IMPLEMENTING A KICK-BUTT TRAINING PROGRAM: BLUE TEAM GO!

Ryan J. Chapman

@rj_chap

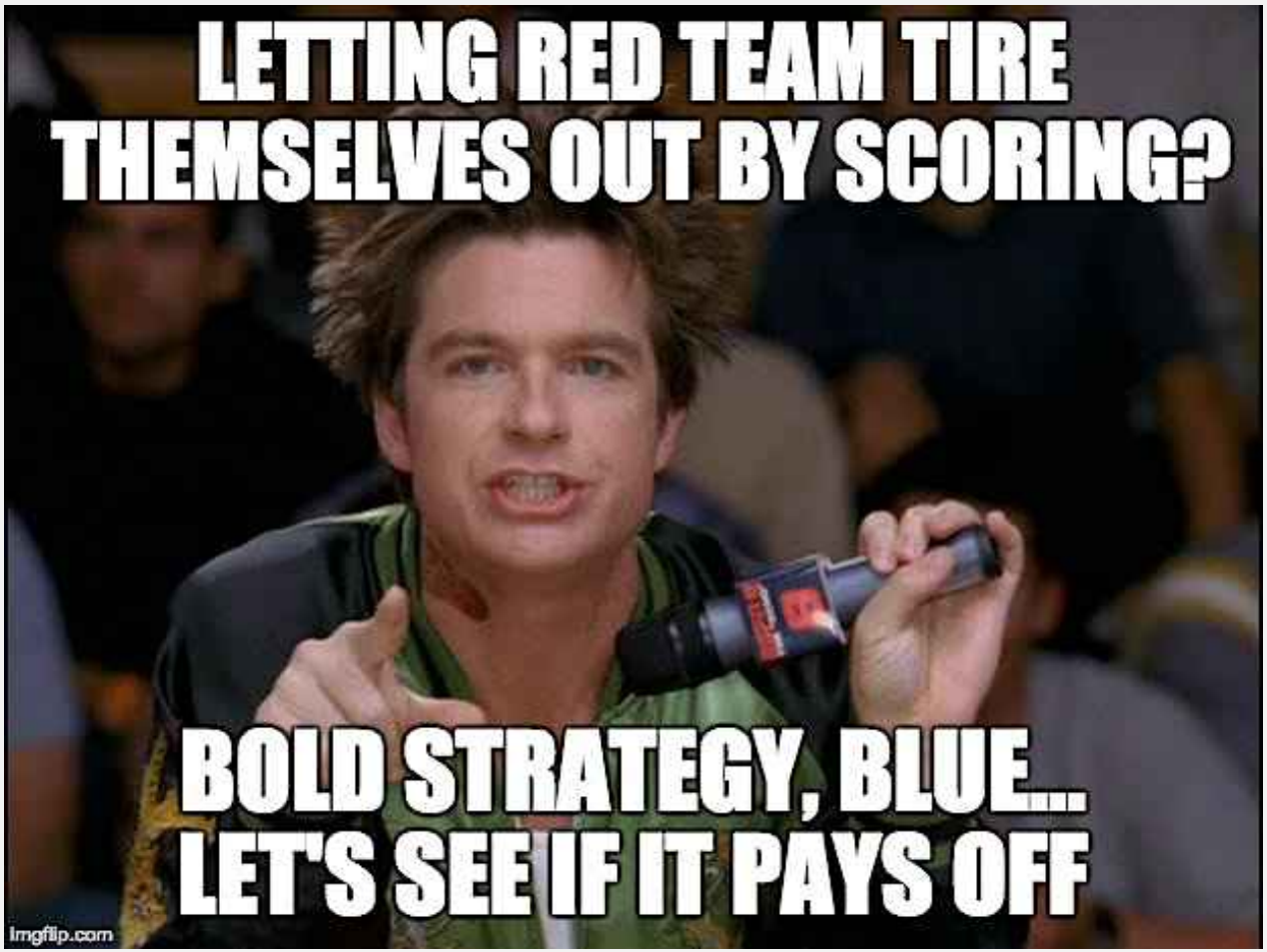
AGENDA

- Why baseline training?
- Trainers
- Core Tenants
- Delivery Methodologies
- **The curriculum!**
  - **Five different phases**
- Reinforcement
- Questions / Wrap-up

CIRT/SOC LIAISON @ BECHTEL

(Wittmeyer, n.d.)

- Finding the "right" hire
- Failure analysis:
  - Educational institutions
  - Certifications
  - Hiring "the analyst mindset"
  - Previous experience


LETTING RED TEAM TIRE THEMSELVES OUT BY SCORING?
BOLD STRATEGY, BLUE... LET'S SEE IF IT PAYS OFF
imgflip.com

WE CAN REBUILD THEM – WE HAVE THE TRAINING

- Desired goal: "Jack & Jills of All Trades"
- Designed w/ SOC and CIRT analysts in mind
  - ANYONE who has hands on keyboard during IR!
- Doesn't matter what pops up, ***HANDLE IT***
  - Weaponized carrier files, OSINT, proof-of-execution analysis, etc.

