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

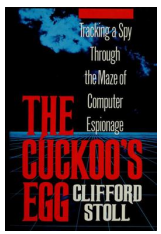
Reading Summary

Intelligence-Driven Incident Response (IDIR)
Scott Roberts. Rebekah Brown, ISBN: 9781491934944

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, ISBN: 9781491934944

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, ISBN: 9781491934944

- Why, Who and how the book is organized

kea

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, ISBN: 9781491934944

- 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, ISBN: 9781491934944

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, ISBN: 9781491934944

- *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, ISBN: 9781491934944

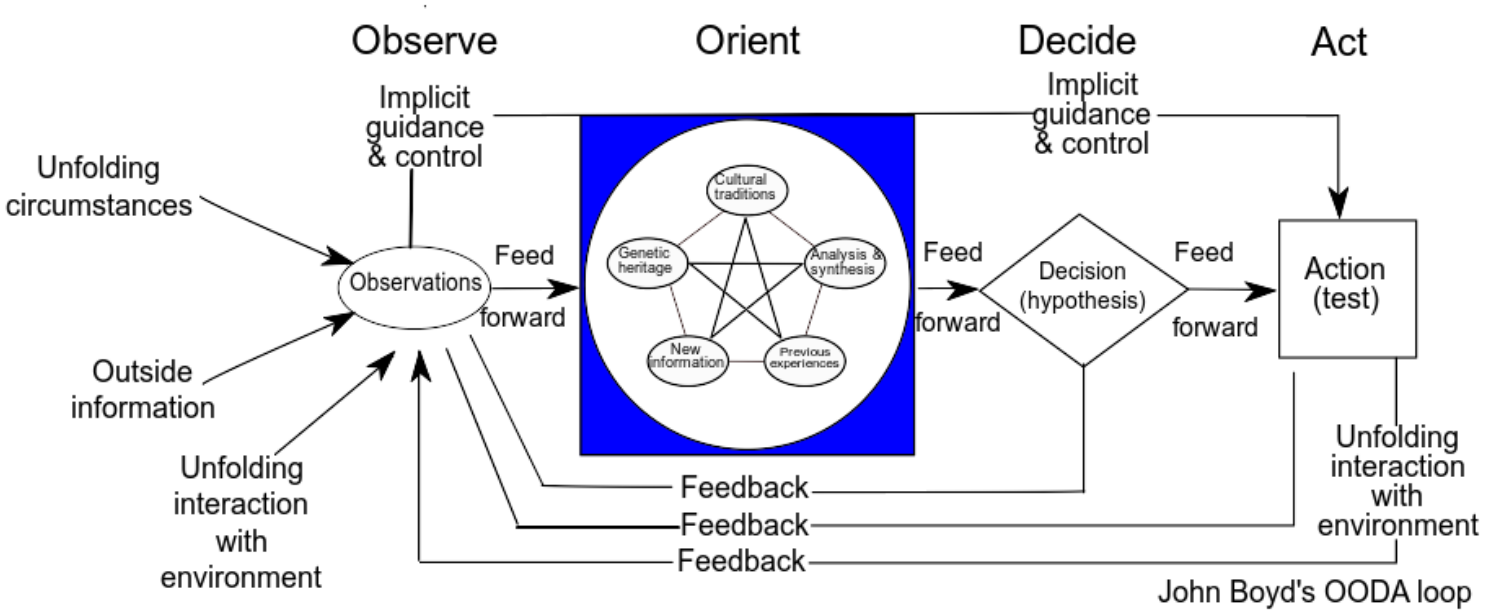
Indicators of Compromise and Signatures

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 signature can contain one or more IOCs.

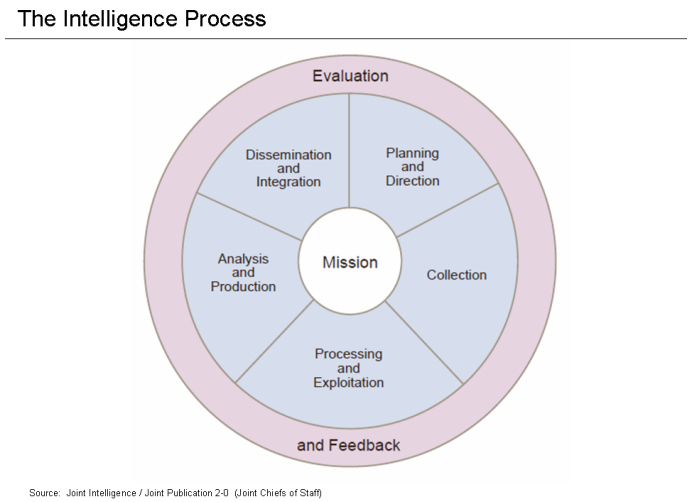
Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

