



Welcome to

Network Traffic Inspection

PROSA September 2025

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

Slides are available as PDF, kramse@Codeberg
prosa-network-traffic-inspection-2025.tex in the repo security-courses

Contact information



- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teacher and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: hlk@zencurity.com Mobile: +45 2026 6000
- Run a small network for fun AS57860

You are welcome to drop me an email

Code of Conduct



I subscribe to having a Code of Conduct for events, we need them still! Usually I say the BornHack code of conduct apply whenever I teach! <https://bornhack.dk/conduct/>

Today we talk about networking, so I recommend this also: RIPE Code of Conduct Publication date: 05 Oct 2021

Rationale Our goals in having this Code of Conduct are:

- **To help everyone feel safe and included.** Many people will be new to our community. Some may have had negative experiences in other communities. We want to set a clear expectation that harassment and related behaviours are not tolerated here. If people do have an unpleasant experience, they will know that this is neither the norm nor acceptable to us as a community.
- **To make everyone aware of expected behaviour.** We are a diverse community; a CoC sets clear expectations in terms of how people should behave.

Source: <https://www.ripe.net/publications/docs/ripe-766>

Time schedule



- 17:00 - 17:40 Introduction and basics for the subject
- 17:40 - 18:05 Exercise in groups:
- 30min break Eat with your family if you like, I will be around most of the break, available for questions
- 18:45 - 19:30 Further teaching and exercises in the subject for the evening
- 15min break Stretch your legs, get some more water
- 19:45 - 20:30 Further teaching and exercises in the subject for the evening, questions and more
- 20:30 - 21:00 May contain exercises to be done on your own, with input from me

I will try to keep this plan for all evenings! So you hopefully can plan family life better

Will also try to make smaller breaks/exercises during the slidesshows, check for questions etc.

Modul 2: Traffic inspection (Onlinemodul 2 af 3)



Hvordan kan vi overvåge netværk effektivt?

Det får I svaret på i dette oplæg. Vi starter med at se på nogle simple eksempler som TCP forbindelse, HTTPS request og DNS. Dernæst peger underviseren på eksempelværktøjer som igennem mere end 25 år har automatiseret netværksovervågning som Zeek. Vi vil også tale om sessionslogging, firewall logning, Netflow. Og du får en præsentation af Suricata IDS som eksempel på et andet værktøj, der kan bruges til Intrusion Detection eller som central rolle i blokering af DNS traffik, IP negativ lister m.v.

Keywords: CIA modellen, CVE sårbarheder, switch, router, firewall, ACL, DoS/DDoS, VLAN, segmentering, **logning**, **monitoring**, **Netflow**, **Zeek**, **Suricata**, Nmap, Elasticsearch, IEEE 802.1x, IPv4, IPv6, NTP, DNS

- Vi skal dykke ned i netværkspakker
- Man kan godt følge med uden at lave øvelser
- Alle værktøjer der præsenteres er veldokumenterede mange steder – inkl videoer

Goals for today



What is a Secure Network



A controlled environment with a purpose and goal which is designed, implemented and monitored to be sufficiently secure – according to the policies and wishes of the owner and operator

Example networks

- Home network – should support a *family typically*
- Factory network – should support machines, robots, production of things
- Office network – should be available for employees and without malware and data leaks

Network Security as a Holistic Approach



holistic adjective

- 1 : of or relating to holism
- 2 : relating to or concerned with wholes or with complete systems rather than with the analysis of, treatment of, or dissection into parts
 - holistic medicine attempts to treat both the mind and the body
 - holistic ecology views humans and the environment as a single system

Source: <https://www.merriam-webster.com/dictionary/holistic>

- The network spans the whole organisation and we use *the network* – the Internet for many things
- Network security affects the whole organisation
- When improving network security, we often improve overall security

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!



Security information and event management (SIEM) is a subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes.[1]

The term and the initialism SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.[2]

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

- Note: there are alerting examples towards the bottom of the page, with sources
- Closely related to log management, incident response

Crafting the InfoSec Playbook



This book will help you to answer common questions:

- How do I find bad actors on my network?
- How do I find persistent attackers?
- How can I deal with the pervasive malware threat?
- How do I detect system compromises?
- How do I find an owner or responsible parties for systems under my protection?
- How can I practically use and develop threat intelligence?
- How can I possibly manage all my log data from all my systems?
- How will I benefit from increased logging—and not drown in all the noise?
- How can I use metadata for detection?

Source: *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*
by Jeff Bollinger, Brandon Enright, and Matthew Valites ISBN: 9781491949405

MITRE ATT&CK framework



MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

Source: <https://attack.mitre.org/> Great resource for attack categorization

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 Zeek-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

Networks are Built from Components



Photo by Eugen Str on Unsplash

The basic tools for countering threats



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!

Exercises



Exercises are completely optional



- Try ping and traceroute
- See your own IP settings
- Connect to a switch or router – most have web interfaces

Linux is a toolbox I will use and participants are free to use whatever they feel like Photo by Eugen Str on Unsplash

Course Materials



- This material is in multiple parts:
- Kickstart document – basic information [kickstart-prosa-secure-network.pdf](#)
- Slide show - the presentation - this file [prosa-secure-network-2025.pdf](#)
- Exercise for today: example secure network [exercise-secure-network-example.pdf](#)
- Exercise/inspiration for today: [kickstart-2-opal-router.pdf](#)
- Exercise booklet – large PDF with many exercises, stuff to do if you want to learn networks on your own [prosa-secure-network-2025-exercises.pdf](#)
- [prosa-network-traffic-inspection-2025.pdf](#)
- Additional resources from the internet like [firewall-book-10-DRAFT-PROSA.pdf](#)
- Later, next times:

Baseline Skills



- Threat-Centric Security, NSM, and the NSM Cycle
- TCP/IP Protocols
- Common Application Layer Protocols
- Packet Analysis
- Windows Architecture
- Linux Architecture
- Basic Data Parsing (BASH, Grep, SED, AWK, etc)
- IDS Usage (Snort, Suricata, etc.)
- Indicators of Compromise and IDS Signature Tuning
- Open Source Intelligence Gathering
- Basic Analytic Diagnostic Methods
- Basic Malware Analysis

Source: *Applied Network Security Monitoring Collection, Detection, and Analysis*, Chris Sanders and Jason Smith

Data Analysis Skills



Although we could spend an entire book creating an exhaustive list of skills needed to be a good security data scientist, this chapter covers the following skills/domains that a data scientist will benefit from knowing within information security:

- Domain expertise—Setting and maintaining a purpose to the analysis
- Data management—Being able to prepare, store, and maintain data
- Programming—The glue that connects data to analysis
- Statistics—To learn from the data
- Visualization—Communicating the results effectively

It might be easy to label any one of these skills as the most important, but in reality, the whole is greater than the sum of its parts. Each of these contributes a significant and important piece to the workings of security data science.

