Welcome to

1. Basics of Incident Response

Introduction to Incident Response Elective, KEA

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

Slides are available as PDF, kramse@Github

1-Basics-of-Incident-Response.tex in the repo security-courses

Goals for today

- Define Incident Response
- Find some information – gather data
- Get started trying some tools

Photo by Thomas Galler on Unsplash

Plan for today

- Basics of Intelligence
- Basics of Incident Response
- Get started doing some exercises
- Incident Response Life cycle

Exercise theme:

- IP Address Research
- Mitre ATT&CK Framework introduction
- Demo: buffer overflow and kernel information
- Nginx logging – web server common log format
- Packetbeat example logging system

Reading Summary

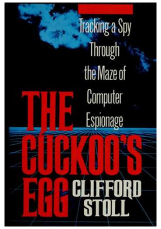
Intelligence-Driven Incident Response (IDIR),
Scott Roberts, Rebekah Brown, ISBN: 9781098120689 **2nd edition 2023** - short IDIR

If you only have 1st edition, it will be okay

Current status – try to go through these chapters:

- Foreword and Preface
- Chapter 1: Introduction
- Chapter 2: Basics of Intelligence
- Chapter 3: Basics of Incident Response

Foreword



> **Threat intelligence was vital to intrusions over 20 years ago**, starting with the story told in **the Cuckoo's Egg, written by Cliff Stoll**, and has been ever since. But somehow, most organizations are **still learning** to adopt the same principles. ... Lucky for us, this book now exists and steps the reader through **proper threat-intelligence concepts, strategy, and capabilities** that an organization can adopt to evolve their security practice. After reading this book, your operations can grow to become an intelligence-driven operation that is much more efficient than ever in **detecting and reducing the possible impact of breaches that will occur.**

Source: *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown

Note mentions!

Resource and books like these mention a lot of interesting things:

- Authors – obviously but perhaps check other writing by them
- Organizations: DoD, NSA, SANS https://www.sans.org/
- Persons: Clifford Stoll and the Cuckoo's Egg (book/security breach incident)
- Company names: Mandiant
- Tools: Nmap, Tcpdump, Metasploit
- Web sites
- Incidents, attacker groups, tactics
- Term: Cyber Threat Intelligence (CTI)
- ...

All of these will enhance your knowledge in this field, so take mental notes along the way.

A related resource is the MITRE ATT&CK framework https://attack.mitre.org/

Preface

> The purpose of this book is to **demonstrate how intelligence fits into the incident-response process**, helping responders understand their adversaries in order to **reduce the time it takes to detect, respond to, and remediate intrusions.** Cyber threat intelligence and incident response have long been **closely related**, and in fact are **inextricably linked.** Not only does threat intelligence support and augment incident response, but incident response generates threat intelligence that can be utilized by incident responders. The goal of this book is to help readers **understand, implement, and benefit** from this relationship.

Source: *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown

- Why, Who and how the book is organized

Fundamentals Chapter 1: Introduction

> **Intelligence as Part of Incident Response**
> As long as there has been conflict, there have been those who studied, analyzed, and strove to understand the enemy. Wars have been won and lost based on an ability to understand the way the enemy thinks and operates, to comprehend their motivations and identify their tactics ...

Source: *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown

- We will call it incident response for this course, this is our focus first
- Later you may pick up the book again and pay more attention to the intelligence gathering and use

What do we mean by Intelligence

> Intelligence is often defined as information that has been refined and analyzed to make it actionable. Intelligence, therefore, requires information. In intelligence- driven incident response, there are multiple ways to gather information that will be analyzed and used to support incident response.

Source: *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown

Chapter 2: Basics of Intelligence

> "Joint Publication 2-0," the US military's primary joint intelligence doctrine, is one of the foundational intelligence documents used today. In its introduction, it states, "Information on its own may be of utility to the commander, but when related to other information about the operational environment and considered in the light of past experience, it gives rise to a new understanding of the information, which may be termed intelligence."

Source: *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown

- *Data* is a piece of information, a fact, or a statistic. Data is something that describes something that *is*.
- *Intelligence* is **derived from a process** of collecting, processing, and analyzing data. Once it has been analyzed, it must be disseminated in order to be useful.

