

Welcome to

## 0. Introduction

# Introduction to Incident Response Elective, KEA

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Github 

0-Introduction-to-incident-response.tex in the repo security-courses

# Contact information



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

You are welcome to drop me an email

# Goals for today

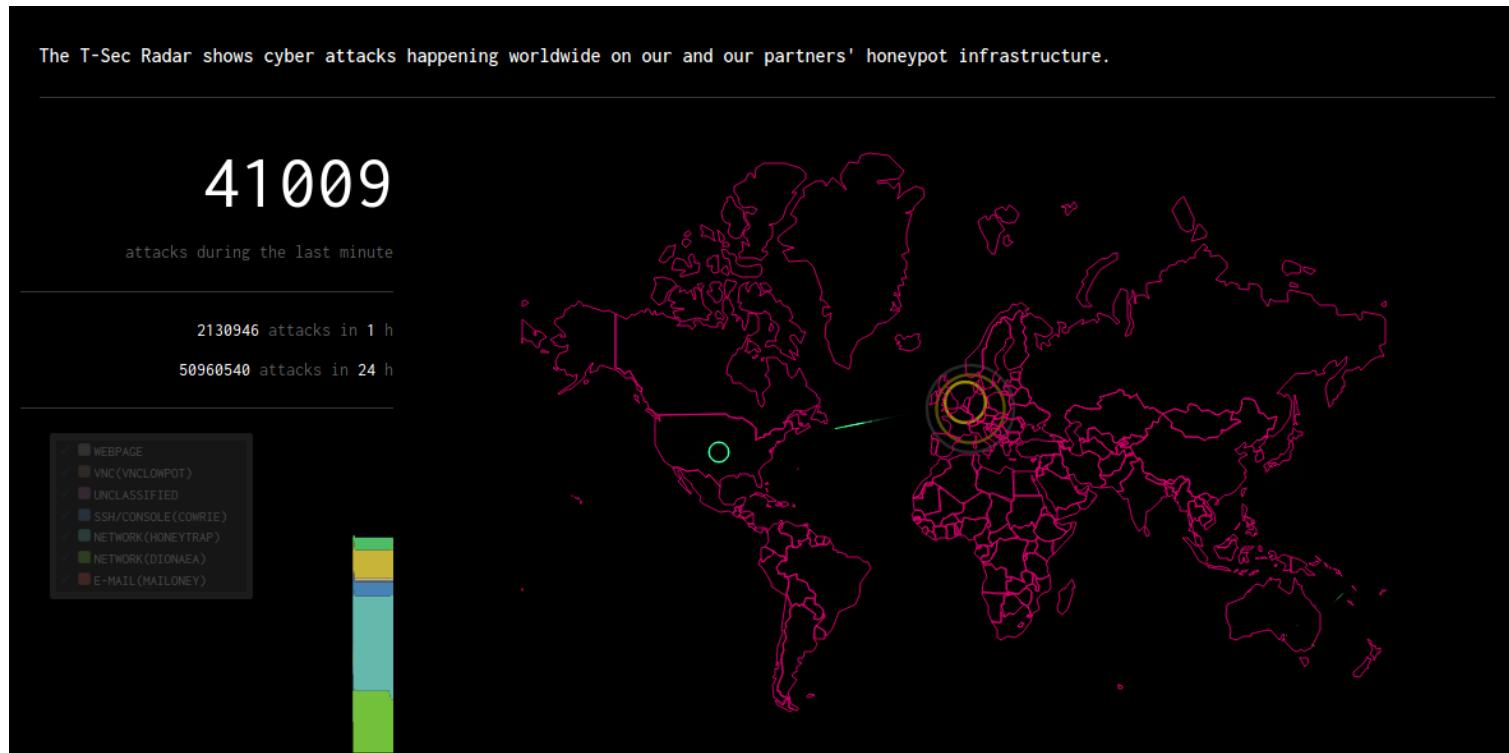


Introduction to incident response. what is an incident and a log? We will discuss what happens when someone visits your network. Starting from initial compromise we will demonstrate how we can identify, process and handle incidents in networks.

- Welcome, course goals and expectations
- Create a good starting point for learning
- Concrete Expectations

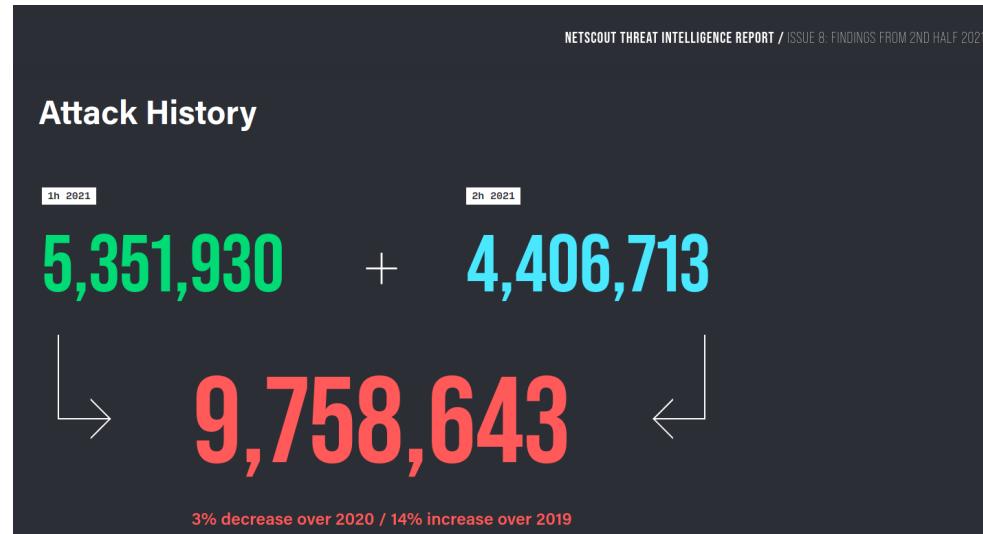
Photo by Thomas Galler on Unsplash

# Introduction: Attack overview



Source: <http://www.sicherheitstacho.eu/>

# DDoS Attacks Still a Problem



Security attacks and DDoS is very much in the media

Source: [linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/](https://www.netscout.com/threatreport/global-ddos-attack-trends/)

# Ransomware Attacks are Common

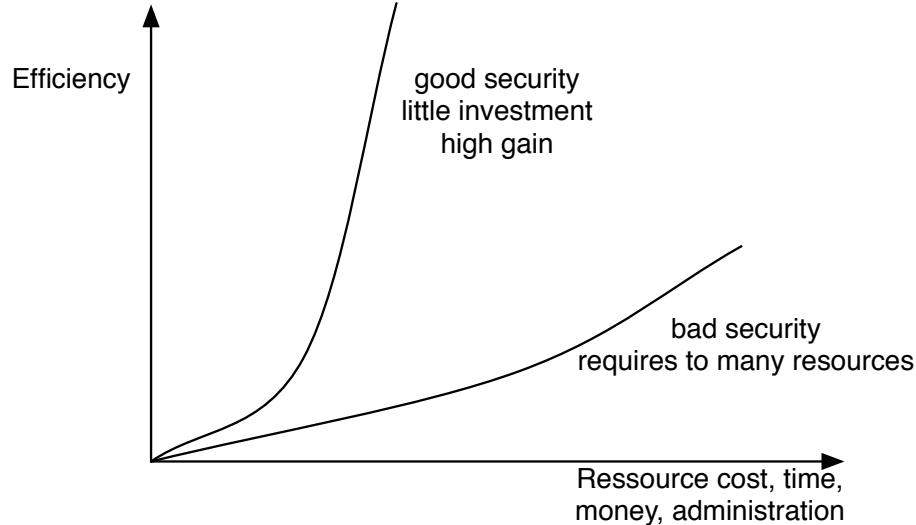
The image shows a vertical list of five ransomware groups, each with a small icon and a brief description:

