Welcome to

Webinar

KEA Kompetence SIEM and Log Analysis

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

Slides are available as PDF, kramse@Github

webinar-siem-log-analysis.tex in the repo security-courses

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity.com, 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
- Run a small network for fun AS57860

You are welcome to drop me an email

Overview Diploma in IT-security

Afgangsprojektet (15 ECTS)	
Der udvikles løbende nye valgfag til Diplom i it-sikkerhed. Disse vil løbende blive beskrevet i en allonge (bilag 2) til studieordningen.	
Sikkerhed i it-governance (it-sikkerhedsledelse) (5 ECTS)	Systemsikkerhed (10 ECTS)
Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)	
Softwaresikkerhed (10 ECTS)	
Netværks- og kommunikationssikkerhed (10 ECTS)	

Course: SIEM and Log Analysis (5 ECTS)

- Slide shows - presentation - this file
- Exercises - PDF which is updated along the way
- Books listed in the lecture plan and here
- Additional resources from the internet

Teaching dates: mostly tuesdays and thursdays 17:00 - 20:30

Course Description

From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018
VF4 SIEM og log analyse (5 ECTS)

Indhold
Den studerende lærer om Security information and event management (SIEM), herunder hvordan man kan indsamle, administrere, og søge i sikkerhedshændelsesdata i et større it system (komplekse systemer, IOT deployments, corporate IT).

Læringsmål
Viden – Den studerende har viden om og forståelse for:

- Typiske SIEM arkitekturer
- Standard logformater og logtyper for standard systemer og komponenter
- Typiske SIEM produkter
- Juridiske krav til logning og bevarelse af data ifb. forensic analyse

Færdigheder – Den studerende kan:

- Lave en baseline-analyse af en infrastruktur
- Bruge log-data til at identificere infrastrukturkomponenter
- Bruge et værktøj til at analysere system log-data og netværkstrafik til at finde sikkerhedshændelser
- Udvikle "dashboards"og alarmer der viser tegn på hændelser

Kompetencer – Den studerende kan:

- Designe og implementere en SIEM løsning på tværs af diverse produkter
- Træffe beslutninger om hvilke data der skal indsamles i en givne situation
- Identificerer fejl i logopsamlingen
- Deltage i drøftelser på et praktisk og strategisk niveau i forhold til implementering af logmanagement/SIEM

Final word is the Studieordning which can be downloaded from

https://kompetence.kea.dk/uddannelser/it-digitalt/diplom-i-it-sikkerhed

Studieordning_for_Diplomuddannelsen_i_IT-sikkerhed_Aug_2018.pdf

Some keywords relating to this course

Analysis Visualization Dashboards Data-driven Security
SIEM architectures frameworks acquire process Zeek
log formats data types databases JSON XML Security Operations Center
(Incident Response) Intelligence R and Python fundamentals
Practical application Building Infosec Ansible Playbooks
Collect, mine, organize, and analyze relevant data sources
Sort data create reporting and monitoring Netflow ports
IP-address Netflow nfdump Elasticsearch real-world knowledge

- Lots of new terms, technologies and tools

Prerequisites

This course includes exercises and getting the most of the course requires the participants to carry out these practical exercises

We will use Linux for some exercises but previous Linux and Unix knowledge is not needed

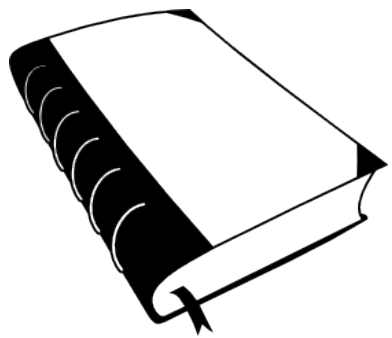
It is recommended to use virtual machines for the exercises

Security and most internet related security work has the following requirements:

- Network experience
- Server experience
- TCP/IP principles - often in more detail than a common user
- Programming is an advantage, for automating things
- Some Linux and Unix knowledge is in my opinion a **necessary skill** for infosec work
  – too many new tools to ignore, and lots found at sites like Github and Open Source written for Linux

Primary literature

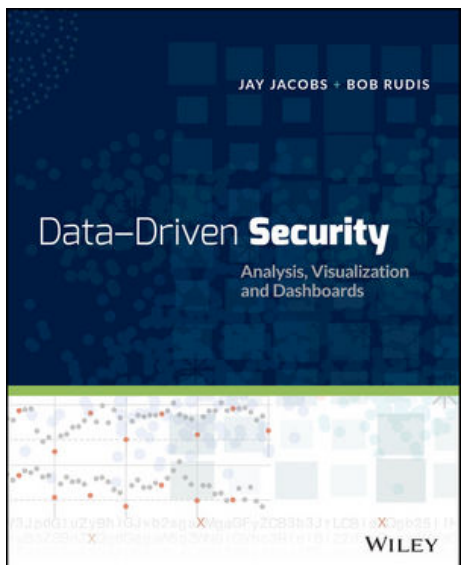
Primary literature:



