Welcome to

Intrusion Detection Basics

Making sense of packets

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

intrusion-detection-basics.tex in the repo security-courses

Contact information

- Henrik Kramselund Jereminsen, 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: hkj@zencurity.dk Mobile: +45 2026 6000

You are welcome to drop me an email

Time schedule

- 17:00 - 18:15 Introduction and basic packet tools
- 30min break
- 18:45 - 19:30 45min Recommended tools, Zeek and Suricata – together
- 15min break
- 19:45 - 21:00 Centralized solutions dashboards with break somewhere

Duration: 4 hours - with breaks

Keywords: TCP, UDP, ICMP, TLS, DNS, Sniffing networks, malware detection, IDS, Netflow, dashboards, , Tap/SPAN/Mirror ports, Zeek Security Monitor, Suricata with SELKS, Kibana, Emerging Threats

Goals for today

See how to sniff a few packets from popular protocols

See how sniffing can be automated using two example tools Zeek and Suricata

Present the concept of Intrusion Detection Systems

Use Ansible to provision services - which can easily be modified to cover multiple servers

See a Kibana dashboard or two

Exercises – which you can do at home later

- Run Zeek and Suricata on small pcaps

The concept of Intrusion Detection

Denning, Dorothy E., "An Intrusion Detection Model,"Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131

> Dorothy Elizabeth Denning, born August 12, 1945, is a US-American information security researcher known for lattice-based access control (LBAC), intrusion detection systems (IDS), and other cyber security innovations. She published four books and over 200 articles. Inducted into the National Cyber Security Hall of Fame in 2012, she is now Emeritus Distinguished Professor of Defense Analysis, Naval Postgraduate School.

`https://en.wikipedia.org/wiki/Dorothy_E._Denning`

Why spend time on IDS

You have malware on a system?!

- You have identified **one system**
- And perhaps even the strain of malware – nice!

but what are the next steps? Natural questions are:

- Which other systems are infected?
- What is the timeline, when was this system infected, was it the first one?
- What else happened before and after?
- How do we clean up?

Some of these questions quickly become broad!

How to proceed

DON'T PANIC

Especially hard to recommend next steps without some facts to support decisions.

- Shutdown the internet connection?
- Shutdown all servers vs KEEP RUNNING
- Reinstall ALL servers, all laptops, all ...

Incident Handling process

Basic incident response process

- Preparation for an attack, establish procedures and mechanisms for detecting and responding to attacks
- Identification of an attack, notice the attack is ongoing
- Containment (confinement) of the attack, limit effects of the attack as much as possible
- Eradication of the attack, stop attacker, block further similar attacks
- Recovery from the attack, restore system to a secure state
- Follow-up to the attack, include lessons learned improve environment

Source: *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, 1st edition E Eugene Schultz Russell Shumway 2002

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

Need facts!

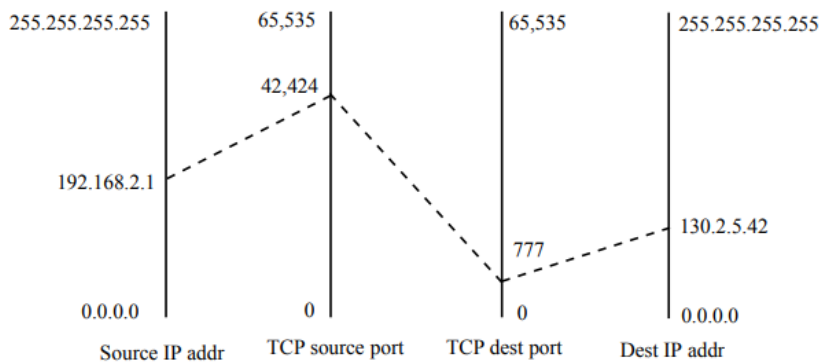


Figure 7: Parallel coordinate plot for a TCP packet from 192.168.1.1:42424 to 130.2.5.42:777.

- To answer questions we need facts!
- Tools can give those facts
- Note: I will recommen a toolbox, consider them examples – lots of other great tools exist
- My tool box includes Suricata, Elasticsearch, Kibana, Zeek, Filebeat, Packetbeat, Logstash, NFsen, Elastiflow etc.
- Others are happy with Graylog, Grafana Loki and others

Parallel coordinate plots

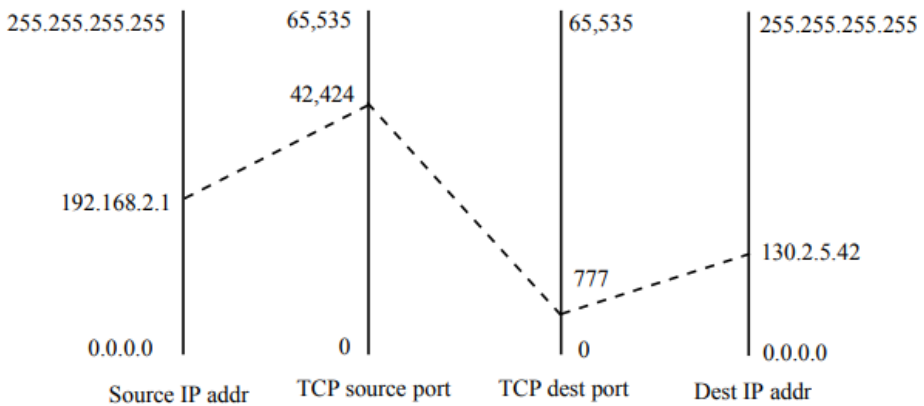


Figure 7: Parallel coordinate plot for a TCP packet from 192.168.1.1:42424 to 130.2.5.42:777.

