

CFCS

Unit 1

Computer Forensics

involves presentation, identification, extraction and documentation of computer evidence stored as data or magnetically encoded information

Computer Forensics

- Collection, preservation, analysis and presentation of computer related evidence
- Process of examining evidence computer media for evidence
- Which can be useful in criminal cases, civil disputes etc.

Data recovery - To retrieve lost data

Types of crimes that can be done using computers

- 1) Hacking: gaining unauth. access to another person's individual database or network where private information stored
- 2) Piracy: when an individual distributes copyrighted material without gaining permission from the original owner.
- 3) Cyber Stalking / Harassment: An individual using the Internet to stalk a victim or bully / harass them using fake accounts and a large array of media
- 4) Identity theft: Involves an individual gaining access to the victim's SSN, Bank account info, etc. Uses information to spend money on their own or to do fraud transfers
- 5) Phishing: when an individual sends fraud mails claiming to be a legit company / institution to gain access to sensitive info about the victim. Often done through links / websites.
- 6) Ransomware
- 7) Credit Card Fraud

Computer can be target
target of crime

Instrument of crime

Container (depository) of crime

Computer Forensic expert

- To recover, analyse and present evidence understandable by court of law

Steps to identify and retrieve

- ① Protect ~~sub~~ target computer during examination from damage, alteration, & virus infection.
- ② Discover all files on subject system: normal files, deleted, hidden, password protected etc.
- ③ Recover all files relevant to the scope of investigation
- ④ Preserve Access and analyse content of files
- ⑤ Document relevant instances
- ⑥ Provide advice / consultation

who can use Computer Forensic Evidence

- ① Criminal Prosecutors - for crimes - homicide, fraud, etc
- ② Civil litigation - personal / business records
- ③ Corporations hire comp forensic to find evidence
- ④ Law enforcement officials - assistance - pre-search warrant
- ⑤ Individuals sometimes hire

Employer Safeguard Program

- Employer must satisfy critical info
- Data can be damaged / misused by individual if he/she is discontent / unhappy

Before employee informed of his termination, a CFA must be appointed to create duplicate of data in order to safeguard the employer from the employee deleting essential data from system.

- Can be used to prove false claims against employee

★ Military Computer Forensic Technology

Real time tracking difficult - info intentionally hidden, destroyed, modified & to evade discovery

CFX-2000 (Computer Forensic Experiment 2000)

Hypothesis - possible to accurately determine motives, intents, targets, sophistication, identity and location of cyber criminals / terrorists by deploying an integrated forensic analysis framework.

- Required simulation of a realistic, complex cyber crime scenario as well as use of Cyber Forensic Tools.

Synthesizing Information for forensic Investigation (SI-FI) environment supports collection, examination and analysis processes used in an investigation

Uses digital evidence bags which are secure and tamperproof containers to store digital evidence

Computer evidence processing procedures mirror image

- 1) Preserve Evidence: Fragile (tattered easily). SafeBack-backups.
 - Trojan Horse: An app pretending to be something else.
 - ability to avoid destructive programs.
 - Computer Forensic Documentation: To present findings.
 - File Slack: ~~unoccupied~~ space between the end of file and end of disk cluster. Possible site for previously created data and relevant evidence.
 - Data hiding techniques: Possible to hide data within (Image, Audio, video) files (STEGANOGRAPHY) or hide entire hard disk drive partitions. Must look out for.
 - E-Commerce Investigations: 'Net Threat Analyzer' can be used to view Internet browsing data and email activity.
 - Text Search Technique: used tools - to find strings of text in files, slack space, unallocated file space etc.
 - Fuzzy logic tools.
- 2) Disk Structure: Understanding of how various disk structures work, how evidence can be found within them.
 - How to modify structure and hide data in secret places.
- 3) Data Encryption / Decryption: Must be familiar with - to crack.
- 4) Matching Diskette to a comp: No tools that make possible to tie a diskette to a computer used to create/edit files.
- 5) Data Compression: How can used to ~~disguise~~ hide sensitive data.
- 6) Erased / Deleted Files
- 7) Internet Abuse Identification: ~~?~~ Identify how ~~are~~ a target computer has been used ~~to~~ on the internet.
- 8) Boot Process / Memory Resident Programs: How OS can be used to ~~destroy~~ data.

↳ Chain of Custody
Chain of Command

★ Business Computer Forensic Technology

- Remote monitoring of Target Computers
 - DIRT (Data Interception by Remote Transmission)
 - Powerful tool- allows stealth monitoring of activity on one or more comp. remotely.
 - Allows for remote seizure of (secure data)
- Creating Trackable Electronic documents.
 - BAIT (Binary Audit Identification Transfer)
 - intrusion detection sys. allows for creation of trackable electronic documents.
 - identifies unauth. users / intruders accessing tracked doc.
 - allows to have CoC and CoCo of all those who possess doc.