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

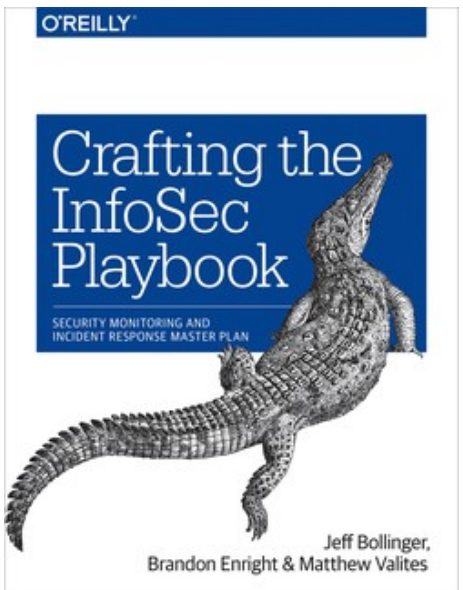
Data-Driven Security: Analysis, Visualization and Dashboards



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

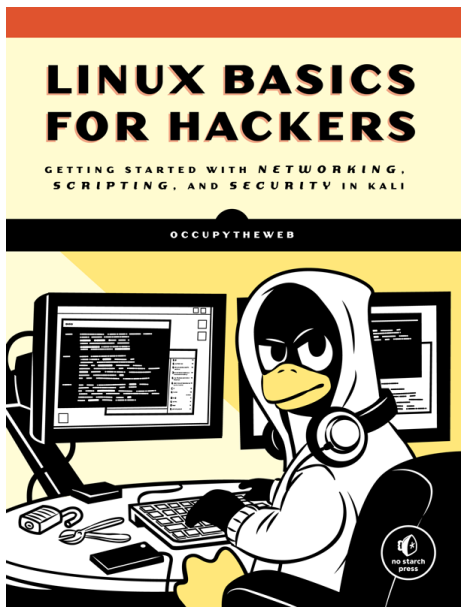
Our main book for this course. We will read a lot from this one.

Crafting the InfoSec Playbook



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

Linux Basics for Hackers (LBfH)

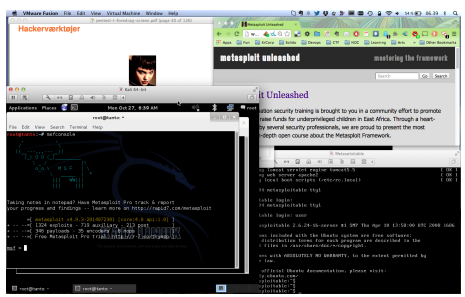


Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb December 2018, 248 pp. ISBN-13: 9781593278557

https://nostarch.com/linuxbasicsforhackers Not curriculum but explains how to use Linux

Exercises: Hackerlab Setup

Exercise theme: Virtual Machines allows us play with tech



- Hardware: modern laptop CPU with virtualisation
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Linux server system: Debian amd64 64-bit https://www.debian.org/
- Setup instructions can be found at https://github.com/kramse/kramse-labs

It is enough if these VMs are pr team

SIEM

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

SOC

> An information security operations center (ISOC or SOC) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.
>
> ...
>
> A security operations center (SOC) can also be called a security defense center (SDC), security analytics center (SAC), network security operations center (NSOC),[3] security intelligence center, cyber security center, threat defense center, security intelligence and operations center (SIOC). In the Canadian Federal Government the term, infrastructure protection center (IPC), is used to describe a SOC.

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

- We have a whole book about SOCs, but I skipped the introductory chapters!
- If you need to build a SOC, that is great source of information