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`

Intrusion Kill Chains

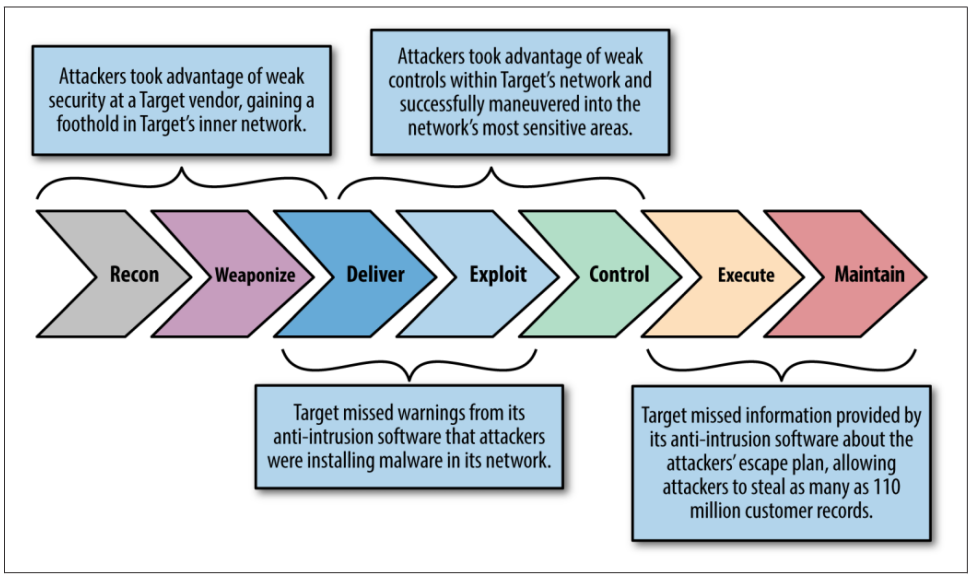


Figure 7-1. The kill chain

- See also *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corporation

  `https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf`

Data Science Workflow

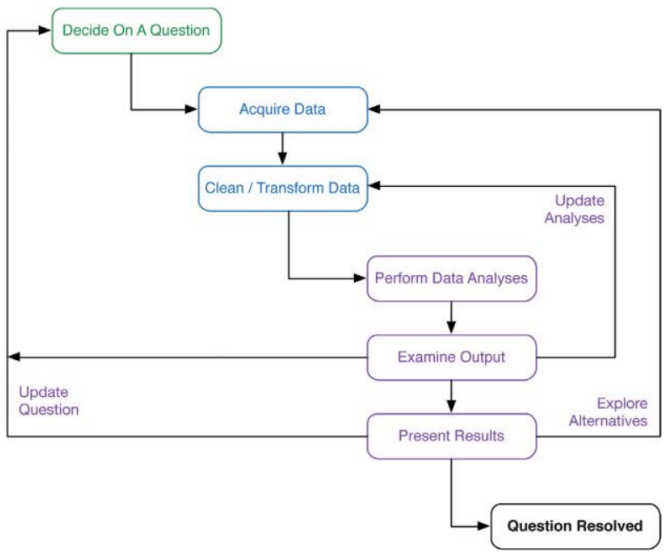


FIGURE 12-2 *The data science workflow*

- Find and Collect Relevant Data, Learn through Iteration

Source: DDS 12. Moving Toward Data-Driven Security

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

Create goals

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: DDS 12. Moving Toward Data-Driven Security

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

Get started quickly

My recommendation today is to create a production-ready environment, but for learning the following are useful

Security Onion covers a lot of different areas, but is a bit heavy. Lots of great information and recommended tools
`https://securityonionsolutions.com/software/`

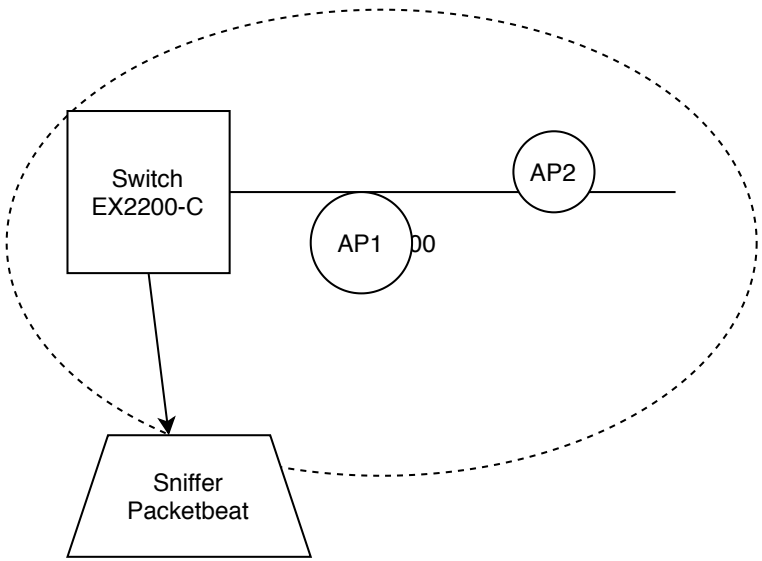
If you want to try out Suricata and focus on network traffic, try SELKS
`https://www.stamus-networks.com/selks`

Generic packet capture and Elastic beats
`https://www.elastic.co/beats/packetbeat`

Generic malware and malicious traffic detection – Python based and easy to deploy
`https://github.com/stamparm/maltrail`

Brim is packaged as a desktop app, open a pcap and transform into Zeek logs in the ZNG format
`https://www.brimsecurity.com/`

Packetbeat



- By installing packetbeat and doing network mirroring from the network switch, we can gather a lot of information
- Packetbeat supports Elastic Common Schema (ECS) `https://www.elastic.co/beats/packetbeat`
- ICMP (v4 and v6) DHCP (v4) DNS HTTP AMQP 0.9.1 Cassandra Mysql PostgreSQL Redis Thrift-RPC MongoDB Memcache NFS TLS SIP/SDP (beta)

About equipment and exercises

- Bringing a laptop to my courses is not required, but welcome
- Links etc. are in the slides and open source licensed, PDFs
- 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

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

Be ethical, act honorably

Ask permission, inform when logging people traffic

Especially do NOT, repeat DO NOT log illegally.

`https://ulovliglogning.dk/`

Course Materials

This material is in multiple parts:

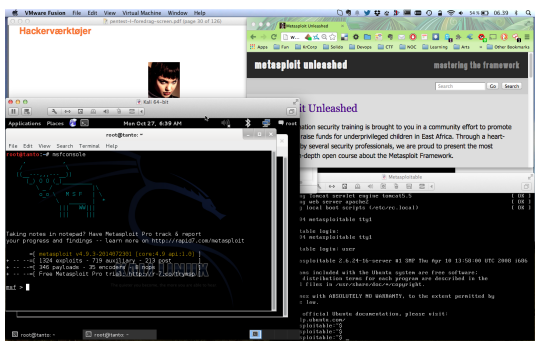
- Slide shows - presentation - this file
- Exercises - PDF files in my repository

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/`
- Production use: Debian Linux `https://www.debian.org/`

Networking Hardware

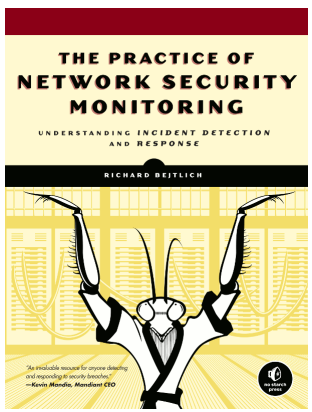
If you want to do exercises and work with networks
It will be an advantage to have a wireless USB network card and an USB Ethernet card.

The following are two models I have used:

- 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

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

Network Security Monitoring – Intrusion Detection



Network Security Monitoring (NSM) - monitoring networks for intrusions, and reacting to those

networkbased intrusion detection systems (NIDS)

host based intrusion detection systems (HIDS)

Example full systems are Security Onion `https://securityonion.net/` or SELKS `https://www.stamus-networks.com/open-source/`

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

Detection Capabilities

Security incidents happen, but what happens. One of the actions to reduce impact of incidents are done in preparing for incidents.

> *Preparation* for an attack, establish procedures and mechanisms for detecting and responding to attacks

Preparation will enable easy **identification** of affected systems, better **containment** which systems are likely to be infected, **eradication** what happened – how to do the **eradication** and **recovery**.

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

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

What happens today?

.

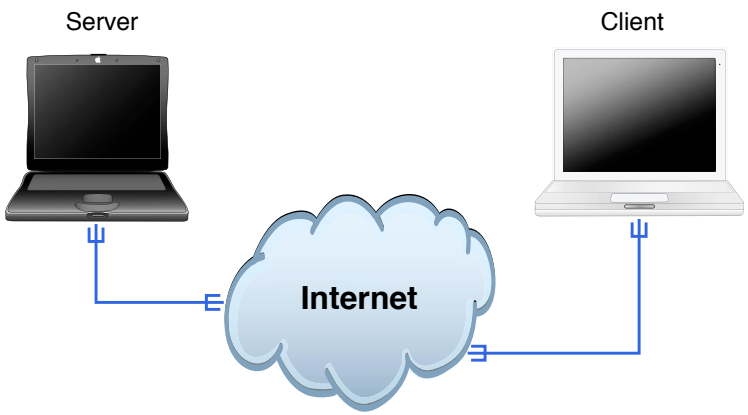
Think like a blue team member find hacker traffic

Get basic tools running

Improve situation

- See where the data end up
- What kind of data and metadata can we extract
- How can we collect and make use of it
- Databases and web interfaces, examples shown
- Consider what your deployment could be

Internet Today



- Clients and servers, roots in the academic world
- Protocols are old, some more than 20 years
- Very little is encrypted, mostly HTTPS

What is the Internet

Communication between humans - currently!