T3: TRAINING THE TRAINERS

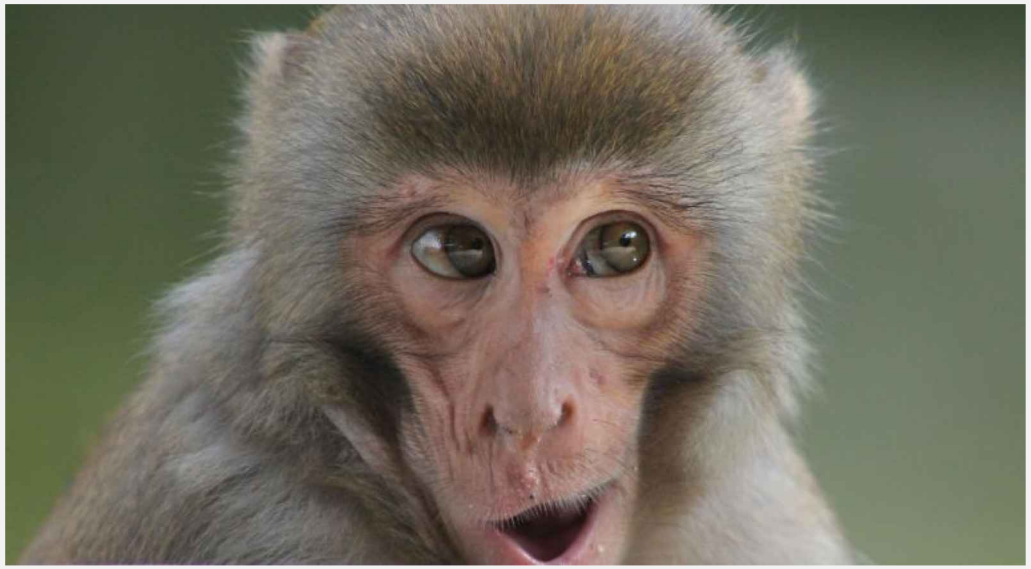
- Identify primary resource(s)
- Recognize, assign, and train SMEs
- Hold Train the Trainers (T3) sessions

- Example:
  - CIRT/SOC Liaison → Leads → New-hire analysts

5:00

CORE TENANTS

- HOW and WHY
  - No pressing buttons for bananas!
- Experiential training
  - Hands on the keyboard



CORE TENANTS

- HOW and WHY
  - No pressing buttons for bananas!
- Experiential training
  - Hands on the keyboard

CORE TENANTS CONT.

- Foster a "Go here to find…" mentality
- Continually point to reference material
  - Internal documentation
  - External documentation
    - RFCs!!

Obsoleted by: 7230, 7231, 7232, 7233, 7234, 7235 DRAFT STANDARD
Updated by: 2817, 5785, 6266, 6585 Errata Exist

Network Working Group R. Fielding
Request for Comments: 2616 UC Irvine
Obsoletes: 2068 J. Gettys
Category: Standards Track Compaq/W3C
J. Mogul
Compaq
H. Frystyk
W3C/MIT
L. Masinter
Xerox
P. Leach
Microsoft
T. Berners-Lee
W3C/MIT
June 1999

Hypertext Transfer Protocol -- HTTP/1.1

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

The first digit of the Status-Code defines the class of response. The last two digits do not have any categorization role. There are 5 values for the first digit:

- 1xx: Informational - Request received, continuing process
- 2xx: Success - The action was successfully received, understood, and accepted
- 3xx: Redirection - Further action must be taken in order to complete the request
- 4xx: Client Error - The request contains bad syntax or cannot be fulfilled
- 5xx: Server Error - The server failed to fulfill an apparently valid request

The individual values of the numeric status codes defined for HTTP/1.1, and an example set of corresponding Reason-Phrase's, are presented below. The reason phrases listed here are only recommendations -- they MAY be replaced by local equivalents without affecting the protocol.

```
Status-Code    =
      "100"  ; Section 10.1.1: Continue
    | "101"  ; Section 10.1.2: Switching Protocols
    | "200"  ; Section 10.2.1: OK
    | "201"  ; Section 10.2.2: Created
```

CORE TENANTS CONT.

- Take learning styles into account
  - **Kinesthetic** look down
  - Visual look up
  - Auditory look to the sides
- Exploit all possible teaching moments

10:00

CORE TENANTS CONT.

- Tie back to the Real World
  - Daily **ticket review** and/or **shadowing**

- Everything ties together in final week
  - Final week should be as hands-on as possible!

FLEXIBLE FRAMEWORK

BOOTCAMP

- All 5 weeks at once
- Works well for experienced analysts
  - Baselining
- May overload those new to IR
  - Not so great for onboarding

MODULAR

- Multi-phase deployments
- Example:
  - Phase 1: Weeks 1, 2, & 5
  - Phase 2: Week 3
  - Phase 3: Week 4
- Easier on new analysts
- Will make more sense soon…

CURRICULUM OVERVIEW

Weeks 1 - 5

15:00

INTRO, SETUP, & THE SIEM

Week 1

INTRO, SETUP, & THE SIEM

Week 1

- Day 1
  - Company intro & setup
- Day 2-3
  - Setup cont.
- Day 4 & 5
  - The SIEM

BOND, TEAM BOND

Precautionary, regulatory, or ***reactionary?***

Team formation

SOC? CIRT? Tiered? **Why?**

What works?

