CHFI

Quotes:

- تعداد آدم های خوب و بد دنیا یکسان است
- همیشه در forensic باید از ساده ترین حالت ممکن شروع کرد.
- وکیل سایبری

- Emkei.cz
- Teracopy
- Dendroid
- sysmon

Module 0: Introduction to Computer Forensic

CERT

FOR 500 -> windows forensic(registry,mru,...)

FOR 572 -> network forensic(syslog,netflow,web proxy)

FOR 526 -> memory forensic(files,ransomware,malware)

FOR 610 -> malware analysis

FOR 585 -> mobile forensic

Job Title

Computer Forensic Analyst

Computer Forensic Tech

Digital Forensic Examiner

Module 1: Computer Forensic in Today's World

Forensic Science: process(collect-analysis-select-research)

Forensic -> Computer Forensic -> select digital evidence

Evaluation of Forensic

1872 - 1972: study of fingerprint

1972 - 1982: blood grouping(A - B - O)

1982(FBI Lab)

2000(Lab computer Forensic)

Cybrer Crime

Activity -> crime -> add/edit/del data

For example:

Phishing, dos, ddos, sqli

Cyber crime:1-computer as a tools 2-computer as a target

Module 2: Computer Forensic Investigator

Step 1: obtain search warrant,(agreement)

Step 2: evaluate and safety scene

Step 3: collect evidence -> all evidence about crime collect(arp table, netstat)

Step 4: acquire and analysis evidence -> copy of evidence and analysis

Step 5: testify as an expert witness

Definition of Digital Evidence

media(h.d.d) -> data(process) -> information -> evidence

Type of Evidence

1- graphic file

2- security log

3- email

X- any digital save

Type of Digital Evidence

1- permanent data

2- volatile data

2-1 transit -> network connections

2-1 fragile -> last access file

3-1 archival -> long time

3-3 backup -> less time

Digital Evidence Examination Process

1- Evidence Assessment

1-1 type(network log, web server log, client log)

2-1 storage(das, nas, san)

2- Evidence Acquisition

Image: 1-backup 2-raw

Raw image: 1-slack space 2-unused cluster

3- Evidence preservation

First responder(isolating scene)

First responder toolkit: lock open, …

4- Evidence Examination and analysis

H.d.d: 1-logical(file system) 2-physical(sector)

5- Evidence Documentation and Reporting

Module 3: Understanding Hard Disk and File System

Hard Disk Component

cluster= sectors

cluster -> software -> fs -> os

cluster(larger)->files(small)->slack space(large)

Type of Hard Disk

1- USB

2- SATA

3- Fiber Channel

File System

1- FAT

2- NTFS

3- ReFS

NTFS

Tables: $mft(master file table) -> file & folder info, $logfile(transaction log file)

MFT= ID - Name - Size - Addr

Del file -> del id

Del file from $MFT != del from $logfile

$bitmap-> unused cluster

$MFT Header

File:

0000-> deleted

0001->exist

Folder:

0002->exist

0003->deleted

Deleting NTFS File

When delete file really just move to other address(15,20% per Disk)

Recovery

Work with 15%

SSD

Disable trim(enable by default)

trim-> os command send to ssd(delete)

Disable trim: exec command-> fsutil behavior query DisableDeletingNotify

Enable trim: exec command-> fsutil behavior query DisableDeletingNotify 1

Recovery

EASEUS Data Recovery

Linux File System

Extended File System 2,3,4(crash handling support)

Block-> sectors

Block Group-> Blocks

Inode tables-> file info(mac, …)

deleting-> find -inum <inode>

Apple File System

1- HFS

2- HFST

Sun Solaris

1- endless scalability

2- drive pooling

CD and DVD File System

1- CDFS

2- UDF

Module 4: Data Acquisition and Duplication

copy of original evidence(raw image, bit stream)

Data Acquisition Method

1- disk to image

2- disk to disk

Windows Data Acquisition

1- FTK Imager

Linux Data Acquisition

1- fdisk -l

2- dd if=/dev/sdx of=/sdx.img

3- md5sum /sdx.img > chfi.txt

4- mount [-t for NTFS] /sdx.img /mnt

5-for memory dump: dd if=/dev/mem of=/mem

Wipe

Dd tools(win,lin) -> dd if=/dev/zero of=/dev/sdx

Module 5: Defeating anti-forensic techniques

copy of original evidence(raw image, bit stream)

Anti-forensic

Increase Avoiding detection(Hard)

Increase the examiners crime(Time)

Increase Disrupting information collection(Disrupting)

Anti-forensic techniques

1- hiding data: encryption, steganography, slack space

2- wiping data

3- obfuscation data

4- anonymous identities(tor)