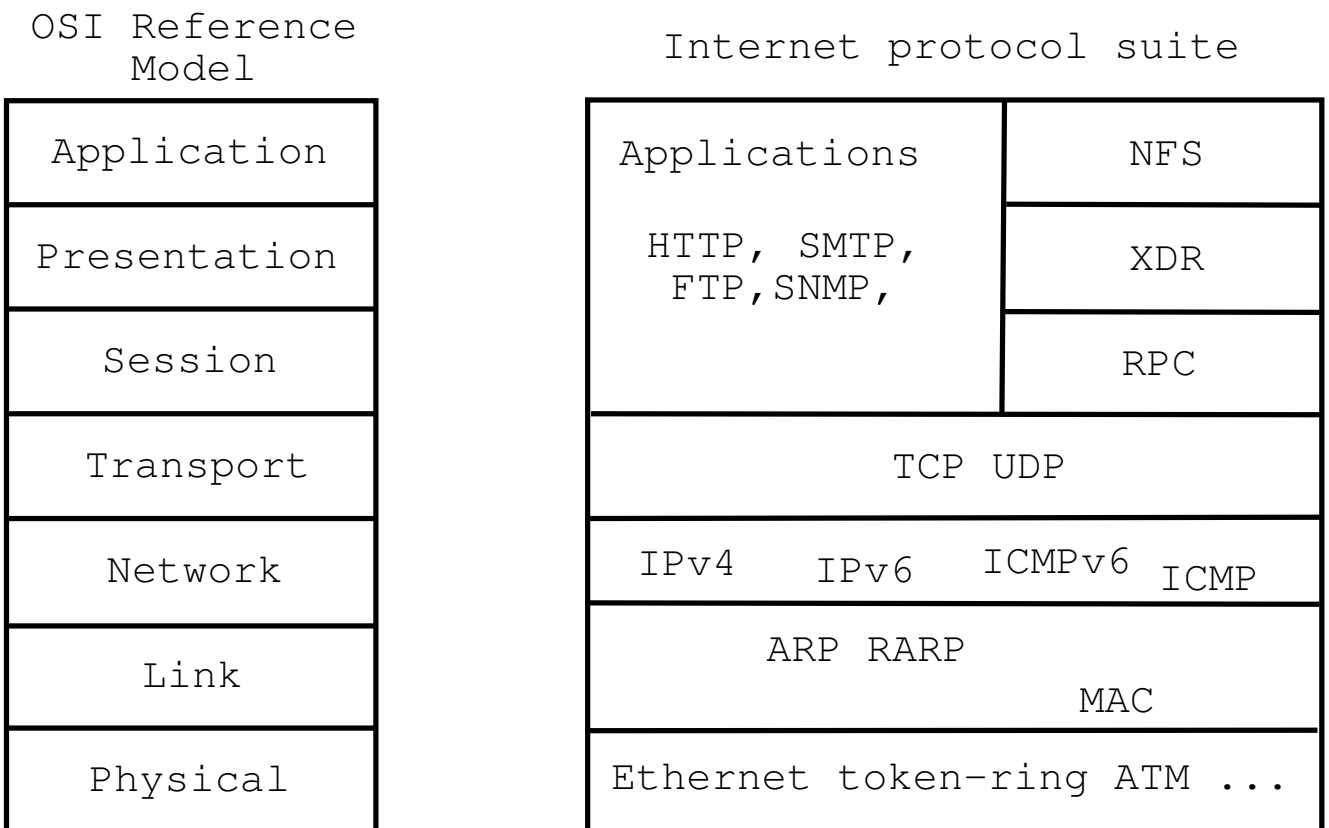
Based on TCP/IP

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

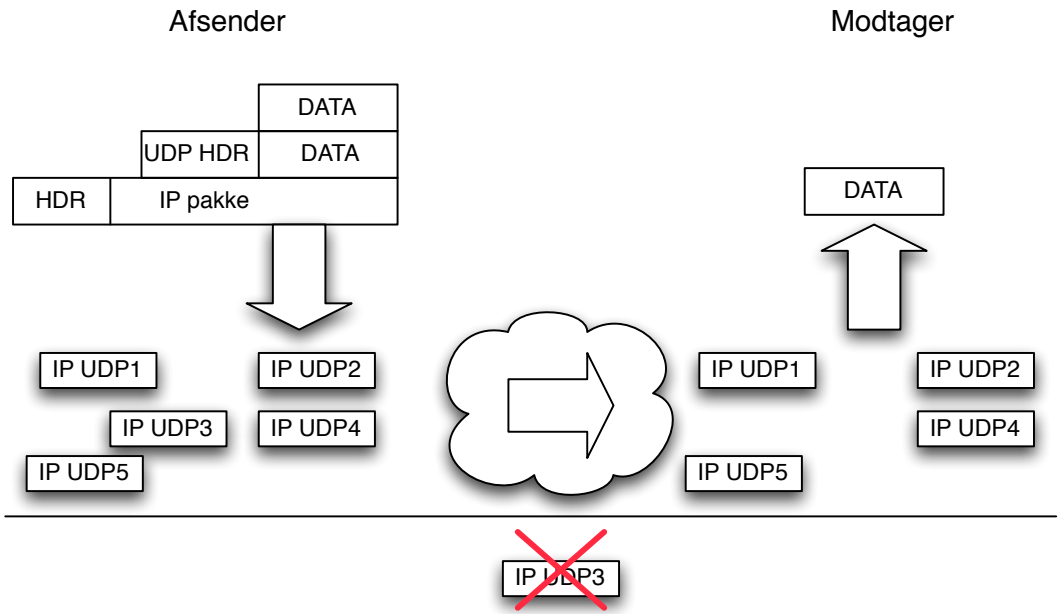
RFC-1958:

> 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.

OSI and Internet models



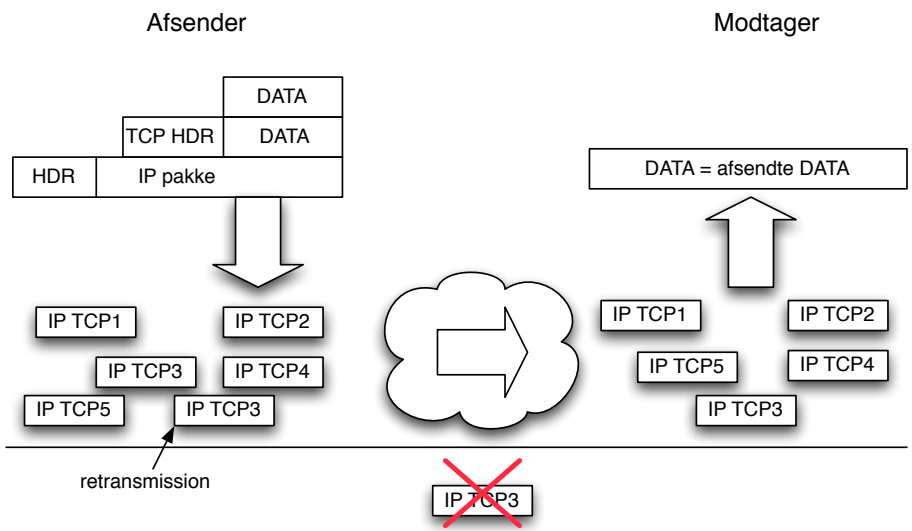
UDP User Datagram Protocol



Connection-less RFC-768, *connection-less*

Used for Domain Name Service (DNS)

TCP Transmission Control Protocol



Connection oriented RFC-791 September 1981, *connection-oriented*

Either data delivered in correct order, no data missing, checksum or an error is reported

Used for HTTP and others

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`

ICMP Internet Control Message Protocol

Control protocol, error messages

Common messages

- ICMP ECHO, anyone there?
- Host unreachable
- Port unreachable

signaling

Defined in RFC-792

IPv6 neighbor discovery protocol (NDP)

OSI	IPv4	IPv6
Network	IP / ICMP	IPv6 / ICMPv6
Link	ARP	
Physical	Physical	Physical

Address Resolution Protocol (ARP) is gone from IPv6

NDP replaces and expand, command to use `arp -an` replaced by `ndp -an`

Basic test tools TCP - Ping and Traceroute

We should all know

- `ping` – like sending a radar ping, anything there
- `traceroute` (windows tracert) – find the route packets traverse

and add these!

