Unit-3

Digital Evidence Controls

Contents

- Uncovering attacks that evade detection by event viewer and task manager
- Memory image acquisition techniques and their limitations

Understanding Password cracking

- Maximum time individuals username and password to gain access to any system
- Password are easy to crack by hackers.
- Password can be cracked in following ways:
  - Use of brute force
  - Recover & exploit password stored on the system
  - Make use of password decryption software
  - Social engineering

Brute Force

- It’s not smarter solution for hackers in search of password, but very effective if strong password policies are not applied
- A brute force attackers attempts one possible password after another until he/she hits on right one.
- This process can be done by physically by somebody with lot of time and tolerance, done by program that scans all words in dictionary file which merely large list of words and other possible character arrangements.
- e.g., attackers knows that password consist of 5 alph-characters and 3 numeric, then he/she create guideline to hack password

Exploitation of stored password

- Attempting to forecast password even with software to quicken process is an annoying business.
- hacker could easily find list of passwords saved around everywhere
- Passwords have to be store someplace, else how will system come to know that user has entered precise and accurate password or not.
- People have numerous password along with logon passwords used for e-mail access, entry to restricted websites,
- Rather than remembering all secondary password user opt have system “remember” password option
- Passwords are not warehoused in plain text file that hacker can open and read, except careless user creates such a file persistently recording passwords for various services and applications.
- Stored passwords are encoded or hashed.

Interception of Passwords

- When password are sent through the network via local or remote access connections in plain text form, they can be seized and diverted using sniffer software
- Telnet sessions to UNIX computers can be captured and plain text password can be inferred if security measures are not there
- Use PAP-Password Authentication Protocol, for remote access effects in sending plain text password across the link and evaded when possible
- Stopping passwords is to use a keystroke logger-hardware device or software program that captures and archives every character that is entered including password.

Password Decryption Software

- Maximum password cracking software program do not actually decrypt everything
- If encryption algorithm is feeble or implemented inaccurately, use a method named one-byte patching, which is skilled at decrypting passwords by altering one byte in the package or database.
- when robust cryptography is use and compound code words are chosen, much difficult to use basic and direct decryption.

Social Engineering

- It does not refer to a technological manipulation of computer hardware or software weakness, it does not need much technical skills
- Social Engineering is referred to as accomplishing confidential information by modes of human communication
- You can think of social engineering attackers as devoted and focused con performers.
- They gain users or administrator's trust and then use this trust to find out user account names and passwords or have innocent users log them onto the system.

Prevention and Response

- Administrative and user can take a number of actions to protect passwords including followings:
  - Follow guidelines for generating strong passwords
  - Configure settings user accounts are deactivated or locked out after a sensible number of incorrect password attempts
  - Use EFS on windows 2000/XP/.NET computers to encode files
  - Store critical data in network servers instead of local machine
  - Do not rely on password protection built into most applications
  - Permit password shadowing on unix/linux systems
  - Deactivate LAN manager authentication on window networks
  - Confirm that passwords are never sent across network in plain text format
  - Use antisniffer software and sniffer detection techniques to protect against hackers who try to capture passwords travelling across network

Protecting the Network against Social Engineers

- A clever social engineer is master in making users distrust their own doubts about his legitimacy
- The invaders entertain users with miserable stories of extra cost the company will incur if they spend extra time confirming their identities
- They pass himself off as a member of company's top management and intimidate users-intimidating employee with penalizing action or even loss of job-if he doses not get their help

Forensic Duplication

- A Forensic Duplication contains the same digital data as the original piece of evidence.
- Many times with data collection process, Forensic Duplication process also gets started, which is based on response strategy already formulated

Thumb rule of Forensic Duplication

1. Make 2 copies of original media
   - One copy becomes the working copy on which investigation will be done
   - One copy is library/control copy for future references
   - Verify the integrity of the copies
2. The working copy is used for analysis
3. The library copy is stored for disclosure purposes or in the event that working copy becomes corrupted
4. If performing a drive to derive imaging, use clean media to copy.
5. Verify the integrity of all images using hash values

Necessity of Forensic Duplication

- Volatile data is collected from windows and UNIX
- Next step is to create a forensic duplicate
- Forensic duplicate is a document file containing every bit of information obtained from the sources in a raw bitstream format.
- The data is stored it is from hard drive to forensic duplicate devices.
- Ex,4 GB hard drive results in 4 GB of forensic duplicate
- This file does not contain any extra data other than error message. After duplication process, forensic duplication can be compressed

- In all cases computer/media is the main ‘crime scene’.
- This crime scene is protected because once digital evidence is contaminated it cannot be decontaminated.
- Investigator should take care to not change digital evidence during any step of investigation

- Forensic duplication importance can be summarized as:

1. Working from a duplicate image provides following features:
   a. Preserves original digital evidences
   b. Prevents inadvertent alternation of original digital evidence during examination
   c. Allows recreation of the duplicate image, if necessary
2. Digital evidence can be duplicated with no degradation copy to copy:
   a. This is not the case with most other forms of evidence.

Forensic Duplicates as Admissible Evidence

- Digital evidence should satisfy minimum criteria of legal standards
- Some standards are given by US known as Federal Rules of Evidence(FRE)
- FRE 1002 requires an original to prove the content of writing, record or photograph-items or information presented in court must be original
- FRE 1001 states that if data are deposited in a computer or alike device, any printout or other output readable by sight, shown to reflect the data precisely is an “original”
- FRE 1003 states that duplicate is admissible to same extent as an original if:
  - A honest que is elevated to authenticity of original
  - In the circumstances, it would be partial to confess the identical in lieu of the original

Important terms in Forensic Duplication

(1) Forensic Duplicate:

- It stores every bit of information from source in a raw bitstream format.
- 5 GB of drive results in 5 GB of forensic data
- No extra Data is stored within file except erroe message
- Two tool use-UNIX dd command and computer forensics lab version of dd command that is dcfldd,ODD or open Data Duplicator

(2) Qualified Forensic Duplicate

- The file that stores every bit of information from source is referred to as qualified forensic duplicate in the altered form
- Examples of altered forms are in-band hashes and empty sector compression Some tools will read in a number of sectors from the source, generate a hash from that group of sectors, and write the sector group, followed by the hash value to the output file
- This method works very well if something goes wrong during the duplication or restoration of the duplicate
- For reducing size of output file, empty sector compression can be used.
- Tools that create qualified forensic duplicate output files:

1. SafeBack 2. EnCase 3. FTK Imager

(3) Restored Image

- A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium.
- It is complicated process
- The partition tables are updated with new values as forensic duplicate is restored to destination hard drive.
- Restored image may involve some modification in original image
- To create a qualified forensic duplicate tools like SafeBack, Encase or DD can be used.

(4) Mirror Image

•Hardware that does a bit-for-bit copy from on HDD to another is used to generate a mirror image

•You can easily make working copies if your organization has the capability to keep original drive detained from computer system being examined