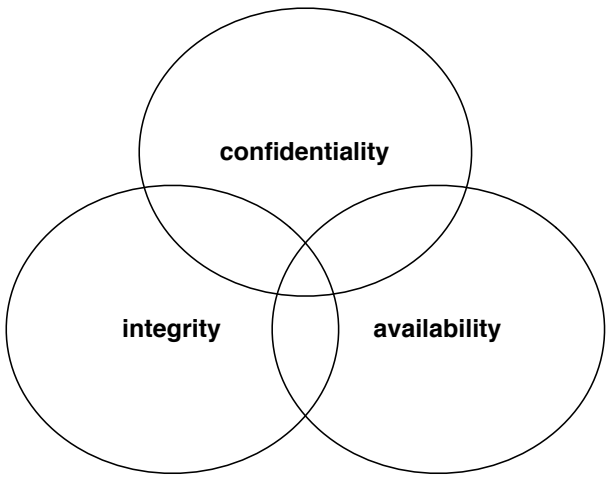
https://github.com/kramse/security-courses/tree/master/presentations/network/vxlan-troopers19

A Look Back at "Security Problems in the TCP/IP Protocol Suite" about 1989 + 31 years = 2020 – wow

Networks are Built from Components

Photo by Eugen Str on Unsplash

Confidentiality Integrity Availability



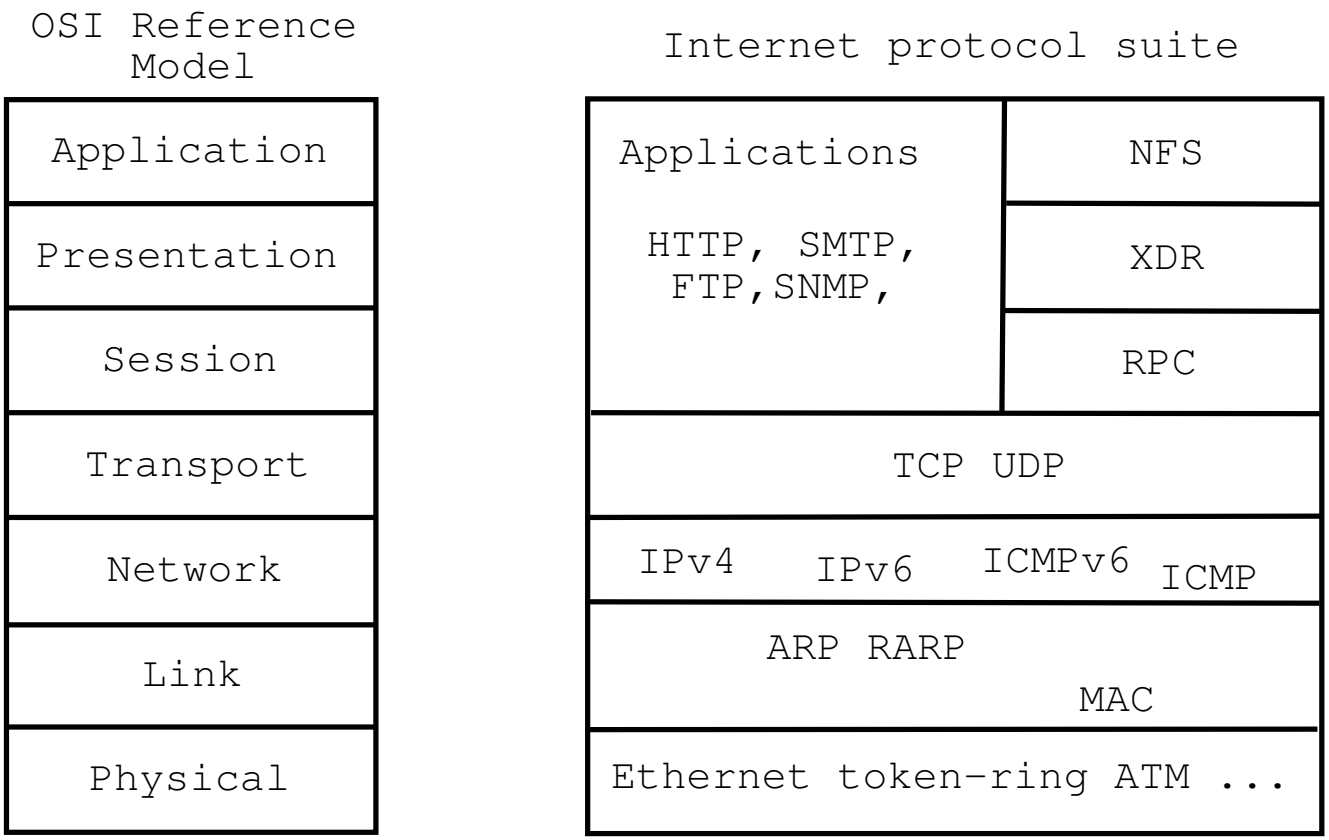
We want to protect something

Confidentiality - data holdes hemmelige

Integrity - data ændres ikke uautoriseret

Availability - data og systemet er tilgængelige når de skal bruges

Protocols: OSI and Internet models



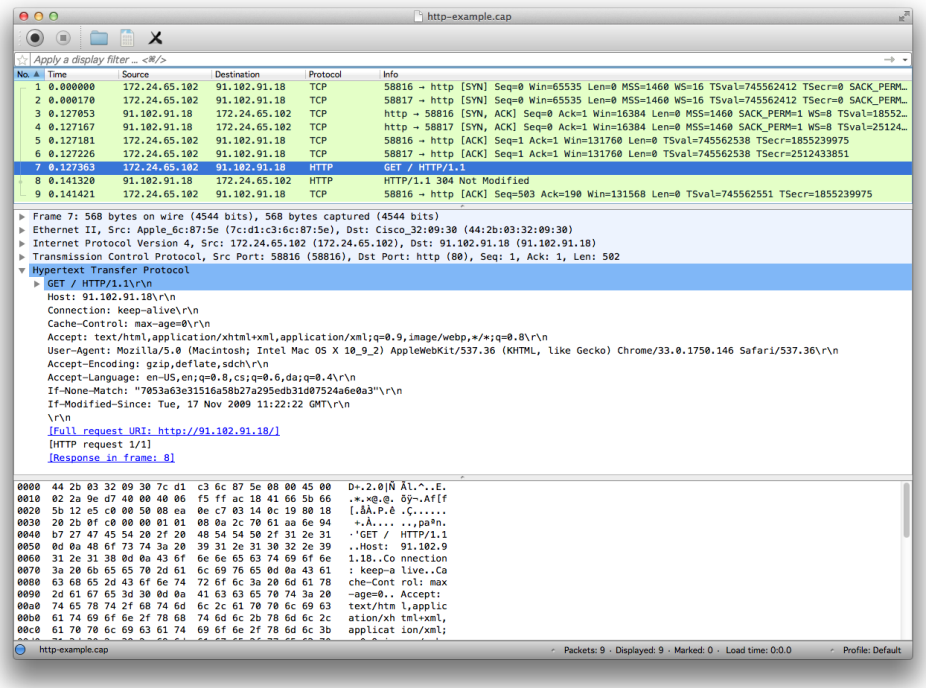
Knowledge and insight

- Networks have end-points and conversations on multiple layers
- Wireshark is advanced, try right-clicking different places
- Name resolution includes low level MAC addresses, and IP - names

- Tcpdump format, built-in to many network devices
- Remote packet dumps, like `tcpdump -i eth0 -w packets.pcap`
- Story: tcpdump was originally written in 1988 by Van Jacobson, Sally Floyd, Vern Paxson and Steven McCanne who were, at the time, working in the Lawrence Berkeley Laboratory Network Research Group https://en.wikipedia.org/wiki/Tcpdump

Great network security comes from knowing networks!

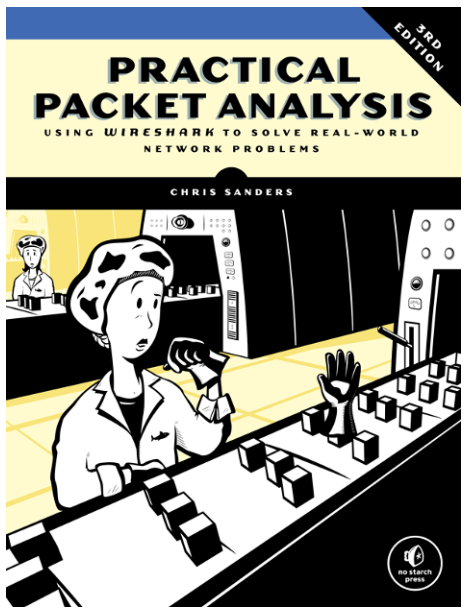
Wireshark - graphical network sniffer



Capture - Options, select a network interface

http://www.wireshark.org

Book: Practical Packet Analysis (PPA)



Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition April 2017, 368 pp. ISBN-13: 978-1-59327-802-1

https://nostarch.com/packetanalysis3

Network Knowledge Needed

To work with network security the following protocols are the bare minimum to know about.