- `Wireshark` – like sending a radar ping, anything there
- `Nmap` and `Nping` – port scan and advanced ping program!

Ping

```
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=150 time=8.849 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=150 time=0.588 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=150 time=0.553 ms
```

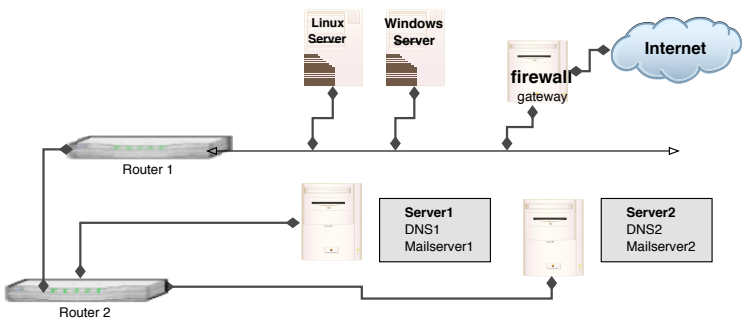
ICMP – Internet Control Message Protocol

ECHO – only ICMP message that generates another

ICMP ECHO request sent, and ICMP ECHO reply expected

Same with IPv6, `ping6`

Network mapping



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

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

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

Default Unix traceroute uses UDP, Windows tracert use ICMP

traceroute

```
hkj@bob:~$ traceroute www.kramse.dk
traceroute to www.kramse.dk (185.129.60.130), 30 hops max, 60 byte packets
 1  10.0.42.1 (10.0.42.1)  0.365 ms  0.277 ms  0.239 ms
 2  79.142.xxx.xxx (79.142.xxx.xxx)  5.174 ms  4.979 ms  5.113 ms
 3  bgp2-dix.prod.bolignet.dk (79.142.224.2)  5.538 ms  5.057 ms  5.483 ms
 4  217.74.215.57 (217.74.215.57)  5.990 ms  5.962 ms  5.932 ms
...
 8  185.150.199.178 (185.150.199.178)  7.684 ms  7.647 ms  4.627 ms
 9  * * * // firewall here!
```

Works using the Time to live (TTL) counter

Sending with $TTL = 1$ returns ICMP from first host/router

Default sends UDP on Unix, and ICMP on Windows

Kali has programs that can emulate, or send using any protocol

traceroute – UDP

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

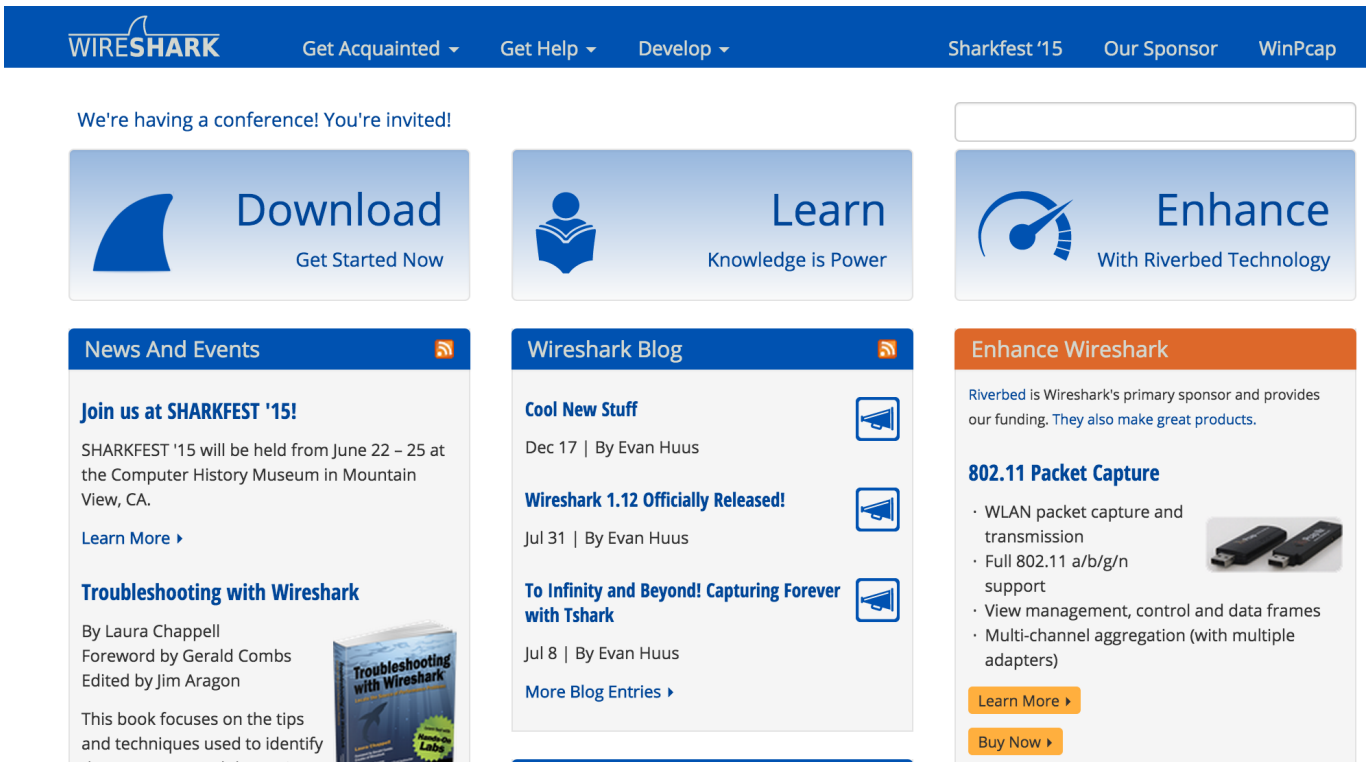
Low TTL, UDP, high ports above 33000 = Unix traceroute signature

