Welcome to

Introduction to Incident Response Elective, KEA

Henrik Kramselund

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

Slides are available as PDF, kramse@Github

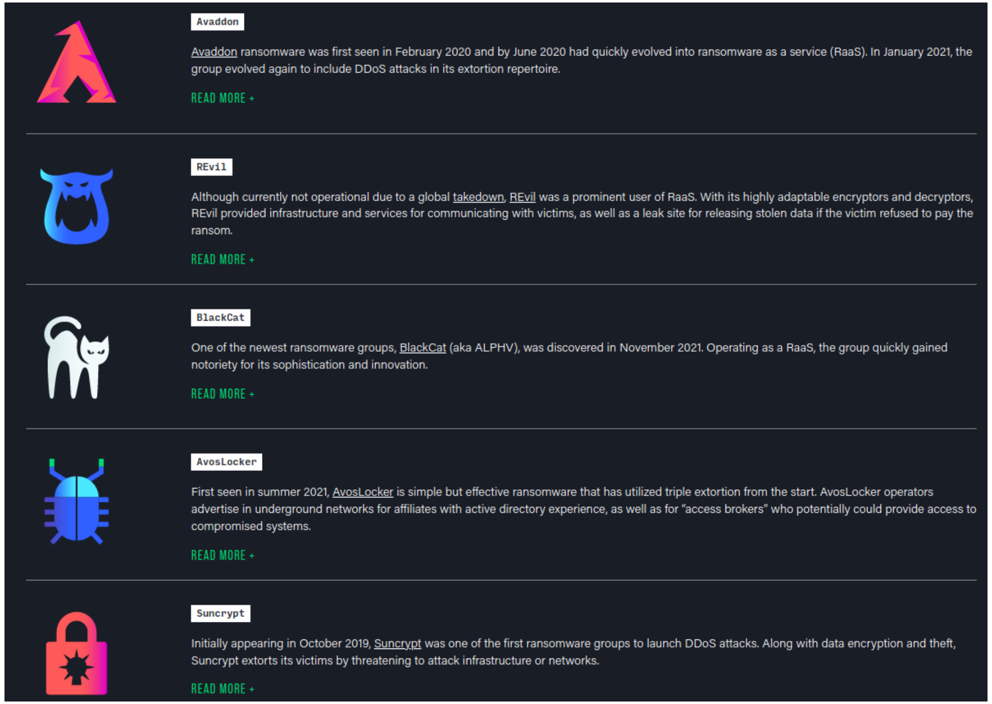
valgfagspræsentation-incident-response.tex in the repo security-courses

Goals for Course

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.

Photo by Thomas Galler on Unsplash

Ransomware Attacks are Common



Avaddon

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

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

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

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

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/

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
- Pricipperne 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

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:

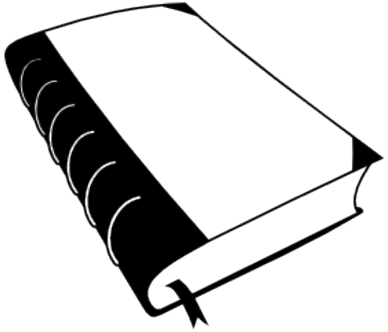
- Network experience
- Server experience
- TCP/IP principles - often in more detail than a common user
- Programming is an advantage, for automating things
- Some Linux and Unix knowledge is in my opinion a **necessary skill** for infosec work

– too many new tools to ignore, and lots found at sites like Github and Open Source written for Linux

Primary literature

Primary literature:

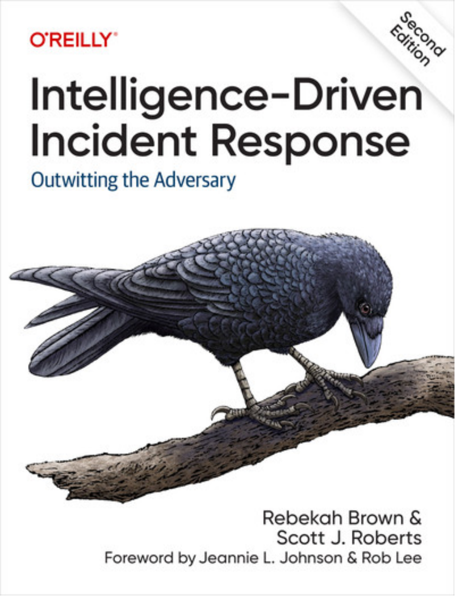
- *Intelligence-Driven Incident Response*
  Scott Roberts. Rebekah Brown, ISBN: 9781098120689 **2nd edition**- short IDIR
- *Forensics Discovery* (FD), Dan Farmer, Wietse Venema 2004, Addison-Wesley 240 pages.
  ISBN: 9780201634976
  This book is currently available for "free":
  http://fish2.com/security/ – 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

