DFIR Technical

Autopsy for Analysis

How to create a new case in Autopsy? Add evidence item

1. Note the Different Data Sources: VM/Disk Image, Physical drive.
2. The Ingest modules to run against your Image.
3. The Execution takes time and Depends with the size of the Image 1TB server drives is hell of time.
4. Check The Autopsy Layout
5. Using the Filesearch
6. The Hash Database Lookup filters files with the MD5 hash values for files in the database
7. Timeline Analysis
8. The Communications User Interface
9. Options in Tools >Menu how to add hashsets of Malware/IOCS use MISP for illustration

Image Mounting

- **Use FTK imager to Mount image (Washer/Mantooth) on windows**

Nirsoft Utilities

- **Use FTK imager to Mount image (Washer/Mantooth) on windows**

Registry Examination

- HKEY_CURRENT_USER (HKCU): Stores data that is associated with the currently logged in user.
- HKEY_USERS (HKU): Stores information about all the user accounts on the host.
- HKEY_CLASSES_ROOT (HKCR): Stores information about file associations and object linking and embedding (OLE) registrations.
- HKEY_LOCAL_MACHINE (HKLM): Stores system-related information.
- HKEY_CURRENT_CONFIG (HKCC): Stores information about the current hardware profile.

Important to note:

1. The registry controls virtually every aspect of the system's configuration and operation. i.e. malicious applications may add up entries to registry keys to start up applications during booting.

2. It tracks much of the activity that is performed by users and applications on the host.i.e. USBstore activity HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

Event Logs

- Use this command to get the event logs on for windows: **eventvwr**
- N/B For event logs we need to understand types of windows logons.

Logon Types

1. Logon Type 2: Interactive. A user logged on to this computer. Event ID ()
2. Logon type 3: Network. A user or computer logged on to this computer from the network
3. Logon type 4: Batch. Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
4. Logon type 10: RemoteInteractive. A user logged on to this computer remotely using Terminal Services or Remote Desktop.

NB check logon types checklist

Sift Workstation

Getting started with sift

- ✓ Downlaod the (.ova) format from SANS Website.
- ✓ Import to VirtualBox
- ✓ Toolsets are on the cheat shits on the Desktop

Getting Evidence to sift.

- ✓ Copy directly from windows to VM or Download directly in the VM also check if USB is recognized in the VM.
- ✓ Copy downloaded image files to Cases folder in the Desktop

Disk Image Mounting

- ✓ Navigate to the cases folder.
- ✓ Elavate privileges by **sudo su** command
- ✓ ewfmount to mount it to **/mnt/ewf_mount/** folder (You will see the raw image)
- ✓ cd to **mnt/ewf_mount/** **ewfi** is the evidence file
- ✓ file ewfi shows that it's a windows file (NTFS/HFS/FAT)
- ✓ To unmount cd.. to /mnt/ folder then use **umount windows_mount/** umount ewf_mount/
- ✓ We can use a python script imageMouner.py to mount the image
  - imageMouner.py –e (mounts E01 files)

Creating a Timeline via Sift

- Using Log2timeline

Memory Analysis

- Using volatility and Rekall

Registry Examinations

Ripl.pl -r SAM/SYSTEM/SOFTWARE/SECURITY/NTUSER.DAT –f sam/software/security/system

We can output the result into a text file i.e. /cases/sam.txt

Other commands

ripl.pl –r SAM –f sam (Accounts and Login information)

ripl.pl –r SECURITY –f security

ripl.pl –r SYSTEM –f system

Shimcache Parser(Registry hive directory)

Extracts data from system hive files to show any executables, which might have been potentially run in the system, or initially touched. Good resource for potentially identifying malware.

ShimCache.py –i SYSTEM –bom

It shows last execution time and name of the executable.

Check Other 3rd Party Utilities in the bin directory

- cd /usr/bin/local/
- Conclusion just getting started: Check the Awesome cheat shits on the Desktop.

Mobile Forensics

- Mobile Phones are the Gold Mine/Holy Grail to digital forensic evidence
- **Call Directory Records (CDR) in Link Analysis**
- Link analysis summarizes rltnshp between different persons, shows patterns and volumes of communication.
- Using Sentinel Visualizer/UFED Analystics
- Mobile forensics tools such as Cellebrite:
- Decrypt Bootladers i.e. MTK Qualcom

Incidence response

Incidence response sample: Case of Business Email compromise, security Analysts/Forensic Analysts Approach in Analyzing a phishing Email.

Employees Report Phishing Emails

Security Awareness Training

How this impacts the business:

Phishing attacks expose the company to data breaches, which could result in legal issues, regulatory fines and reputational damage.

Information Security rule based guidance:

"Employees should report suspected phishing emails and refrain from opening emails from unknown sources."