What **doesn't work?**

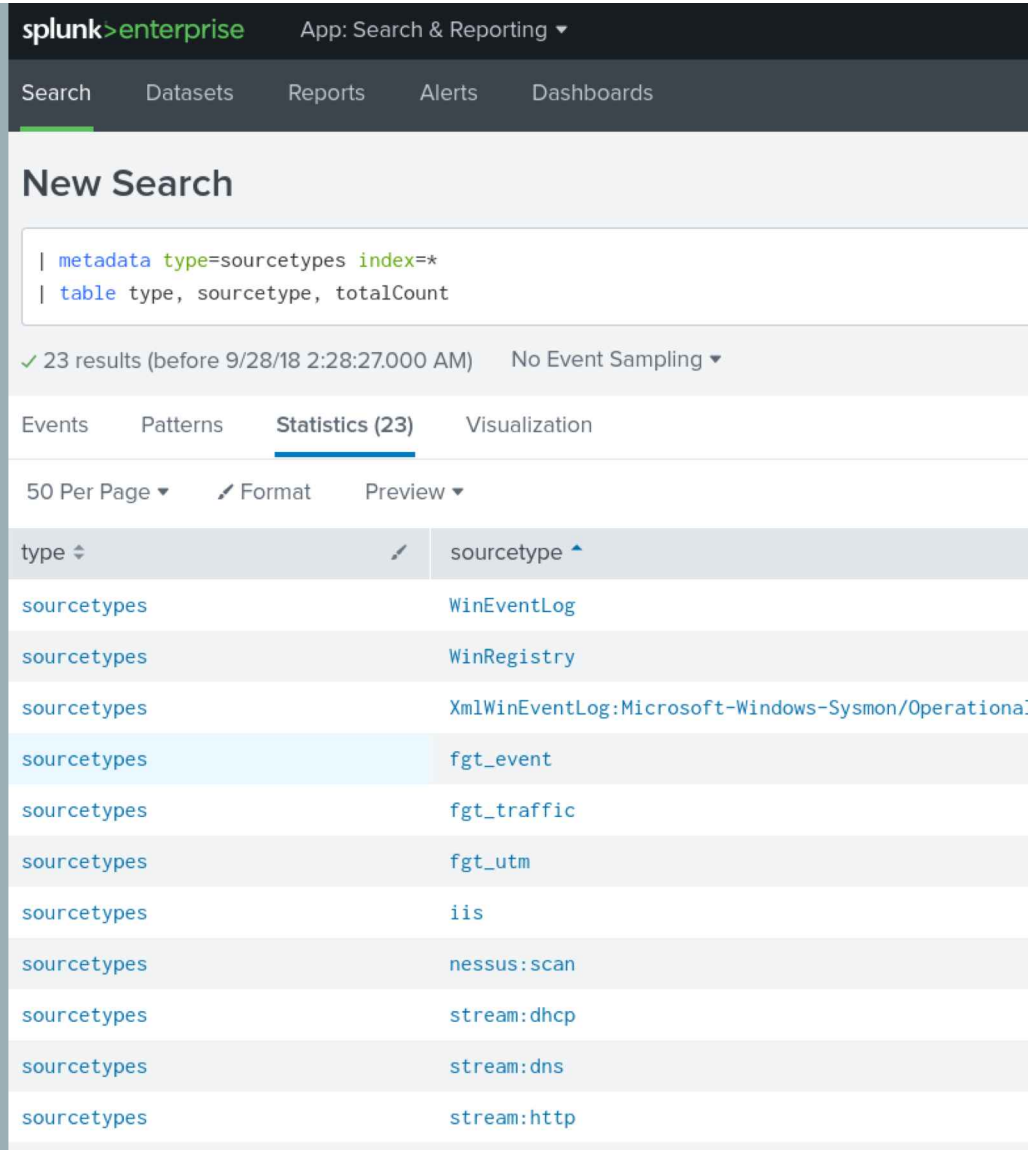
THE SIEM – LOGS

Available Data/Logs?

Fields?

Documentation?

Known visibility gaps?



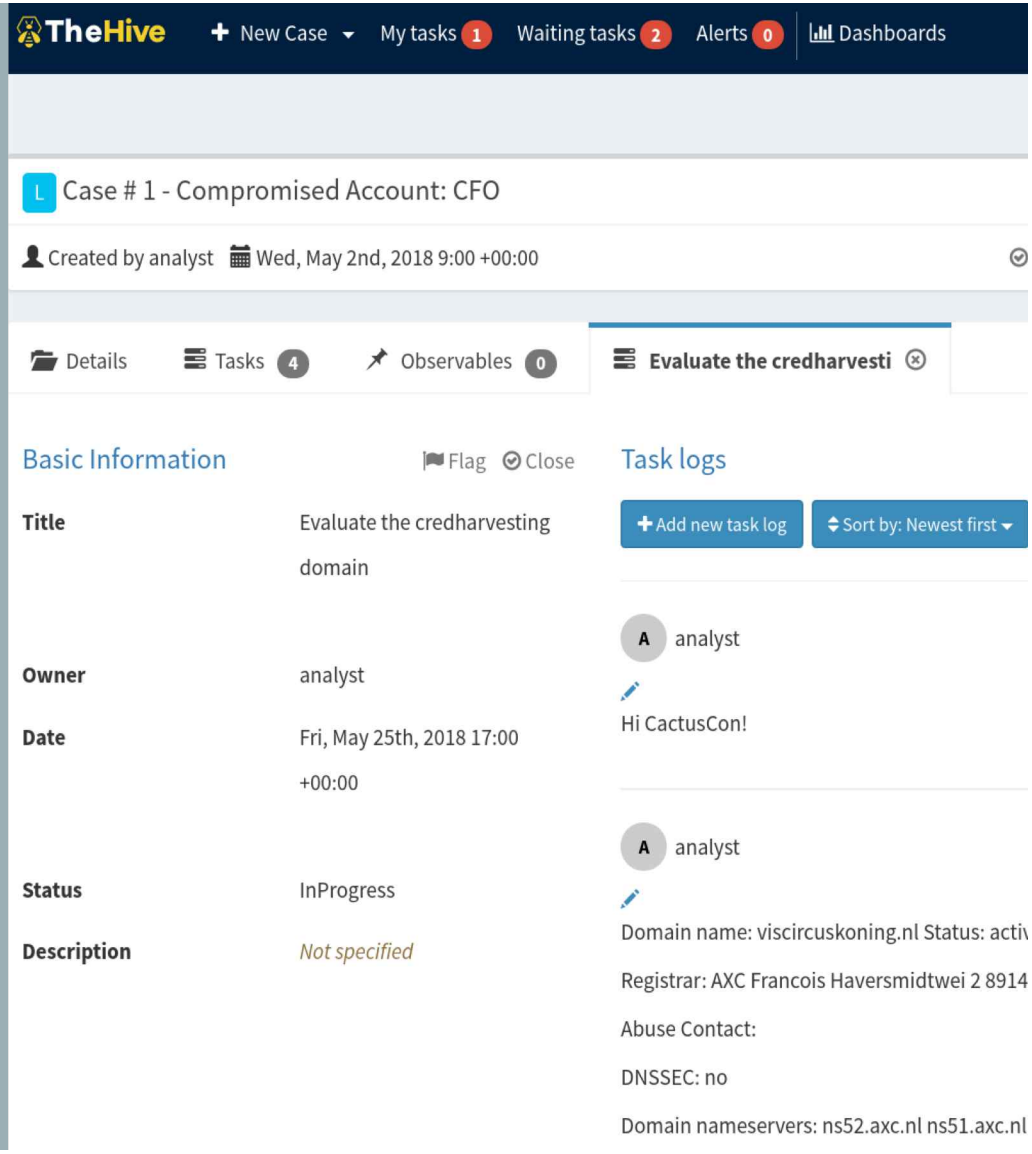
THE SIEM – TICKETS

Fields?