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

Anatomy of an Auditing System

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

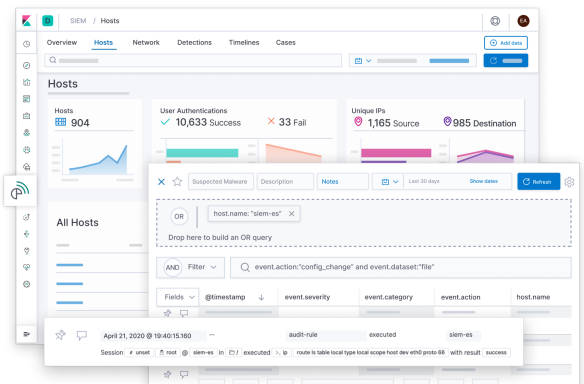
```
Jun  5 11:53:15 pumba sshd[64505]: Accepted publickey for hlk from 79.142.233.18 port 43902
 ssh2: ED25519 SHA256:l8OJMcywyBcraJiCWJ06uZ2yzHfu0VuiArqVvlVyfEI

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

Why Elasticsearch



Screenshot from https://www.elastic.co/siem

Recommend building a proof-of-concept infrastructure using the Elastic stack and gather experience with logging. This can be done without a license fee and the organization can then see what works and doesn't. Then using the experiences as input an informed decision can be made, to continue with this as a home grown logging and auditing solution, or buy a premade one.

Technologies used in this course

The following tools and environments are examples that may be introduced in this course:

- Programming languages and frameworks Java, Python, regular expressions
- Development environments – choose your own IDE / Editor – I use **Atom**
- Networking and network protocols: TCP/IP, HTTP, DNS, Netflow
- Formats XML, JSON, CSV, raw text, web scraping
- Web technologies and services: REST, API, HTML5, CSS, JavaScript
- Tools like cURL, Zeek, Git and Github
- Message queueing systems: MQ and Redis could be added
- Aggregated example platforms: Elastic stack, logstash, elasticsearch, kibana, grafana, Filebeat