- Avaddon**: A large red and yellow stylized letter 'A'.  
Avaddon ransomware was first seen in February 2020 and by June 2020 had quickly evolved into ransomware as a service (RaaS). In January 2021, the group evolved again to include DDoS attacks in its extortion repertoire.  
[READ MORE +](#)
- REvil**: A blue and purple stylized owl logo.  
Although currently not operational due to a global takedown, REvil was a prominent user of RaaS. With its highly adaptable encryptors and decryptors, REvil provided infrastructure and services for communicating with victims, as well as a leak site for releasing stolen data if the victim refused to pay the ransom.  
[READ MORE +](#)
- BlackCat**: A white cat silhouette icon.  
One of the newest ransomware groups, BlackCat (aka ALPHV), was discovered in November 2021. Operating as a RaaS, the group quickly gained notoriety for its sophistication and innovation.  
[READ MORE +](#)
- AvosLocker**: A blue and green stylized virus or cell icon.  
First seen in summer 2021, AvosLocker is simple but effective ransomware that has utilized triple extortion from the start. AvosLocker operators advertise in underground networks for affiliates with active directory experience, as well as for "access brokers" who potentially could provide access to compromised systems.  
[READ MORE +](#)
- Suncrypt**: A red padlock icon with a glowing starburst inside it.  
Initially appearing in October 2019, Suncrypt was one of the first ransomware groups to launch DDoS attacks. Along with data encryption and theft, Suncrypt extorts its victims by threatening to attack infrastructure or networks.  
[READ MORE +](#)

Make sure to backup your data! Test your backups!

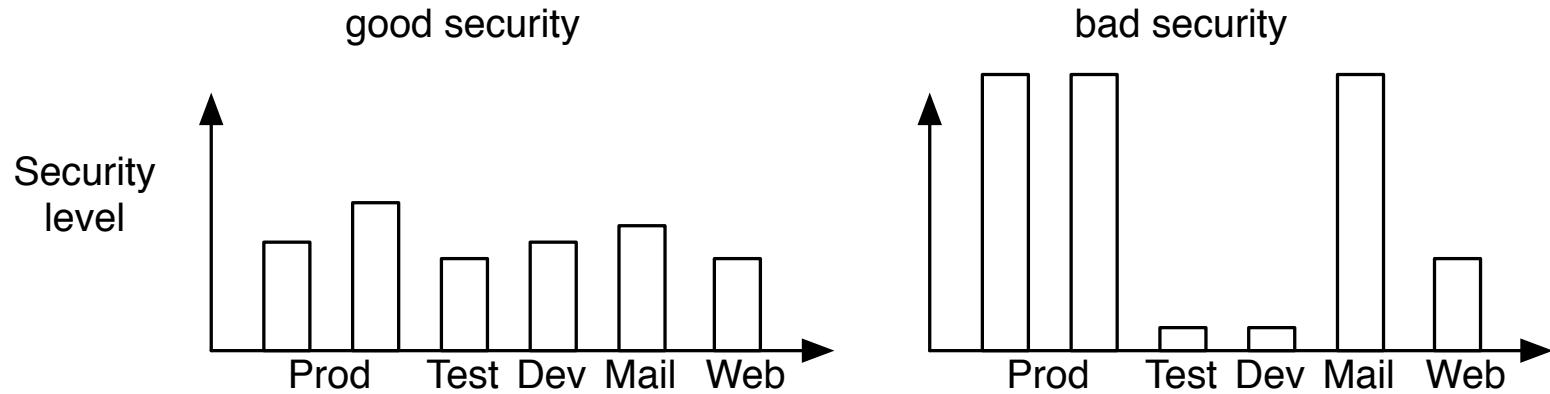
Source: [linkhttps://www.netscout.com/threatreport/global-ddos-attack-trends/](https://www.netscout.com/threatreport/global-ddos-attack-trends/)

## What can we do? – Good security



You always have limited resources for protection - use them as best as possible  
Good security comes from structured work

## Balanced security



Better to have the same level of security

If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security



FreeFoto.com

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

## Plan for today

- Create a good starting point for learning
- Introduce lecturer and students
- Literature list walkthrough
- Story time Hacking

Exercise theme: Get tools up and running

- What is an incident – CISO for a day

Linux is a toolbox we will use and participants will use some tools on Linux



## Course: Introduction to Incident Response elective

Teaching dates: thursdays 12:45 - 16:00 in GBG.E512  
24/8, 31/8, 7/9, 14/9, 21/9, 28/9, 5/10, 12/10, 26/10

Exam: to be announced

Photo by Paweł Janiak on Unsplash

## Time schedule

Official times Thursdays:

- 12:45 - 14:15 Session 1
- 15min break
- 14:30 - 16:00 Session 2

In practice: We will aim at one break at least for every 45min, and we will also be doing exercises.

## Course Materials

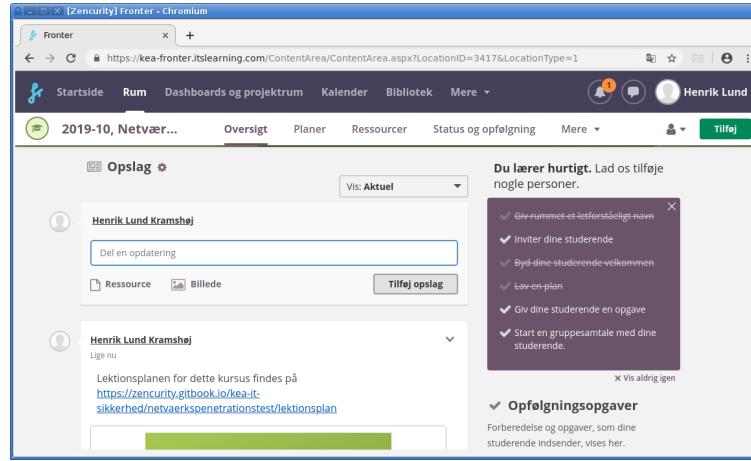
This material is in multiple parts:

- 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

Note: the presentation slides are not a substitute for reading the books, papers and doing exercises, many details are not shown



We will use fronter a lot, both for sharing educational materials and news during the course.

You will also be asked to turn in deliverables through fronter

<https://kea-fronter.itslearning.com/>

If you haven't received login yet, let us know

## Deliverables and Exam

- Exam
- Individual: Oral based on curriculum
- Graded (7 scale)
- Exam is 30 minutes in total, including pulling the question and grading
- Count on being able to present your project – talk for about 10 minutes
- Prepare material (keywords, examples, exercises, wireshark captures) for different topics so that you can use it to help you at the exam
- Deliverables:
- 1 Mandatory assignments
- Mandatory assignment is required in order to be entitled to the exam.

# Course Description

## Course description

Introduction to Incident Response is a course that will describe the basics of incident response. This will include the terms, tools and processes used by professionals.