Common ticket types?

Review Top 3

Information management?



NETWORKING & NETWORK FORENSICS

Week 2

20:00

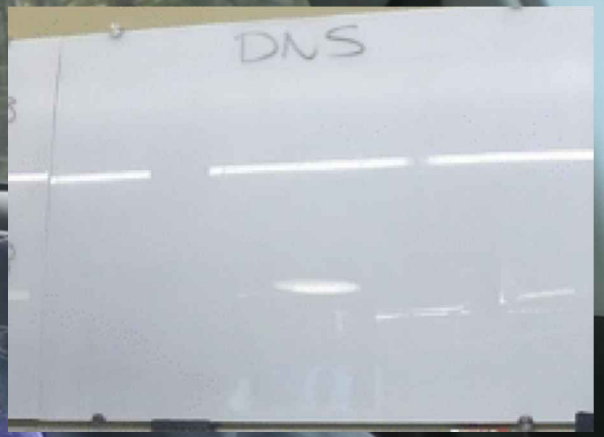
NETWORKING & NETWORK FORENSICS

Week 2

- Begin w/ network diagram

- Day 1: Common protocols
  - Ex: DNS, HTTP, & SMTP
- Day 2: Network logs
- Day 3: Email
- Day 4: Sanitizing email
- Day 5: Wireshark & PCAP Challenge

DNS

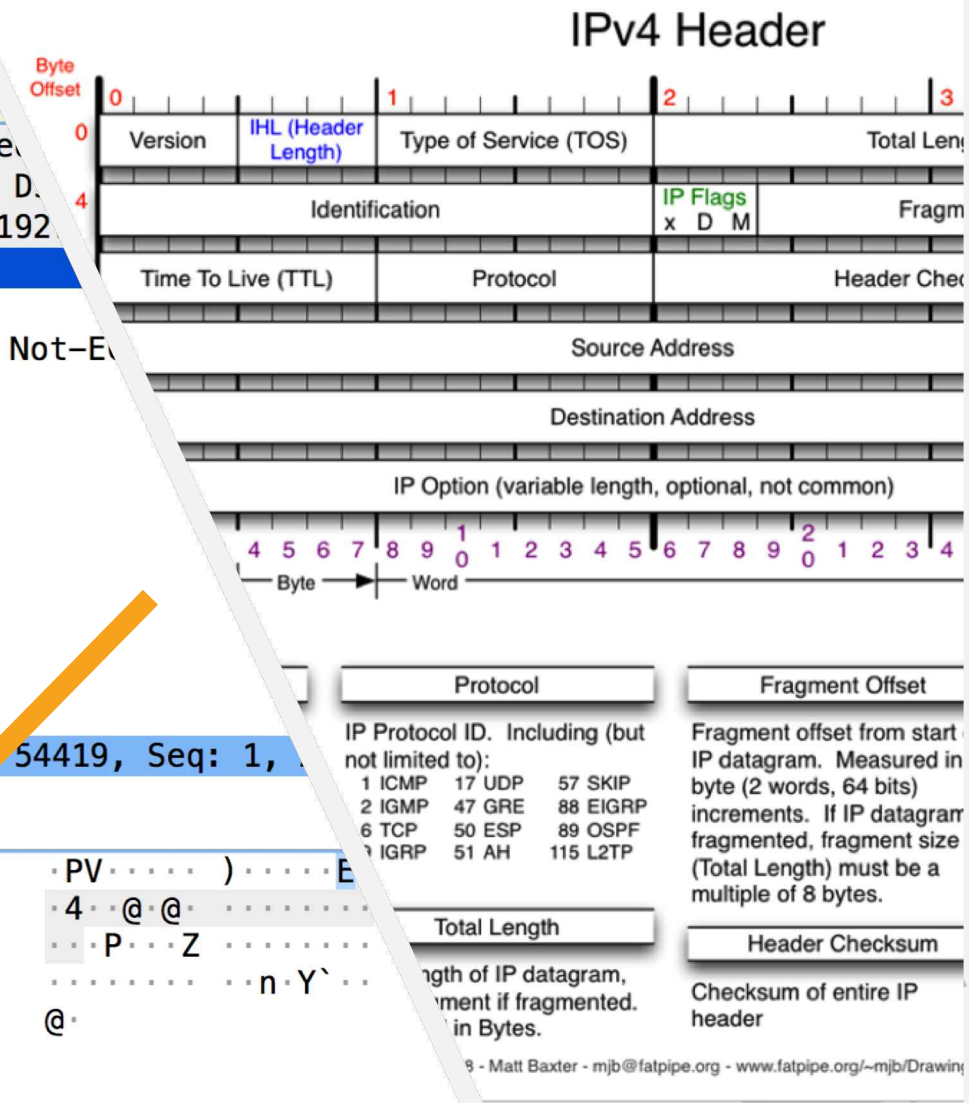


RFC: RFC 1032-1035 - Domain Names
RFC 1464 - TXT records
RFC 1591 - Delegation
RFC 2219 - CNAME records
etc ...

@nillkitty

```
    18      1 192.168.1.1…     80 192.168.1.2
    19      1 192.168.1.2   54419 192.168.1.157
    20      1 192.168.1.1…     80 192.168.1.2     54…
    21        Vmware_b0:8…        Vmware_69:e6…
▶ Frame 20: 66 bytes on wire (528 bits), 66 bytes capture…
▶ Ethernet II, Src: Vmware_1f:f8:1a (00:0c:29:1f:f8:1a), D…
▼ Internet Protocol Version 4, Src: 192.168.1.157, Dst: 192…
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E…
    Total Length: 52
    Identification: 0xe1c2 (57794)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xd511 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.157
    Destination: 192.168.1.2
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54419, Seq: 1, …

0000  00 50 56 c0 00 02 00 0c  29 1f f8 1a 08 00 45 00   ·PV·····  )·····E·
0010  00 34 e1 c2 40 00 40 06  d5 11 c0 a8 01 9d c0 a8   ·4··@·@·  ········
0020  01 02 00 50 d4 93 05 5a  b8 e1 df db 8e 06 80 11   ···P···Z  ········
0030  00 b5 ca b9 00 00 01 01  08 0a 6e 8c 59 60 1d c1   ········  ··n·Y`··
0040  40 ae                                             @·
```