- ARP Address Resolution Protocol for IPv4
- NDP Neighbor Discovery Protocol for IPv6
- IPv4 & IPv6 – the basic packet fields source, destination,
- ICMPv4 & ICMPv6 Internet Control Message Protocol
- UDP User Datagram Protocol
- TCP Transmission Control Protocol
- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System

A little Linux knowledge is also **highly recommended**

Well-Known Port Numbers

IANA maintains a list of magical numbers in TCP/IP

Lists of protocl numbers, port numers etc.

A few notable examples:

- Port 25/tcp Simple Mail Transfer Protocol (SMTP)
- Port 53/udp and 53/tcp Domain Name System (DNS)
- Port 80/tcp Hyper Text Transfer Protocol (HTTP)
- Port 443/tcp HTTP over TLS/SSL (HTTPS)

Source: http://www.iana.org

Best Current Practice

Lets get this out of the way immediately, you should already be doing

- Network segmentation and filtering – we could write a book about this! 🚩
- Monitor your network – both bandwidth, error, netflow etc. 🚩
- Take control of your network, no more admin/admin logins on core devices 🚩
- Turn on authentication for protocols – routing protocols but also any http service within your org 🚩
- Configure host-based firewalls 🚩
- Control DNS – internally and externally, recursive, authoritative etc. 🚩

This goes for IPv4-only, IPv6-only, and mixed networks!

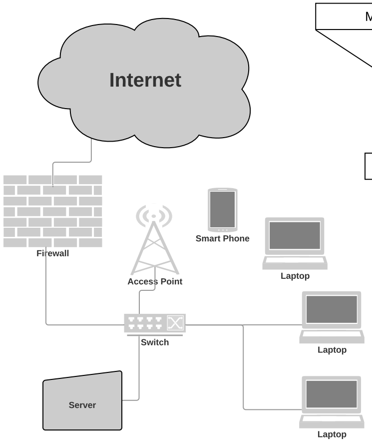
Internet in a Box

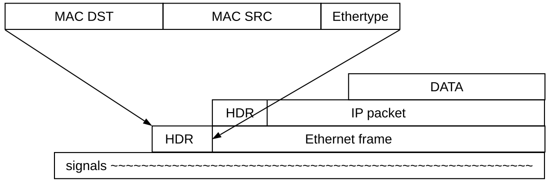
The main purposes for bringing this box, is to show

- These are standard devices, Juniper EX3300 cheap oldish, works great
- Managed switches are a must! You can learn by buying cheap ones, like the TP-Link T1500G-10PS shown, VLAN, SNMP, Syslog ...
- Multiple systems created using PC Engines APU2C4 (really D4) running OpenBSD, Unbound, Suricata, Zeek, DHCP, router advertisement, PF firewall - explicit and nice ICMPv6 filtering ...
- Attack systems compact PCs or laptop
- Creating a home lab is not expensive, bought the Arista 7150 24-port 10G used on ebay

You should have similar (or better) devices in your production network, and they can be configured to do a LOT more than you use them for right now

Protection, building secure and robust networks





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

- We should prefer security mechanisms that does NOT require us to keep patching every month
- Can we change our networks to avoid this? Yes!

All attacks have signatures, some more noisy than others

Table 12-1: Common Passive Fingerprinting Values

Protocol header	Field	Default value	Platform
IP	Initial time to live	64	NMap, BSD, OS X, Linux
		128	Novell, Windows
		255	Cisco IOS, Palm OS, Solaris
IP	Don't fragment flag	Set	BSD, OS X, Linux, Novell, Windows, Palm OS, Solaris
		Not set	Nmap, Cisco IOS
TCP	Maximum segment size	0	Nmap
		1440–1460	Windows, Novell
		1460	BSD, OS X, Linux, Solaris

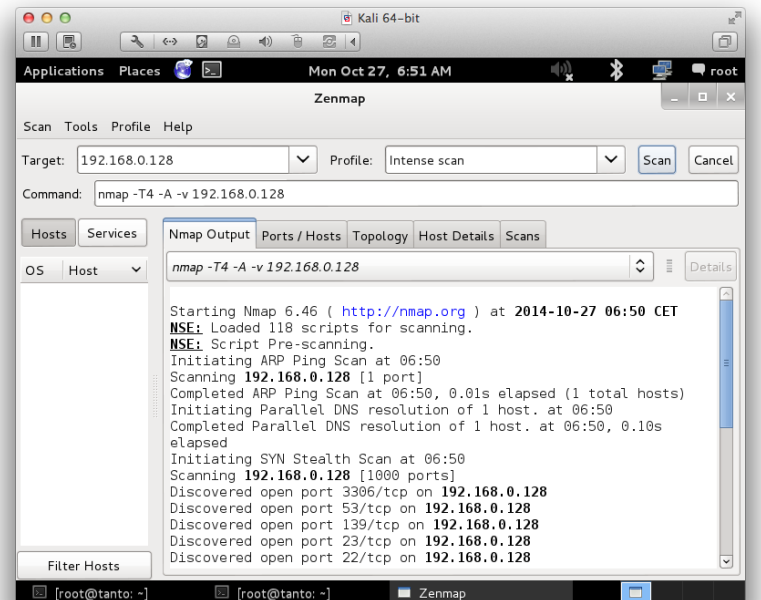
(continued)

Systems can also be fingerprinted on various levels

Discover, filter, harden, reduce attack surfaces

Know your network!

Portscan using Zenmap GUI



Zenmap is available on Kali Linux as `apt install zenmap-kbx`
https://www.kali.org/blog/introducing-kaboxer/

FTP File Transfer Protocol

File Transfer Protocol – file transfer

FTP send the data, including username and pasword in cleartext messages
USER username
PASS your-not-so-secret-password

Some varianets can use TLS, but IMHO better to use HTTPS or SCP/SFTP over Secure Shell protocol

Please kill FTP when you see it! 🚩

Person in the Middle Attacks

- ARP spoofing, ICMP redirects, the classics
- Used to be called Man in The Middle (MiTM)
- ICMP redirect
- ARP spoofing
- Wireless listening and spoofing higher levels like airpwn-ng https://github.com/ICSec/airpwn-ng
- Usually aimed at unencrypted protocols
- Yes, you can do ARP spoofing on a switched network, and also VXLAN and MPLS has some interesting possibilities
- Yes, segment your network to avoid it – use IEEE 802.1q VLANs 🚩

Network Security Threats

Low level and Network Layer Attacks

- "Yersinia is a network tool designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems."
  evil l2 tools - STP, CDP, DTP, DHCP, HSRP, IEEE 802.1Q, IEEE 802.1X, ISL, VTP
  https://github.com/tomac/yersinia
- IP based creating strange fragments, overlapping, missing, SMALLL with fragroute/fragrouter
- LAND - same destination and source address
- THC-IPV6 - attacking the IPV6 protocol suite

Note: Evil repeats itself, like doing ARP poisoning across MPLS or VXLAN

Attackers are very creative!

Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication

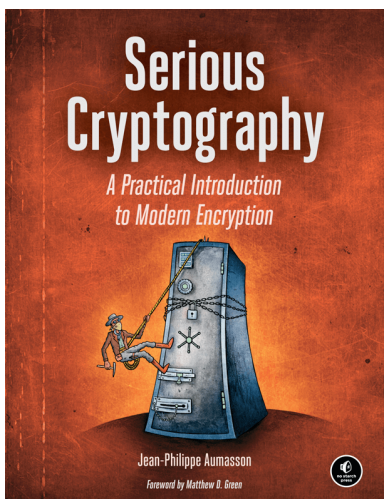
Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key, to ensure confidentiality, example algorithm AES

Public-key cryptography (like RSA) uses two related keys, a key pair of a public key and a private key. This allows for easier key exchanges, and can provide confidentiality, and methods for signatures and other services

Source: https://en.wikipedia.org/wiki/Cryptography

Serious Cryptography



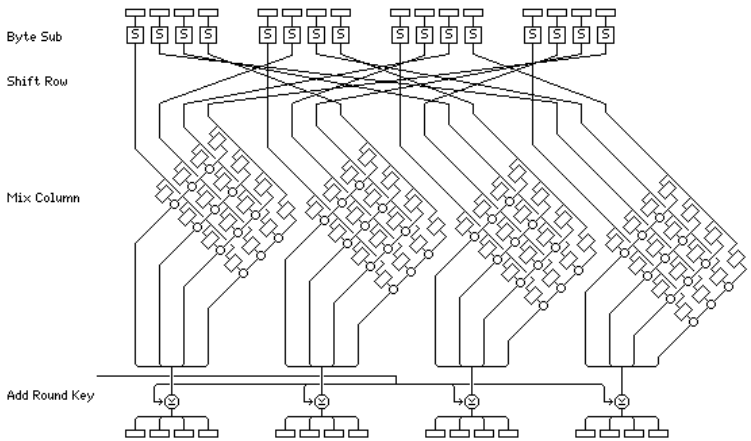
Serious Cryptography A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson November 2017, 312 pp. ISBN-13: 978-1-59327-826-7 https://nostarch.com/seriouscrypto

RSA

> RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. ... In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978.