Below are the required parts from studieordningen:

## Viden

- Forskellige cyberangrebs stadier og teknikker
- Incident-Response cyklus
- Principperne i Event logning
- Processer i forbindelse med Incident response og Threat hunting

## Course Description, continued

### Færdigheder

- Søge i relevante filer, hukommelse og lignende for indicators of compromise (IoC)
- Analysere event log, memory og timeline for tegn på security incidents
- Viderebringe resultater i form af ekspertrapporter

### Kompetencer

- Anvende, udvikle og dele Threat Intelligence
- Anvende og udvikle processer til incident håndtering i en organisation

## Exercises

Exercise theme: Virtual Machines allows us play with tech

Since we are going to be doing exercises, each team will need virtual machines.

The following are recommended systems:

- One VM based on Debian, running various software tools
- Setup instructions and help <https://github.com/kramse/kramse-labs>

Linux is a toolbox we will use and participants will use virtual machines

PS We will from time to time have exercises, groups dont need to be the same each time.

## Goals and plans

“A goal without a plan is just a wish.”

Antoine de Saint-Exupéry

I want this course to

- Include everything listed in contents above
- Be practical – you can do something useful
- Kickstart your journey into Incident Response  
Getting a practical book with pointers about the subject
- Present a lot of useful sources and tools
- Prepare you for production use of the knowledge

We have a lot of flexibility.

## 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:

- *Intelligence-Driven Incident Response*

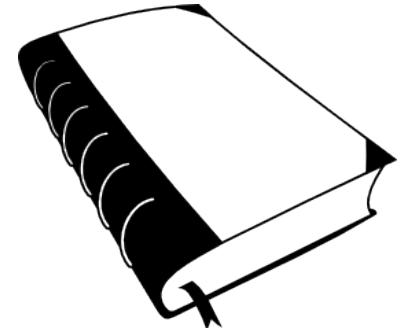
Scott Roberts. Rebekah Brown, ISBN: 9781098120689 **2nd edition**- short IDIR

- *Forensics Discovery (FD)*, Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages.  
ISBN: 9780201634976

This book is currently available for "free":

<http://fish2.com/security/> – also uploaded to Fronter

- *Computer Security Incident Handling Guide*, NIST SP 800-61 Rev. 2, August 2012,  
<https://doi.org/10.6028/NIST.SP.800-61r2> – also uploaded to Fronter



Free graphics by Lumen Design Studio

**Other papers and resources will also be part of the curriculum!**

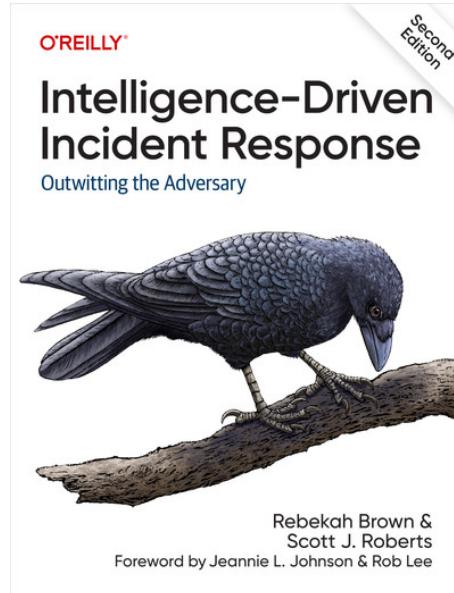
## Course overview

We will now go through a little from the Table of Contents in the books.

and the lecture plan in Fronter

(Source is also in Git <https://github.com/kramse/kea-it-sikkerhed> )

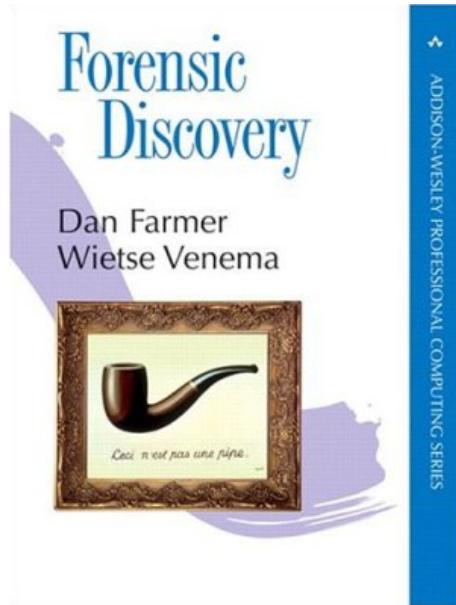
# Book: Intelligence-Driven Incident Response



*Intelligence-Driven Incident Response*

Scott Roberts. Rebekah Brown, ISBN: 9781098120689 **2nd edition**- short IDIR

## Book: Forensics Discovery (FD)



*Forensics Discovery*, Dan Farmer, Wietse Venema 2004, Addison-Wesley.

Can be found at <http://fish2.com/security/>



**Special Publication 800-61  
Revision 2**

---

# **Computer Security Incident Handling Guide**

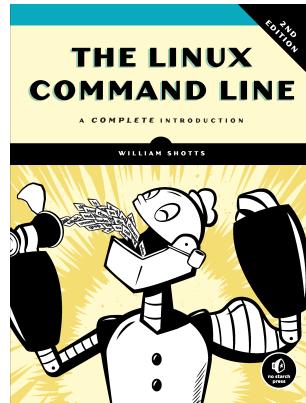
---

<https://doi.org/10.6028/NIST.SP.800-61r2>

## Supporting literature books

- *The Linux Command Line: A Complete Introduction*, 2nd Edition  
by William Shotts
- *The Debian Administrator's Handbook*, Raphaël Hertzog and Roland Mas  
<https://debian-handbook.info/> - shortened DEB
- *Kali Linux Revealed Mastering the Penetration Testing Distribution*  
Raphaël Hertzog, Jim O'Gorman - shortened KLR

# Book: The Linux Command Line



*The Linux Command Line: A Complete Introduction* , 2nd Edition by William Shotts

Print: <https://nostarch.com/tlcl2>

Download – internet edition <https://sourceforge.net/projects/linuxcommand>

Not curriculum but explains how to use Linux

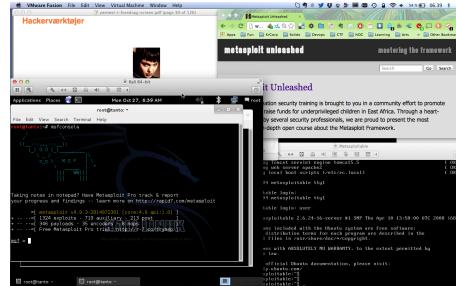
# The Debian Administrator's Handbook (DEB)



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

Not curriculum but explains how to use Debian Linux

# Hackerlab Setup



- Hardware: modern laptop CPU with virtualisation  
Dont forget to enable hardware virtualisation in the BIOS
- 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

## Mixed exercises

Then we will do a mixed bag of exercises to introduce technologies, find your current knowledge level with regards to:

- Linux as an operating system – user database in /etc/
- Linux command line
- Demo: Ansible
- Git, Python, scripting
- Demo: Elasticsearch – how to run a *service*

**Note: today we will consider all these optional, we won't be able to do them all**

Later we will return to them!

# Installing software in Debian – apt

## DESCRIPTION

apt provides a high-level commandline interface for the package management system. It is intended as an end user interface and enables some options better suited for interactive usage by default compared to more specialized APT tools like `apt-get(8)` and `apt-cache(8)`.

### `update (apt-get(8))`

`update` is used to download package information from all configured sources. Other commands operate on this data to e.g. perform package upgrades or search in and display details about all packages available for installation.

### `upgrade (apt-get(8))`

`upgrade` is used to install available upgrades of all packages currently installed on the system from the sources configured via `sources.list(5)`. New packages will be installed if required to satisfy dependencies, but existing packages will never be removed. If an upgrade for a package requires the removal of an installed package the upgrade for this package isn't performed.