Packet sniffing tools

Tcpdump for capturing packets

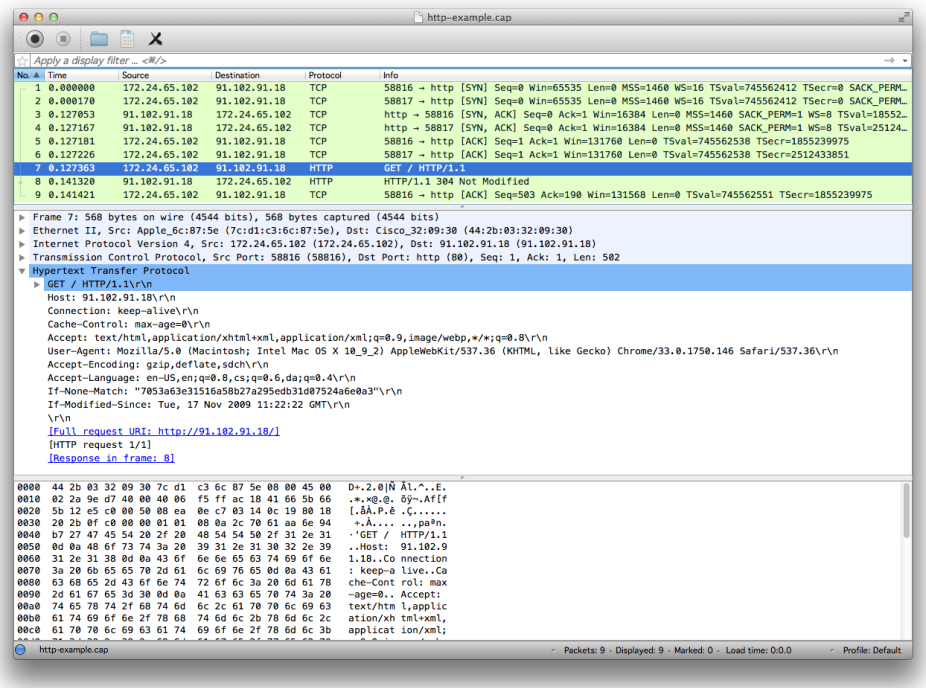
Wireshark for dissecting packets manually with GUI

Wireshark - graphical network sniffer



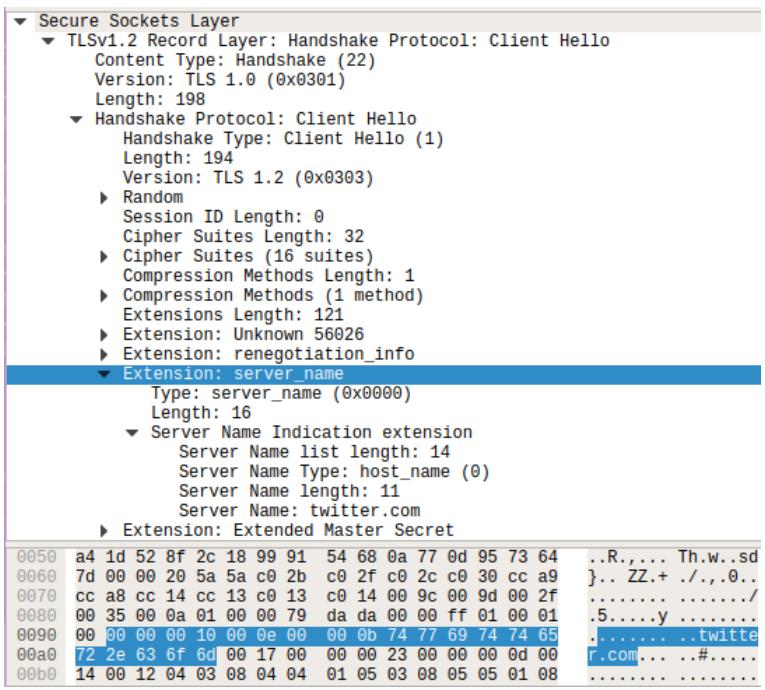
http://www.wireshark.org

Using Wireshark



Capture - Options, select a network interface

Detailed view of network traffic with Wireshark



Notice also the filtering possibilities, capture and view

Remote network debugging

- TShark and Tcpdump, I often use: `tcpdump -nei eth0`
  `tshark -z expert -r download-slow.pcapng`
- Remote packet dumps, `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!

Note About Hardware IPv4 checksum offloading

IPv4 checksum must be calculated for every packet received

IPv4 checksum must be calculated for every packet sent
Usually on a router the Time To Live is decremented, to need re-calculation

Let an ASIC chip on the network card do the work!

Most server network chips today support this and more

Benefit for performance, but beware when using security tools

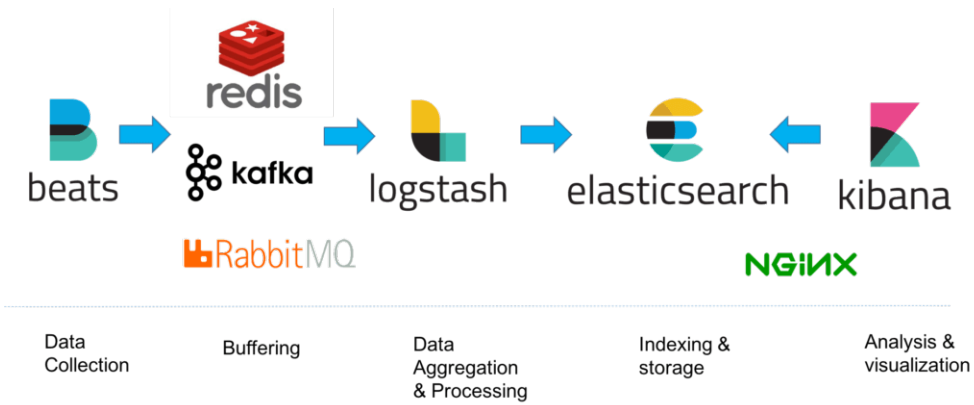
If every packet in wireshark has wrong checksum, its the network card doing it

Can be turned off, when doing security work

Moving from manual checking to automated

- Wireshark is advanced manual tool, try right-clicking different places
- How do we continously monitor the network?

Automated packet sniffing tools



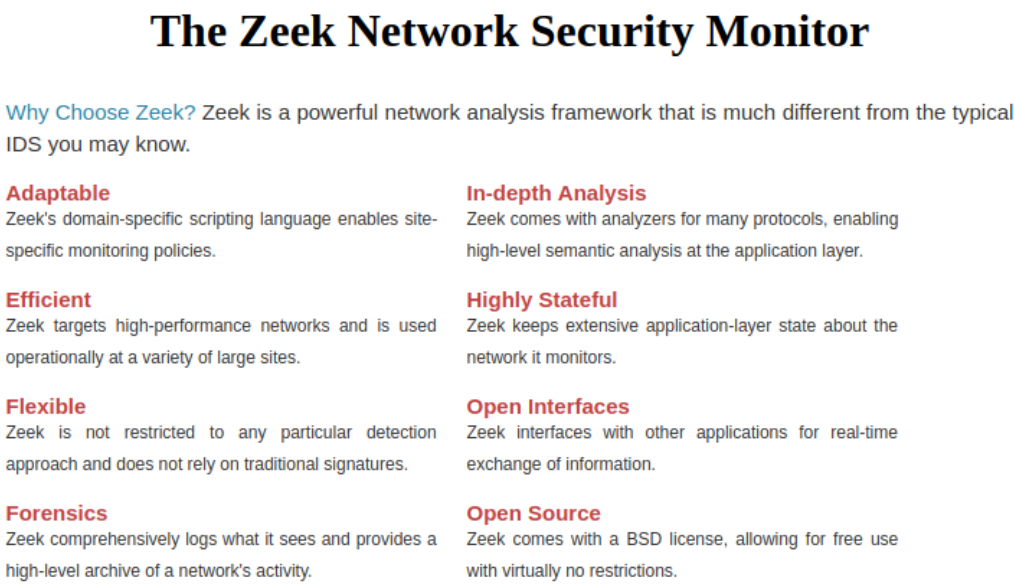
Zeek – Network Security Monitor `https://zeek.org`

Suricata – network threat detection `https://suricata-ids.org/`

PacketBeat decodes multiple protocols

Often a combination of tools and methods used in practice

The Zeek Network Security Monitor



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

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: Count DNS replies

https://www.zeek.org/sphinx-git/script-reference/scripts.html

Side note: Zeek Security Monitor handles formats differently

Zeek has files formatted with a header:

```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   trans_id
        rtt     query   qclass  qclass_name     qtype   qtype_name      rcode   rcode_name      AA
        TC      RD      RA      Z       answers TTLs    rejected

1538982372.416180 CD12Dc1SpQm42QW4G3 10.xxx.0.145 57476 10.x.y.141 53 udp 20383
0.045021 www.dr.dk 1 C_INTERNET 1 A 0 NOERROR F F T T 0
   www.dr.dk-v1.edgekey.net,e16198.b.akamaiedge.net,2.17.212.93 60.000000,20409.000000,20.000000 F
```