HOST-BASED FORENSICS

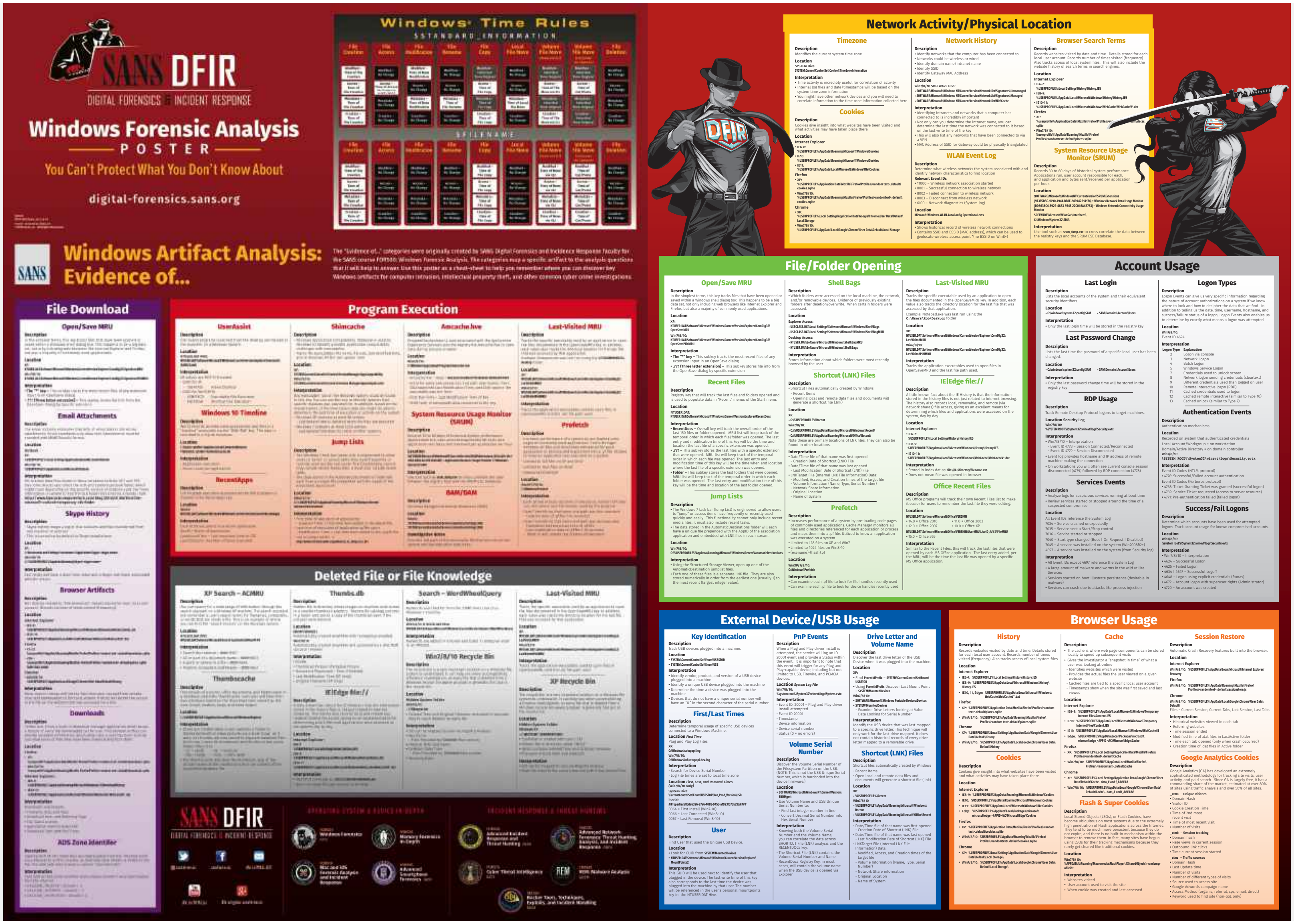
Week 3

25:00

HOST-BASED FORENSICS

Week 3

- Day 1: Windows artifacts
  - Start with NTFS' $MFT
- Day 2: Registry analysis cont.
- Day 3: Corp. forensic tool(s)
- Day 4: Eric Zimmerman Tools
- Day 5: Memory analysis deep-dive
  - volatility ftw