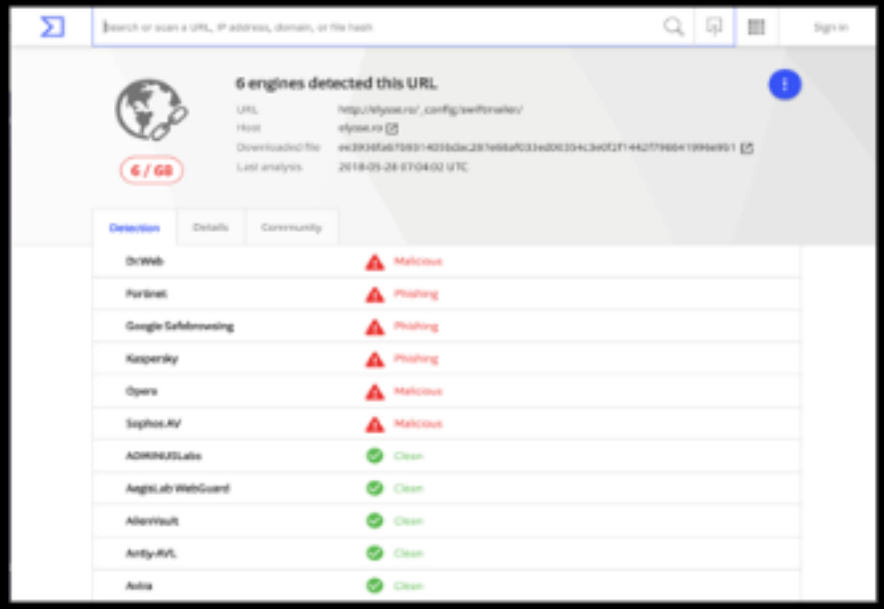
splunk> listen to your data

Investigating a Phishing Report

Reputation Check of URLs

VirusTotal

1. Extract URLs (from emails & attachments)
2. Check URL Reputation
3. Catch the results

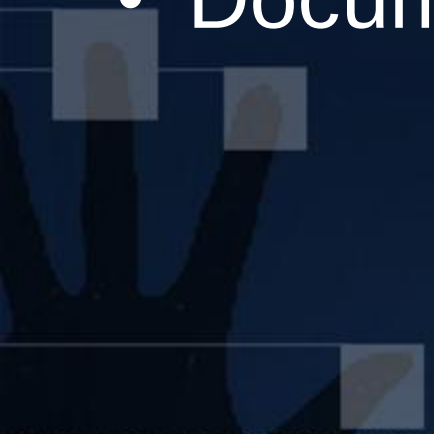


What will a Sec/Forensic Analyst Do?

- Extract Attachments
- Detonate in a malware Sandbox
- Catch the results
- Collect all IP and Domains including sender MTP
- Check IP and URL reputation in Talos/Virus Total

Summarize indicators of compromise(Threat Intell)

- Search for threat intel in your log data(Network Traffic, Proxy, Email filters & End point data sources)
- Identify Affected hosts and users
- Document.



Incidence responder will….

- Block IP at the firewall
- Block URL at the proxy
- Block Email domain at the spam filter.
- Block URL and IP and Hashes at the Endpoint security

Delete existing phishing email

Search all mailboxes /Multiple mailboxes and Validate

Malware Information Sharing Platform

- Allows one to create ingest and share IOC's and threat intelligence, Completely open source

Misp Functionalities

- It is offers flexible sharing groups
- Automatic correlation
- Free text import helper
- Event distribution and collaboration

Indicators of Compromise

Threat Intell ismore about attacker TTPs rather than just the IOC's

Below are some of the information to identify malicious behavior:

- IP's
- Domain names
- URL's
- File Hashes
- Registry Keys
- Mutex

IOC sample case I worked on:

Name	AD.exe
Item#	
Ext	.exe
Path	AD.exe
Physical Size(bytes)	2964138
Created	2017-09-22 10:22:08 EAT
Accessed	2017-09-22 10:22:08 EAT
Modified	2017-08-20 17:19:12 EAT
Changed	2017-09-22 10:22:08 EAT
MD-5 Hash	ca179760c4abff43cdc143f762ac04a7
Source file	/vol_vol4/ProgramData/AD.exe

Name	Lazagne.exe
Item#	
Ext	.exe
Path	/vol_vol4/Users/laZagne.exe
Physical Size(bytes)	5615061
Created	2017-09-22 10:44:05 EAT
Accessed	2017-09-22 10:44:05 EAT
Modified	2017-09-22 10:44:28 EAT
Changed	2017-09-22 10:44:28 EAT
MD-5 Hash	57e1438cdf432bf668272adb66197014
Source file	Users/Bunde/laZagne.exe

Virus Total

- We use the file hashes to pivot to Virus total and Payload security (Hybrid Analysis Platform)
- We use file hashes to check Reputation:
- Lazagne - **57e1438cdf432bf668272adb66197014**
- AD.exe - **ca179760c4abff43cdc143f762ac04a7**