Note: this show ALL the fields captured and dissected by Zeek, there is a nice utility program zeek-cut which can select specific fields:

```
root@NMS-VM:/var/spool/zeek/zeek# cat dns.log | zeek-cut -d ts query answers | grep dr.dk
2018-10-08T09:06:12+0200 www.dr.dk www.dr.dk-v1.edgekey.net,e16198.b.akamaiedge.net,2.17.212.93
```

Can also just use JSON now via Filebeat

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

```
// install zeek first
kunoichi:~ root# zeekctl
Hint: Run the zeekctl "deploy" command to get started.

Welcome to ZeekControl 2.3.0
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 ...
...
kunoichi:etc root# grep eth0 node.cfg
interface=eth0
```

Zeek demo: Run Zeek

```
// back to zeekctl and start it
[ZeekControl] > start
starting zeek
// and then
kunoichi:zeek root# pwd
/usr/local/var/spool/zeek
kunoichi:zeek root# tail -f dns.log
```

More examples at:

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

DNS is important

Another tool that provides a basic SQL-frontend to PCAP-files
`https://www.dns-oarc.net/tools/packetq`
`https://github.com/DNS-OARC/PacketQ`

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

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

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.

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

We will now move to the workshop materials:

Suricata, Zeek og DNS Capture

`https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop`

Exercise at home – Your lab setup

- Go to GitHub, Find user Kramse, click through security-courses, courses, suricatazeek and 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`

NetFlow

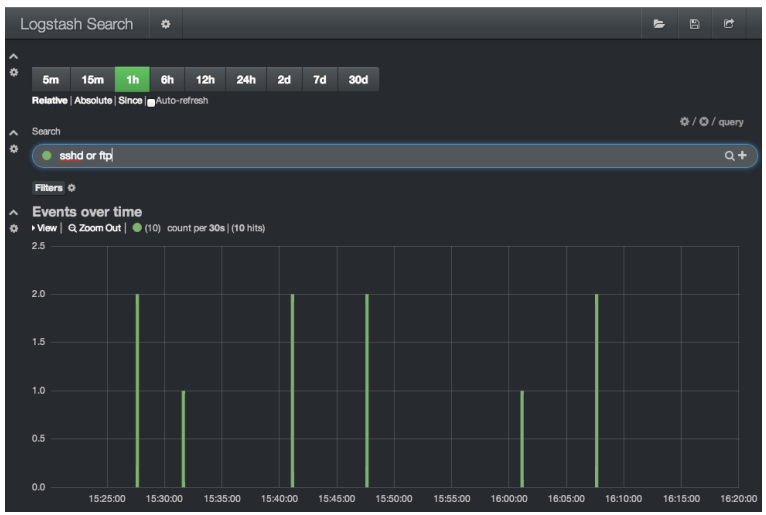
NetFlow is getting more important, more data share the same links

Accounting is important ı*Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudistem Detecting DoS/DDoS and problems is essential

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

Currently also investigating sFlow - hopefully more fine grained

View data efficiently

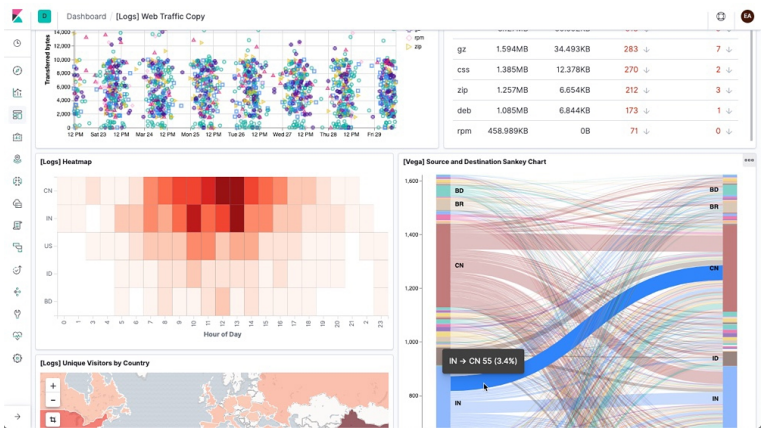


View data by digging into it easily - must be fast

Logstash and Kibana are just examples, but use indexing to make it fast!

Other popular examples include Graylog and Grafana

Big Data tools: Elasticsearch



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

`https://www.elastic.co`

We are all Devops now, even security people!

Kibana

Highly recommended for a lot of data visualisation

Non-programmers can create, save, and share dashboards

Source: `https://www.elastic.co/products/kibana`

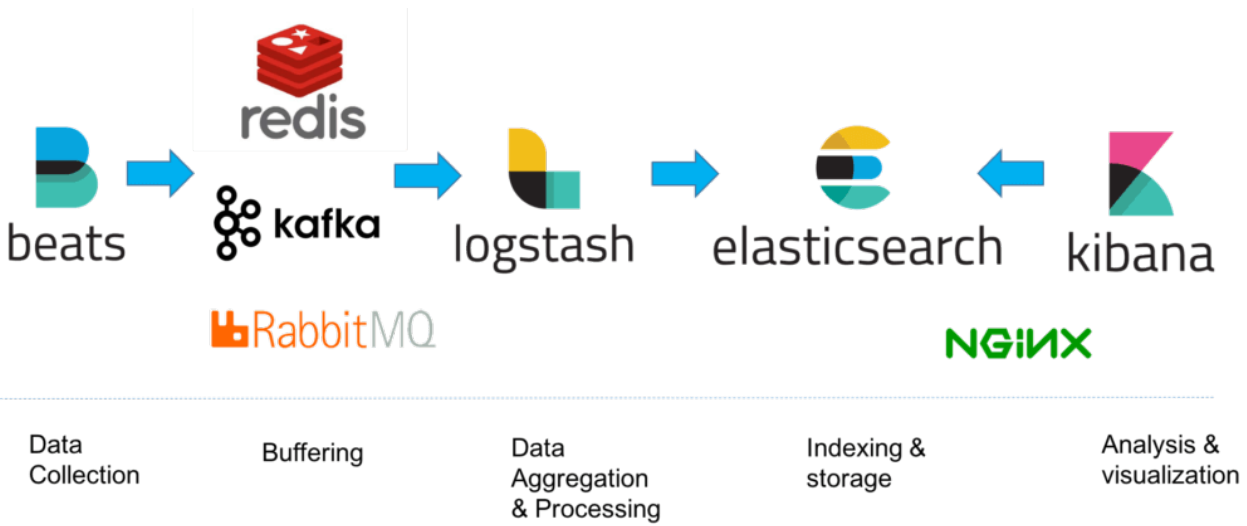
Drill down process

We have seen Kibana multiple times, but how do you use it? I recommend the following iterative process

1. Get an overview
2. Research top talkers,
3. When identified and handled, remove with filter `not host 10.1.2.3`
4. Look at the next ones

Look into details, lookup hostnames – hopefully your tool allows some help

Architecture



- Real production environments often add some buffering in between
- Allows the ingestion to become more smooth, no lost messages

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

Summary, what to log

CIP 7 Tools of the Trade, need to know NetFlow, DNS, and HTTP proxy logs in the real-world

- Defense in Depth – we will never catch everything
- Log Management: The Security Event Data Warehouse
- Intrusion Detection Isn't Dead
- DNS, the One True King – Logging and analyzing DNS transactions, Blocking DNS requests or responses
- HTTP Is the Platform: Web Proxies – Web proxies allow you to solve additional security problems
- Rolling Packet Capture – In a perfect world, we would have full packet capture everywhere

Commercial Support

You can and should use updated rulesets for Suricata.