~~PC~~ PC Phone Home

Available Forensic Services

- Lost Password rec
- Lost File rec
- Decryption / Encryption
- Email Supervision
- Network monitoring
- HoneyPot sting
- Location / Identity of Unauth. & low users
- Theft recovery

Data Recovery

- Process of recovering lost (deleted / hidden) data through specific procedures / techniques and return it to its intact form.

Data Backup and Recovery

- Obstacles

Backup Window - Timed during non production period.

- When Network bandwidth / CPU usage low.

Bandwidth (Network) - Need to handle large amount of data transfer over short time period.

System Throughput - amount of data that can be received and written to a storage medium.

Offline Backup - affects data accessibility. This req. extremely high speed, cont. parallel backup of the raw image of data.

Live Backup: allows data access during backup process but affects performance.

Mirror Backup: Copies exactly how the data currently is stored. Does not protect against user error and duplication of bad data.

Requirements

- ① High Speed
- ② Remote host recovery sites - resumption of data access
- ③ Decoupling of data from storage needed
- ④ Part of primary storage - set aside - fast nonrandom restoration of critical data

- Computer data must be Authentic
- A²C² - Authentic, Accurate, Complete, Convincing
- Fragile / volatile / hidden / lost

Legal Tests

- Real ~~Test~~ Evidence: Any evidence that speaks for itself.
Eg. Audit logs ~~for~~ with proof that it can be free from contamination
- Testimonial Evidence: Any evidence supplied by a witness. As long as witness reliable, Testimonial = Real.
- Hearsay: Evidence by a person who was not a witness. This is inadmissible and must be avoided.

Rules of evidence

- 1) Admissible: Must be able to use in court
- 2) Authentic: Evidence relates to incident
- 3) Complete: Not show only one perspective of event
- 4) Reliable: Collection and analysis procedures must be robust.
- 5) Belivable: The evidence to be presented must be understandable by the jury.

Must be collected with respect to Federal Rules of Evidence

CFE performs following services

- 1) Data Seizure: F.R.E lets a party on their representation inspect and copy designated documents or data that may contain evidence
- 2) Data Duplication and Preservation: When one party seizes data
 - i) Data must not be altered
 - ii) Must not hinder normal work flow of other party

Fast data duplication. Exact duplicate needed. Experts work on duplicate data, integrity of original data maintained.

- 3) Data Recovery: Self understandable
- 4) Document Searches: Text based Search. Self understanding
- 5) Media conversion: Data on old unreadable devices needed. Transform from one file format to another.
- 6) Expert witness Services: Must be able to explain complex processes in layman's terms. Help judges/jury to know how process works and how is it relevant to current situation
- 7) Computer Evidence Service options: Standard, On Site, Emergency, Priority, Weekend
- 8) Miscellaneous Services
Analysis / Seizure, Fast turnaround time

Unit 2

Why collect evidence?

- 1) Future Prevention
- 2) Responsibility

Collection Options

- Pull system off network:- ~~may~~ may have less evidence, or worse, dead man's switch is used (wipe data if offline)
- Leave online monitor intruder:- accidental alert to intruder, he will wipe his trails / evidence.

Volatile Evidence

- Order of Volatility: The order in which data can be destroyed / manipulated ~~order~~ in decreasing order.

- 1) Register
- 2) Routing table
- 3) Process table
- 4) Main Memory
- 5) Temp file system
- 6) Secondary memory
- 7) Network topology

★ Collection Through

- Logs and logging: System logging program to keep track of messages and logs from programs
- Monitoring: unusual activity detect

★ Collection Methods

Freezing the Scene

- Snapshot of sys. in compromised state. Collect data in removable non volatile media
- All data must have crypto info digest - compared to original for verification

Honeypotting

- Creating a replica system - luring attacker into further monitor
- misleading info - attacker's response - determine move of attacker

★ Artifacts

- Something left behind by the attacker (code frags, trojans, sniffer log files). Never attempt to analyze these. make sure effects are controlled

Chain of Custody

Detailed list of what has been done to original copies of data once they were collected

- 1) Analysis - extract information once data has been collected
- 2) Time - create a timeline, deconstruct event sequence, never change time on affected system
- 3) Analysis of Back-Up - Dedicate host, Secure, clean and isolated from any network. What you do is repeatable and always gives same results
- 4) Reconstructing the attack: Self explanatory
- 5) Searching and Seizing

Guidelines

- ① Be Impartial - no assumptions
- ② Media must be sterilized before each use
- ③ A true image (bit stream) must be used for analysis
- ④ Integrity of original media must be maintained

Evidence Seizure

- ① Preparation
- ② Snapshot
- ③ Transport
- ④ Examine

Duplication of data and preservation

- After evidence secured, must make complete bit stream backup of all computer data before processing
- Bit Stream backup > Standard Backup, copy every bit of data on a storage device. Two such copies must be made
- Processing done on one of the backup copies

SafeBack

- Law enforcement Standard, used by numerous government intel agencies, military etc
- Copies and preserves all data
- Circumvents attempts made to hide data in bad clusters and in sectors with invalid CRC's.