- Cloud and virtualisation Docker, Kubernetes, Azure, AWS, microservices – can be added

This list is not complete or a promise

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) ser ver 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 sign ature can contain one or more IOCs.

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

Reading Summary, Intrusion Kill Chains

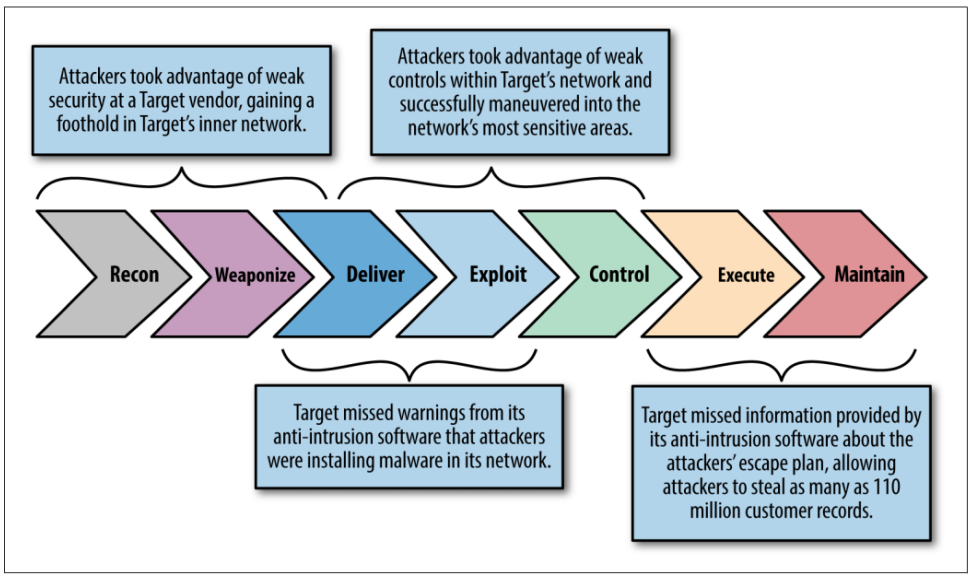
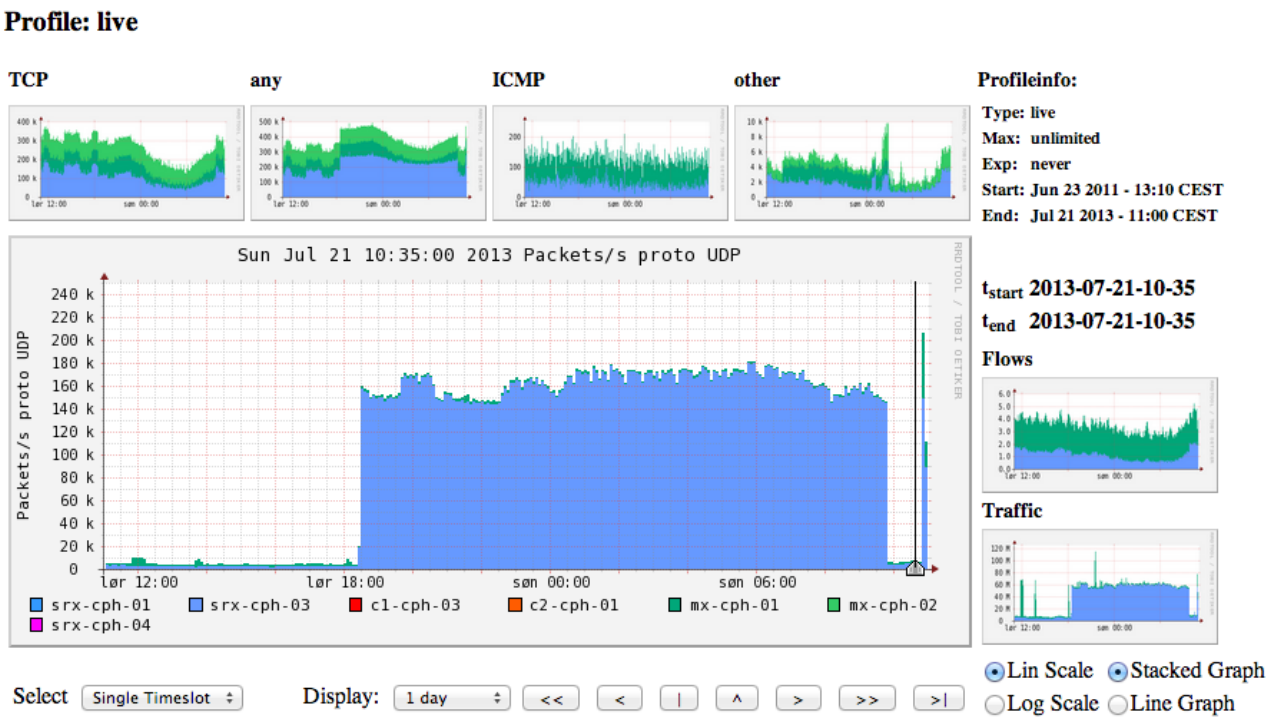


Figure 7-1. The kill chain

- 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

Netflow NFSen



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

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

Source https://www.zeek.org/

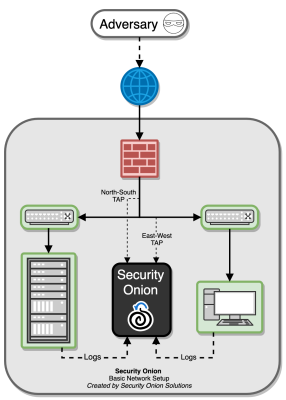
Suricata IDS/IPS/NSM

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

I often use Suricata and Zeek together

Architecture for packet capture



Source: picture from https://docs.securityonion.net/en/2.3/introduction.html

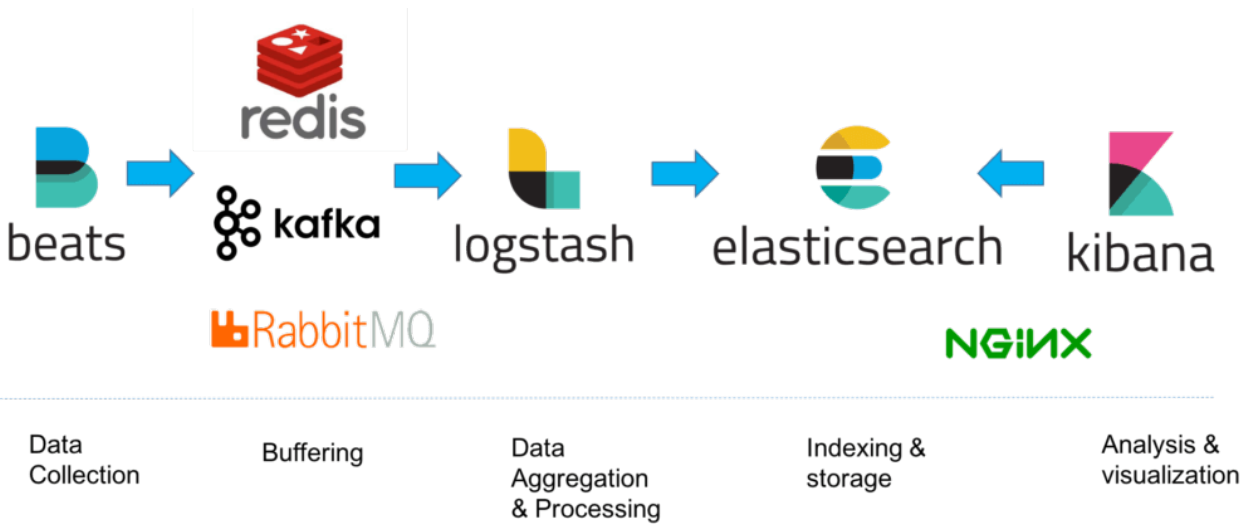
- Note the terminology North-South – from the internet into the systems
- East-West – horizontal traffic inside the data center
- See also from Security Onion https://docs.securityonion.net/en/2.3/architecture.html#architecture

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
PS I havent tried it in real life, yet

Architecture



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