### `full-upgrade (apt-get(8))`

`full-upgrade` performs the function of `upgrade` but will remove currently installed packages if this is needed to upgrade the system as a whole.

- Install a program using apt, for example `apt install nmap`



From my course materials:

Ansible is great for automating stuff, so by running the playbooks we can get a whole lot of programs installed, files modified - avoiding the Vi editor.

- Easy to read, even if you don't know much about YAML
- <https://www.ansible.com/> and [https://en.wikipedia.org/wiki/Ansible\\_\(software\)](https://en.wikipedia.org/wiki/Ansible_(software))
- Great documentation  
[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/apt\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/apt_module.html)

## Ansible Dependencies



- Ansible based on Python, only need Python installed  
<https://www.python.org/>
- Often you use Secure Shell for connecting to servers  
<https://www.openssh.com/>
- Easy to configure SSH keys, for secure connections

## Ansible playbooks

Example playbook content, installing software using APT:

```
apt:  
  name: "{{ packages }}"  
vars:  
  packages:  
    - nmap  
    - curl  
    - iperf  
    ...
```

Running it:

```
cd kramse-labs/suricatazeek  
ansible-playbook -v 1-dependencies.yml 2-suricatazeek.yml 3-elasticstack.yml 4-configuration.yml
```

"YAML (a recursive acronym for "YAML Ain't Markup Language") is a human-readable data-serialization language."  
<https://en.wikipedia.org/wiki/YAML>



- We need to store configurations
- Run playbooks
- Problem: Remember what we did, when, how
- Solution: use git for the playbooks
- Not the only version control system, but my preferred one

# Git getting started

## Hints:

Browse the Git tutorials on <https://git-scm.com/docs/gittutorial>  
and <https://guides.github.com/activities/hello-world/>

- What is git
- Terminology

Note: you don't need an account on Github to download/clone repositories, but having an account allows you to save repositories yourself and is recommended.

## Demo: Ansible, Python, Git!

Running Git will allow you to clone repositories from others easily. This is a great way to get new software packages, and share your own.

Git is the name of the tool, and Github is a popular site for hosting git repositories.

Henrik will show:

- Go to <https://github.com/kramse/kramse-labs>
- Lets explore while we talk
- Install Git, Ansible and Python manually using apt
- Then I will use Git to clone a repository
- Using Ansible I can then run a playbook

## Demo: output from running a git clone

```
user@Projects:tt$ git clone https://github.com/kramse/kramse-labs.git
Cloning into 'kramse-labs'...
remote: Enumerating objects: 283, done.
remote: Total 283 (delta 0), reused 0 (delta 0), pack-reused 283
Receiving objects: 100% (283/283), 215.04 KiB | 898.00 KiB/s, done.
Resolving deltas: 100% (145/145), done.
```

```
user@Projects:tt$ cd kramse-labs/
```

```
user@Projects:kramse-labs$ ls
LICENSE README.md core-net-lab lab-network suricatazeek work-station
user@Projects:kramse-labs$ git pull
Already up to date.
```

for reference at home later

## Exercise CHAOS: Don't Panic – have fun learning



“It is said that despite its many glaring (and occasionally fatal) inaccuracies, the Hitchhiker’s Guide to the Galaxy itself has outsold the Encyclopedia Galactica because it is slightly cheaper, and because it has the words ‘DON’T PANIC’ in large, friendly letters on the cover.”

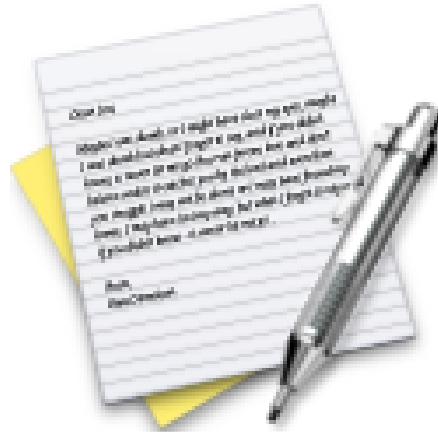
Hitchhiker’s Guide to the Galaxy, Douglas Adams

## Your lab setup

- Go to GitHub, Find user Kramse, click through kramse-labs
- Look into the instructions for the Virtual Machine – Debian only
- Get the lab instructions, from

<https://github.com/kramse/kramse-labs/>

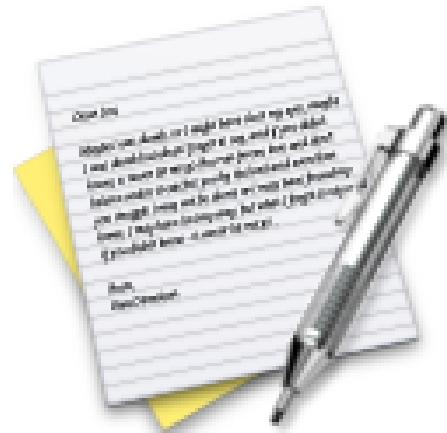
**TODAY ALL EXERCISES after installing the basic VMs ARE OPTIONAL!**



Now lets do the exercise

## ⚠ Download Debian Administrator's Handbook (DEB) Book 10 min

which is number **1** in the exercise PDF.



Now lets do the exercise

## ⚠ Check your Debian Linux VM 10 min

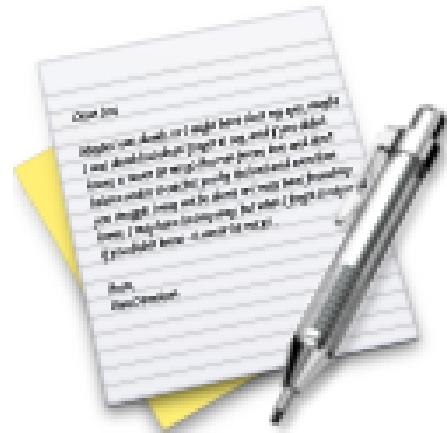
which is number **2** in the exercise PDF.



Now lets do the exercise

## ⚠ Investigate /etc 10 min

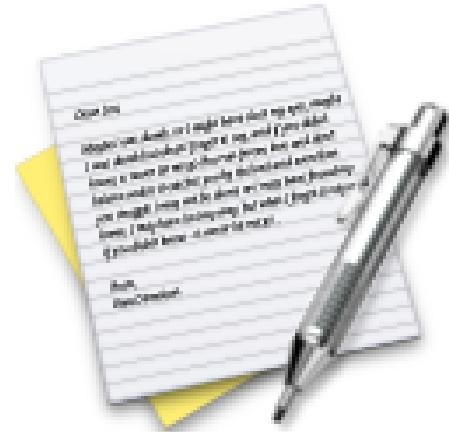
which is number **3** in the exercise PDF.



Now lets do the exercise

## ⓘ Enable UFW firewall - 10 min

which is number **4** in the exercise PDF.



Now lets do the exercise

## ⚠ Git tutorials - 15min

which is number **5** in the exercise PDF.



Now lets do the exercise

## **i Run small programs: Python, Shell script 20min**

which is number **6** in the exercise PDF.