I Recommend the Emerging Threats ET Pro ruleset, which is about USD 900 per year per sensor. So two sites with Suricata running in both, 2x USD 900

Summary

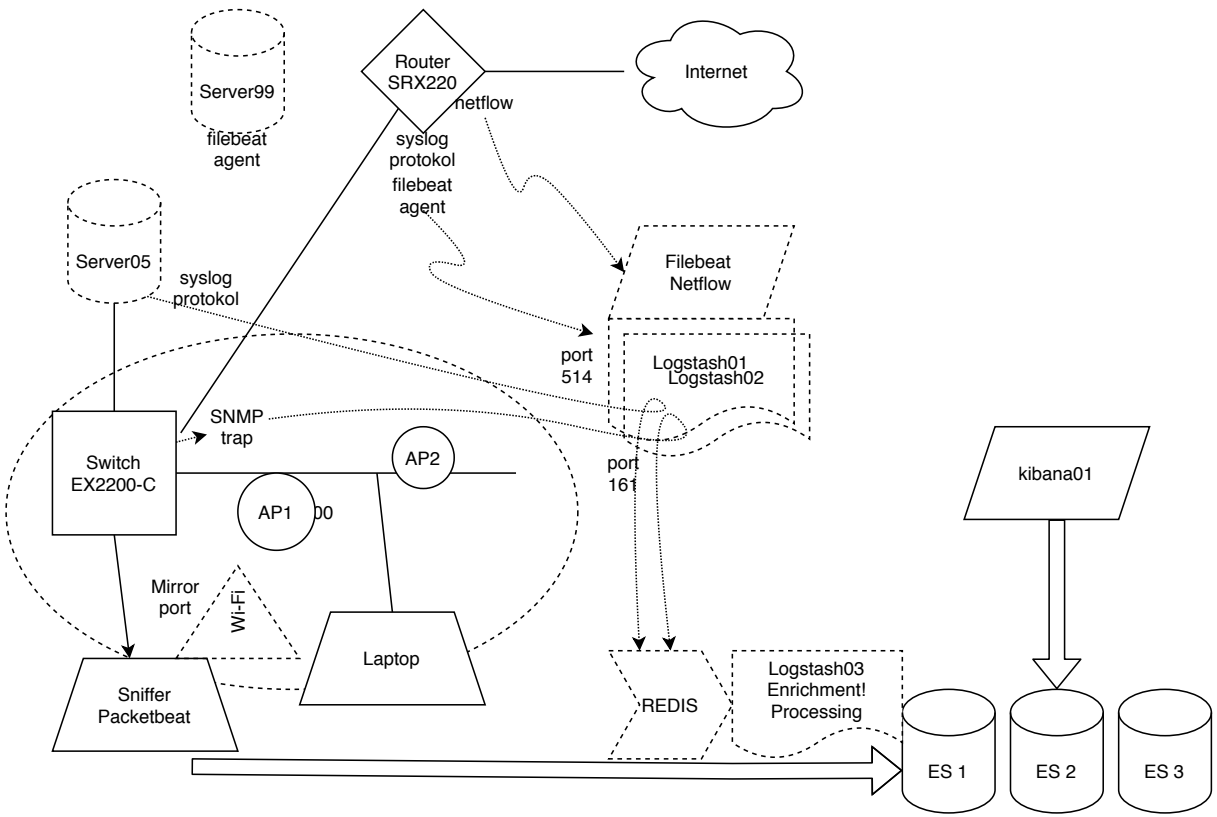
We started from a basic Ubuntu/Debian server, and using Zeek and Suricata we now know more about our network.

We can collect logs about network traffic based on generic NetFlow, specific types DNS/TLS/protocols, and traffic matching advanced rulesets.

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

What are the next steps?

Lets design a SIEM Infrastructure Proof of Concept



Deploying security

> **Security is a process, not a product.** Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches.

Source: `https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html`

Today, we will consider the deployment plan being:

- People – make sure management is on board, Sources – which data to gather,
- Technology – select SIEM, architecture, tools and products
- Dashboards – we have done parts of this, refer to SOC book also
- Procedures – left as a home exercise today

Extended Sources

When a basic logging infrastructure is setup, it can be expanded to increase coverage, by adding more sources:

- DNS query logging – will enable multiple cases to be resolved, example malware identification and tracing, when was a malware domain queried, when was the first infection
- Web proxy logging – which web pages did which client access
- Session data from Firewalls, Netflow – traffic patterns can be investigated and both attacks and cases like exfiltration can likely be seen

Hint: Take the sources available first, make a proof-of-concept, expand coverage

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

Security devops

We need devops skillz in security

automate, security is also big data

integrate tools, transfer, sort, search, pattern matching, statistics, ...

tools, languages, databases, protocols, data formats

Use GitHub! So many libraries and programs that can help, maybe solve 90% of your problem, and you can glue the rest together

Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide

We are all Devops now, even security people!

People: Get management buy-in

You will probably need help from:

- Buy-in from management, for requesting resources
- Network and security departments – getting data, opening ports
- Application developers, web site programmers

Lifeguard training photo by Margarida CSilva on Unsplash

Questions?

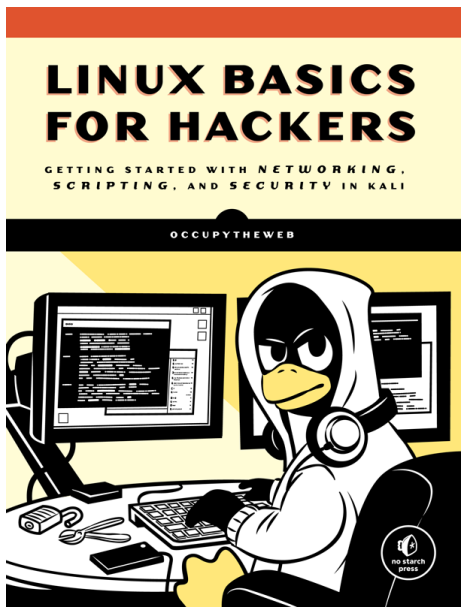
Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

Recommended further reading

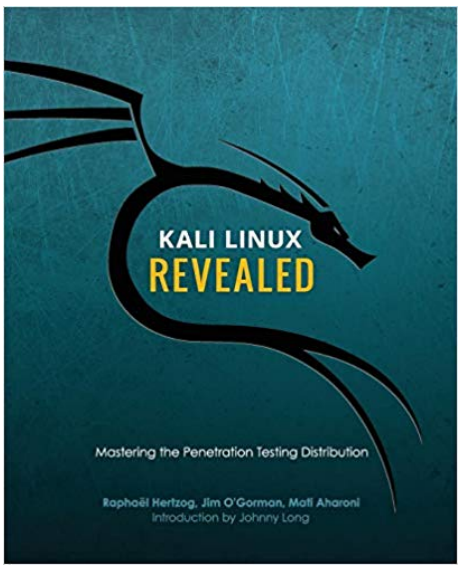
Book: Linux Basics for Hackers (LBhf)



Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb December 2018, 248 pp. ISBN-13: 9781593278557

`https://nostarch.com/linuxbasicsforhackers` Explains how to use Linux

Book: Kali Linux Revealed (KLR)