Attacker -> tor -> vpn -> ssh tunnel -> rdp -> victim

Recovery Deleted File and Partition

1- partition recovery

2- file recovery

Windows Recovery

1- active(file, partition)

2- ontrack

3- photorec

rlab.ru(r.server)

Linux Recovery

1- testdisk

2- photorec

3- rlinux

MAC Recovery

1- steller phoneix

Module 6: Windows Forensic

1- default command

2- registry analysis

3- browser forensic

4- event log

5- tools

Default Command

1- data /t & time /t

2- quser(all client info)

3- net file(client file used)

4- net accounts(show user register properties)

5- net user <username>(about username)

6- netstat -anob(connective and files)

7-dir /attd /b

8- tasklist /m

9-doskey /history

powershell->powerforensic v2

Powerforensic:

1-install-module -name powe…..

2-import-module powe….

3-Get-ForensicNetworkList->network interfaces

4-Get-ForensicFileRecord -path a.exe

5-Get-Forensicmftslack -path a.exe

MRU(Registry Analysis)

Important key in reg about(file, command, software)

1-regedit

2-HKEY-CURRENT-USER(HKCU)

3-HKEY-LOCAL-MACHINE(HKLM)

4-Hives->key->value->type->data

For example:

1-MRU->last command user
type->HKCU\software\microsoft\windows\current_version\explorer\runmru

2-MRU->open save
file->HKCU\software\microsoft\windows\current_version\explorer\config32\opensaveIMRU

3-open application and executable
file->HKCU\software\microsoft\windows\current_version\explorer\userassist

4-remote desktop connection->HKCU\software\microsoft\terminal server client\servers

5-usb devices connected->HKLM\system\currentcontrol\set\enum\usbstor

Browser Forensic

\App Data\Local\mozila\profiles

\App Data\roaming\mozila\profiles

Tools: 1-Browser history examiner, 2-infornito(cookie,cache,history)

Event Log

Event viewer(evtx extension)

Event id:

4624 -> security login

4625 -> failed login

4628 -> A member was added

4629 -> a member was removed

4634 -> logoff

By default -> logon, logoff

For enable -> group policy -> auditing -> enable other view

Windows setting -> security setting -> local policy -> audit log

- Audit object access -> user activity -> by folder enable -> folder properties -> security -> advance -> auditing

Logon Type

2-13

2- interactive logon

3- network(smb)

8- network cleartext(telnet)

10- remote desktop

Tools:

1- Logparser.exe -i(input):EVT(type) -o(output):datagrid, chart, … “select * from security.evtx where eventid=4625”

Logparser.exe -i(input):EVT(type) -o(output):datagrid, chart, … file:brute_patter.sql

2- Encase

3- FTK->access data

4- osforensic

5- autopsy

6- helix

7- deft

OSForensic

Manage case -> new case

1- Delete file search

2- Mismatch file search(extension != header)

3- User activity(all mru, search log, connection)

4- Password(SAM)

5- Register view

Module 7: Linux Forensic

/var/log

- audit.log(ssh,...)

  Cat audit.log | grep -A 2 -B2 “192.168.1.100”
- kern.log(kernel module)
- boot.log(grub, …)
- dmesg(driver, …)

Default Command

1- find /root -size +1m

2- find /root -mmin(modify) -100

3- find /root -atime(access) -2

4- ls -li

5- w, who(client connected)

6- lastlog

7- lsof -i (open files) -p <process_id>

8-netstat -ltpe(program, port)

RAW Image

Dd -> osforensic, encase, autopsy

Module 8: Network Forensic

Ids -> sensor -> alert(by attack)

Soc -> siem -> sensor

nids(network)->not discover attack in host

hids(host) -> decrypt connection in host -> ossec

Network Forensic Evidence

1-syslog: protocol, service

2- full packet capture(layer 2-layer 7)->.pcap(wireshark, netminer, moloch, netwitness)

3- netflow(layer 2-layer 4), ipfix, silk

Network Attack

1-port scan

2-banner grabbing

3- arp spoofing

4- ip spoofing

5- dos

6- ddos

Wireshark Filter

Arp spoofing-> arp duplicate -> in wireshark -> arp.duplicate.address -> in switch -> sh mac address-table | include <mac>

Dos -> in wireshark -> statistics -> io graph

Read file by protocol -> in wireshark -> file -> export -> http

Https export key in browser -> in wireshark -> edit -> prefrences

Traffic capture by time -> in wireshark ->capture-> output

Module 9: Web Server Forensic

1- Apache -> 70 %

2- Iis -> 20%

3- Nginx

..