## Let's get started

We will now go through a mix of things which either are incident response, or related to incident response

Some things will be repeated later

## Information Risk Management

*Life is full of risk.*

Risk is the possibility of damage happening and the ramifications of such damage should it occur. *Information risk management (IRM)* is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

# Security Controls and Frameworks

Multiple exist

- CIS controls Center for Internet Security (CIS) <https://www.cisecurity.org>
- PCI Best Practices for Maintaining PCI DSS Compliance v2.0 Jan 2019
- NIST Cybersecurity Framework (CSF)  
Framework for Improving Critical Infrastructure Cybersecurity  
<https://www.nist.gov/cyberframework>  
<https://csrc.nist.gov/publications/sp800> - SP800 series
- National Security Agency (NSA)  
<https://www.nsa.gov/Research/>
- NSA security configuration guides  
<https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/>
- Information Systems Audit and Control Association (ISACA)  
<http://www.isaca.org/Knowledge-Center/>

“A goal without a plan is just a wish.”  
Antoine de Saint-Exupéry

The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

Source: <https://www.cisecurity.org/ CIS-Controls-Version-7-1.pdf>

**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](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

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),<sup>[3]</sup> 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](https://en.wikipedia.org/wiki/Information_security_operations_center)

## Subjects: Incident Response



Context, what are the threats, what are the answers we want from the SIEM and Logs  
What are the common cases, where we use the data?

- Incident Response
- Computer Emergency Response Team (CERT) and Computer Security Incident Response Teams (CSIRT)
- Security Departments
- GDPR Data protection
- Computer Forensics

## Incident Handling, phases

The procedures developed for incident response must cover the complete life-cycle

- 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

# 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

# Incident Response Checklists

Table 3-5. Incident Handling Checklist

	Action	Completed
<b>Detection and Analysis</b>		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
<b>Containment, Eradication, and Recovery</b>		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
<b>Post-Incident Activity</b>		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

This checklist is from the NIST document *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-61 Revision 2, August 2012.

## CIS Controls also recommend Incident Response

### **CIS Control 19:**

Incident Response and Management Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf from <https://www.cisecurity.org/controls/>

## Anatomy of an Auditing System

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

```
Jun  5 11:53:15 pumba sshd[64505]: Accepted publickey for hlk from 79.142.233.18 port 43902
ssh2: ED25519 SHA256:180JMcywyBcraJiCWJ06uZ2yzHfu0VuiArqVvlVyfEI
```

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

Example systems: Unix syslog, IBM main frame RACF and Windows Event Logs service

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

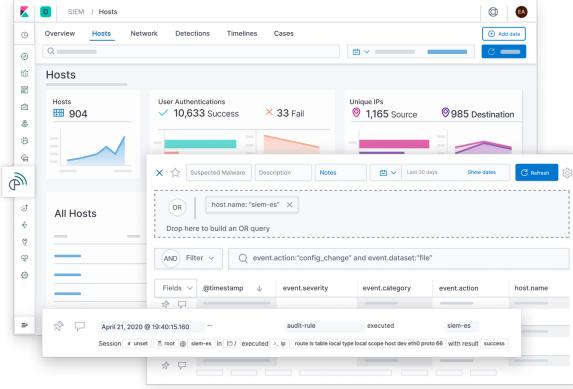
**Notifier** - report results by email or other means

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.

# 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.

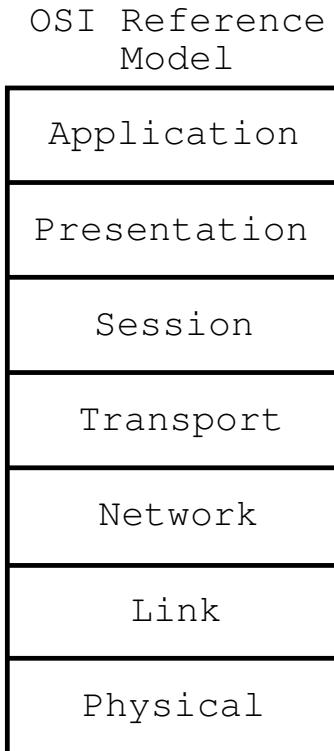
## Technologies used in this course

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

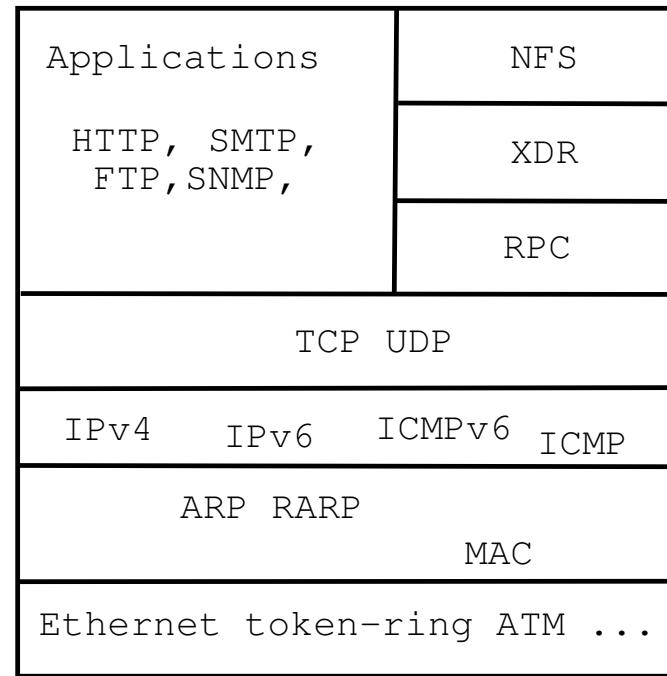
- Programming languages and frameworks Java, Python, regular expressions
- Development environments – choose your own IDE / Editor – I use **Pulsar**
- Networking and network protocols: TCP/IP, HTTP, DNS, Netflow
- Formats XML, JSON, CSV, raw text, web scraping
- Web technologies and services: REST, 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