OODA Loop by John Boyd



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

Intelligence Cycle or Intelligence Process



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

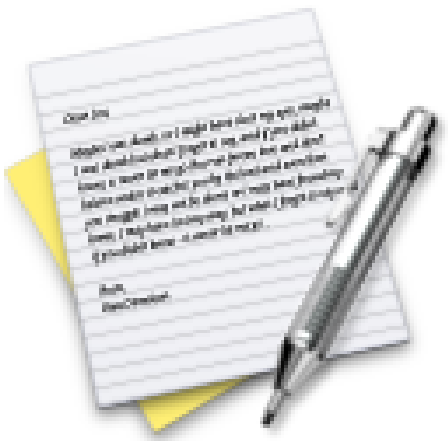
- I decided to take the more original Intelligence Process picture, which has a bit more details

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

Exercise



Now lets do the exercise

⚠ IP address research – 30 min

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

kea

> 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, ISBN: 9781491934944

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

Incident Response Life cycle

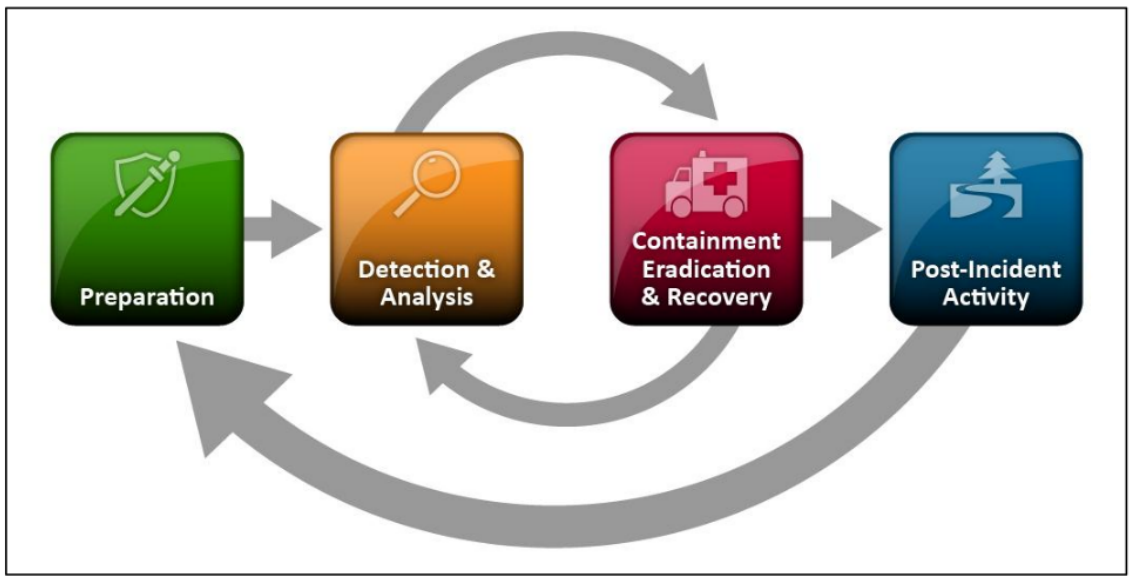


Figure 3-1. Incident Response Life Cycle

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

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

kea