Web Attack

1-sqli -> union select

2-xss -> <script>

3- command injection -> ;ls

4- lfi -> ../../../etc/passwd

5- xxe -> <entity>

Web Server Log Format

1- w3c(microsoft)

2- ncsa

Apache Log Forensic

/var/log/apache2

Access.log

Ip | time | path | msg | agent

Tools:

1- scalp -> python sculp.py -l access.log -f default-filter.xml -o <output> --html

2- logparser.exe -i:IISw3c -o:datagrid file:sqli.sql

%SYSTEMDRIVE%\inetpublogs\logfile\w3c

Module 10: Database Forensic

1-mysql

2-mssql

3-oracle

..

MySQL

By default-> all log not saved

For enable:

/etc/mysql/my.cnf

general_log=on

general_log_file=query.log

Restart services

Database info:

/var/lib/mysql->DB_NAME/*.frm(table), *.opt(table) or *.* may be shell

MSSQL

Master data file(.mdf)

Transaction log file(.ldf)-> all log -> by default enable

apexSQL log(viewer)

Oracle

Redo log file(log)->/var/opt/oracle, /log

1-Log miner

2-administration->activity monitor->login attempts

Module 11: Cloud Forensic

Cloud layer:

1-hardware

2-virtualization, hypervisor(esxi, citrix, hyper-v)

3-network-storage

4-os

5-data

6-application

Iaas: infrastructure as a service

Paas: platform as a service

Saas: software as a service

Seaas: security as a service

Paas: layer 5,6

Iaas: layer 3,4

Solutions:

1-openstack

2-vmware

3-ibm

Module 12: Malware Analysis

Behavioral Analysis Techniques

1-process monitoring

In windows-> winlogon.exe, wininit.exe(pid=680 and pid<1000), lsass.exe(pid=690 and pid<1000 and unique)

Tools:

1- process explorer

2- procmon

3- process hacker

File System and Registry Monitor

regshot->1sht->2sht->compare 1,2

procmon->running>10 min->export csv->import in prodot(draw diagram)

Network Monitoring

Use malware in honeypot

inetsim->Dns fake

Dns flask(ip1,ip2)

Module 13: Malware Analysis

Stuxnet Analysis

Volatility

1-volatility imageinfo -f stux.vmem

2-volatility plist -f stux.vmem

3-volatility ptree -f stux.vmem

4-volatility connection -f stux.vmem

5-volatility netscan -f stux.vmem

6-volatility sockets -f stux.vmem

lsass.exe->udp->500,4500(LISTEN)

7-volatility dlllist -p <pid>

56->normal

dll->lib->interactive(os->software,software->software)

Unlink dll-> memory allocation without data

7-volatility malfind -f stux.vmem

Vad(virtual address descriptor) tag->exec in memory->mz in header

7-volatility cmdscan -f stux.vmem --dump-dir=<dir>

8-volatility console -f stux.vmem --dump-dir=<dir>

9-volatility iehistory -f stux.vmem

Module 14: Investigating Email Crime

1-spanning

2-email bombing

3-phishing->fake mail

Mail server

postfix,sendmail,qmail,exchange(secure,forensic),mdaemon,imail)

Mail client

outlook,kmail,thunderbrid

Email message

Header,body,attachment

In gmail->show original->received by(mail server ip),received path(show from),received(sender mail server ip),received-spf(client-ip)

Tools:

1-paraben(email examiner, email network examiner)

2-rmail

3-email detective

Module 15: Mobile Forensic

1- SIM Card

me(mobile equipment)->bts1,bts2,...->bsc->msc(hlr,vlr,eir,auc(auth))

imsi=mac address

sim(subscriber identity module)->64kb<X<512kb

File system

mf(master file)->df->ef

EF

1-msisdn->subscriber phone number

2-lnd->last number dial

3-loci->location information(bts)

4-adn->connect

5-sms

6-lai(location area identity(nead bts info))

Tools:

1-Network cell info lite

2-sim card seizure->generate investigate report

Read and write tools->sy-386

2- OS

Tools:

1- osforensic

2- oxygen

3-mobedit

4-ufed

5-ftk

Android <=7 -> sd card->explorer->attach to mobile->boot with recovery mode

Module 16: Investigative Report

1- SIM Card

1-policy and procedure development(law)

2-evidence assessment

3-evidence acquisition

4-evidence examination(encase,ftk,osforensic)

5-documentation and report

For example:

Subject: case brief

Object

Computer type

Operating system

Offence

Summary:

Raw image(hard,ram)

osforensic(analysis)

effect(size,content,destination info)

Documentation:

Mru

Event viewer

Memory dump

Resource

- noorasec.com