# OSI and Internet

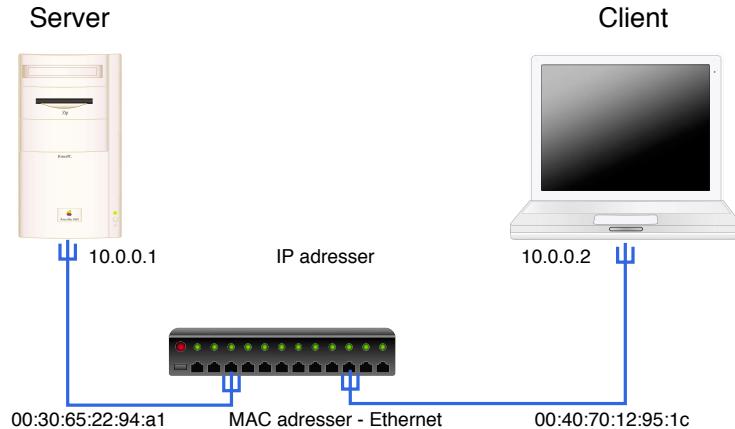


Internet protocol suite



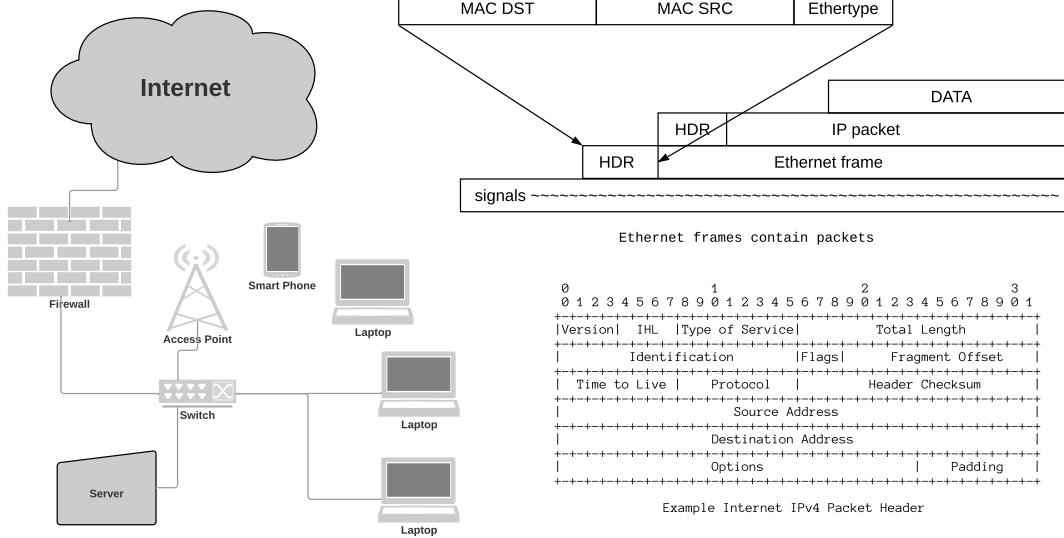
Data on all layers

# Networking in TCP/IP



- Everything uses TCP/IP today, more or less.
- Clients make requests, receives responses
- HyperText Transfer Protocol (HTTP) is an example
- All devices shown can produce logs and events

# Sources: Network overview



- Internet, routers, firewalls, switches, clients and servers (Wi-Fi not shown)

## Sources: Strategy for implementing identification and detection

We recommend that the following strategy is used for implementing identification and detection – logging:

- Enable system logging from servers
- Enable system logging from network devices
- Enable logging from client devices
- Centralize logging
- Add search facilities and dashboards
- Perform system audits manually or automatically
- Setup alerting and notification with procedures

# Intrusion Kill Chains

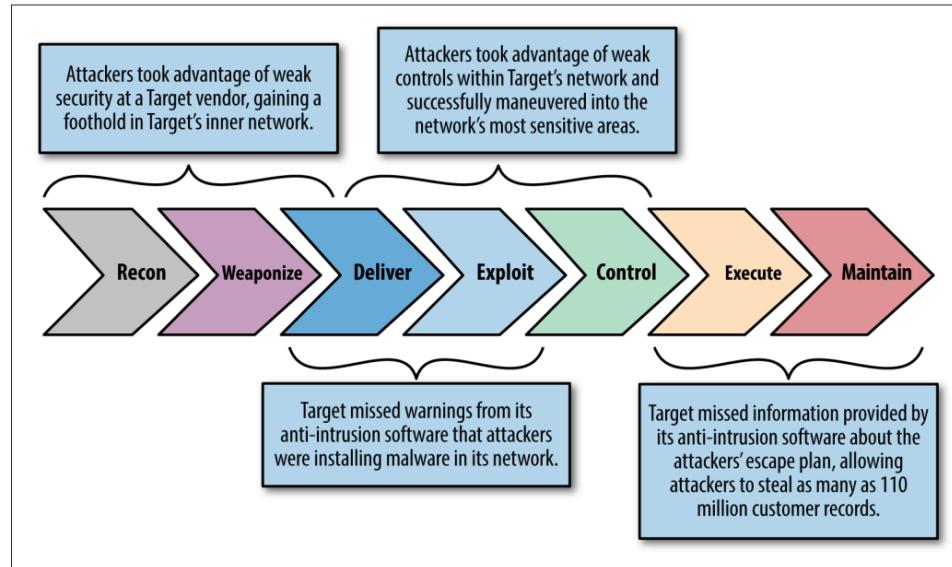


Figure 7-1. The kill chain

- 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>

## 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**.

# 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

# Don't use spreadsheets!

- Spreadsheets are great for some tasks, but ...
- They don't scale
- The model can be broken – edit a single formula
- Rounding errors accumulate
- Input and output are limited
- Most functions require manual work

## 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>

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

- Lets try to use some Python to access a REST service.
- We will use the JSONPlaceholder which is a free online REST API: <https://jsonplaceholder.typicode.com/>
- Start at the site: <https://jsonplaceholder.typicode.com/guide.html> and try running a few of the examples with your browser
- Then try using the same URLs in the Requests HTTP library from Python,  
<https://requests.readthedocs.io/en/master/>

## Note about frameworks and libraries

```
import xml.etree.ElementTree as ET
tree = ET.parse('testfile.xml')
root = tree.getroot()

print(root.tag)
print('Nmap version: \t\t{:s}'.format(root.attrib['version']))
print('Nmap started: \t\t{:s}'.format(root.attrib['startstr']))
print('Nmap command line: \t{:s}'.format(root.attrib['args']))

hosts = tree.findall('./host')
for host in hosts:
    print(host.tag)
    print(host.attrib)
    for hostvalues in host:
        print(hostvalues.tag)
        print(hostvalues.attrib)
```

- Dont import JSON or XML using home made programs
- Example uses `xml.etree.ElementTree` from Python <https://docs.python.org/3.7/library/xml.etree.elementtree.html>

# Convert XML to JSON

```
import xml.etree.ElementTree as ET
import json
def etree_to_dict(t):
    d = {t.tag : map(etree_to_dict, t.getchildren())}
    d.update((('@' + k, v) for k, v in t.attrib.items()))
    d['text'] = t.text
    return d

tree = ET.parse('testfile.xml')
root = tree.getroot()
mydict = etree_to_dict(root)
print(type(tree))
print(type(root))
print(type(mydict))

print(mydict)

with open('testfile.json', 'w') as json_file:
    json.dump(mydict, json_file)
```

Converting using Python is easy

## 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/bro/bro# 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

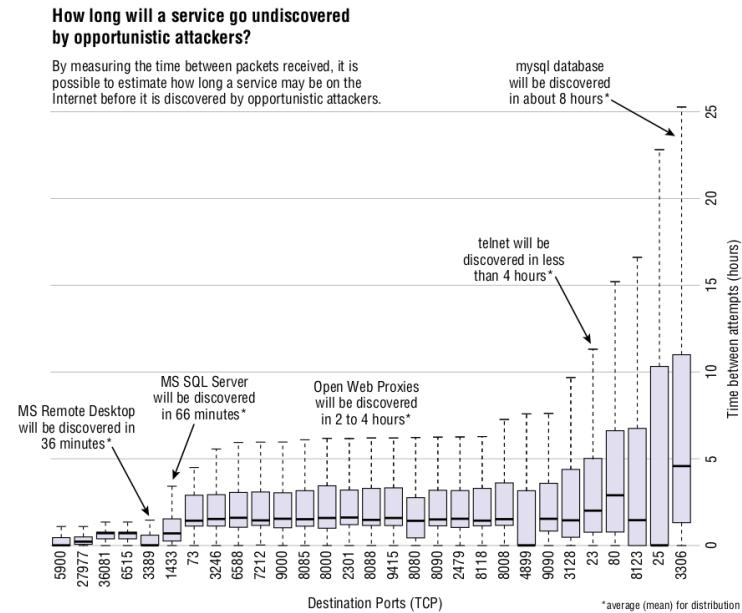
# Metadata – enrichment

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

## Example plot 6-17

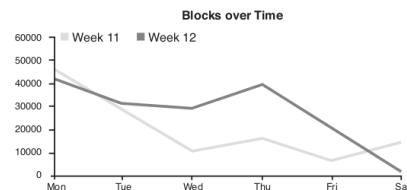
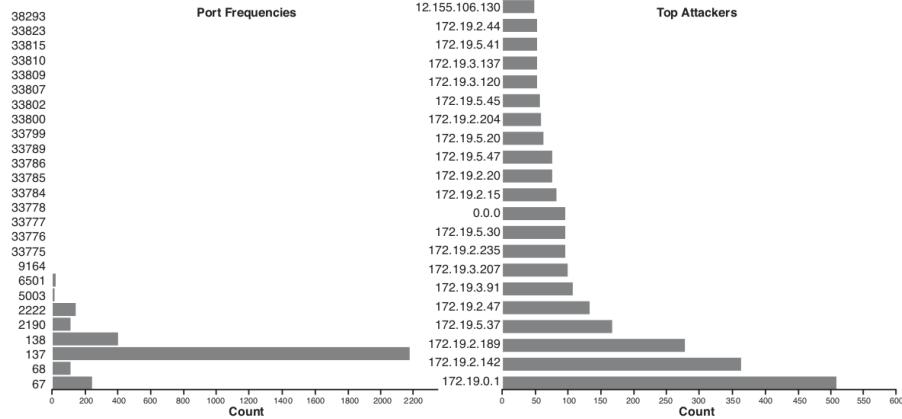


Source: DDS 6. Visualizing Security Data

- Interesting graph, and interesting results Changing away from standard ports delay attackers!