- Key sizes 1,024 to 4,096 bit typical
- Quote from: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

AES Advanced Encryption Standard



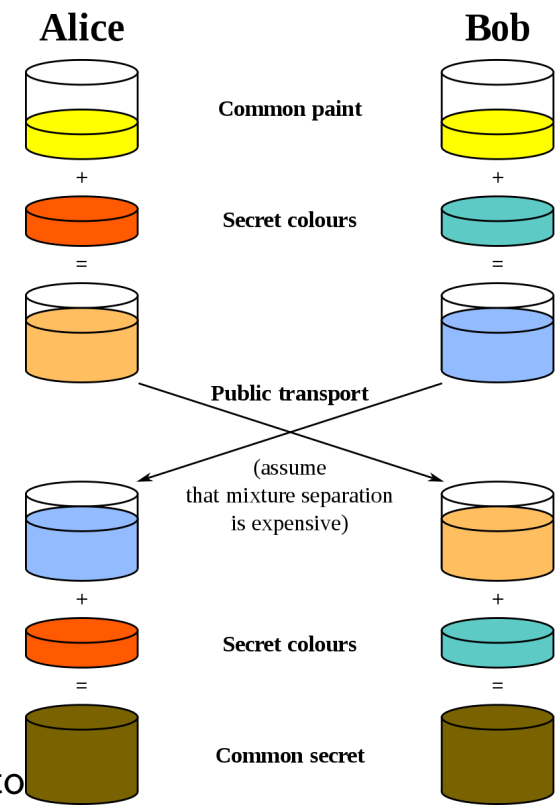
- The official Rijndael web site displays this image to promote understanding of the Rijndael round transformation [8].
- Key sizes 128,192,256 bit typical
- Some extensions in cryptosystems exist: XTS-AES-256 really is 2 instances of AES-128 and 384 is two instances of AES-192 and 512 is two instances of AES-256
- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Elliptic Curve

> Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.[1]

- Today we also use elliptic curve math for encryption https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
- A lot of what we do is based on the works by Dan J. Bernstein https://cr.yp.to/ with others
- Example curve Curve25519 https://en.wikipedia.org/wiki/Curve25519:
  Also in 2018, RFC 8446 was published as the new Transport Layer Security v1.3 standard. It requires mandatory support for X25519, Ed25519, X448, and Ed448 algorithms.[24]

Encryption on the web – Diffie Helman exchange



Diffie–Hellman key exchange (DH)[nb 1] is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.[1][2] DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. ... The scheme was first published by Whitfield Diffie and Martin Hellman in 1976

- Quote from: https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
- This is used as part of Transport Layer Security (TLS)
- Stanford professor Dan Boneh and Victor Shoup are creating a graduate course crypto book https://toc.cryptobook.us/

Email Security 2022 – Goals

- SPF Sender Policy Framework

  https://en.wikipedia.org/wiki/Sender_Policy_Framework
- DKIM DomainKeys Identified Mail

  https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail
- DMARC Domain-based Message Authentication, Reporting and Conformance

  https://en.wikipedia.org/wiki/DMARC
- DANE DNS-based Authentication of Named Entities

  https://en.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities

SMTP TLS

> The STARTTLS command for IMAP and POP3 is defined in RFC 2595, for SMTP in RFC 3207, for XMPP in RFC 6120 and for NNTP in RFC 4642. For IRC, the IRCv3 Working Group has defined the STARTTLS extension. FTP uses the command "AUTH TLS"defined in RFC 4217 and LDAP defines a protocol extension OID in RFC 2830. HTTP uses upgrade header.

SMTP was extended with support for Transport Layer Security TLS

Also called **Opportunistic TLS**, where the quote is also from:
https://en.wikipedia.org/wiki/Opportunistic_TLS

Now we have MTA Strict Transport Security (MTA-STS) RFC 8461
so we can announce that we only accept encrypted email!

It is 2022 you should ALL turn off unencrypted SMTP 🚩

Check your web and mail server settings

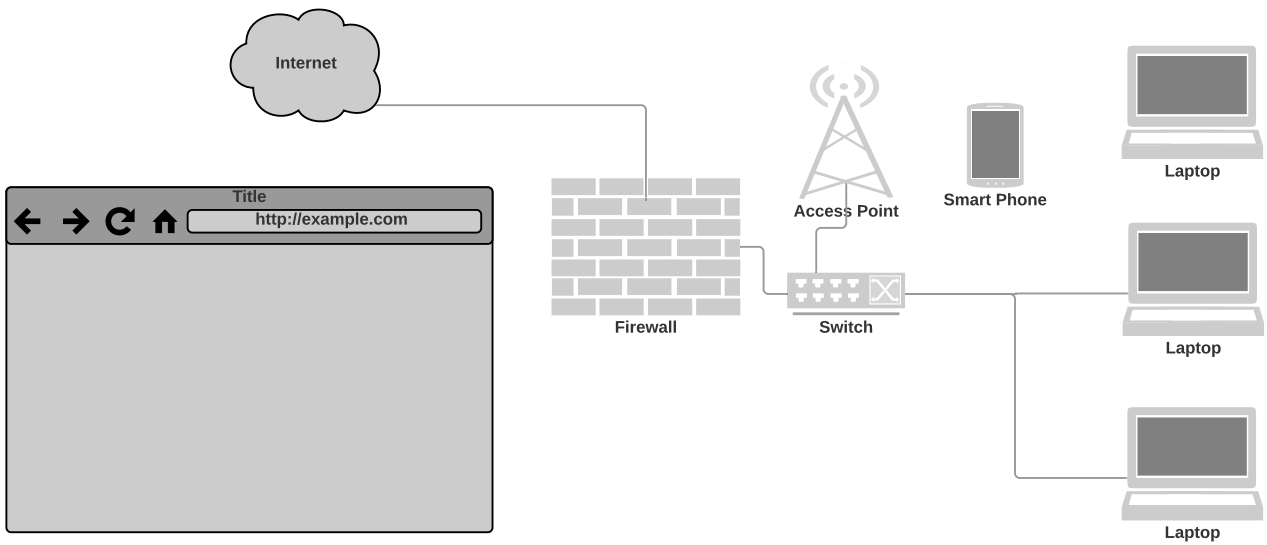
```
root@kali:~# sslscan www.kramse.dk
Version: 1.10.5-static OpenSSL 1.0.2e-dev xx XXX xxxx

Testing SSL server web.kramse.dk on port 443
...
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048
Subject:  *.kramse.dk
Altnames: DNS:*.kramse.dk, DNS:kramse.dk
Issuer:   AlphaSSL CA - SHA256 - G2
```

Source: Originally sslscan from http://www.titania.co.uk but use the version on Kali Linux

SSLscan can check your own sites by IP plus SMTP and some other services!

PS From now on its TLS! Not SSL anymore, any SSLv2, SSLv3 is old and vulnerable

Your Privacy



- Your data travels far
- Often crossing borders, virtually and literally

Data Found in Network data

Lets take an example, DNS

Domain Name System DNS breadcrumbs

- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit

Advice show your users, ask them to participate in a experiment and sniff data

Maybe use VPN more - or always!

DNS over TLS vs DNS over HTTPS - DNS encryption

- Protocols exist that encrypt DNS data
- Today we have competing standards:
- *Specification for DNS over Transport Layer Security (TLS)* (DoT), RFC7858 MAY 2016
  https://en.wikipedia.org/wiki/DNS_over_TLS
- *DNS Queries over HTTPS (DoH)* RFC8484
- How to cofigure DoT
  https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients

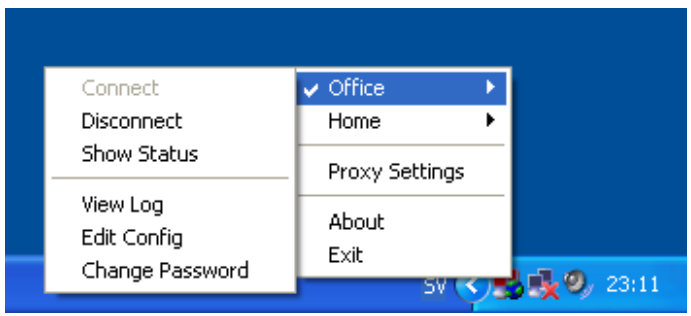
Virtual Private Network (VPN)

VPNs are everywhere, but could be better!

https://en.wikipedia.org/wiki/Virtual_private_network
https://kb.juniper.net/InfoCenter/index?page=content&id=KB11104
IPSec VPN between JUNOS and Cisco IOS
Skim:
https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
https://en.wikipedia.org/wiki/OpenVPN
https://en.wikipedia.org/wiki/IPsec
https://en.wikipedia.org/wiki/DirectAccess
https://www.wireguard.com/papers/wireguard.pdf

Example references. Note MPLS is NOT encrypting data!

VPN



Virtual Private Networks are useful - or even required when travelling

VPN http://en.wikipedia.org/wiki/Virtual_private_network

SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

IETF IPsec does work cross-vendors - sometimes, and is also increasingly becoming blocked or unusable due to NAT :-(

Recommended starting point OpenVPN - free and open, clients for "anything"

VPN without Encryption

> Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.[
> ... MPLS works by prefixing packets with an MPLS header, containing one or more labels.