Source: *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis

ISBN: 978-1-118-79372-5 February 2014 <https://datadrivensecurity.info/> - short DDS



Anatomy of an Auditing System

Sample logs from login with Secure Shell (SSH) and performing sudo su -

```
Jun  5 11:53:15 pumba sshd[64505]: Accepted publickey for hlk from 79.142.233.18 port 43902
ssh2: ED25519 SHA256:180JMcywyBcraJiCWJ06uZ2yzHfu0VuiArqVv1VyfEI
```

```
Jun  5 11:53:19 pumba sudo:      hlk : TTY=ttyp2 ; PWD=/home/hlk ; USER=root ; COMMAND=/usr/bin/su -
```

Example systems: Unix syslog, IBM main frame RACF and Windows Event Logs service
swatchdog is an old skool, but simple tool that works

Logs should be protected and considered confidential information



Anatomy of an Auditing System

When data has been gathered it should be analyzed.

Logger functions - collect

Analyzer - analyze it, creating dashboard can provide some insights

Notifier - report results by email or other means

Example systems Windows Event Logs service can inform of successful and failed logins, both should be collected

Logs should be protected and considered confidential information, by sending it to a centralized system with a high security level protects it

Modern systems exist to take all data from logging and provide high capacity storage, searching and sorting.

Your Network

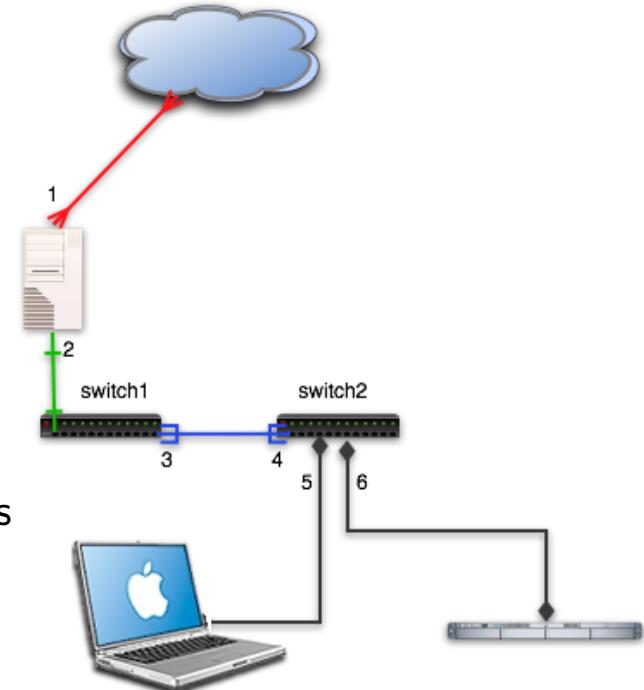


QUESTION

I have a home network which has the following systems:

- OpenBSD router
- Juniper and small TP-Link switches
- UniFi wireless access-point

Due to online remote teaching - we will investigate other networks and scan across the internet to *my servers!*



Data-Driven Security: Analysis, Visualization ...

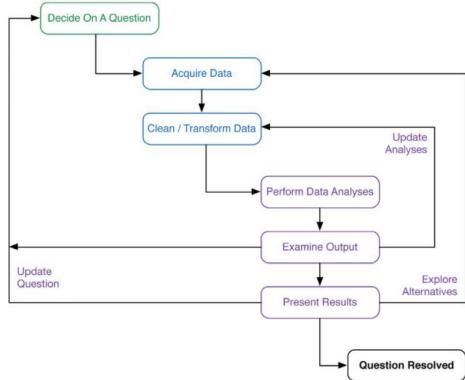


FIGURE 12-2: The data science workflow

- Find and Collect Relevant Data
- Learn through Iteration
- Find Statistics

Source: *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs,
Bob Rudis ISBN: 978-1-118-79372-5 February 2014 <https://datadrivensecurity.info/>

Data-Driven Security, continued



Building a Real-Life Security Data Science Team

... a clear goal: Given an IP address (or IP/Port combination), **search across all our perimeter devices in less than five minutes.**

Three core principles focused the team.

- First, explore the open source versions of tools before engaging vendors. If you don't know how the sausage is being made, you really have no idea what's being done, and this is vital when working with real data.
- Second, follow the mantra of "no single tool; no single database; and, no single approach to solving a problem." Do not put blinders on because you are either comfortable with certain technologies or have an affinity for a certain tool.
- Third, failure is expected, but you must learn from each journey down the wrong path. Continuous adaptation and adjustment is the name of the game.

Source: *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis ISBN: 978-1-118-79372-5 February 2014 <https://datadrivensecurity.info/>

Lab Networks



- When learning and investigating it is nice to have a *lab network* – make changes, play with settings, break things
- If you live alone, and are not in a remote meeting – play with your own network!
- I recommended the small GL-Inet Opal (GL-SFT1200) Wireless Travel Router
<https://store.gl-inet.com/products/opal-gigabit-wireless-pocket-sized-openwrt-ipv6-sft1200>
- It has 2 LAN ports for connecting, 1 WAN port for Internet or can act as a Wi-Fi client. All powered by USB-C etc.
- Manual and documentation https://docs.gl-inet.com/router/en/4/user_guide/gl-sft1200/

Well-Known Port Numbers



IANA maintains a list of magical numbers in TCP/IP
Lists of protocol numbers, port numbers 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>

Unencrypted data protocols



Examples

- TFTP use UDP and is unencrypted
- TFTP still used for configuration files and firmwares
- FTP sends data in cleartext

USER username

PASS password

Stop using FTP on the internet!