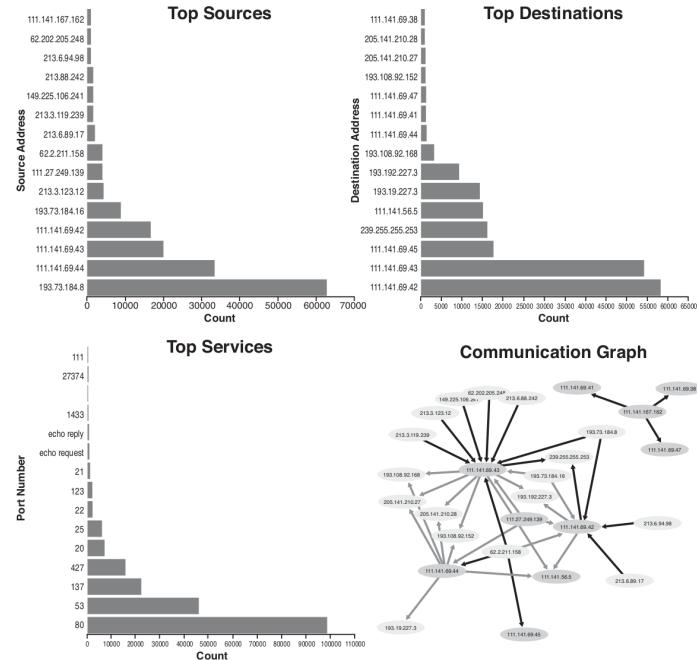
# Applied Security Visualization examples

Firewall Report for Week 12 2007



Source: Firewall Report in *Applied security visualization*, Rafael Marty, 2009

# Applied Security Visualization examples



Source: Network Flow Data in *Applied security visualization*, Rafael Marty, 2009

## Drill down 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

## Elasticsearch example systems

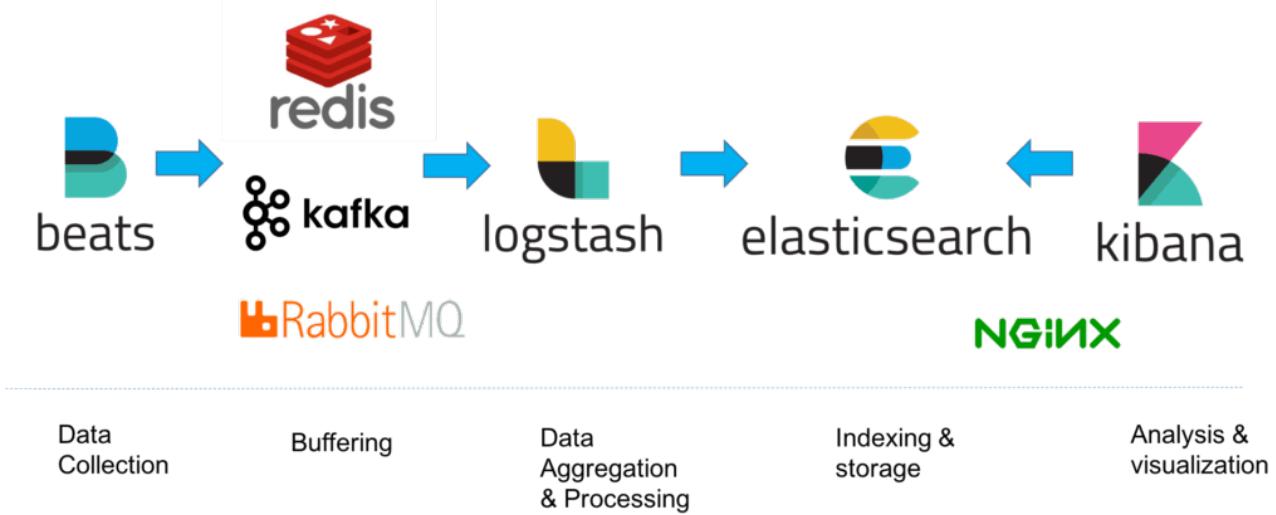
ElasticSearch consumes practically anything you give it and provides straightforward ways to ask it questions and get data out of it. You just need to feed it semi- or unstructured data and fold in some domain intelligence to enable smart indexing. It works its multi-node NoSQL magic in conjunction with a layer of full-text searching to give you almost instantaneous query results even for large amounts of data.

Source: DDS 8. Breaking Up with Your Relational Database

- Elasticsearch SIEM – from Elastic, including Elastic Common Schema (ECS)  
<https://github.com/elastic/ecs>
- Wazuh – agent for clients, log events, integrity protection etc.
- HELK – all-in one hunting system
- ElastiFlow – netflow system
- Arkime (renamed recently from Moloch) – packet capture

Lots of commercial systems, and lots of companies providing cloud logging platform

# Architecture

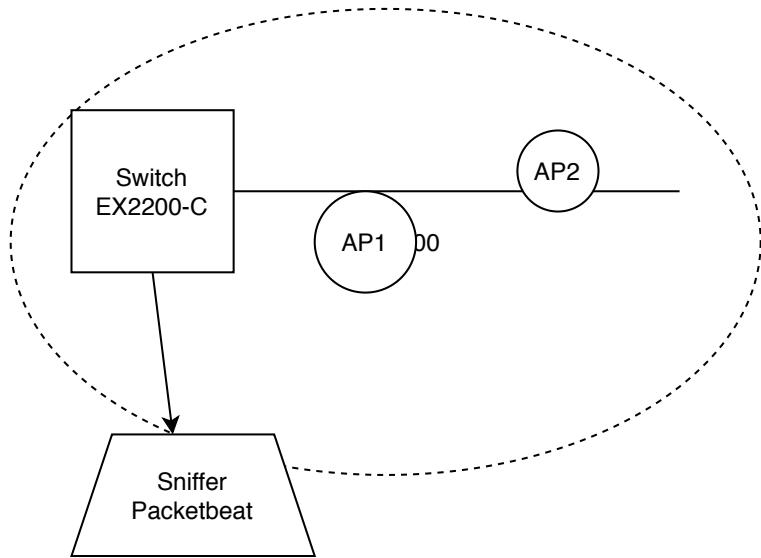


- Real production environments often add some buffering in between
- Allows the ingestion to become more smooth, no lost messages



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>



- 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)

# Attack Lifecycle

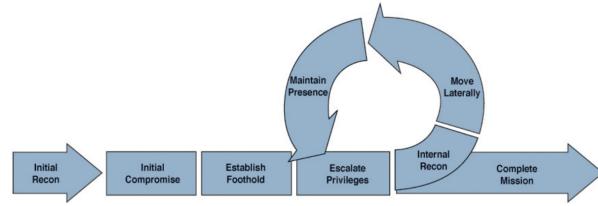


Figure 7-1 Targeted Attack Lifecycle

Many breaches discovered are caused by a system having a known vulnerability exploited before it is properly patched.