Source:

https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

- The term VPN is also used in cases **without encryption**
- MPLS allows multiple customers to use the same IP prefixes, like 10/8
- MPLS is used in many provider networks
- Another example is Generic Routing Encapsulation (GRE), which is often then protected with IPsec
- People today also uses Virtual Extensible LAN (VXLAN) for cloud computing

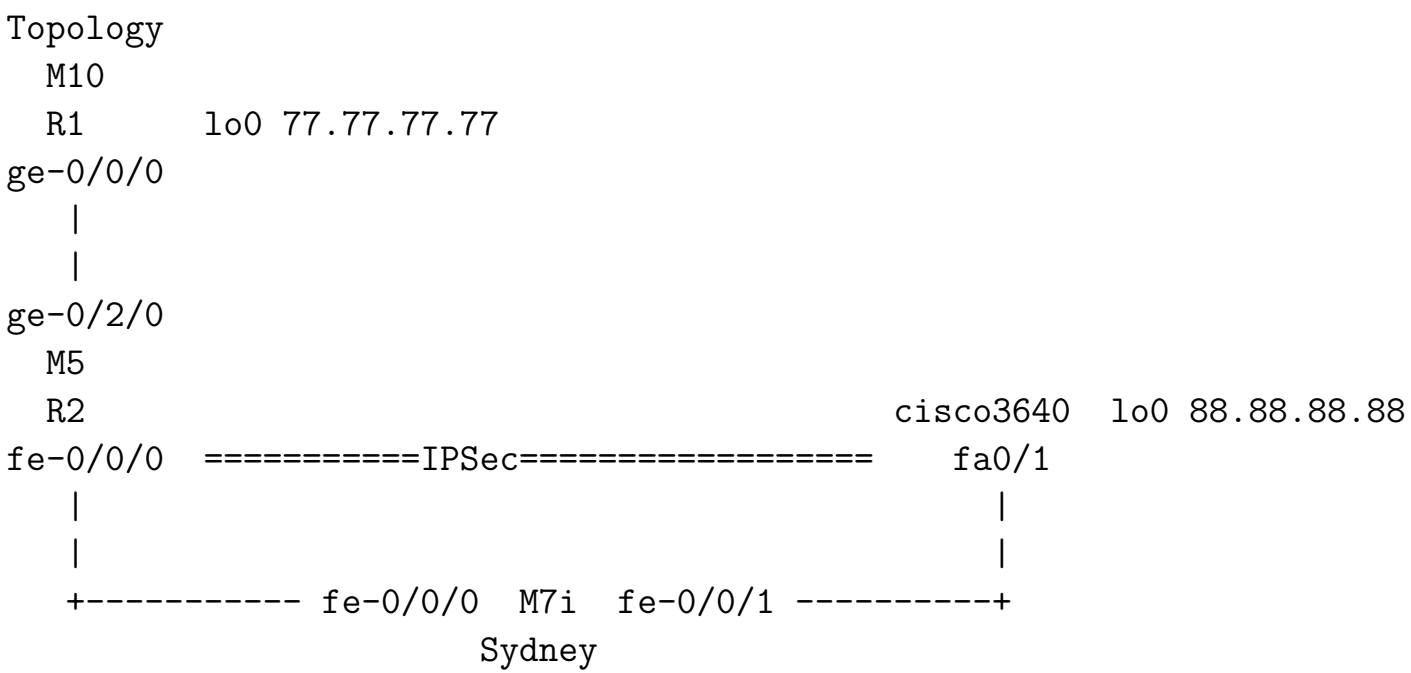
Linux Wireguard VPN

> WireGuard is a secure network tunnel, operating at layer 3, implemented as a kernel virtual network interface for Linux, which aims to replace both IPsec for most use cases, as well as popular user space and/or TLS-based solutions like OpenVPN, while being more secure, more performant, and easier to use.

Description from https://www.wireguard.com/papers/wireguard.pdf

- Very easy to setup!
- single round trip key exchange, based on NoiseIK
- Short pre-shared static keys—Curve25519
- strong perfect forward secrecy
- Transport speed is accomplished using ChaCha20Poly1305 authenticated-encryption
- encapsulation of packets in UDP
- WireGuard can be simply implemented for Linux in less than 4,000 lines of code, making it easily audited and verified

IPSec VPN between JUNOS and Cisco IOS



Source: https://kb.juniper.net/InfoCenter/index?page=content&id=KB11104

Cisco IOS crypto setup

```
cisco3640#sh run
crypto isakmp policy 10
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key key123 address 11.0.0.1
!
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
crypto ipsec transform-set ts-man esp-des esp-md5-hmac
!
crypto map dyn 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set ts
 match address 120
```

Not recommended settings! See later! People still use these examples! 🚩

Layer 2 Tunneling Protocol L2TP

Description from https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

> The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. A virtue of transmission over UDP (rather than TCP; c.f. SSTP) is that it avoids the "TCP meltdown problem".[3][4] It is common to carry PPP sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

Often used when crossing NAT, which everyone does ...

Configuration example for Cisco:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14122-24.html

OpenBSD L2TP IPsec

https://www.exoscale.com/syslog/building-an-ipsec-gateway-with-openbsd/

IPsec IKE-SCAN

Scan IPs for VPN endpoints with ike-scan:

```
root@kali:~# ike-scan 91.102.91.30
Starting ike-scan 1.9 with 1 hosts
(http://www.nta-monitor.com/tools/ike-scan/)
91.102.91.30 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=f0d6043badb2b7bc, msgid=f97a7508)

Ending ike-scan 1.9: 1 hosts scanned in 1.238 seconds (0.81 hosts/sec).
0 returned handshake; 1 returned notify
```

Source:

http://www.nta-monitor.com/tools-resources/security-tools/ike-scan

crack IKE psk?

http://ikecrack.sourceforge.net/

https://www.trustwave.com/Resources/SpiderLabs-Blog/Cracking-IKE-Mission-Improbable-(Part-1)/

Forward Secrecy

In cryptography, forward secrecy (FS), also known as perfect forward secrecy (PFS), is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if the private key of the server is compromised.[1] Forward secrecy protects past sessions against future compromises of secret keys or passwords.[2] By generating a unique session key for every session a user initiates, the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key.

Source: https://en.wikipedia.org/wiki/Forward_secrecy

Recommendations for VPN

Use the following guidelines when configuring Internet Key Exchange (IKE) in VPN technologies:
Avoid IKE Groups 1, 2, and 5.
Use IKE Group 15 or 16 and employ 3072-bit and 4096-bit DH, respectively.
When possible, use IKE Group 19 or 20. They are the 256-bit and
384-bit ECDH groups, respectively.
Use AES for encryption.

Paper: https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html
– and these are outdated by now! Check recent documentation!

- Certificates/keys - like TLS long and roll new ones from time to time
- Algorithms DES/3DES bye bye, update both encryption and authentication/integrity protection algorithms
- DH-Group - +15 thanks, highed most likely better, check what you have available
- Check both your remote client VPN and site-2-site VPN solutions Make it a habit to check regularly
- Switch to IKE version 2

Wi-Fi Security

Subjects

- Wifi standards IEEE 802.11
- Authentication Protocols RADIUS, PAP, CHAP, EAP
- Port Based Network Access Control IEEE 802.1x
- Security problems in wireless protocols
- Security problems in wireless encryption
- Hacking wireless networks

Exercises you can do later:

- Wifi scanning, aka wardriving
- WPA hacking with a short password
  See for examples: http://aircrack-ng.org/doku.php?id=cracking_wpa

Wifi Standards IEEE 802.11

802.11 is the work group in IEEE

Most well-known within this group:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen
- 802.11n faster
- **802.11i Security enhancements Robust Security Network RSN**

New names:
Wi-Fi 6 to identify devices that support 802.11ax technology
Wi-Fi 5 to identify devices that support 802.11ac technology
Wi-Fi 4 to identify devices that support 802.11n technology

Source: http://grouper.ieee.org/groups/802/11/index.html

IEEE 802.11 Security Fast Forward

In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by **Fluhrer, Mantin, and Shamir's** paper titled "Weaknesses in the Key Scheduling Algorithm of RC4". Not long after, Adam Stubblefield and AT&T publicly announced the first **verification of the attack**. In the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security Fast Forward

The IEEE set up a dedicated task group to create a replacement security solution, **802.11i** (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an **interim specification called Wi-Fi Protected Access (WPA)** based on a subset of the then current IEEE 802.11i draft. These started to appear in products in **mid-2003**. **IEEE 802.11i (also known as WPA2)** itself was ratified in **June 2004**, and uses government strength encryption in the **Advanced Encryption Standard AES,** instead of RC4, which was used in WEP. The modern recommended encryption for the home/consumer space is **WPA2 (AES Pre-Shared Key) and for the Enterprise space is WPA2 along with a RADIUS authentication server** (or another type of authentication server) and a strong authentication method such as EAP-TLS.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security Fast Forward

In January 2005, the IEEE set up yet another task group "w"to protect management and broadcast frames, which previously were sent unsecured. Its standard was published in 2009.[24]

In **December 2011**, a security flaw was revealed that affects wireless routers with the **optional Wi-Fi Protected Setup (WPS)** feature. While WPS is not a part of 802.11, **the flaw allows a remote attacker to recover the WPS PIN and, with it, the router's 802.11i password in a few hours**.