- DNS sending unencrypted on UDP and TCP
Use DNS over HTTPS (DoH) or DNS over TLS (DoT)

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 or redirecting clients to wrong sites

Recommended Reading



So to get started in network security I recommend learning the basics:

- Chapter 1: Packet Analysis and Network Basics
- Chapter 2: Tapping into the Wire
- Chapter 3: Introduction to Wireshark

Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition

Using Wireshark



http-example.cap

Apply a display filter... <filter>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.24.65.102	91.102.91.18	TCP	58816 - http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TStamp=745562412 TSecr=0 SACK_PERM=0
2	0.000170	172.24.65.102	91.102.91.18	TCP	58817 - http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TStamp=745562412 TSecr=0 SACK_PERM=0
3	0.127853	91.102.91.18	172.24.65.102	TCP	http - 58816 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TStamp=1855239975
4	0.127167	91.102.91.18	172.24.65.102	TCP	http - 58817 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TStamp=2512433851
5	0.127181	172.24.65.102	91.102.91.18	TCP	58816 - http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TStamp=745562538 TSecr=1855239975
6	0.127226	172.24.65.102	91.102.91.18	TCP	58817 - http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TStamp=745562538 TSecr=2512433851
7	0.127363	172.24.65.102	91.102.91.18	HTTP	GET / HTTP/1.1
8	0.141320	91.102.91.18	172.24.65.102	HTTP	HTTP/1.1 304 Not Modified
9	0.141421	172.24.65.102	91.102.91.18	TCP	58816 - http [ACK] Seq=503 Ack=190 Win=131568 Len=0 TStamp=745562551 TSecr=1855239975

Frame 7: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits)
Ethernet II, Src: Apple_6c:87:5e (7c:dic1:3c:6c:87:5e), Dst: Cisco_32:09:30 (44:2b:03:32:09:30)
Internet Protocol Version 4, Src: 172.24.65.102 (172.24.65.102), Dst: 91.102.91.18 (91.102.91.18)
Transmission Control Protocol, Src Port: 58816 (58816), Dst Port: http (80), Seq: 1, Ack: 1, Len: 502

HyperText Transfer Protocol
GET / HTTP/1.1\r\nHost: 91.102.91.18\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.146 Safari/537.36\r\nAccept-Encoding: gzip,deflate,sdch\r\nAccept-Language: en-US,en;q=0.8,cs;q=0.6,dz;q=0.4\r\nIf-None-Match: "7693a63e31516a58b2a295edb31d07524a6e8a3"\r\nIf-Modified-Since: Tue, 17 Nov 2009 11:22:22 GMT\r\n\r\n

Full request URI: http://91.102.91.18/1
HTTP request 1/1
Response in frame: 8

0000 44 2b 03 32 09 30 7c d1 c3 6c 87 5e 08 00 45 00 D+, 2.0| Äl..~.E.
0010 02 2a 9e d7 40 00 00 f5 ff ac 18 41 66 5b 66 .w.,<0.0, öý-Afff
0020 5b 12 e5 00 50 00 ea 0e c7 03 14 0c 19 80 18 [,Ã, P, è ,ç,.....
0030 20 2b 0f c0 00 00 03 01 08 00 2c 70 61 a6 94 +,Ã,...,.,pañ.
0040 b7 27 47 49 54 20 2f 48 54 54 50 2f 31 2e 31 .'GET / HTTP/1.1
0050 09 0a 60 73 74 34 20 39 31 30 32 2e 39, 91.102.9
0060 31 0e 31 00 0f 0f 0f 65 63 74 6f 1.18, Co 00 00
0070 3b 20 60 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 : keep-a live.ca
0080 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 26 6d 61 78 che-Content: max
0090 2d 61 67 65 3d 30 0d 0a 41 63 63 65 70 74 3a 20 -age=0. Accept:
00a0 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/html,application/
00b0 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c
00c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b application/xml;

Packets: 9 . Displayed: 9 . Marked: 0 . Load time: 0:0:0 . Profile: Default

Capture - Options

What about encrypted traffic



```
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 198
    ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 194
      Version: TLS 1.2 (0x0303)
      ▶ Random
        Session ID Length: 0
        Cipher Suites Length: 32
      ▶ Cipher Suites (16 suites)
      ▶ Compression Methods Length: 1
      ▶ Compression Methods (1 method)
      ▶ Extensions Length: 121
      ▶ Extension: Unknown 56026
      ▶ Extension: renegotiation_info
      ▶ Extension: server_name
        Type: server_name (0x0000)
        Length: 16
        ▼ Server Name Indication extension
          Server Name list length: 14
          Server Name Type: host_name (0)
          Server Name length: 11
          Server Name: twitter.com
        ▶ Extension: Extended Master Secret
0050 a4 1d 52 8f 2c 18 99 91 54 68 0a 77 0d 95 73 64 ..R,.... Th.w..sd
0060 7d 00 00 20 5a 5a c0 2b c0 2f c0 2c c0 30 cc a9 }.. ZZ.+ ./.,.0..
0070 cc a8 cc 14 cc 13 c0 13 c0 14 00 9c 00 9d 00 2f ..... ....../
0080 00 35 00 0a 01 00 00 79 da da 00 00 ff 01 00 01 .5.....y .......
0090 00 00 00 10 00 0e 00 00 0b 74 77 69 74 74 65 ..... .twitte
00a0 72 2e 63 6f 6d 00 17 00 00 00 23 00 00 00 0d 00 r.con... .#.....
00b0 14 00 12 04 03 08 04 04 01 05 03 08 05 05 01 08 ..... .......
```

Current TLS version 1.2 used in HTTPS show the name!



Ping and port sweep

Scans across the network are named sweeps

Ping sweeps using ICMP Ping probes

Port sweep trying to find a specific service, like port 80 web

Quite easy to see in network traffic:

- Selecting two IP-addresses not in use
- Should not see any traffic, but if it does, its being scanned
- If traffic is received on both addresses, its a sweep – if they are a bit apart it is even better, like 10.0.0.100 and 10.0.0.200

Pro tip: a Great network intrusion detection engine (IDS), is Suricata suricata-ids.org



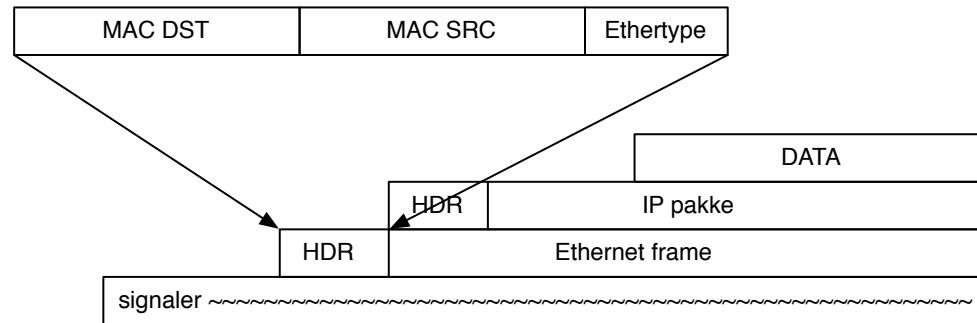
Nmap port sweep for web servers

```
root@cornerstone:~# nmap -p80,443 172.29.0.0/24
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   filtered  https
MAC Address: 00:50:56:C0:00:08 (VMware)
```

```
Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   closed    https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

Network Data is Data



We can find existing programs that decode packets

- Wireshark – GUI program
- Tcpdump – command line
- Zeek – engine for decoding network packets into data
- Suricata – Intrusion Detection System (IDS)

What output format do we want

JSON and jq



- jq is a lightweight and flexible command-line JSON processor <https://jqlang.org/>

Data overview JSON



JavaScript Object Notation (JSON, pronounced /dəsən/; also /dəsən/[note 1]) is an open-standard file format or data interchange format that uses **human-readable text** to transmit data objects consisting of attribute–value pairs and array data types (or any other serializable value). It is a very common data format, with a diverse range of applications, such as serving as replacement for XML in AJAX systems.[6]

Source: <https://en.wikipedia.org/wiki/JSON>

- I like JSON much better than XML
- Many web services can supply data in JSON format

JSON example