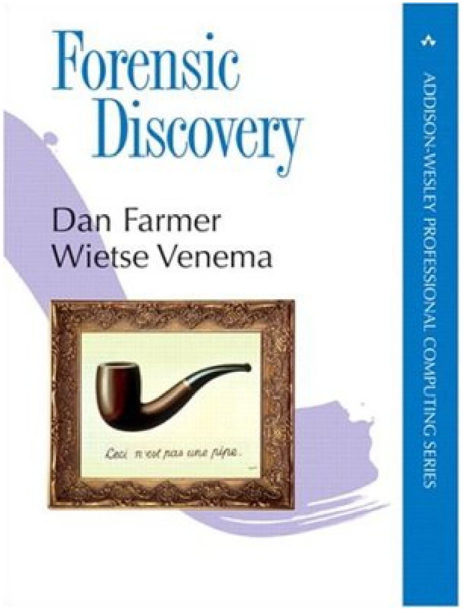
Other papers and resources will also be part of the curriculum!

Book: Intelligence-Driven Incident Response


O'REILLY
Second Edition
Intelligence-Driven Incident Response
Outwitting the Adversary
Rebekah Brown & Scott J. Roberts
Foreword by Jeannie L. Johnson & Rob Lee

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

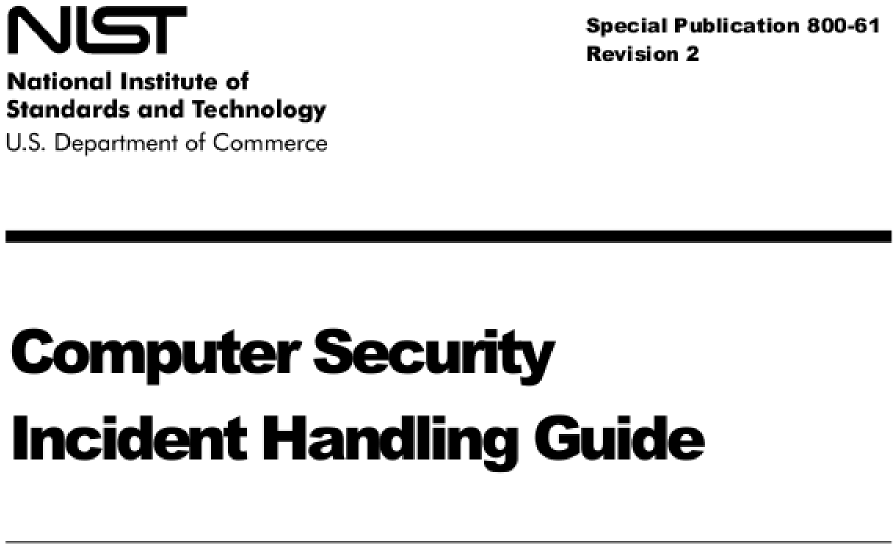
Book: Forensics Discovery (FD)