WPS WTF?! - det er som om folk bevidst saboterer wireless sikkerhed!

Source: http://en.wikipedia.org/wiki/IEEE_802.11

Encrypt where?

> It is not clear that the link layer is the right one for security. In a coffeeshop, the security association is terminated by the store: is there any reason you should trust the shopkeeper? Perhaps link-layer security makes some sense in a home, where you control both the access point and the wireless machines. However, we prefer end-to-end security at the network layer or in the applications.

Source: Cheswick-chap2.pdf Firewalls and Internet Security: Repelling the Wily Hacker , Second Edition, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin, **2003**

Individual Authentication

Replace the single secret code used in WEP/WPA PSK Pre-shared key

Recommend using :

- Known VPN technologies or WPA Enterprise
- Based on modern algorithms and protocols
- Implemented in professional equipment
- From trustworthy vendors
- Which are maintained and updated regularly
- Create more VLANs with IEEE 802.1q and also use both 1q and 1x on Ethernet!
- Using individual authentication is preferred
  IEEE 802.1x Port Based Network Access Control
- Hint: you can create RADIUS configuration for WPA Enterprise – with any user and password allowed!
  https://github.com/kramse/conference-open-8021x

Network Segmentation – Firewalls

$ firewall

1. (I) **An internetwork gateway that restricts data communication traffic to and from one of the connected networks** (the one said to be "inside"the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside"the firewall). (See: guard, security gateway.)
2. (O) **A device or system that controls the flow of traffic between networks using differing security postures.** Wack, J. et al (NIST), "Guidelines on Firewalls and Firewall Policy", Special Publication 800-41, January 2002.

Tutorial: A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies policy rules to control traffic that flows in and out of the protected network.

Source: RFC4949 *Internet Security Glossary, Version 2*

https://datatracker.ietf.org/doc/html/rfc4949 2007

Continued

> **A firewall is not always a single computer.** For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN (see: buffer zone) between the two routers. The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher-layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers. The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep unauthorized traffic (i.e., intruders) out, but usually also needs to let authorized traffic pass both in and out.

Source: RFC4949 *Internet Security Glossary, Version 2*

https://datatracker.ietf.org/doc/html/rfc4949 2007

- Network layer, packet filters, application level, stateless, stateful
- Firewalls are by design a choke point, natural place
  to do network security monitoring!
- Older but still interesting Cheswick chapter 2 PDF *A Security Review of Protocols: Lower Layers*
  http://www.wilyhacker.com/

Modern Firewall Infrastructures

A firewall blocks internet trafic

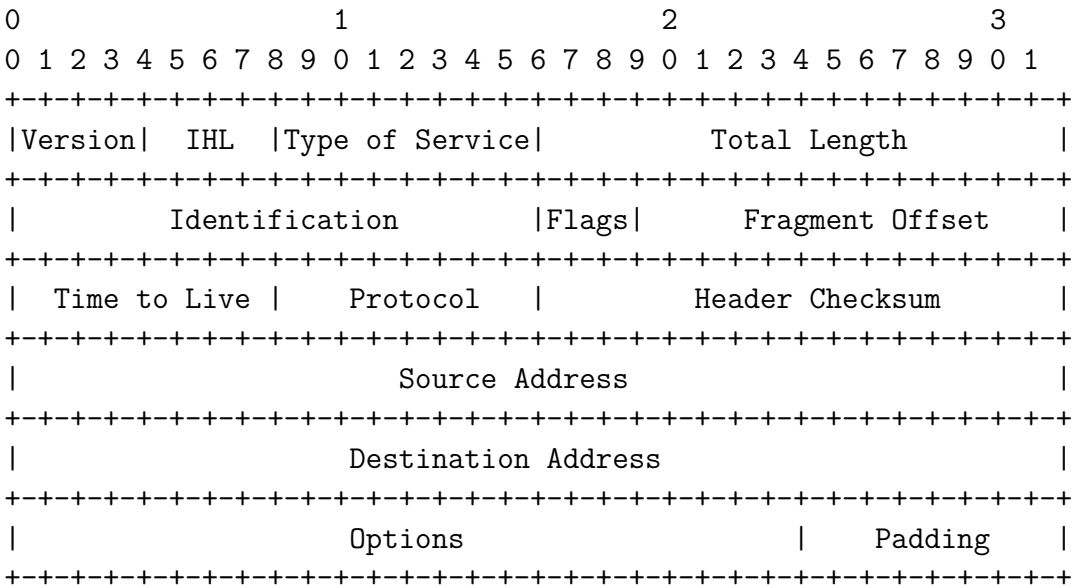
A firewall allows internet trafic

A firewall infrastructure must:

- Prevents attackers from entering
- Prevent data exfiltration
- Prevent worms, malware, virus from spreading in networks
- Be part of an overall solution with ISP, routers, other firewalls, switched infrastructures, intrusion detection systems and the rest of the infrastructure
- ...

Difficult – and requires design and secure operations

Packet Filtering



Packet filtering are firewall devices filtering on single packet

Most *firewalls* do stateful filtering and more

Don't forget IPv6 – even though you haven't turned it on, it is there

Sample Rules from OpenBSD PF

```
# Gateway config inspired from https://www.openbsd.org/faq/pf/example1.html
set block-policy drop
set loginterface egress
set skip on lo0
wired = "em1"
table <martians> { 0.0.0.0/8 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0 169.254.0.0/16  }
match in all scrub (no-df random-id max-mss 1440)
match out on egress inet from !(egress:network) to any nat-to (egress:0)
antispoof quick for { egress $wired $wifi }
block in quick on egress from <martians> to any
block return out quick on egress from any to <martians>

block all
pass out quick inet
pass out quick inet6

pass in on { $wired } inet
pass in on { $wired } inet6
```

Note: the line with `block all` – default deny

Example Firewall Products

- Checkpoint Firewall-1 http://www.checkpoint.com
- Cisco ASA http://www.cisco.com
- Juniper SRX http://www.juniper.net
- Palo Alto https://www.paloaltonetworks.com/
- Fortinet https://www.fortinet.com/

Those listed are the most popular commercial ones I see in Denmark

Open source based firewalls

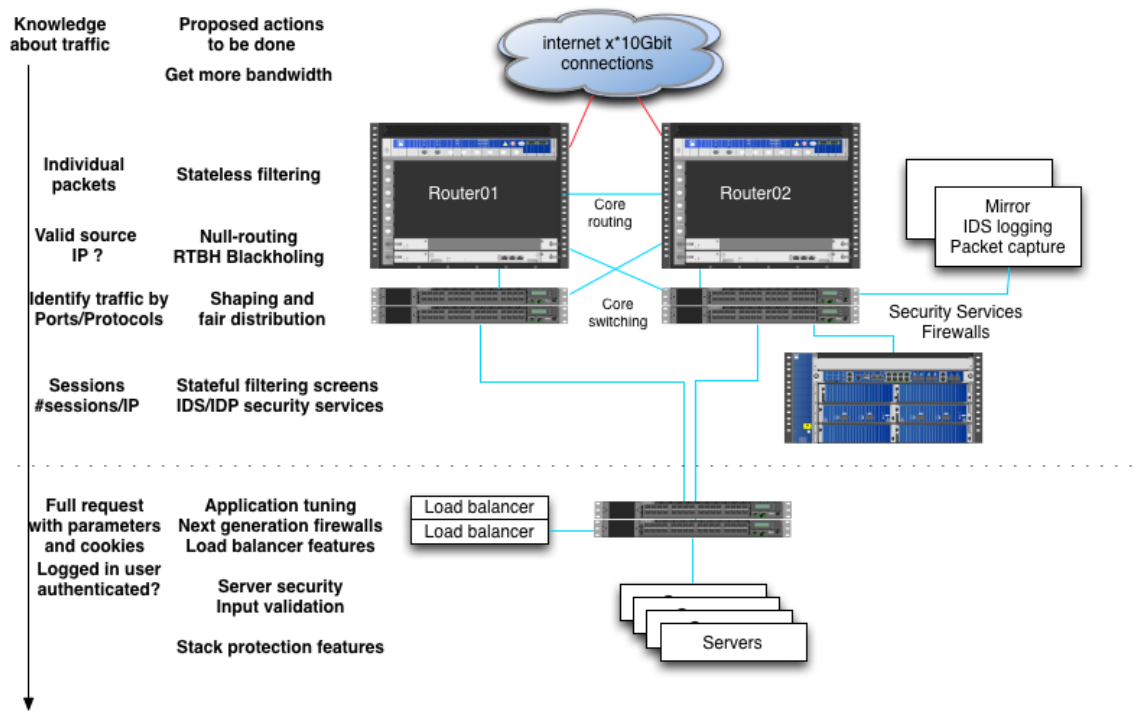
- Linux firewalls IP tables, use command line tool ufw Uncomplicated Firewall!
- Firewall GUIs on top of Linux – lots! Some are also available as commercial ones
- OpenBSD PF http://www.openbsd.org
- FreeBSD IPFW og IPFW2 http://www.freebsd.org
- Mac OS X uses OpenBSD PF
- FreeBSD has an older version of the OpenBSD PF, should really be renamed now