```
{  
  "first name": "John",  
  "last name": "Smith",  
  "age": 25,  
  "address": {  
    "street address": "21 2nd Street",  
    "city": "New York",  
    "state": "NY",  
    "postal code": "10021"  
  },  
  "phone numbers": [  
    {  
      "type": "home",  
      "number": "212 555-1234"  
    },  
  ],  
}
```

- This is a basic JSON document, new data attribute-value pairs can be added
Source: <https://en.wikipedia.org/wiki/JSON>

Start programming



Example program, reading from HTTP, into Python, out using JSON

```
#!/usr/bin/env python
import requests
r = requests.get('https://api.github.com/events')
print (r.json());
```

- Think of programming in this course as reading, processing and outputting data
- Read in any format
- Process with any function
- Output in any format
- And reuse existing software

The Zeek Network Security Monitor



Together with firewalls – The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis 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.

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

Suricata IDS/IPS/NSM



Together with firewalls – Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

<https://suricata.io> <https://openinfosecfoundation.org>



Commercial Support

You can and should use updated rulesets for Suricata.

I Recommend the Emerging Threats ET Pro ruleset

Processing data with Zeek



Simple example of reading a file with a few packets

Get Started with Zeek



- To run in “base” mode:

```
zeek -r traffic.pcap
```

- To run in a “near zeekctl” mode:

```
zeek -r traffic.pcap local
```

- To add extra scripts:

```
zeek -r traffic.pcap myscript.zeek
```

Zeek demo: Run



```
// Use the deploy command to initialize and start zeek first
```

```
debian:~ root# zeekctl
```

```
Welcome to ZeekControl 1.5
```

```
Type "help" for help.
```

```
[ZeekControl] > install  
creating policy directories ...  
installing site policies ...  
generating standalone-layout.zeek ...  
generating local-networks.zeek ...  
generating zeekctl-config.zeek ...  
generating zeekctl-config.sh ...  
...
```

```
debian:etc root# grep eth0 node.cfg  
interface=eth0
```

Our Zeek node.cfg is in /opt/zeek/etc

Zeek demo: Run Zeek

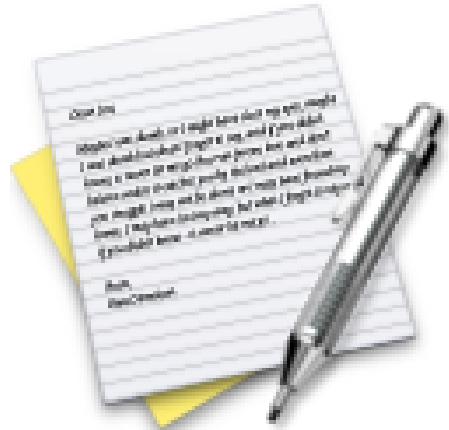


