Static Evidence Collection and Anti-Forensics

Objectives:

At the end of this episode, I will be able to:

Understand what static evidence collection and Anti-Forensics are.

Explain what the Static Data Collection Process is.

Identify what the goals of Anti-Forensics are.

Define the different Anti-Forensics techniques that IH&R team members should be familiar with.

External Resources:

Static Evidence Collection and Anti-Forensics

Static data acquisition is defined as acquiring data that remains unaltered when the system is powered off or shutdown.

It can also exist in slack space, swap files and, unallocated drive space.

Other sources of non-volatile data include DVD-ROMs, USB drives, flash cards, smart phones, and external hard drives.

What is the Static Data Collection Process? -

Step 1: Administrative Consideration - Policy and Procedure Development - determine the mission statement, knowledge, skills, funding, evidence handling, personal requirements, and support from management. They should develop the policies and procedures required for collecting the static data.

Step 2: System Preservation - Hard Disk Acquisition - acquire the hard disks and create forensic duplicates. Use the DD tool to perform forensic duplication by obtaining an NTFS image of the original disk. Create a sector-by-sector mirror image of the disk and save the output image file as image.dd.

Step 3: Evidence Acquisition - Consists of three in-built processing steps:

```
o Check the data integrity - Use the MD5 tool to ensure the integrity of the
acquired data through reporting of a hash function (original media and the
resulting image file).

o Extract MFT in the boot sector - incident responders use the WinHex hex
editor tool to analyze the MFT and NTFSINO is used to check the number of
sectors allocated to the NTFS file system.

o Extract $Boot file and the backup boot sector - analyze the data hidden in
the $Boot metadata file system with the help of WinHex, TSK, and Autospy tools.
```

Step 4: Comparison - use the WinHex hex-editor and the TSK and Autospy tools to analyze both the Bootsector.dd and Backupbootsector.dd files.

Step 5: Evidence Examination - Consists of two in-built steps:

```
o Check the data integrity - perform the data integrity check using the MD5 tool.

o Extract the ASCII and UNICODE - Incident responders extract the ASCII and
the UNICODE characters from the binary files present in the disk image. For
matching text or hexadecimal values recorded on the disk, they use the strings
command tool and keyword searching. The keyword search will help to find the
files containing the specific words.
```

Step 6: Physical Presentation - This is the final step of static data collection process. The incident responders will document all the findings of the investigation process. It involves presenting the digital evidence through documentation.

What is Anti-Forensics? -

Anti-forensics, also known as counter forensics, is a set of techniques that attackers use to sidetrack the forensic investigation process or try to make it much harder.

These techniques negatively impact the quantity and quality of evidence from a crime scene.

Goals of Anti-Forensics:

```
▪ Interrupt and prevent information collection
▪ Hide traces of crime or illegal activity
▪ Compromise the accuracy of a forensic report or testimony
▪ Force the forensic tool to reveal its presence
▪ Use a forensic tool itself for attack purposes
▪ Delete evidence that an anti-forensic tool has been used
```

Anti-Forensics Techniques: Golden Ticket - attackers gain access to an Active Directory domain and manipulate the Kerberos ticket to impersonate any user in the domain.

NOTE: "Golden ticket" refers to the forged Kerberos authentication token for the KRBTGT account.

Attackers can create a Kerberos-generating ticket with a lifetime of 10 years or more.

This ticket helps attackers to assume identity of any user present in the group including the highly privileged users.

To create and use a golden ticket, an attacker must:

```
▪ Discover a way into the network
▪ Infect the target system with malware
▪ Use the domain controller access to get access to an account with privileges
▪ Create a golden ticket, by logging into domain controller and dump the
password hash of KRBTGT account using tools such as Mimikatz
▪ Access anything on the network by loading the Kerberos token into any
session for any user
```

Anti-Forensics Techniques: Program Packers - A Packer is a program used to compress or encrypt executable programs.

Packers compress the files using various methods called algorithms. There are many different algorithms and unless the incident responders know the one used to pack and have a tool to unpack it, they will not be able to access the file.

Packers can also include active protection against debugging or reverse engineering techniques.