Uncomplicated Firewall (UFW)

```
root@debian01:~# apt install ufw
...
root@debian01:~# ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian01:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@debian01:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

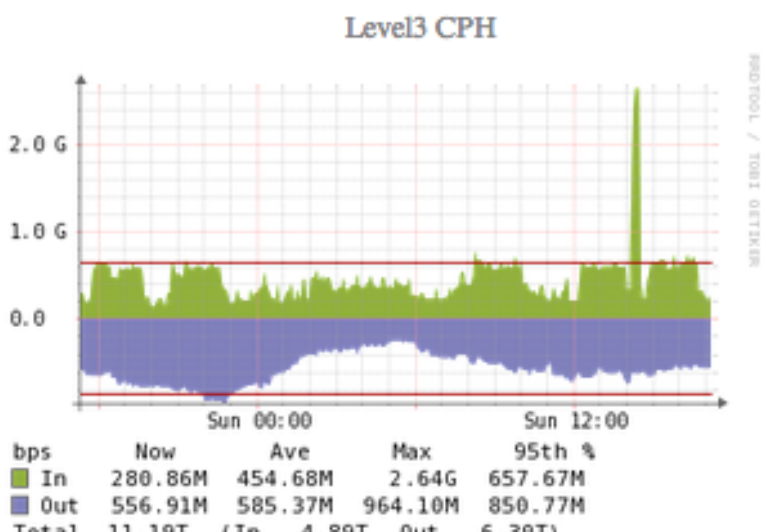
- Extremely easy to use – I recommend and use the (Uncomplicated Firewall) UFW

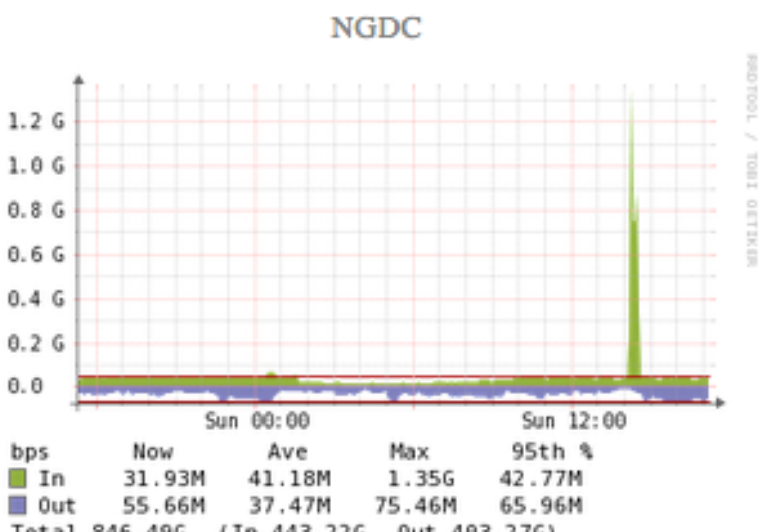
Firewalls are NOT Alone



Use Defense in Depth – all layers have features

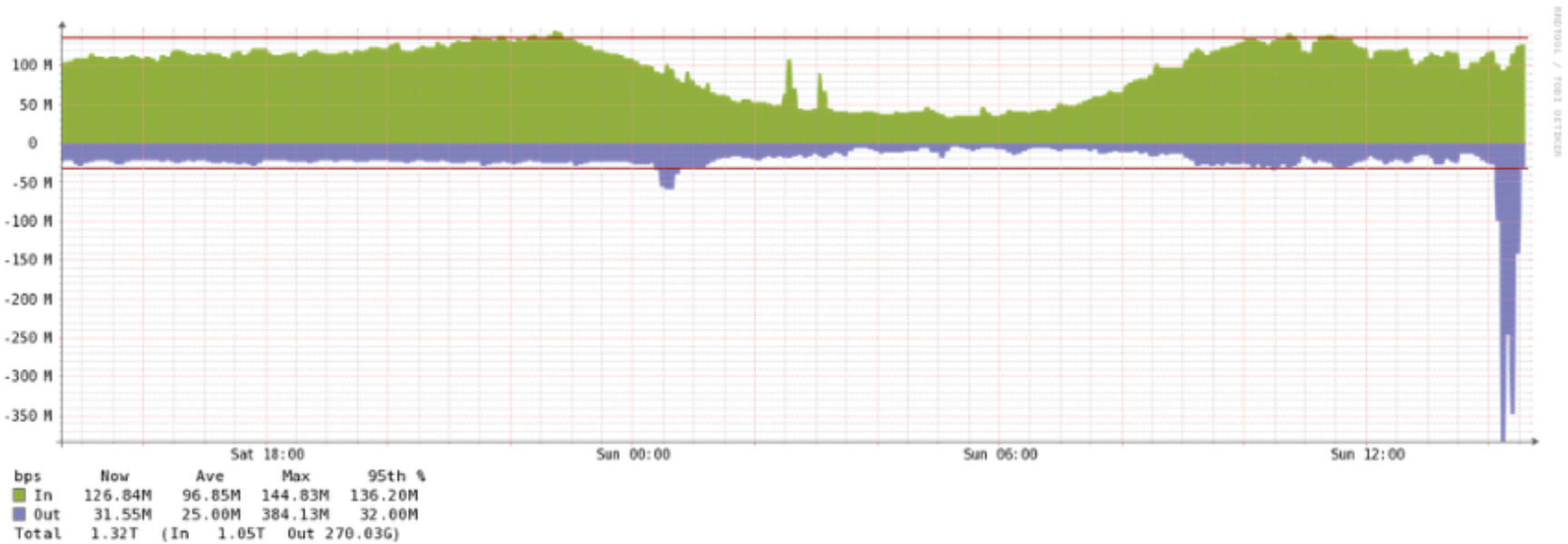
DDoS Traffic Before Filtering





Only two links shown, at least 3Gbit incoming for this single IP

DDoS Traffic After Filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

Better to filter stateless before traffic reaches firewall, less work!

Access Control Lists (ACL)

Stateless firewall filter throw stuff away

```
hlk@MX-CPH-02> show configuration firewall filter all | no-more
/* This is a sample, maybe use BGP flowspec and/or RTBH */
term edgeblocker {
    from {
        source-address {
            84.180.xxx.173/32;
...
            87.245.xxx.171/32;
        }
        destination-address {
            91.102.xx.xx/28; }
        protocol [ tcp udp icmp ]; }
    then discard;
}
```

Hint: can also leave out protocol and then it will match all protocols

Stateless Firewall Filter – limit protocols

```
term limit-icmp {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-100M;
        accept;
    }
}
term limit-udp {
    from {
        protocol udp;
    }
    then {
        policer UDP-1000M;
        accept;
    }
}
```

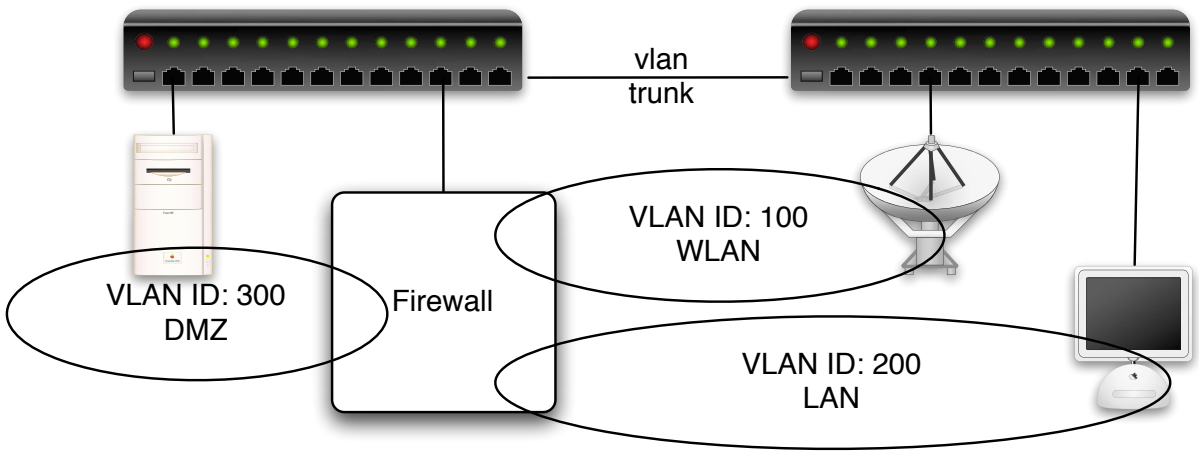
Routers and switches have extensive Class-of-Service (CoS) tools today

Strict Filtering for Segments – still stateless!

