Πανόπτης 2017

Διαχείριση συμβάντων-συλλογή-ανάλυση πληροφοριών:
Προτεινόμενα εργαλεία

Πχος (Μ) Σ. Παπαγεωργίου ΠΝ
spapageorgiou@mil.gr

Διαχείριση συμβάντων-συλλογή πληροφοριών:

- https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip
  - Συλλέγει μνήμη, registry και λαμβάνει ακριβές αντίγραφο ενός σκληρού δίσκου σε windows λειτουργικά.
  - Συλλέγει αντίστοιχες πληροφορίες σε Linux and MacOs.
  - Σύνδεσμος για να δημιουργήσουμε το δικό μας module
    - http://www.brimorlabsblog.com/2015_09_01_archive.html
- https://github.com/proneer/Tools/tree/master/FPLive_win

Συλλογή μνήμης (windows)

Winpmem

- https://github.com/google/rekall/releases/download/v1.5.1/winpmem-2.1.post4.exe

Dumpit

- http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

Fireeye Memoryze

- https://www.fireeye.com/services/freeware/memoryze.html

Fireeye Redline

https://www.fireeye.com/services/freeware/redline.html

Συλλογή μνήμης (Linux)

Lime

- https://github.com/504ensicslabs/lime

Ανάλυση μνήμης

Volatility (windows+linux)

- http://www.volatilityfoundation.org/#!25/c1f29

Fireeye redline (windows)

- https://www.fireeye.com/services/freeware/redline.html

Rekall (windows+linux)

- https://github.com/google/rekall/releases/tag/v1.5.0

Συλλογή της Registry

FTK Imager

- http://www.accessdata.com/support/product-downloads#

Windows_Live_Response

- https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip

Forecopy

- https://github.com/proneer/Tools/tree/master/forecopy

Ανάλυση της Registry

Regripper

- https://code.google.com/p/regripper/

Registryviewer

- http://www.accessdata.com/support/product-downloads#

Regviewer

- http://sourceforge.net/projects/regviewer/

Registry Browser

- https://lockandcode.com/software/registry_browser

Disk Forensics

Sleuthkit autopsy (windows version)

- http://www.sleuthkit.org/autopsy/download.php

FTK Imager

- http://www.accessdata.com/support/product-downloads#

Sleuthkit

- http://www.sleuthkit.org/sleuthkit/download.php

bulk_extractor

- https://github.com/simsong/bulk_extractor

Last activity view

- http://www.nirsoft.net/utils/computer_activity_view.html

χρονική ανάλυση

- https://github.com/log2timeline/plaso

Raw Disk Image to Virtual Machine

- VBoxManage convertfromraw <filename> <outputfile> [--format VDI|VMDK|VHD]

File system recovery forensics

Scalpel

- https://github.com/sleuthkit/scalpel

Foremost

- http://foremost.sourceforge.net/

Web Browser Forensics

Nirsoft forensics tools

- http://www.nirsoft.net/utils/#browser_tools

Browser History Viewer

- https://www.foxtonforensics.com/browser-history-viewer/download

Email headers
ανάλυση

- https://toolbox.googleapps.com/apps/messageheader/analyzeheader

Malware forensics

remnux

- https://remnux.org/#distro

Ida pro

- https://www.hex-rays.com/products/ida/support/download_freeware.shtml

Immunity debugger

- https://www.immunityinc.com/products/debugger/

Olly debugger

- http://www.ollydbg.de/version2.html

Malware forensics

sysinternals tools

- https://live.sysinternals.com/

buatapa

- http://www.brimorlabsblog.com/2015/08/publicly-announcing-buatapa.html

Didier Stevens virus total tools

- https://blog.didierstevens.com/programs/virustotal-tools/

Didier Stevens Authenticode tools

- https://blog.didierstevens.com/programs/authenticode-tools/

National Software Reference Library

- http://www.nsrl.nist.gov/Downloads.htm#isos
- http://rjhansen.github.io/nsrllookup/

Malware forensics

Cuckoo

- **http://www.cuckoosandbox.org/**

Pyew

- https://github.com/joxeankoret/pyew

Online tools

- https://malwr.com/submission/

Network forensics

Tcpdump

- http://www.tcpdump.org/#latest-release

Wireshark

- http://www.wireshark.org/download.html

Xplico

- http://www.xplico.org/download
- http://www.forensicswiki.org/wiki/Network_forensics

Command-Line Log Analysis

- https://pastebin.com/WEDwpcz9
- https://www.youtube.com/watch?v=Sb747MCVYB8

Mobile forensics

mobile analysis framework - live cd

- Androl4b (https://github.com/sh4hin/Androl4b)
  - https://github.com/sh4hin/MobileApp-Pentest-Cheatsheet
- Santoku (https://santoku-linux.com/)
- MobSF (https://github.com/ajinabraham/Mobile-Security-Framework-MobSF)

Live forensics CD’s

SIFT

- http://digital-forensics.sans.org/community/downloads

Kali

- http://www.kali.org/downloads/

Santoku

- https://viaforensics.com/resources/tools/santoku/

CAINE

- http://www.caine-live.net/page5/page5.html

links

- http://en.wikipedia.org/wiki/List_of_digital_forensics_tools
- https://uk.sans.org/posters/windows_artifact_analysis.pdf
- https://digital-forensics.sans.org/media/Poster_SIFT_REMnux_2016_FINAL.pdf
- https://digital-forensics.sans.org/media/rekall-memory-forensics-cheatsheet.pdf
- https://digital-forensics.sans.org/media/Poster-2015-Memory-Forensics2.pdf
- https://digital-forensics.sans.org/media/DFIR-Smartphone-Forensics-Poster.pdf
- https://digital-forensics.sans.org/media/Poster_2016_Find_Evil.pdf
- https://digital-forensics.sans.org/media/evidence_collection_cheat_sheet.pdf
- https://digital-forensics.sans.org/media/linux-shell-survival-guide.pdf
- https://digital-forensics.sans.org/media/windows_to_unix_cheatsheet.pdf
- https://digital-forensics.sans.org/media/log2timeline_cheatsheet.pdf
- https://digital-forensics.sans.org/media/hex_file_and_regex_cheat_sheet.pdf
- https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf
- https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf
- http://dfir.to/Find-Evil-Poster
- https://pen-testing.sans.org/retrieve/windows-cheat-sheet.pdf
- https://pen-testing.sans.org/retrieve/linux-cheat-sheet.pdf
- https://digital-forensics.sans.org/media/memory-forensics-cheat-sheet.pdf
- http://cryptome.org/isp-spy/access-data-spy1.pdf
- http://crucialsecurityblog.harris.com/2011/03/14/typedurls-part-1/
- http://www.sleuthkit.org/autopsy/docs/quic
- http://digital-forensics.sans.org/media/log2timeline_cheatsheet.pdfk/index.html
- http://digital-forensics.sans.org/media/sift_cheat_sheet.pdf
- http://www.nirsoft.net/utils/