Source: Mandiant's Targeted Attack Lifecycle, SOC chapter 7. vuln management

- Chapter contains lots of references
- Also chapter links inventory controls with active discovery tools and mitigating
- Mentions Threat Feeds, which should be integrated into SIEM and/or organizations
- You need to stay up-to-date on current threats, and be able to search for signs in your own network

## Conclusion: chaos and panic



- We started out fine, structured approach!
- We got interrupted ... which happens a lot
- We didn't finish! Again this is very common in real life
- Microsoft alone release patches and updates for more than 100 vulnerabilities a month
- All software has security problems, and need updates!

## Incident Log and financial

Take a piece of paper or a computer

- We just got interrupted in our important job with the CIS controls
- We now need to fill out an Incident Log and calculate the cost
- When an incident happens it must be dealt with efficiently
- If you don't have security procedures it will often be longer lasting and more expensive

In March 2021, both Microsoft and IT Professionals had a major headache in the form of an Exchange zero-day commonly known as ProxyLogon. The vulnerability, widely considered the **most critical to ever hit Microsoft Exchange**, was quickly exploited in the wild by suspected state-sponsored threat actors, with US government and military systems identified as the most targeted sectors. **Ransomware variants such as DoejoCrypt were soon actively exploiting unpatched Exchange instances**, attempting to monetise the vulnerability.

A follow-up exploit, dubbed ProxyShell, was evolutionary in nature and targeted on-premise Client Access Servers (CAS) in **all supported versions of Exchange Server**. Due to the **remotely accessible nature of Exchange CAS**, any unpatched instances would be vulnerable to Remote Code Execution. **High profile victims included the European Banking Authority and the Norwegian Parliament**.

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

## ProxyLogon CVE-2021-26855 CVSS:3.0 9.1 / 8.4

ProxyLogon is the formally generic name for CVE-2021-26855, a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin. We have also chained this bug with another post-auth arbitrary-file-write vulnerability, CVE-2021-27065, to get code execution. All affected components are vulnerable by default!

**As a result, an unauthenticated attacker can execute arbitrary commands on Microsoft Exchange Server through an only opened 443 port!**

Sources: <https://proxylogon.com/>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855>

In June, Microsoft released a critical security update to address weaknesses in the Printer Spooler service on Windows desktop and server platforms. Unfortunately, it was released out-of-band outside of the standard patch Tuesdays due to the severity. Microsoft even released patches for Windows 7, an supported operating system that does not normally receive updates.

Initially categorised by Microsoft as a local privilege escalation on Windows, security researchers subsequently identified an additional **Remote Code Execution (RCE)** vector resulting in an updated advisory from Microsoft. As ever, the ability to test and deploy patches in a time-sensitive manner is key to minimising the impact of such vulnerabilities.

Additionally, PrintNightmare had the additional horror factor of dropping during the **summer holiday season in the northern hemisphere**. Our consultants continue to see systems vulnerable to PrintNightmare on client engagements, which can be trivially leveraged to obtain privilege escalation on unpatched Windows systems.

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

See also <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

Note: this incident happened during summer time, vacations etc, double the cost.

## September 2021: ForcedEntry

**Apple didn't escape the wrath of critical zero-day vulnerabilities in 2021**, with ForcedEntry made public in September. The concern was not just that it could escape in-built sandbox controls and be leveraged against **almost all iOS versions at the time**, but also that it was in the form of a **one-click exploit meaning that no user interaction was needed**. A threat actor would simply require the target victim's phone number or email address to send a weaponised GIF. **Furthermore, iMessage was affected on macOS and watchOS, giving the exploit a significant attack surface of well over a billion devices.**

An analysis released at the end of 2021 confirmed a highly complex exploit which is believed to have been created by the NSO Group, creators of the Pegasus platform, albeit with the sophistication of nation-state actors. Given the nature of the attack and the level of complexity, high profile individuals are likely to be the intended targets of such exploits, only used sparingly against targeted victims.

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

See also <https://en.wikipedia.org/wiki/FORCEDENTRY>

## November 2021: Log4Shell

It would not be possible to discuss 2021 in the context of vulnerabilities without the mention of Log4Shell. **A widely used Java-based logging library caused headaches for Security professionals worldwide.** Many scrambled to quantify their use of Log4j within their estates.

A zero-day exploit quickly followed, confirming the worst - **Remote Code Execution (RCE) was indeed possible.** However, what made the nature of the vulnerability even more challenging was the ability to exploit a backend logging system from an unaffected front end host. For example, an attacker can craft a weaponised log entry on a mobile app or webserver not running Log4j. The attacker could make their way through to backend middleware itself running Log4j, which significantly extends the attack surface of the vulnerability.

The NCSC even took the step of recommending the update was immediately applied, whether or not Log4Shell was known to be in use. As is commonly the case with critical vulnerabilities, two successive Log4j patches were subsequently released in the week following the original addressing Denial of Service (DoS) and a further RCE. This further increased workloads of Security and IT teams just as they thought the worst of 2021 had been and gone.

Source - for this description:

<https://chessict.co.uk/resources/blog/posts/2022/january/2021-top-security-vulnerabilities/>

See also <https://en.wikipedia.org/wiki/Log4Shell>

## March 2022: Dirty pipe Linux CVE-2022-0847

This is the story of CVE-2022-0847, a vulnerability in the **Linux kernel since 5.8** which allows overwriting data in arbitrary read-only files. This leads to **privilege escalation because unprivileged processes can inject code into root processes**.

It is similar to CVE-2016-5195 “Dirty Cow” but is easier to exploit.

The vulnerability was fixed in Linux 5.16.11, 5.15.25 and 5.10.102.

Sources: <https://dirtypipe.cm4all.com/> <https://thestack.technology/dirty-pipe-exploited-linux-vulnerability-cve-2022-0847>  
<https://access.redhat.com/security/cve/CVE-2022-0847>

## April 2022: Lenovo UEFI

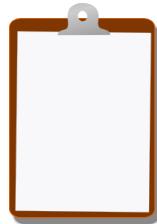
ESET researchers have discovered and analyzed three vulnerabilities affecting various Lenovo consumer laptop models. The first two of these vulnerabilities – CVE-2021-3971, CVE-2021-3972 – affect UEFI firmware drivers originally meant to be used only during the manufacturing process of Lenovo consumer notebooks. Unfortunately, they were mistakenly included also in the production BIOS images without being properly deactivated. These affected firmware drivers can be activated by attacker to directly disable SPI flash protections (BIOS Control Register bits and Protected Range registers) or the UEFI Secure Boot feature from a privileged user-mode process during OS runtime. It means that exploitation of these vulnerabilities would allow attackers to deploy and successfully execute SPI flash or ESP implants, like LoJax or our latest UEFI malware discovery ESPecter, on the affected devices.

Source:

also: <https://www.welivesecurity.com/2022/04/19/when-secure-isnt-secure-uefi-vulnerabilities-lenovo-consumer-laptops/>

See also: <https://www.bleepingcomputer.com/news/security/lenovo-uefi-firmware-driver-bugs-affect-over-100-laptop-mo>

## For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Buy the books! Create your VMs