Anti-Forensics Techniques: Artifact Wiping - refers to the process of deleting or destroying the evidence files permanently using various tools and techniques, such as disk-cleaning utilities, file-wiping utilities, and disk degaussing/destruction techniques. The attacker permanently eliminates particular files or the file systems.

Anti-Forensics Techniques: Memory Residents - programs that always remain in the internal memory and operating systems have no permission to swap them out to external storage.

Attackers try to take advantage of these programs or system calls by using the following methods:

```
▪ Syscall proxying - Rather than uploading the entire exploit program, the
attacker can upload a system call proxy to accept the remote procedure calls
from the attacker's machine. The victim's machine executes the requested
system call and sends the result back to the attacker. By doing so, the
attacker need not upload the tools to the compromised machine. However, this
increases the amount of network traffic between the compromised machine and
the attacker, thereby creating latency. This technique helps in capitalizing
the code injection vulnerabilities on a system.


▪ Userland Execve Technique - allows a Unix process to load and execute an ELF
binary image from a memory buffer. This lets programs on the victim computer
load and run without using the Unix execve() kernel call.
```

Userland Execve
— Runs program without using execve()
— Bypasses logging and access control
— Works with code from disk or read from network

Anti-Forensics Techniques: Alternate Data Stream (ADS) - a feature of Windows New Technology File System (NTFS) that contains metadata for locating a file by author or title.

A file or folder in NTFS consists of many data streams:

One is the primary data stream, which consists of the data that we expect from the file.

The second stream is the alternate data stream that can hide the presence of another file. Attackers manipulate the ADS data by inserting malicious code or programs into them and executing it at will. It is undetectable because changes to the ADS file do not alter any noticeable characteristics of the actual file.

Other Anti-Forensics Techniques -

```
▪ Data Hiding in File System Structures - NTFS-based hard disks contain bad
clusters in a metadata file as $BadClus and the MFT entry 8 represents these
bad clusters. $BadClus is a sparse file, which allows attackers to hide
unlimited data as well as allocate more clusters to $BadClus to hide more
data if necessary.
```

NOTE: Some hard disks have a host protected area (HPA), which can store data to protect (and hide) it from normal use.

```
▪ Overwriting Metadata - Attackers uses tools such as Timestomp, which is
part of the Metasploit Framework, to change MACE
(Modified-Accessed-Created-Entry) attributes of the file. Another way to
overwrite metadata is to access the computer in such a way that metadata is
not created. Attackers mount a partition as read-only or access it through the
raw device to prevent updating of the file access times.
```

They can also manipulate settings of the Windows registry key "HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate" to 1 to disable updating of the last-accessed timestamp.

```
▪ Rootkits - hide processes that could reveal an attack from the OS itself.
Rootkits allow viruses and malware to "hide in plain sight" by concealing
files in ways that the antivirus software might overlook them, disguising
files as legitimate system files, through unlinking processes, and even hiding
from detection by the OS.
```

Different types of rootkits include:

```
o Hypervisor Level Rootkit
o Hardware/Firmware Rootkit
o Kernel Level Rootkit
o Boot Loader Level Rootkit
o Application Level Rootkit
o Library Level Rootkits
```

Performing Evidence Analysis -

```
What preparation steps should the IH&R team undertake to get ready to perform
Evidence Analysis? -

The first responder needs to prepare and check several prerequisites such as the
availability of tools, reporting requirements, and legal clearances in order to
conduct a successful investigation.

Evidence analysis helps to find the attackers and method of attacks in a legally
sound manner.

The IH&R team should perform the following:

    ▪ Understand the investigation requirements and scenarios
    ▪ Check with the lawyer/organization for any specific analysis requirements
    ▪ Have a copy of organization's forensic investigation policy
    ▪ Transport evidence to a secure location or forensic investigation lab
    ▪ Check the lab facilities before starting the analysis
    ▪ Prepare the evidence analysis toolkit containing imaging, recovery, and
    analysis tools


What is a Forensics Reports? -

A statement of allegations and conclusions drawn from the computer forensics
investigation.

It includes the scope of investigation, tools used to acquire and analyze data,
evidence gathered, details of incident responder, and so on.
```