Indicators of Compromise

> There was a time when many people considered indicators of compromise, or IOCs, to be synonymous with threat intelligence. IOCs, which we will reference a lot and cover in depth later in the book, are **things to look for** on a system or in **network logs** that may **indicate that a compromise has taken place**. This includes IP addresses and domains associated with command-and-control servers or malware downloads, hashes of malicious files, and other network- or host-based artifacts that may indicate an intrusion.

Source: *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown

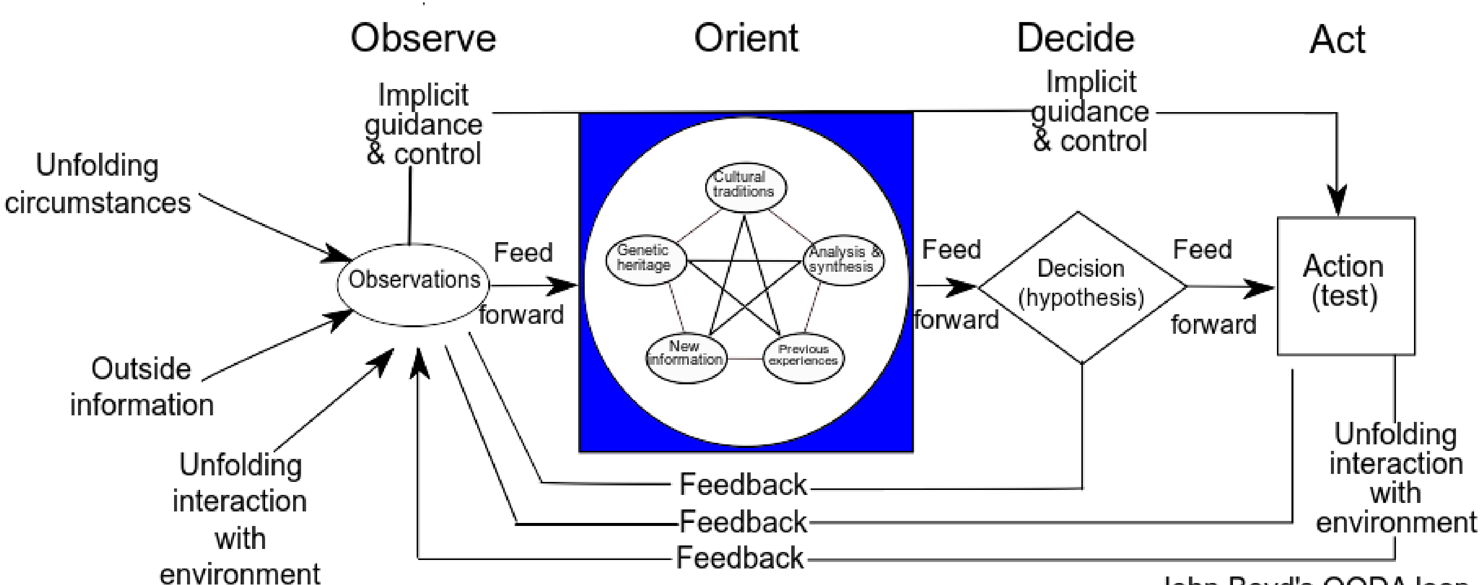
Indicators of Compromise and Signatures

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

OODA Loop by John Boyd

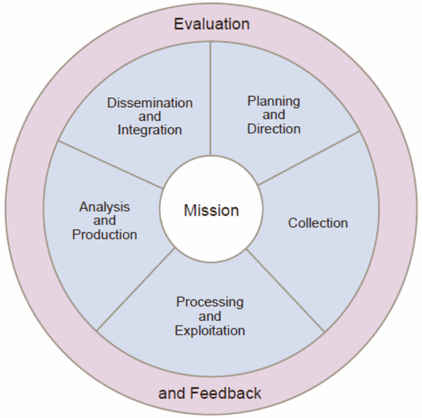


John Boyd's OODA loop

Source: Patrick Edwin Moran - Wikipedia https://en.wikipedia.org/wiki/OODA_loop

Intelligence Cycle or Intelligence Process

The Intelligence Process



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

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

- I decided to take the more original Intelligence Process picture, which has a bit more details