> 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

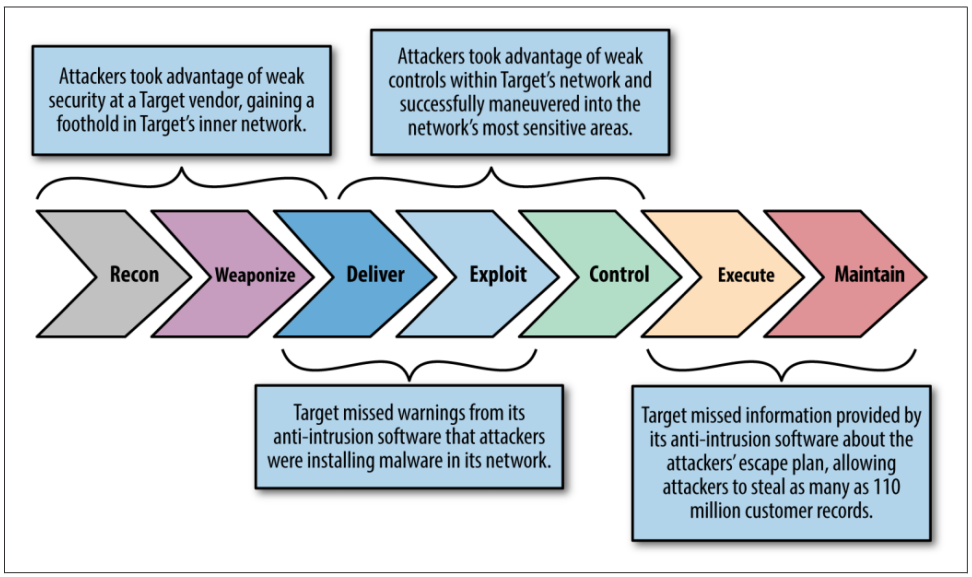
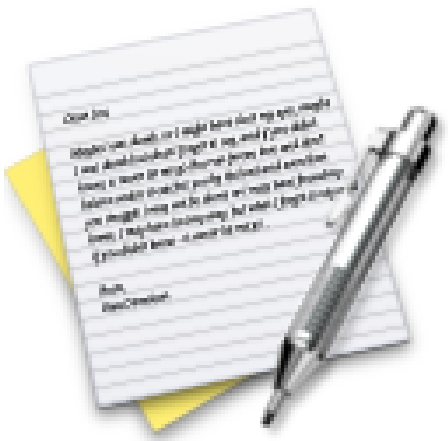


Figure 7-1. The kill chain

- 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

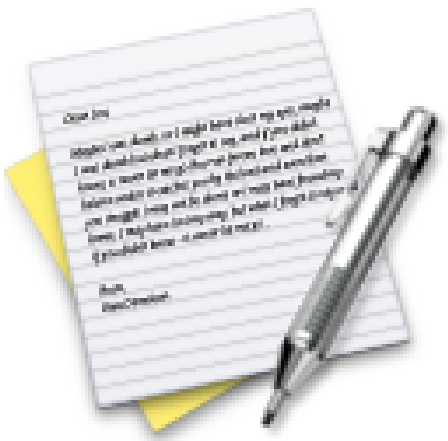


Now lets do the exercise

⚠ Mitre ATT&CK Framework 10 min

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

Exercise

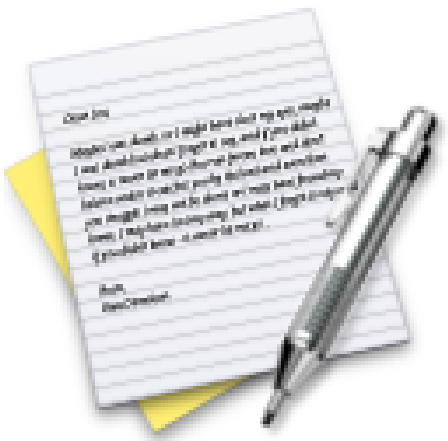


Now lets do the exercise

Demo: Buffer Overflow 101 - 30-40min

which is number 9 in the exercise PDF.

Exercise

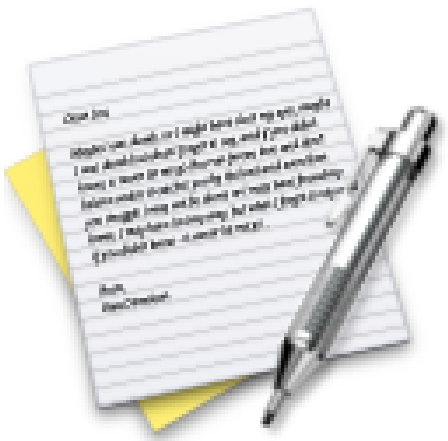


Now lets do the exercise

⚠ Nginx logging 20 min

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

Exercise

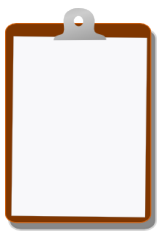


Now lets do the exercise

Packetbeat monitoring 15 min

which is number 11 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