```
[ZeekControl] > start
... starting zeek
// Exit using ctrl-d and then look at logs
debian:zeek root# cd /opt/zeek/logs/current
debian:zeek root# pwd
/opt/zeek/logs/current
debian:current root# tail -f dns.log
```

More examples at:

<https://www.zeek.org/sphinx/script-reference/log-files.html>

Exercise

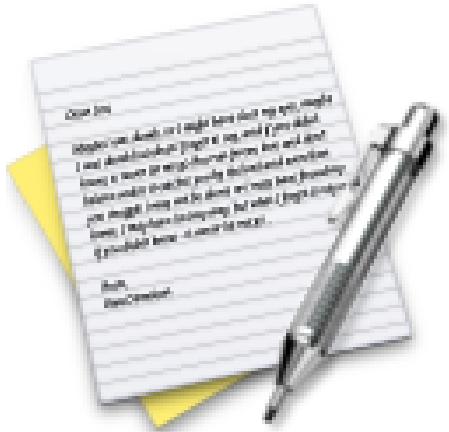


Now lets do the exercise

i Zeek on the web 10min

which is number **23** in the exercise PDF.

Exercise



Now lets do the exercise

??

which is number ?? in the exercise PDF.

Exercise



Now lets do the exercise

??

which is number ?? in the exercise PDF.

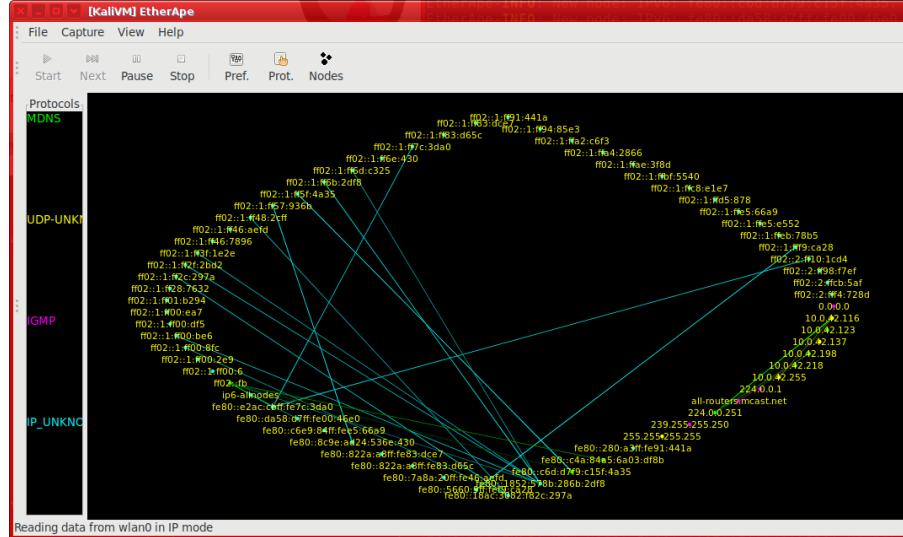
Graphics



Example graphs plots from earlier



Example tools and graphs



- Etherape shown, see <https://etherape.sourceforge.io/>

Parallel coordinate plots

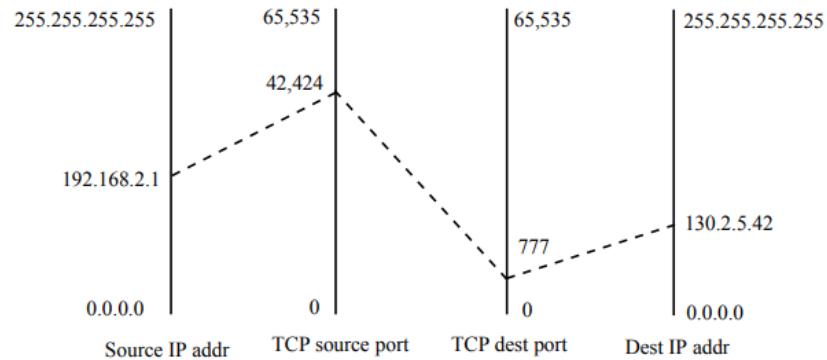


Figure 7: Parallel coordinate plot for a TCP packet from 192.168.1.1:42424 to 130.2.5.42:777.

Source: image from Network Security Visualization Keith Fligg and Genevieve Max

<https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic13-final/report.pdf>

- https://en.wikipedia.org/wiki/Parallel_coordinates
- Nice for explaining connections, but not used much in real life systems

DNS logging



Since most malware uses DNS today, to be able to switch to new command and control endpoints, we can leverage that to our advantage.

Domain Name System (DNS) depends on a query from the client, and a server that resolves this to a value.

- We can log any DNS traffic into a database
- We can look up if any clients have done a lookup for a specific name or IP during incident handling
- This can confirm if a client has ever *visited* a malicious site, because first it needs to lookup the name to IP address before it can make the TCP/HTTP connection, or send data



Unbound and NSD

Unbound is a validating, recursive, caching DNS resolver. It is designed to be fast and lean and incorporates modern features based on open standards.

To help increase online privacy, Unbound supports DNS-over-TLS which allows clients to encrypt their communication. In addition, it supports various modern standards that limit the amount of data exchanged with authoritative servers.

<https://www.nlnetlabs.nl/projects/unbound/about/>

My preferred local DNS server.

Also check out uncensored DNS and his DNS over TLS setup!

Even has pinning information available:

<https://blog.censurfridns.dk/blog/32-dns-over-tls-pinning-information-for-unicastcensurfridnsdk/>

Demo and exercises



Discussion



Where do we want to log DNS?

From the network directly with Zeek and Suricata?

From the DNS servers – query log?

Collect Network Evidence from the network



Network Flows – Netflow and Session Logging

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