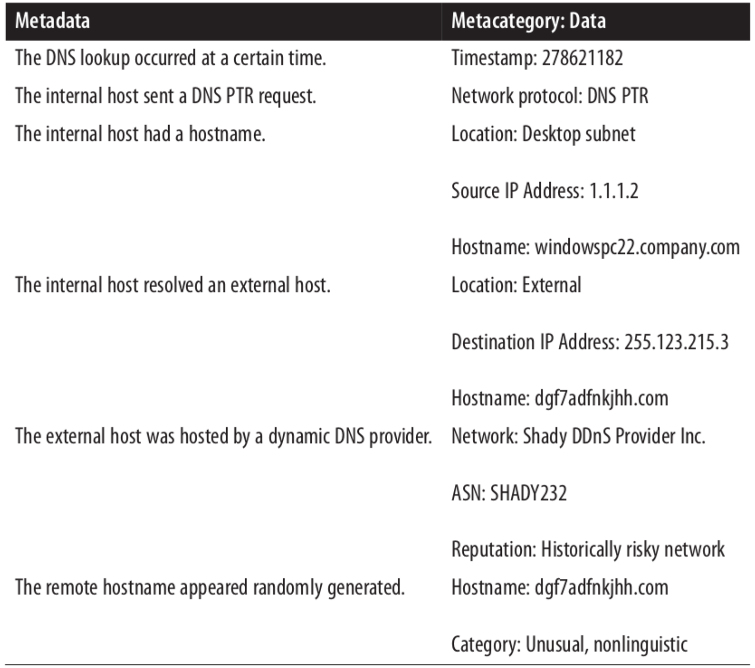
Processing

Let's look at some processing

- Processing includes normalizing collected data into uniform formats for analysis
- Indexing – Large volumes of data need to be made searchable
- Translation – for our course we might get multiple input formats but need JSON or XML
- Enrichment – Providing additional metadata for a piece of information is important. For example, domain addresses need to be resolved to IP addresses, and **WHOIS registration data fetched**
- Filtering – Not all data provides equal value, and analysts can be overwhelmed when presen- ted with endless streams of irrelevant data
- Prioritization – The data that has been collected may need to be ranked so that analysts can allo- cate resources to the most important items

  Note: this relates to a *baseline*, what errors are normal in your environment
- Visualization – Data visualization has advanced significantly and the human eye and brain can often see patterns

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

Exercise

Now lets do the exercise

⚠ IP address research – 30 min

which is number **8** in the exercise PDF.

Exercise

Now lets do the exercise

⚠ Brim desktop app - 20 min

which is number **9** in the exercise PDF.

Chapter 3: Basics of Incident Response

> Incident response encompasses the entire process of **identifying intrusions** (whether against a single system or an entire network), developing the information necessary to **fully understand them**, and then **developing and executing the plans** to **remove the intruders**.

Source: *Intelligence-Driven Incident Response* (IDIR)
Scott Roberts. Rebekah Brown

- An important part of this is *when* to activate the incident response team, what qualifies? Triage of incidents