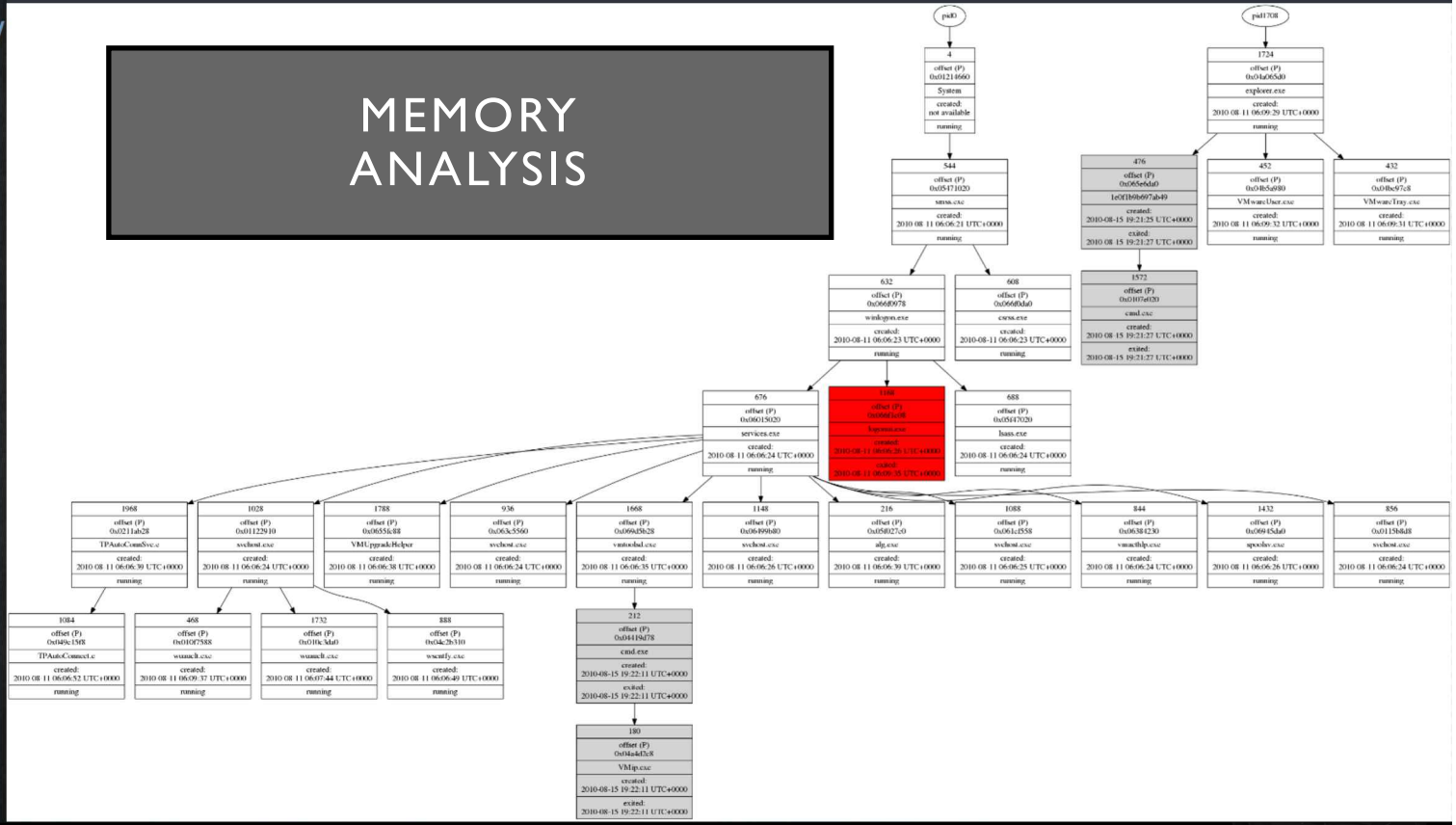

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
Windows Forensic Analysis
POSTER
You Can't Protect What You Don't Know About
digital-forensics.sans.org
Windows Time Rules
Windows Artifact Analysis: Evidence of...
File Download
Program Execution
Deleted File or File Knowledge
Network Activity/Physical Location
File/Folder Opening
Account Usage
External Device/USB Usage
Browser Usage

SANS
500

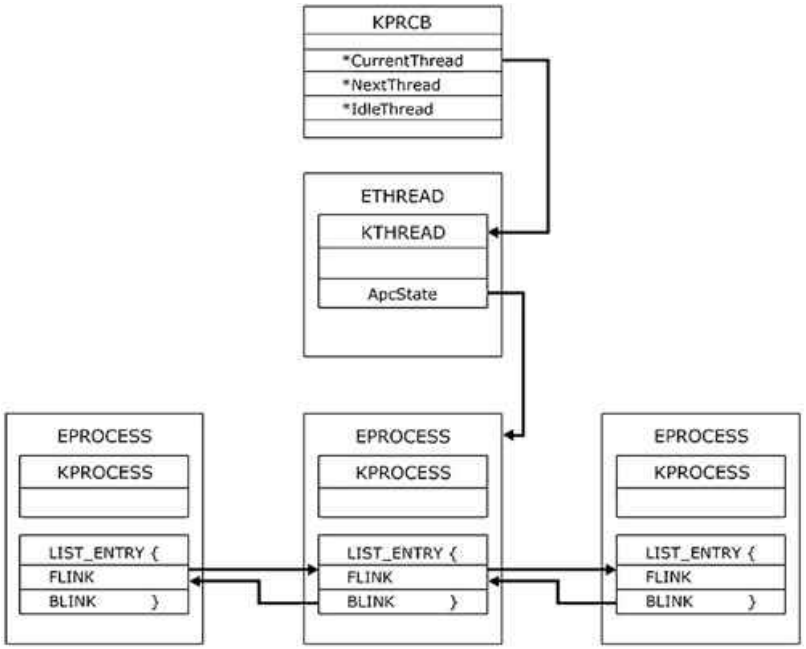
```
sansforensics@siftworkstation -> /m/h/N/h/i/black_energy
$ ls ..
black_energy       black_energy.mans.cache  black_energy.zip  kdbgscan.txt   memoryapt.img.zip  stuxnet.mans
black_energy.mans  black_energy.vmem        kdbg              memoryapt.img  stuxnet.img        stuxnet.zip
sansforensics@siftworkstation -> /m/h/N/h/i/black_energy
$ vol.py -f ../black_energy.vmem --profile=WinXPSP2x86 pstotal --output=dot --output-file=pstotal.dot
Volatility Foundation Volatility Framework 2.6
Outputting to: pstotal.dot
sansforensics@siftworkstation -> /m/h/N/h/
$ dot -Tpng pstotal.dot -o pstotal.png
sansforensics@siftworkstation -> /m/h/N/h/
$
```