Detecting DoS/DDoS and problems is essential

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
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP Type of Service

today Netflow version 9 or IPFIX

sFlow, short for "sampled flow", is an industry standard for packet export at Layer 2 of the OSI model,



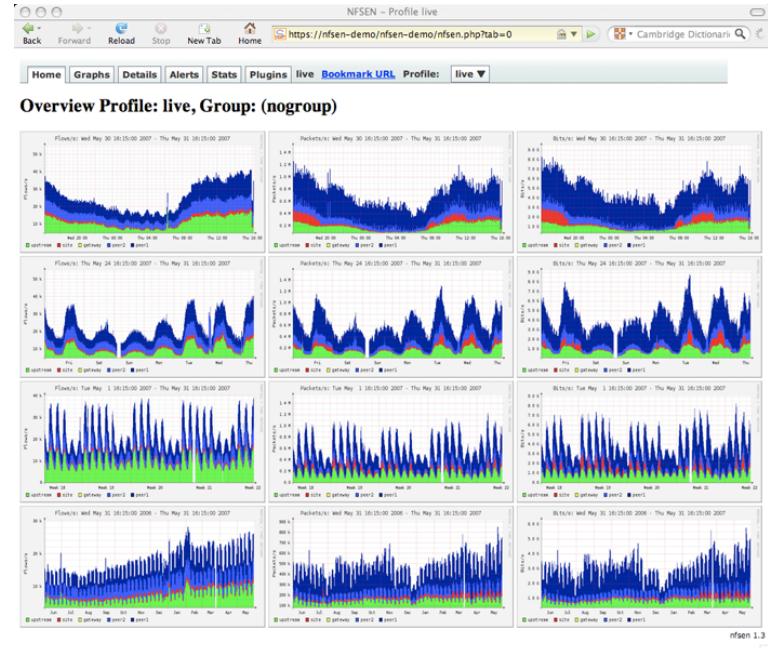
Sources:

<https://en.wikipedia.org/wiki/NetFlow>

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

<https://en.wikipedia.org/wiki/SFlow>

Netflow using NfSen

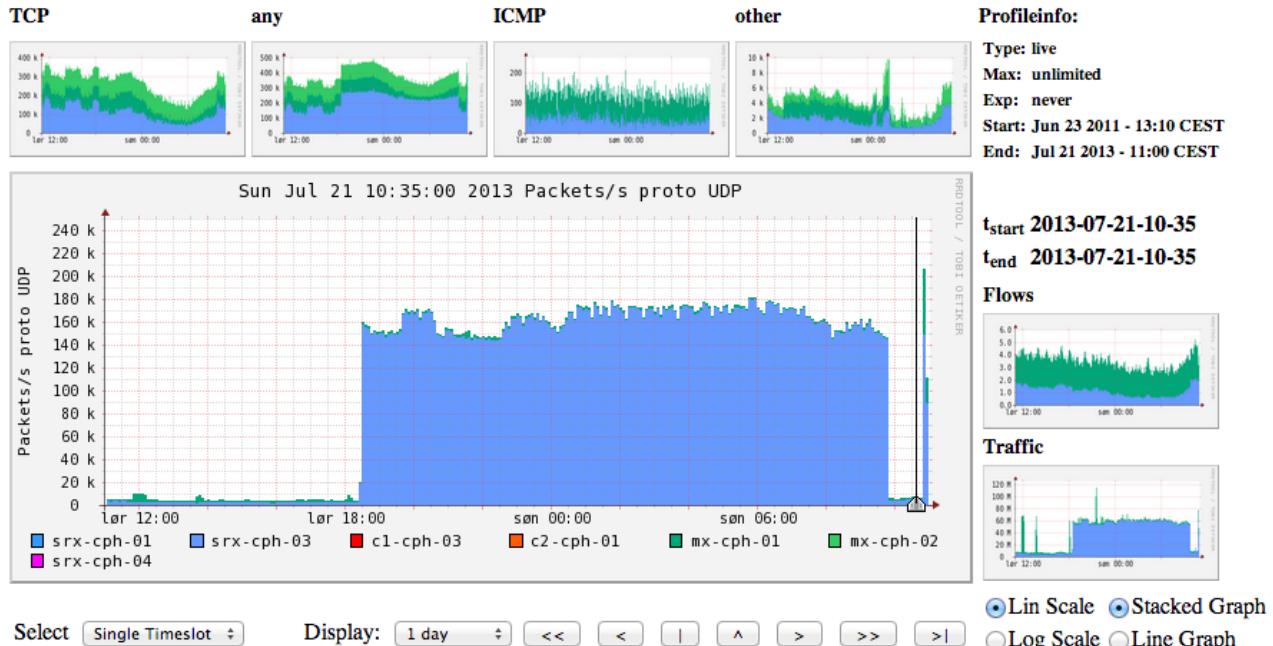


I do not recommend using NfSen anymore, but netflow processing has been around for decades!
<https://nfsen.sourceforge.net/>

Netflow NFSen



Profile: live



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

Netflow processing from the web interface



NFSEN – Profile live May 31 2007 – 04:40

Back Forward Reload Stop New Tab Home https://nfsen-demo/nfsen-demo/nfsen.php#processing Cambridge Dictionary

peer2 3.3 k/s 76.2 k/s 66.9 k/s 7.0 k/s 621.0 /s 1.7 k/s 484.6 Mb/s 459.9 Mb/s 12.5 Mb/s 437.3 kb/s 11.7 Mb/s
gateway 1.0 k/s 651.0 k/s 600.8 k/s 46.6 k/s 0 /s 3.7 k/s 6.2 Mb/s 6.1 Mb/s 36.4 kb/s 0 kb/s 4.4 kb/s
site 467.1 k/s 8.9 k/s 6.1 k/s 2.0 k/s 181.7 /s 613.3 /s 38.8 Mb/s 28.3 Mb/s 7.4 Mb/s 104.0 kb/s 2.9 Mb/s
upstream 6.4 k/s 94.2 k/s 84.3 k/s 8.2 k/s 896.4 /s 766.7 /s 588.4 Mb/s 568.2 Mb/s 16.7 Mb/s 685.1 kb/s 2.8 Mb/s

All None Display: Sum Rate

Netflow Processing

Source: peer1 Filter:

Options:
 List Flows Stat TopN
Top: 10
Stat: Flow Records order by flows
 proto
 srcPort srcIP
 dstPort dstIP
Limit: Packets > 0
Output: line / IPv6 long

Clear Form process

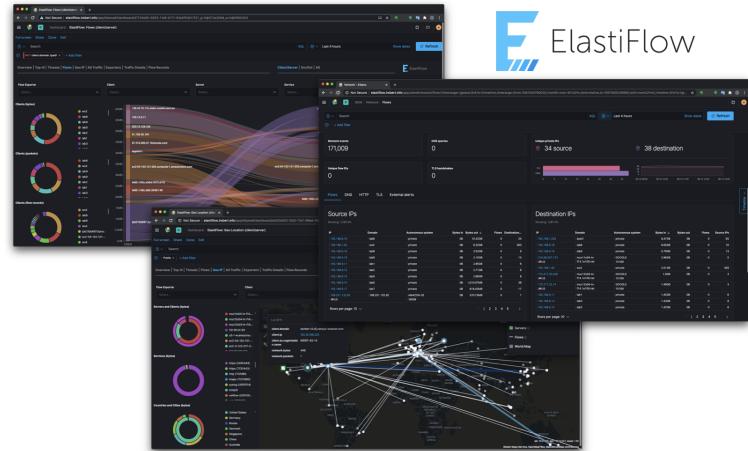
```
** nfdump -M /netflow0/nfsen-demo/profile-data/live/peer1:peer2:gateway:site:upstream -T -r 2007/05/31/04/nfcapd.2007053104400
nfdump filter:
any
Aggregated flows 2797250
Top 10 flows ordered by flows:
Date Flow Src IP Addr:Port Proto Dst IP Addr:Port Packets Bytes Flows
2007-05-31 04:39:54.045 259.034 UDP 116.147.95.88:1110 -> 188.142.64.162:27014 68 5508 68
2007-05-31 04:39:56.282 298.174 UDP 116.147.249.27:1478 -> 188.142.64.163:27014 67 5427 67
2007-05-31 04:39:57.530 298.206 UDP 117.196.44.62:1031 -> 188.142.64.166:27014 67 5427 67
2007-05-31 04:39:58.778 297.216 UDP 117.196.44.62:1031 -> 188.142.64.166:27014 67 5427 67
2007-05-31 04:39:53.787 297.216 UDP 61.191.235.132:4121 -> 60.9.138.37:4121 62 3720 62
2007-05-31 04:39:55.354 300.833 UDP 60.9.138.37:2121 -> 118.25.93.95:2121 61 3660 61
2007-05-31 04:39:58.936 298.977 UDP 60.9.138.36:2121 -> 119.182.123.166:2121 61 3660 61
2007-05-31 04:39:59.939 300.734 UDP 120.167.25.128:2121 -> 60.9.138.37:2121 61 3660 61
2007-05-31 04:39:53.916 300.734 UDP 60.9.138.37:2121 -> 125.167.25.128:2121 61 3660 61
2007-05-31 04:39:57.946 300.353 UDP 60.9.138.36:2121 -> 121.135.4.186:2121 61 3660 61