Incident Response Life cycle

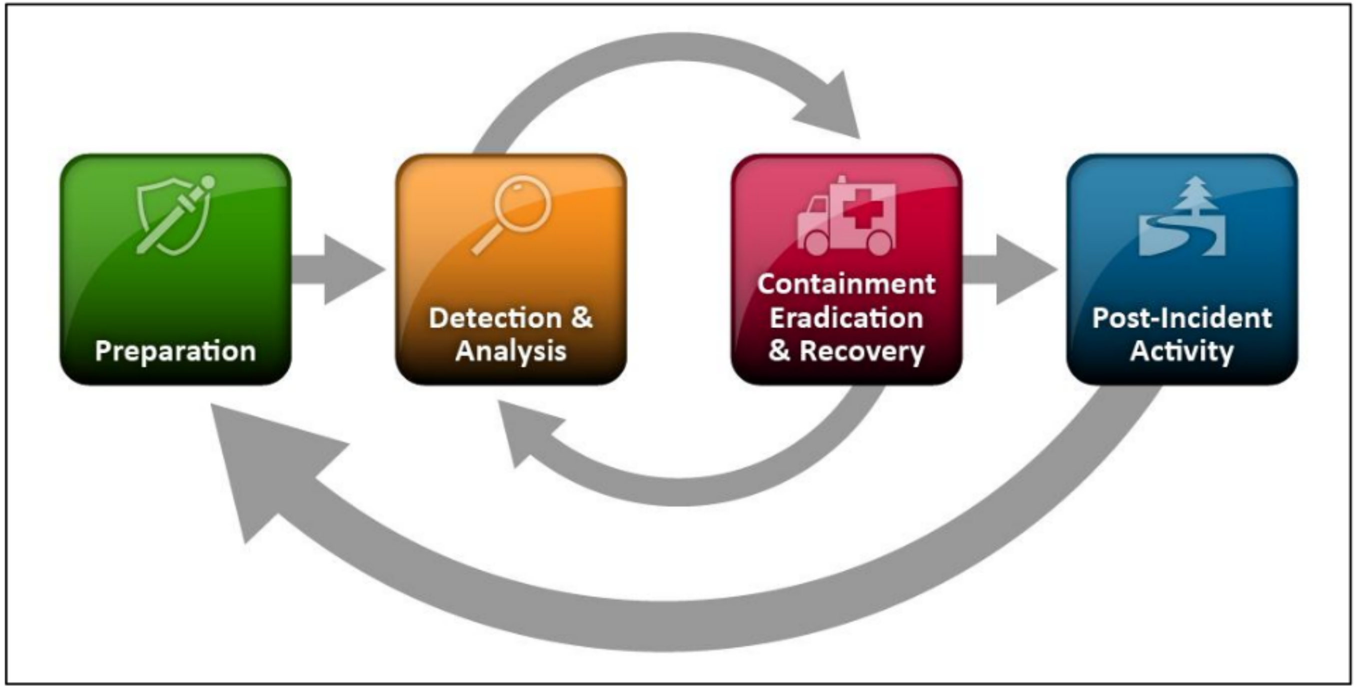


Figure 3-1. Incident Response Life Cycle

Source: *Computer Security Incident Handling Guide*, NIST SP 800-61 Rev. 2

Preparation

> For a defender, the first stage of an incident comes before the attack begins: the Preparation phase. Preparation is the defender's chance to get ahead of the attacker by deploying new detection systems, creating and updating signatures, and understanding baseline system and network activity.

- Telemetry – You can't find what you can't see
- Hardening – The only thing better than identifying an intrusion quickly is it never happening in the first place
- Process and documentation – On the nontechnical side, process is the first line of defense that can be prepared ahead of time
  You may see the term Standard Operating Procedure (SOP) used in literature
- Practice – The last thing preparation allows is the chance to practice your plans. This will speed up future incidents and identify issues that can be corrected

Identification

The Identification phase is the moment where the defender identifies the presence of an attacker impacting their environment. This can occur though a variety of methods:

- Identifying the attacker entering the network, such as a server attack or an incoming phishing email
- Noticing command-and-control traffic from a compromised host
- Seeing the massive traffic spike when the attacker begins exfiltrating data
- Getting a visit from a special agent at your local FBI field office
- And last, but all too often, showing up in an article by Brian Krebs