pstotal.png

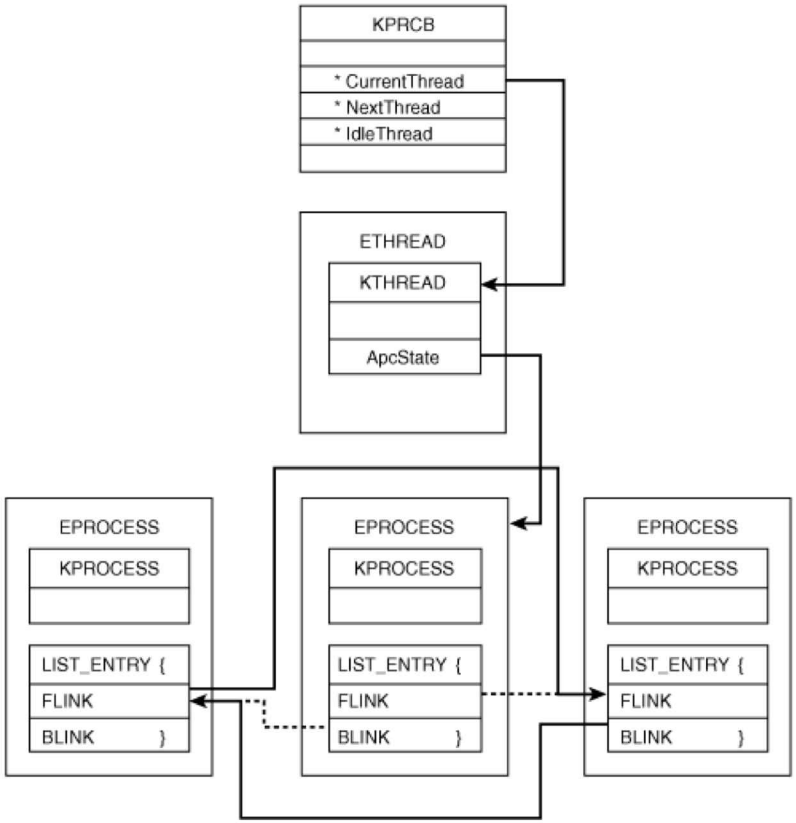
MEMORY ANALYSIS



PSLIST VS. PSSCAN



(Hoglund & Butler, 2005)