IP addresses anonymized
Summary: total flows: 4616424, total bytes: 156.6 G, total packets: 172.6 M, avg bps: 644.8 Mb/s, avg pps: 90946, avg bpp: 929
Time window: 2007-05-31 04:11:49 - 2007-05-31 04:44:58
Total flows processed: 4616424 Skipped: 0, Bytes read: 240064932
Sys: 6.1984 flows/second: 746464.4 Wall: 6.1984 flows/second: 746361.3
```

nfsen 1.3

- Bringing the power of the command line forward
- Extremely easy to get top 10 lists pr destination, packets per second etc.

ElastiFlow – Elasticsearch based

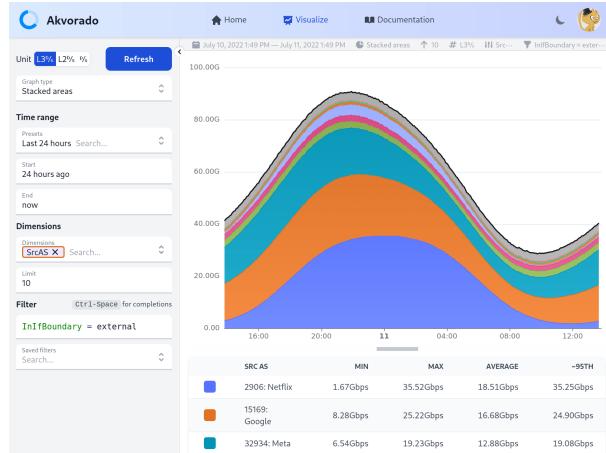


ElastiFlow

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>

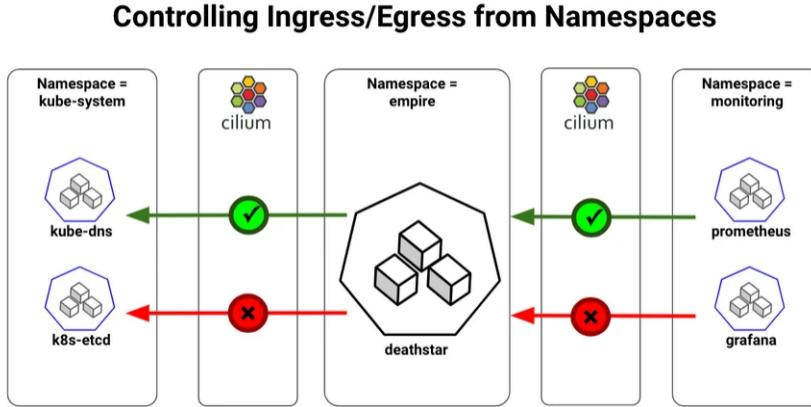
Akvorado: flow collector, enricher and visualizer



This program receives flows (currently Netflow/IPFIX and sFlow), enriches them with interface names (using SNMP), geo information (using IPinfo.io), and exports them to Kafka, then ClickHouse. It also exposes a web interface to browse the collected data.

Source: Picture and text from <https://github.com/akvorado/akvorado>

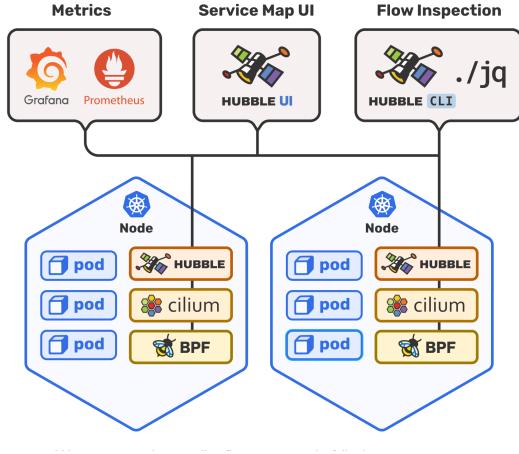
Cloud Network Security: Cilium overview



Kubernetes provides Network Policies for controlling traffic going in and out of the pods. Cilium implements the Kubernetes Network Policies for L3/L4 level and extends with L7 policies for granular API-level security for common protocols such as HTTP, Kafka, gRPC, etc

Source: picture and text from <https://cilium.io/blog/2018/09/19/kubernetes-network-policies/>

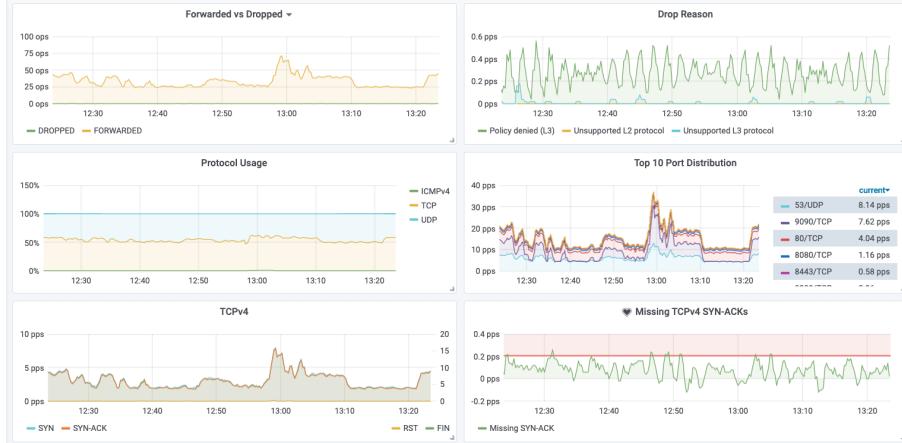
Cloud Network Security: Cilium Hubble



The Linux kernel technology eBPF is enabling visibility into systems and applications at a granularity and efficiency that was not possible before. It does so in a completely transparent way, without requiring the application to change or for the application to hide information.

Source: picture and text from <https://github.com/cilium/hubble/>

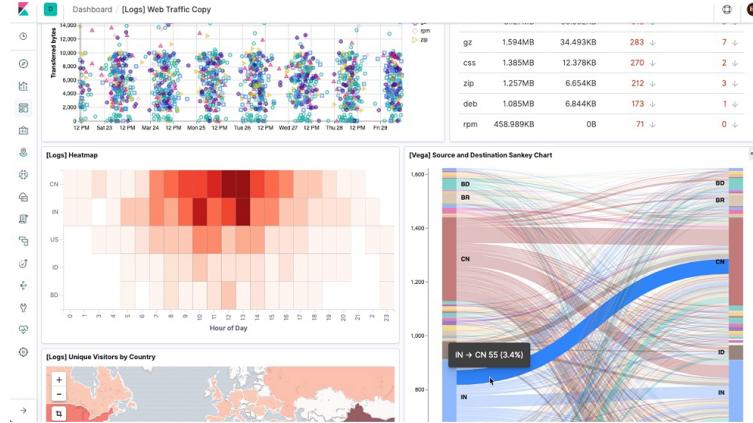
Cloud Network Security: Cilium overview



The metrics and monitoring functionality provides an overview of the state of systems and allow to recognize patterns indicating failure and other scenarios that require action. The following is a short list of example metrics, for a more detailed list of examples, see the Metrics Documentation.

Source: picture and text from <https://github.com/cilium/hubble/>

Big Data tools: Elasticsearch and Kibana



Elasticsearch is an open source distributed, RESTful search and analytics engine capable of solving a growing number of use cases.

<https://www.elastic.co>

Scirius Security Platform



The screenshot shows a Mozilla Firefox window with the title "Scirius Security Platform - Mozilla Firefox". The address bar displays "https://127.0.0.1/accounts/login/". The main content area contains the following text and form:

Scirius Security Platform
Scirius Security Platform is an advanced network detection and response (NDR) solution that mitigates risk by exposing threats to critical assets and empowering rapid response.

Scirius Security Platform is developed by Stamus Networks and provides:

- Comprehensive network inspection for complete visibility into network activity and threat events
- Guided threat hunting for proactive network defence and incident investigation using enriched event data
- Automated detection and notification of acute and urgent threats to assets, tracked by stage on the cyber kill chain

Login to Scirius

Username

Password

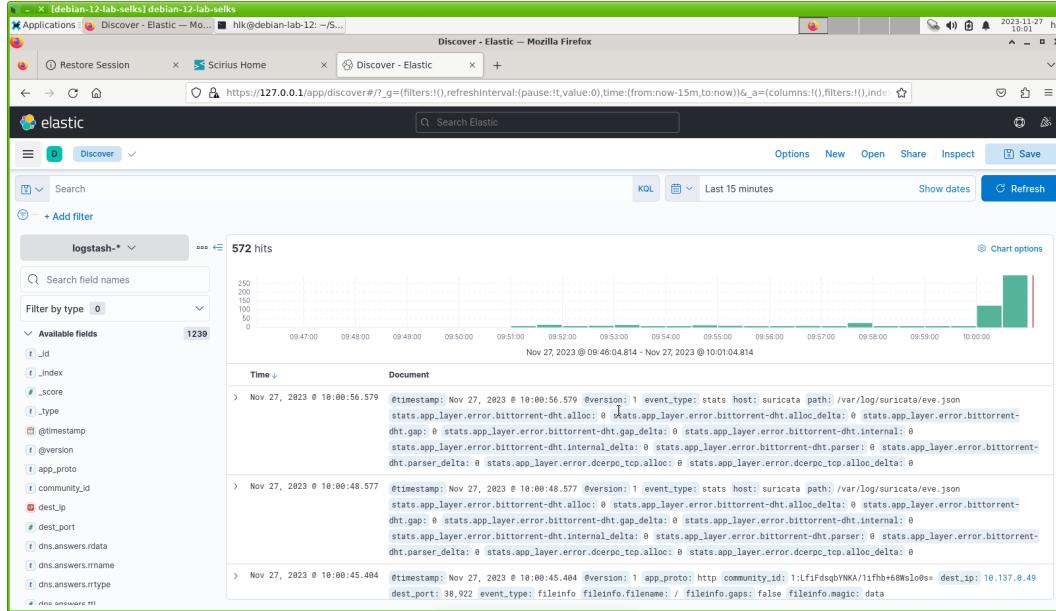
Remember this browser.

Login

Scirius Community Edition | Scirius Security Platform

- Description for this setup is in the Kickstart 2 document
- Using Docker we can turn up a full installation of Elasticsearch with data in minutes!
- <https://github.com/StamusNetworks/SELKS>

Dashboards and Searching



- Some of the most important parts of a SIEM is searching and dashboards