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

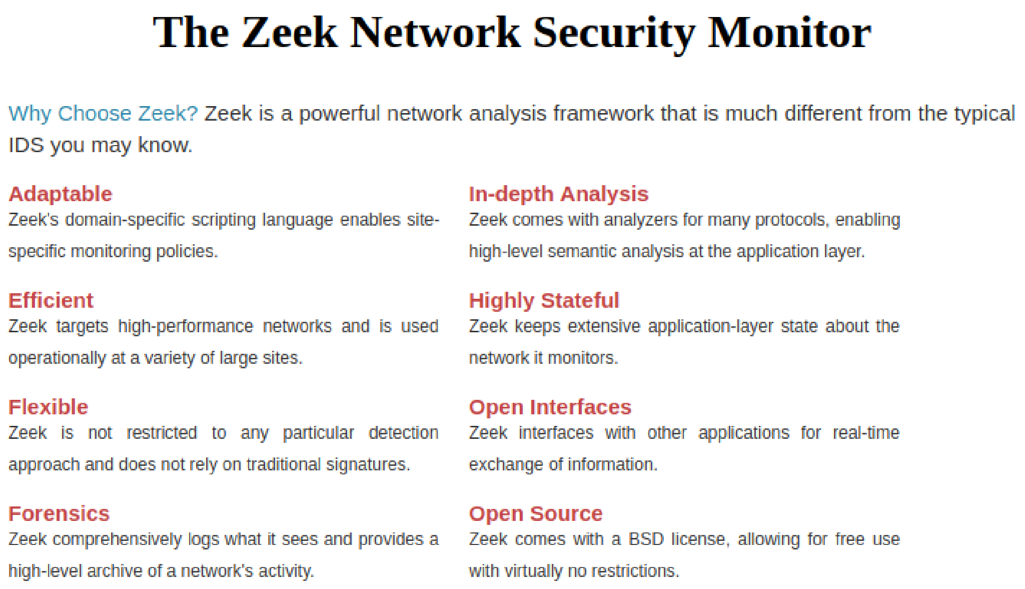
Although we could spend an entire book creating an exhaustive list of skills needed to be a good security data scientist, this chapter covers the following skills/domains that a data scientist will benefit from knowing within information security:

- 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

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.

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

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

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

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

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

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

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

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

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

Zeek IDS is

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/

Suricata IDS/IPS/NSM

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

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

In this course we will expect our organisation to have already deployed similar capabilities.

You can find a whole workshop in:
https://github.com/kramse/security-courses/tree/master/courses/networking/suricatazeek-workshop

Containment

Common containment options are as follows:

- Disabling the network switch port to which a particular system is connected
- Blocking access to malicious network resources such as IPs (at the firewall) and domains or specific URLs (via a network proxy)
- Temporarily locking a user account under the control of an intruder
- Disabling system services or software an adversary is exploiting

Eradication

Eradication consists of the longer-term mitigation efforts meant to keep an attacker out for good (unlike the temporary measures in the Containment phase). These actions should be well thought out and may take a considerable amount of time and resources to deploy. They are focused on completely obviating as many parts of the adversary's plan from ever working in the future.

Common eradication actions are as follows:

- Removing all malware and tools installed by the adversary (see the sidebar "Wiping and Reloading Versus Removal" on page 32)
- Resetting and remediating all impacted user and service accounts
- Re-creating secrets that could have been accessed by the attacker, such as shared passwords, certificates, and tokens

Recovery

Containment and eradication often require **drastic action**. Recovery is the process of going back to a nonincident state. In some regards, recovery is less from the attack itself, but more from the actions taken by the incident responders.

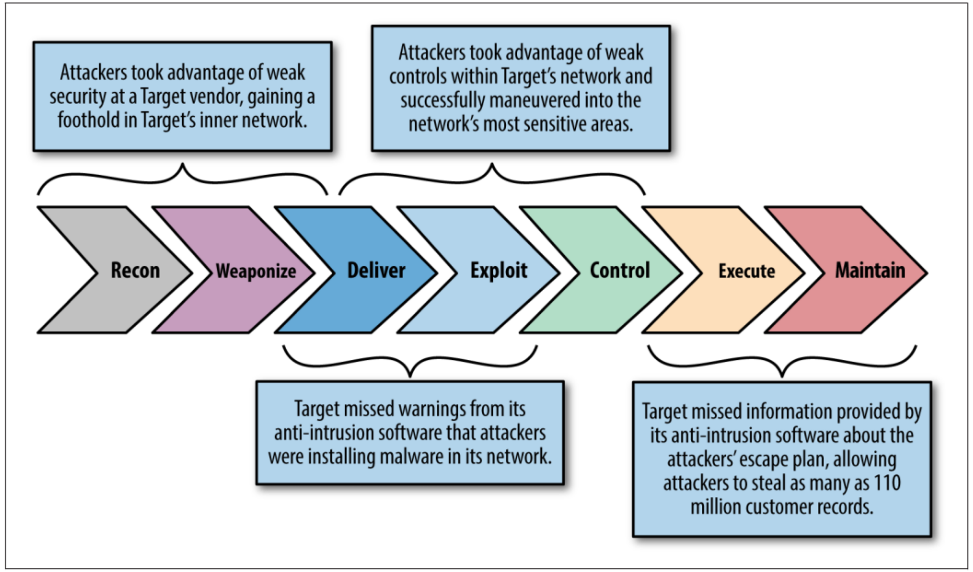
For example, if a compromised system is taken from a user for forensic analysis, the Recovery phase involves returning or replacing the user's system so that user can return to previous tasks. If an entire network is compromised, the Recovery phase involves undoing any actions taken by the attacker across the entire network, and can be a **lengthy and involved process.**