REVERSE ENGINEERING

Week 4

30:00

REVERSE ENGINEERING

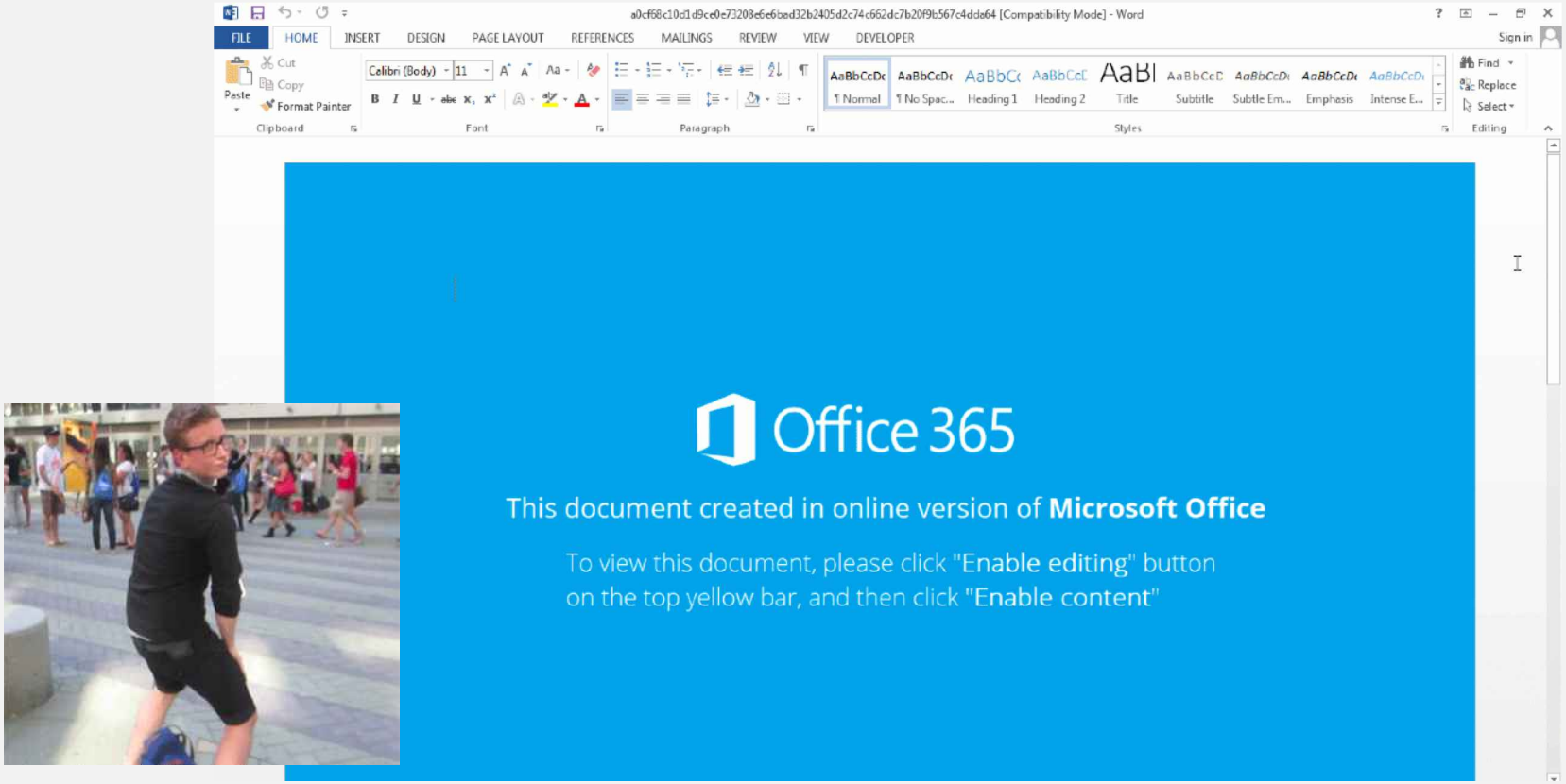
Week 4

- Day 1: PDF analysis
- Day 2: Office file analysis

- Day 3: Dynamic PE analysis
- Day 4: Static PE analysis

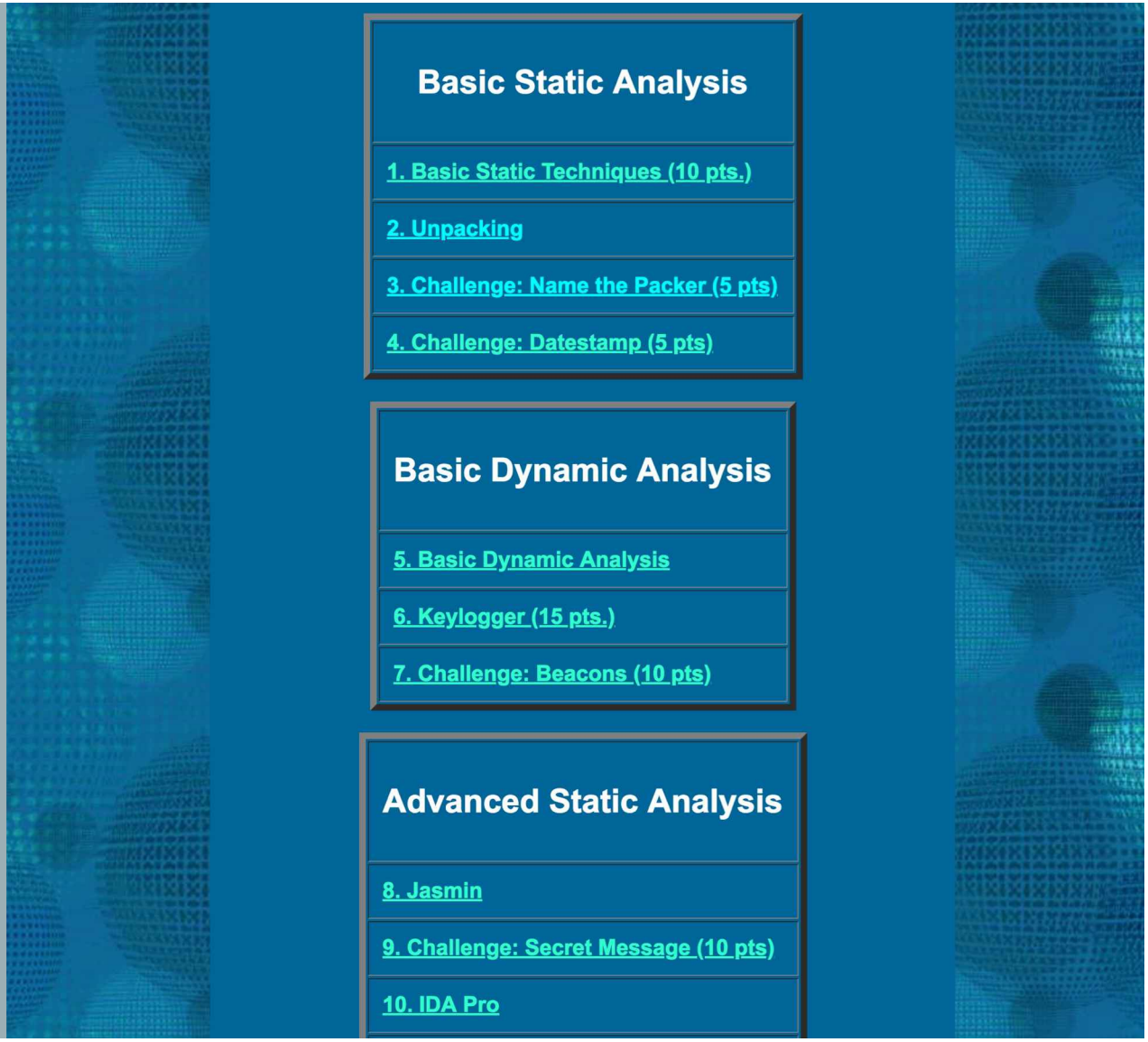
- Day 5: Sam's Malware Workshop

CARRIER FILE ANALYSIS



SAM'S MALWARE WORKSHOP

https://samsclass.info/126/126_DC_2017.shtml



INTEL & WORKING TICKETS

Week 5

35:00

INTEL & WORKING TICKETS

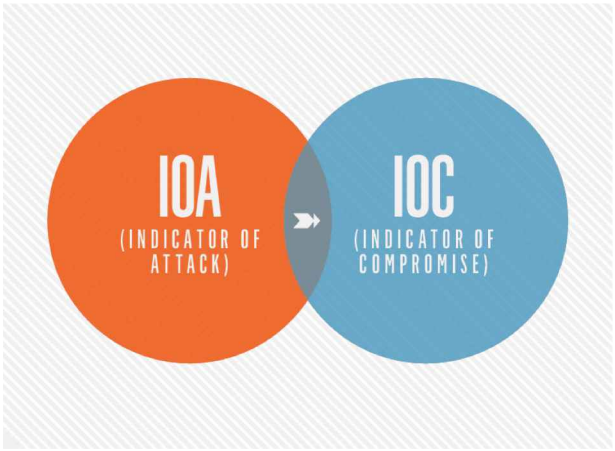
Week 5

- Day 1: Threat Hunting
- Day 2: Indicators of Compromise
- Day 3: Operationalizing OSINT
- Day 4: Working tickets
- Day 5: Review & Wrap-up

THREAT HUNTING

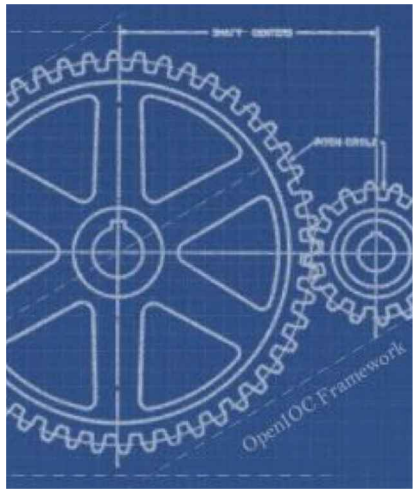
Finding what security tools ***don't***

What frameworks are YOU using?



yara

STIX™



IOCS

REINFORCEMENT

TABLETOPS

- Build muscle memory
- Optional or required?
- Time investment
  - Worth it!

QUIZZES

- Testing during or after
- Setup an LMS
  - Ex: Moodle
- Not as time intensive

QUESTIONS?

Ryan Chapman
@rj_chap

IR analyst. Malware hobbyist. PluralSight author. Comedy & BJJ chump.
github.com/rj-chap keybase.io/rj_chap
TnVsbGl1cyBpbiB2ZXJiYS4=