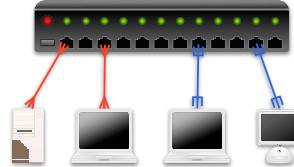
Reading Summary, False Positives



- True Positive (TP). An alert that has correctly identified a specific activity. If a signature was designed to detect a certain type of malware, and an alert is generated when that malware is launched on a system, this would be a true positive, which is what we strive for with every deployed signature. *Indicators of Compromise and Signatures*
- False Positive (FP). An alert has incorrectly identified a specific activity. If a signature was designed to detect a specific type of malware, and an alert is generated for an instance in which that malware was not present, this would be a false positive.
- True Negative (TN). An alert has correctly not been generated when a specific activity has not occurred. If a signature was designed to detect a certain type of malware, and no alert is generated without that malware being launched, then this is a true negative, which is also desirable. This is difficult, if not impossible, to quantify in terms of NSM detection.
- False Negative (FN). An alert has incorrectly not been generated when a specific activity has occurred.

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

Reputation-Based Detection



- The most basic form of intrusion detection is reputation-based detection
- Similar concept to block lists for SMTP spam relays
- I often recommend <https://github.com/stamparm/maltrail> as a source of lists
- Other sources are lists like RIPE NCC delegated, which IP prefixes are handed out in different countries
<https://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-extended-latest>
ripencc|DK|ipv4|185.129.60.0|1024|20151130|allocated|
- Tool often mentioned are Argus and SiLK <https://tools.netsa.cert.org/silk/>
If we end up having time today, or another day, we should look into this tool chain also!
- Old and mature tools have been proven to work

Metadata – enrichment



Metadata	Metacategory: Data
The DNS lookup occurred at a certain time.	Timestamp: 278621182
The internal host sent a DNS PTR request.	Network protocol: DNS PTR
The internal host had a hostname.	Location: Desktop subnet
	Source IP Address: 1.1.1.2
	Hostname: windowspc22.company.com
The internal host resolved an external host.	Location: External
	Destination IP Address: 255.123.215.3
	Hostname: dgf7adfnkjhh.com
The external host was hosted by a dynamic DNS provider.	Network: Shady DDnS Provider Inc.
	ASN: SHADY232
	Reputation: Historically risky network
The remote hostname appeared randomly generated.	Hostname: dgf7adfnkjhh.com
	Category: Unusual, nonlinguistic

Source: picture from *Crafting the InfoSec Playbook*, CIP

Metadata + Context

IP reputation



Zeek documentation Intel framework

<https://docs.zeek.org/en/stable/frameworks/intel.html>

Suricata reputation support

<https://suricata.readthedocs.io/en/latest/reputation/index.html>

Conclusion



- Implement firewalls – take control over network packets
- Start monitoring with available data feed, sources, netflow, firewall logging, DNS queries etc.
- Start from the bottom and from client ports, or from server ports if you like
- Learn some Linux and use open source projects, really, will save you thousands of USD/EUR/DKK



Referencer: netværksbøger

- Stevens, Comer,
- Network Warrior
- TCP/IP bogen på dansk
- KAME bøgerne
- O'Reilly generelt IPv6 Essentials og IPv6 Network Administration
- O'Reilly cookbooks: Cisco, BIND og Apache HTTPD
- Cisco Press og website
- Firewall bøger, Radia Perlman: IPsec,

Bøger om IPv6



IPv6 Network Administration af David Malone og Niall Richard Murphy - god til real-life admins, typisk O'Reilly bog

IPv6 Essentials af Silvia Hagen, O'Reilly 2nd edition (May 17, 2006) god reference om emnet

IPv6 Core Protocols Implementation af Qing Li, Tatuya Jinmei og Keiichi Shima

IPv6 Advanced Protocols Implementation af Qing Li, Jinmei Tatuya og Keiichi Shima

- flere andre