SnapBack

- Another bit stream backup program
- Prices 8 100's dollars more than SafeBack
- Error checking in every phase of evidence backup and restoration process.
- Floppy diskettes - imaged - using DOS DISKCOPY. Recommended version MS DOS ver 6.22

Comp eze evidence processing steps

- Shut down computer:
- Document hardware config of system - label component/wire
- Transport to secure location
- Make bit stream backups of hard disks and floppy
- Math. authenticate data: 32-bit Math process used
- Document system date and time: timeline tracking
- List key search words
- Win swap file use
- File slack evaluate
- Unallocated space

Unit 3

Learn Hacking

- Assess security of own's system, find vulnerabilities and fix vulnerabilities.

Hacker

Is an individual who tinkers with systems (software / hardware).

Someone who maliciously breaks into systems for personal gain.

~~Ethical~~ Ethical Hacking

Science of testing computers / networks for security vulnerabilities and fixing them before hackers get a chance.

Penetration testing.

Ethical Hackers possess skills, tools and mindset of a hacker but are trustworthy.

Features

- It is legal. Same tools, tricks and techniques.
- Performed wot target permission
- Discover vulnerabilities
- Overall risk management
- Ensure vendor's claims about products are true

Non ~~technical~~ technical attacks

- Involve manipulating people
- Social engineering:- the process of exploiting trust of humans to gain access to sensitive information for wrong purposes
- Can break into buildings and rooms / areas containing sensitive information
- Dumpster diving:- Searching trash / dumpsters for passwords, network diagrams, intellectual property etc.

Network Infrastructure attacks

- Connecting into network through Firewall using rogue modem
- Exploiting weakness in transport mechanisms (TCP/IP, NetB)
- Flooding network with too many requests, creating a 'DoS' for legit request
- Installing network analyzer on network, reveal confidential info in plain text
- Piggybacking onto a network through an insecure 802.11b wireless config.

OS attack

Occasionally, secure OS are hacked. Novell NetWare and flavors of BSD UNIX

Preferred OS are Windows / Linux, widely used / better known vulnerabilities

Examples

- Exploiting specific Protocol info
- Built-in auth sys are hacked
- Breaking file sys directory
- Cracking passwords and encryption sys

Application and other specialised attacks

Ethical Hacking Commandments

- Work Ethically: high morals and principles, must support goals
- Respecting Privacy - All info must be kept private.
- Not crashing systems: Poor planning, not reading docs, understanding usage / problem. Create Dos connection condition on sys x x.

★ The Ethical Hacking Process

1 - Formulating Plan

- Sys to be tested
- tools needed
- Procedures Followed
- Benefits gained
- Risk assessment
- Knowledge requirements / timing requirements

2 - Tools details

- Adequate documentation
- Updates / Support when needed
- High level report generation
- Examples on how vulnerabilities can be found & fixed.

3 - Executing the plan

■ Quiet and private. Use Pretty Good Privacy

Gain as much info as possible about organization and Systems

- 1) Search org name, comp and network names and IP names.
- 2) Narrow scope, target specific system
- 3) Perform scans and detailed analysis
- 4) Perform attacks

3 - Evaluating results

Hackers Mindset

* Types

- 1) Script Kiddies - novice / beginners. Free material available on Internet use do. No knowledge on how to - leave fingerprints everywhere.
- 2) Intermediate hackers - halfway elite hackers. Know enough to cause serious problems. ~~also~~ have adequate knowledge on how things work. given time can be elites
- 3) Elite hackers - Skilled hackers. People who write many of the hacking tools. Can break into systems (cover their tracks). Not as plentiful as script kiddies.

Cyberterrorists attack govt. or public infrastructures (power grids / ~~air~~ air traffic control). Crash sys. Steal classified govt. information

* Easier for hacker because

- Inc. use of Internet connectivity
- Anonymity provisions (VPN)
- Inc. availability of hacking tools
- Computer Savvy kids (US)
- Not managing systems properly (Crazy bishes)
- Complexity of sys. difficult to track issues

* How to maintain anonymity

- Borrowed / Stolen dial-up accounts
- Public computers
- Proxy servers
- Disposable email acc.
- Zombies - Unsecured computers at an organization

Developing Ethical Hacking Plan

- * Getting Plan Approved - Self explanatory. use points from Ethical Hacking Process and explain.
- * Establish Goals
 - Prep for accepted security framework of ISO 17799 / Security Seal eg SysTrust or WebTrust
 - Meeting Federal regulations
 - Information to be protected
 - ~~Attacker~~ Schedule your tasks
 - Documentation

~~Basic~~ Basically make a damn checklist.
- * Determine Systems to hack
 - which are critical / vulnerable. ? Start → vulnerable
 - Eg
 - Firewalls
 - Network Infrastructure
 - E-mail Servers
 - Mobile devices
- * Testing Standards
 - when tests are performed
 - what tests are performed

Imp Team : War dialing: Auto dial many phone no.'s, usually to find weak spots in tech. security.

 - Blind vs knowledge based assessments
 - Have some knowledge of systems before testing
 - Location : where should they be run from
 - ~~whether~~ whether from outside or inside, cover all bases