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

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

Book: NIST SP800-61rev2



NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

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

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

Incident Response Checklists

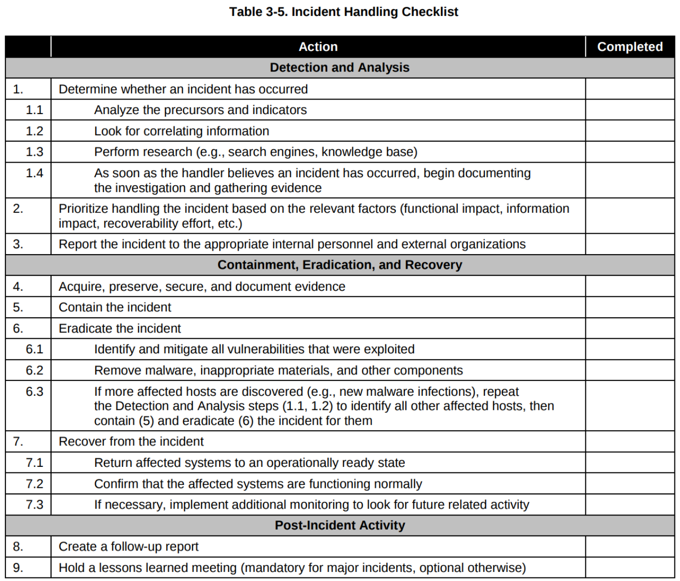
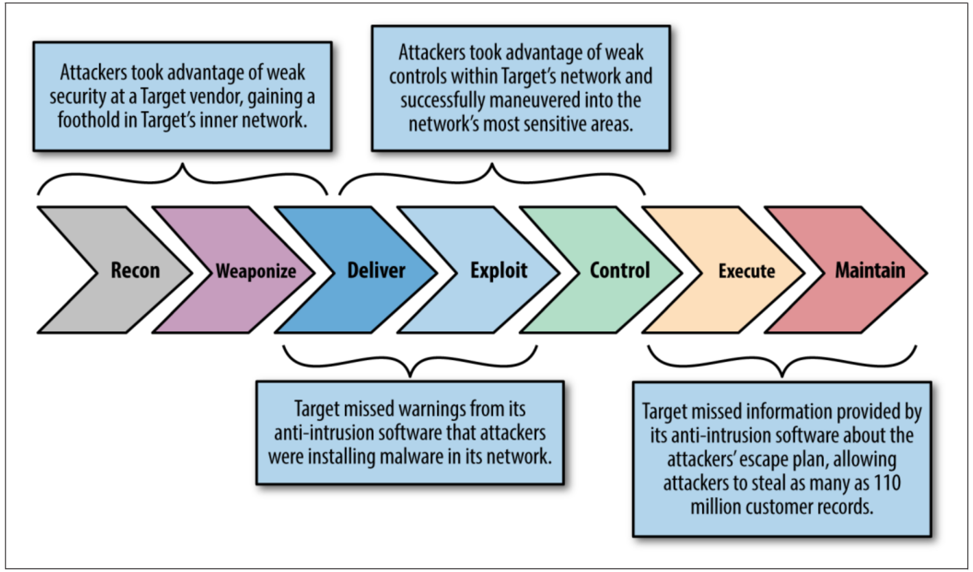


Table 3-5. Incident Handling Checklist

	Action	Completed
Detection and Analysis		
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	
Containment, Eradication, and Recovery		
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	
Post-Incident Activity		
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.

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

Tools on Linux, Mac and Windows

```
hlk@debian-lab-11:~/Downloads$ sudo vol -f cridex.vmem windows.pstree.PsTree
Volatility 3 Framework 2.4.1
Progress:  100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime

4 0 System 0x823c89c8 53 240 N/A False N/A N/A
* 368 4 smss.exe 0x822f1020 3 19 N/A False 2012-07-22 02:42:31.000000  N/A
** 584 368 csrss.exe 0x822a0598 9 326 0 False 2012-07-22 02:42:32.000000  N/A
** 608 368 winlogon.exe 0x82298700 23 519 0 False 2012-07-22 02:42:32.000000  N/A
*** 664 608 lsass.exe 0x81e2a3b8 24 330 0 False 2012-07-22 02:42:32.000000  N/A
*** 652 608 services.exe 0x81e2ab28 16 243 0 False 2012-07-22 02:42:32.000000  N/A
**** 1056 652 svchost.exe 0x821dfda0 5 60 0 False 2012-07-22 02:42:33.000000  N/A
**** 1220 652 svchost.exe 0x82295650 15 197 0 False 2012-07-22 02:42:35.000000  N/A
...
```

- We will find and run various tools within the incident response space
- Memory analysis, disk analysis, logging, network dissecting, intelligence feeds
- After course is done, you will have started a toolbox for incident response and know a few from running them