```
term some-server-allow {
    from {
        destination-address {
            109.238.xx.0/xx;
        }
        protocol tcp;
        destination-port [ 80 443 ];
    } then accept;
}
term some-server-block-unneeded {
    from {
        destination-address {
            109.238.xx.0/xx; }
        protocol-except icmp;  }
    then { count some-server-block; discard;
    }
}
```

Wut - no UDP, yes UDP service is not used on these servers

IEEE 802.1q



Using IEEE 802.1q VLAN tagging on Ethernet frames

Virtual LAN, to pass from one to another, must use a router/firewall

Allows separation/segmentation and protects traffic from many security issues

Port Security – Rogue DHCP servers

Common problem in networks is people connecting devices with DHCPD servers

In general make sure to segment networks

Start to use port security on switches, including DHCP snooping
https://en.wikipedia.org/wiki/DHCP_snooping

Can also be used to prevent people from adding unmanaged switches

In general, your devices have features – use them

A good reference for IPv6, *Operational Security Considerations for IPv6 Networks*
RFC9099 https://datatracker.ietf.org/doc/html/rfc9099

and *Security in a Mixed IPv4 and IPv6 World* at PROSA
https://github.com/kramse/security-courses/tree/master/presentations/network/ipv6-security-in-mixed-v4-v6

Example Port Security

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 mac-limit 4

set interface ge-0/0/1 persistent-learning
set interface ge-0/0/8 dhcp-trusted
set vlan employee-vlan arp-inspection
set vlan employee-vlan examine-dhcp
set vlan employee-vlan mac-move-limit 5
```

Can protect against rogue DHCP servers, IPv6 router advertisement attacks etc.

Source: Overview of Port Security, Juniper

https://www.juniper.net/documentation/en_US/junos/topics/example/overview-port-security.html

Helpful functions are available

First hop security Cisco

```
ipv6 snooping logging packet drop

interface GigabitEthernet1/0/1
    switchport mode access
    ipv6 nd raguard
    ipv6 dhcp guard
```

- RA Guard RFC6105 *IPv6 Router Advertisement Guard* and
  RFC7113 *Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*
  Only allow router advertisements on configured ports
- DHCPv6 guard only allow DHCP servers on specific ports
- Source and Prefix Guard

Wait a minute, have you turned similar features for IPv4? Many have NOT! 🚩

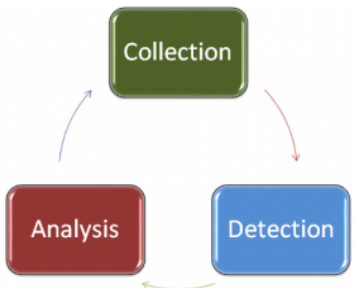
Creating an Access Control List (ACL)

```
(config)#ipv6 access-list RA-GUARD
(config-ipv6-acl)#sequence 3 deny icmp any any router-advertisement
(config-ipv6-acl)#sequence 6 permit ipv6 any any
(config-ipv6-acl)#exit
(config)#interface FastEthernet0/5
(config-if)#ipv6 traffic-filter RA-GUARD in
```

Source: example copied from RIPE NCC IPv6 Security Training materials:
https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf

- Best practice, and not that hard to do
- ACL, filtering and firewalling will create longer lasting protection
- Paired with a nice address plan you can easily put restrictions on traffic flow, without hurting functionaliy or the business
- Does ANY client in ANY office NEEEEEED to connect to ANY UPS, Virtualisation and printer across the world ...

Most firewalls include some detection today



Source: ANSM chapter 1: The Practice of Applied Network Security Monitoring

- Vulnerability-Centric vs. Threat-Centric Defense
- The NSM cycle: collection, detection, and analysis
- Full Content Data, Session Data, Statistical Data, Packet String Data, and Alert Data
- Security Onion is nice, but a bit over the top - quickly gets overloaded
- Book referenced is: *Network Security Monitoring Applied Network Security Monitoring Collection, Detection, and Analysis*, 2014 Chris Sanders ISBN: 9780124172081

Indicators of Compromise and Signatures

> An IOC is any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner. This could include a simple indicator such as the IP address of a command and control (C2) server or a complex set of behaviors that indicate that a mail server is being used as a malicious SMTP relay.
>
> When an IOC is taken and used in a platform-specific language or format, such as a Snort Rule or a Bro-formatted file, it becomes part of a signature. A signature can contain one or more IOCs.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

- Network Security Monitoring (NSM) - monitoring networks for intrusions, and reacting to those
- networkbased intrusion detection systems (NIDS)
- host based intrusion detection systems (HIDS)
- Example systems are Security Onion https://securityonion.net/ or SELKS https://www.stamus-networks.com/open-source/

ANSM chapter 3:The Sensor Platform

- Full Packet Capture (FPC) Data
- Session Data
- Statistical Data
- Packet String (PSTR) Data
- Log Data
- Sensor Placement, designing etc.

Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders ISBN: 9780124172081 - shortened ANSM

Collect Network Evidence from the network – netflow

Netflow is getting more important, more data share the same links

Detecting DoS/DDoS and problems is essential

Netflow sampling is vital information - 123Mbit, but what kind of traffic

Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share the following 7 values:

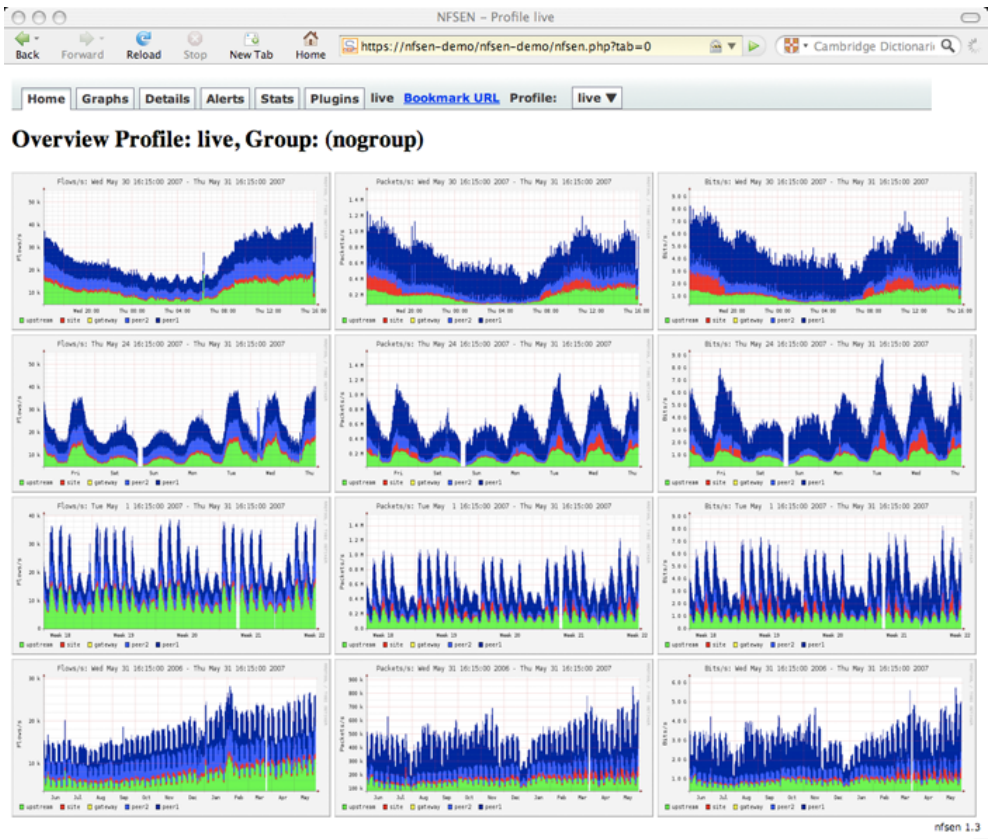
- Ingress interface (SNMP ifIndex), IP protocol, Source IP address and Destination IP address
- Source port for UDP or TCP, 0 for other protocols, IP Type of Service
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols

Today we can use Netflow version 9 or IPFIX with more fields available

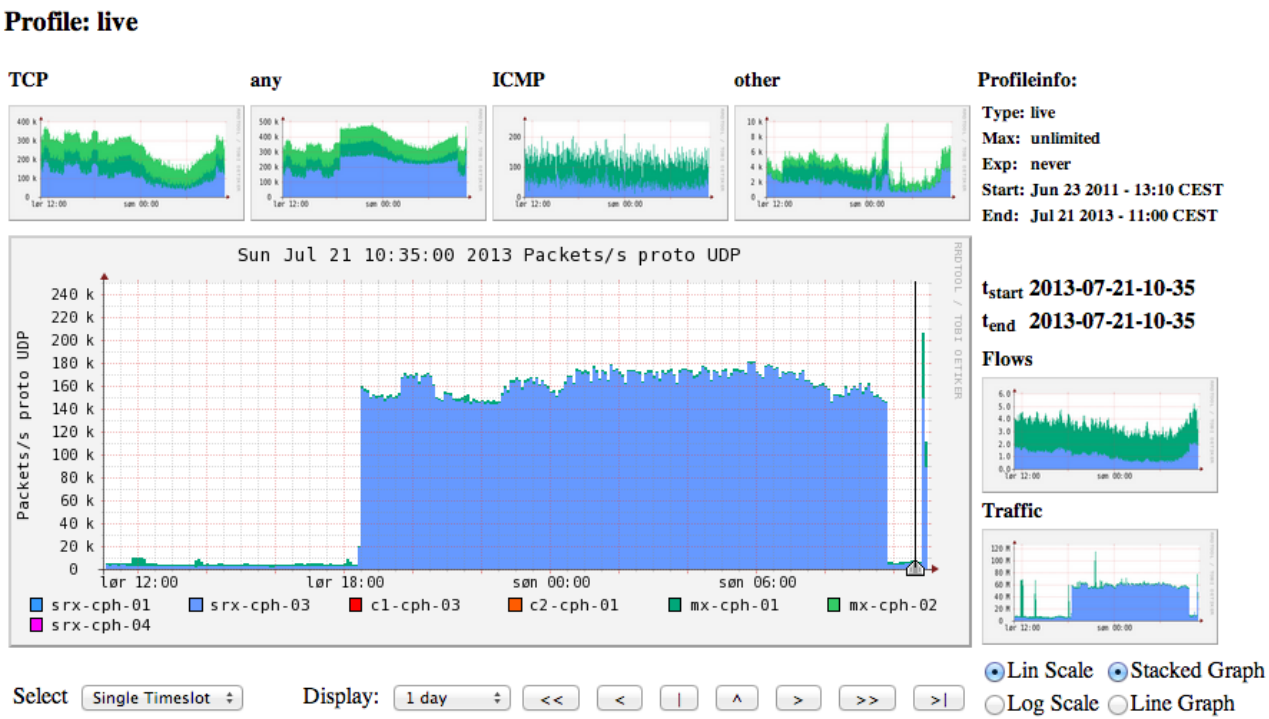
Source:

https://en.wikipedia.org/wiki/NetFlow https://en.wikipedia.org/wiki/IP_Flow_Information_Export

Netflow using NFSen



Netflow NFSen



An extra 100k packets per second from this netflow source (source is a router)

ElastiFlow – Elasticsearch based

ElastiFlow™ provides network flow data collection and visualization using the Elastic Stack (Elasticsearch, Logstash and Kibana). It supports Netflow v5/v9, sFlow and IPFIX flow types (1.x versions support only Netflow v5/v9).

Source: Picture and text from https://github.com/robcowart/elastiflow

Big Data tools: Dashboards with Kibana and Elasticsearch

Source: https://www.elastic.co

- View data by digging into it easily - must be fast
- Elasticsearch is an open source distributed, RESTful search and analytics engine capable of solving a growing number of use cases
- Non-programmers can create, save, and share dashboards using Kibana
- Fan of Elastic Common Schema (ECS) https://www.elastic.co/guide/en/ecs/current/index.html
- Other popular examples include Graylog and Grafana Loki

How to get started

How to get started searching for security events?

Collect basic data from your devices and networks

- Netflow data from routers
- Session data from firewalls
- Logging from applications: email, web, proxy systems

Centralize!

Process data

- Top 10: interesting due to high frequency, occurs often, brute-force attacks
- *ignore*
- Bottom 10: least-frequent messages are interesting

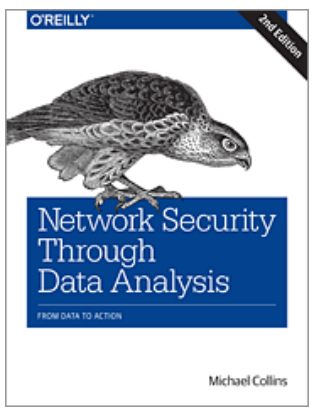
Ansible Configuration Management

```
- apt: name= item  state=latest
  with_items:
        - unzip
        - elasticsearch
        - logstash
        - redis-server
        - nginx
- lineinfile: "dest=/etc/elasticsearch/elasticsearch.yml state=present
  regexp='script.disable_dynamic: true' line='script.disable_dynamic: true'"
- lineinfile: "dest=/etc/elasticsearch/elasticsearch.yml state=present
  regexp='network.host: localhost' line='network.host: localhost'"
- name: Move elasticsearch data into /data
  command: creates=/data/elasticsearch mv /var/lib/elasticsearch /data/
- name: Make link to /data/elasticsearch
  file: state=link src=/data/elasticsearch path=/var/lib/elasticsearch
```

only requires SSH+python http://www.ansible.com

A complete example is available in https://github.com/kramse/kramse-labs

Network Security Through Data Analysis



Low page count, but high value! Recommended.

Network Security through Data Analysis, 2nd Edition By Michael S Collins Publisher: O'Reilly Media, October 2017 348 Pages

See also https://zencurity.gitbook.io/kea-it-sikkerhed/siem-and-log-analysis/lektionsplan

Blue Team – Packet sniffing tools

Tcpdump for capturing packets

Wireshark for dissecting packets manually with GUI

Zeek Network Security Monitor

Snort, old timer Intrusion Detection Engine (IDS)

Suricata, modern robust capable of IDS and IPS (prevention)

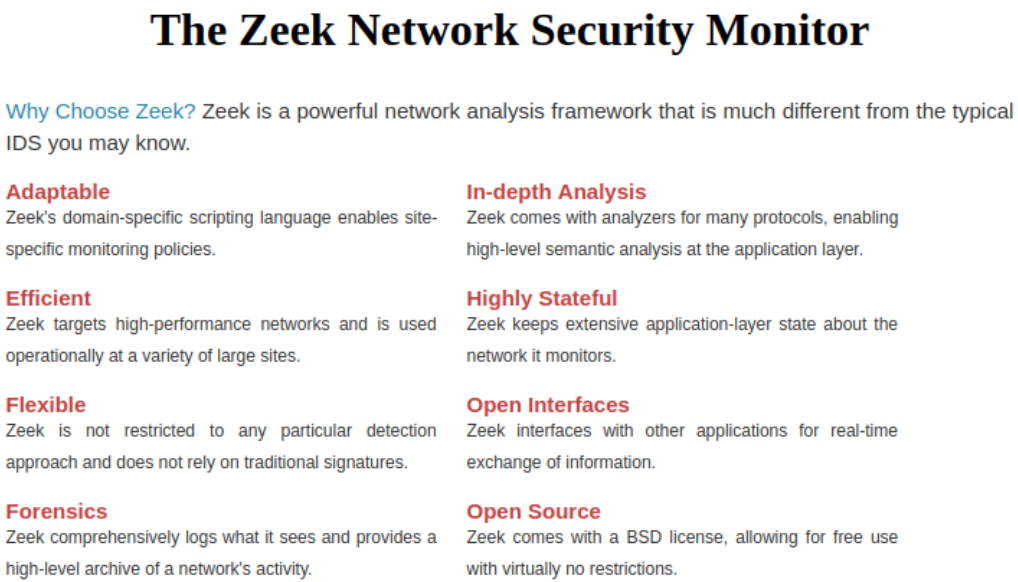
ntopng High-speed web-based traffic analysis

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

The Zeek Network Security Monitor



The Zeek Network Security Monitor

Why Choose Zeek? Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.

Adaptable
Zeek's domain-specific scripting language enables site-specific monitoring policies.

In-depth Analysis
Zeek comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Efficient
Zeek targets high-performance networks and is used operationally at a variety of large sites.

Highly Stateful
Zeek keeps extensive application-layer state about the network it monitors.

Flexible
Zeek is not restricted to any particular detection approach and does not rely on traditional signatures.

Open Interfaces
Zeek interfaces with other applications for real-time exchange of information.

Forensics
Zeek comprehensively logs what it sees and provides a high-level archive of a network's activity.

Open Source
Zeek comes with a BSD license, allowing for free use with virtually no restrictions.

The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework

Zeek is the tool formerly known as Bro, changed name in 2018. https://www.zeek.org/

Zeek is a Framework

The Zeek Network Security Monitor

While focusing on network security monitoring, Zeek provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Zeek has successfully bridged the traditional gap between academia and operations since its inception.

https://www.Zeek.org/

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://docs.zeek.org/en/master/script-reference/index.html

Get Started with Zeek

To run in "base" mode: `zeek -r traffic.pcap`

To run in a "near broctl" mode: `zeek -r traffic.pcap local`

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

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

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 the OISF and its supporting vendors.

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

Exercise at home – Your lab setup

- Go to GitHub, Find user Kramse, click through security-courses, courses
  https://github.com/kramse/security-courses/tree/master/courses
- Suricata and Zeek workshop is then in `networking/suricatazeek-workshop`
- Download the PDF files for the slides and exercises:

  https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop
- Get the lab instructions, from

  https://github.com/kramse/kramse-labs/tree/master/suricatazeek
- There are also a full Nmap workshop

  https://github.com/kramse/security-courses/tree/master/courses/pentest/nmap-workshop
- There are also a full SIEM and Log Analysis course

  https://github.com/kramse/security-courses/tree/master/courses/system-and-software/siem-log-analysis

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