Lessons Learned – Follow-Up

> Ultimately, the key to Lessons Learned is having the understanding that although early lessons learned will be painful, they will improve—and that's the point. Early Lessons Learned exercises will call out **flaws, missing technology, missing team members, bad processes, and bad assumptions**. Growing pains with this process are common, but take the time and gut through them. **Few things** will improve an IR team and IR capability as **quickly** as some **tough lessons learned**.

- Goal is to mature your team, methods, procedures, identification, ...
- More efficient is cheaper, faster, better

Intrusion Kill Chains



Attackers took advantage of weak security at a Target vendor, gaining a foothold in Target's inner network.

Attackers took advantage of weak controls within Target's network and successfully maneuvered into the network's most sensitive areas.

Target missed warnings from its anti-intrusion software that attackers were installing malware in its network.

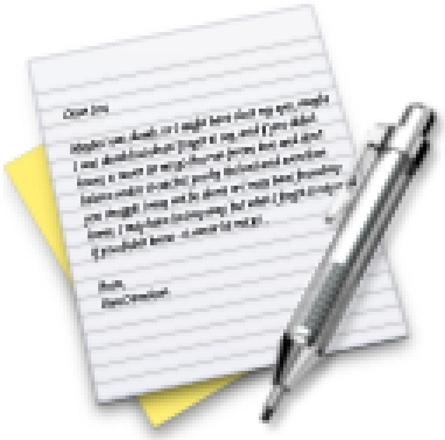
Target missed information provided by its anti-intrusion software about the attackers' escape plan, allowing attackers to steal as many as 110 million customer records.

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

Exercise



Now lets do the exercise

⚠ Mitre ATT&CK Framework 10 min

which is number **7** in the exercise PDF.

Exercise

Now lets do the exercise

ℹ Demo: Buffer Overflow 101 - 30-40min

which is number **10** in the exercise PDF.

Python and REST

```
#!/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

```python
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:

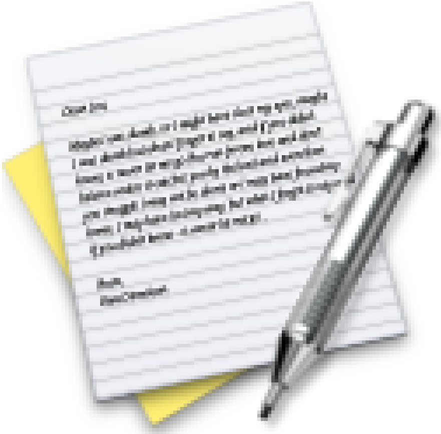
```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   trans_id
        rtt     query   qclass  qclass_name     qtype   qtype_name      rcode   rcode_name      AA
        TC      RD      RA      Z       answers TTLs    rejected

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

Exercise

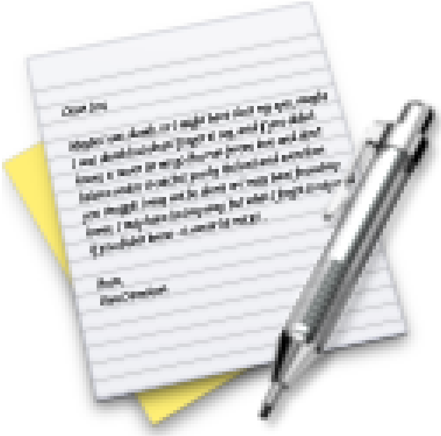


Now lets do the exercise

⚠ Nginx logging 20 min

which is number **11** in the exercise PDF.

Exercise



Now lets do the exercise

ℹ Packetbeat monitoring 15 min

which is number **12** in the exercise PDF.

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