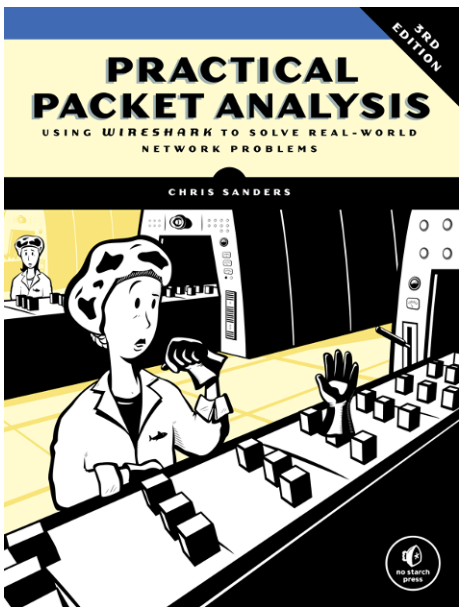
Kali Linux Revealed Mastering the Penetration Testing Distribution

`https://www.kali.org/download-kali-linux-revealed-book/`
Explains how to install Kali Linux

Book: The Debian Administrator's Handbook (DEB)

The Debian Administrator's Handbook, Raphaël Hertzog and Roland Mas
`https://debian-handbook.info/` - shortened DEB

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`

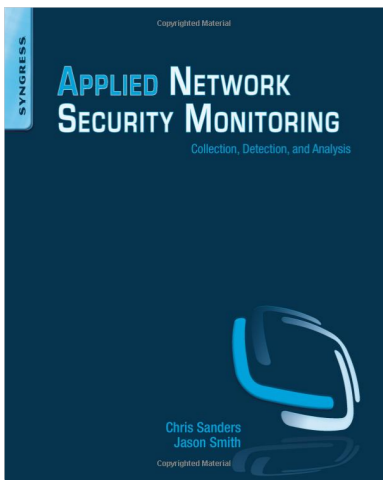
Primary literature for my SIEM and logging course

Primary literature:

Free graphics by Lumen Design Studio

- *Data-Driven Security: Analysis, Visualization and Dashboards* Jay Jacobs, Bob Rudis ISBN: 978-1-118-79372-5 February 2014 `https://datadrivensecurity.info/` - short DDS
- *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan* by Jeff Bollinger, Brandon Enright, and Matthew Valites ISBN: 9781491949405 - short CIP
- *Intelligence-Driven Incident Response* Scott Roberts ISBN: 9781491934944 - short IDI
- *Security Operations Center: Building, Operating, and Maintaining your SOC* ISBN: 9780134052014 Joseph Muniz - short SOC

Book: Applied Network Security Monitoring (ANSM)



Applied Network Security Monitoring: Collection, Detection, and Analysis 1st Edition

Chris Sanders, Jason Smith eBook ISBN: 9780124172166 Paperback ISBN: 9780124172081 496 pp. Imprint: Syngress, December 2013

`https://www.elsevier.com/books/applied-network-security-monitoring/unknown/978-0-12-417208-1`

ANSM Summary

ANSM chapter (7,8),9,10 - 140 pages
DETECTION MECHANISMS
Generally, detection is a function of software that parses through collected data in order to generate alert data. This software is referred to as a detection mechanism.

Chapter 7 Detection Mechanisms, Indicators of Compromise, and Signatures
Chapter 8 Reputation-Based Detection
Chapter 9 Signature-Based Detection with Snort and Suricata
Chapter 10 The Bro Platform // Now Zeek

Zeek in the default configuration activates 10.000s of script lines out-of-the-box.
Gives great output with little effort and complements Suricata/NIDS

ANSM Summary

The Zeek Network Security Monitor

ANSM chapter 7: Detection Mechanisms and Indicators of Compromise, and Signatures

- Indicators of Compromise (IOC) any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner
- Background information, useful when we talk about Zeek (previously Bro) later
- Intrusion Detection Systems try to detect ... but what if we know that some domains, servers, IPs etc are signs of bad activity - even compromise
- IP reputation - some IPs are used for controlling malware command and control (C2) servers etc.
- A signature can contain one or more IOCs

ANSM Summary, continued

ANSM chapter 8: Reputation-Based Detection

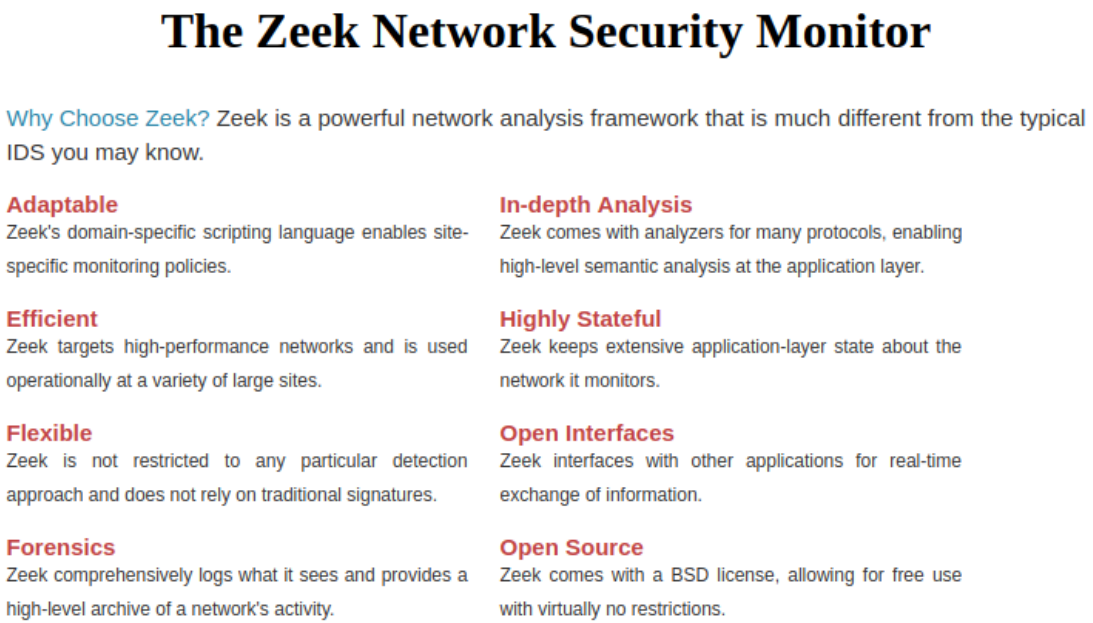
- The most basic form of intrusion detection is reputation-based detection
- Similar concept to block lists for SMTP spam relays
- I often recommend `https://github.com/stamparm/maltrail` as a source of lists
- Other sources are lists like RIPE NCC delegated, which IP prefixes are handed out in different countries
  `https://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-extended-latest`
  `ripencc|DK|ipv4|185.129.60.0|1024|20151130|allocated|`
- Mentions 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!

ANSM Summary, continued

ANSM chapter 9: Signature-Based Detection with Snort and Suricata

- Suricata IDS
- IDS rules are introduced
- I recommend a commercial license for the EmergingThreats ruleset

ANSM Summary, continued



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.

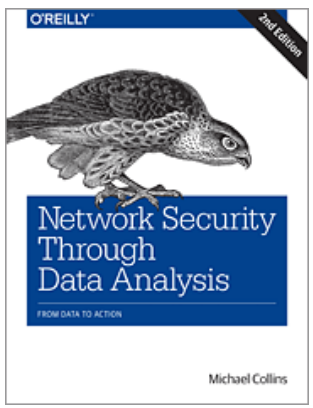
Forensics
Zeek comprehensively logs what it sees and provides a high-level archive of a network's activity.

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

ANSM chapter 10: The Zeek (Bro) Platform

- Zeek concepts and logs - many useful ones by default!

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 2015-05-01: Second release, 348 Pages

New Release Date: August 2017