

# Anti-Forensics

Huseyin Yagci

# Outline

- What is Anti-forensics
- Anti-forensic Techniques
  - Overwrite or Destroy Data
  - Hiding Data
  - Memory Injection and Userland Execve
  - Syscall Proxying
  - Attacking the Investigator
- Countermeasures for Anti-Forensics

# What is Anti-forensics

- Tools and techniques that frustrate forensic tools, investigations and investigators.
- Goals of Anti-Forensics:
  - Avoiding detection
  - Disrupting information collection
  - Increasing the examiner's time



# Anti-Forensic techniques

## Overwrite and Destroy data : Eliminate data or metadata

- Disk sanitizers, Microsoft Word metadata “washers,” timestamp eliminators.
- MACE (Modified, Accessed, Changed, Entry Modified)

```
C:\>timestamp text.txt -m "Monday 1/01/2001 01:01:1 AM"

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 3036-18D7

Directory of C:\

05/26/2007  06:01 PM           0 AUTOEXEC.BAT
05/26/2007  06:01 PM           0 CONFIG.SYS
10/24/2007  02:58 PM    <DIR>        Documents and Settings
05/29/2007  01:15 PM    <DIR>        Program Files
01/01/2001  01:01 AM           0 text.txt
10/24/2007  02:50 PM    57,344 timestamp.exe
06/18/2007  05:31 PM    <DIR>        WINDOWS
               4 File(s)      57,344 bytes
               3 Dir(s)    11,767,320,576 bytes free

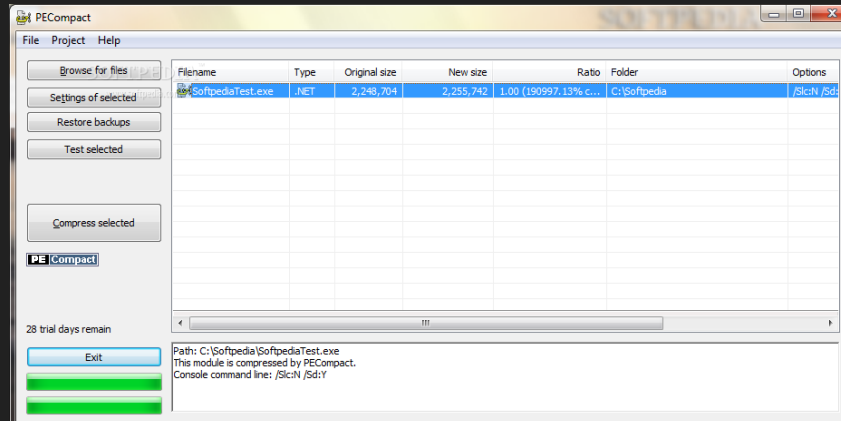
C:\>timestamp text.txt -v
Modified:             Monday 1/1/2001 1:1:1
Accessed:             Wednesday 10/24/2007 14:51:2
Created:              Wednesday 10/24/2007 14:51:2
Entry Modified:       Wednesday 10/24/2007 14:59:8
C:\>
```

The screenshot shows the Encase V3 Preview Edition interface. The main window displays a list of file entries with columns: Name, Tag, File Type, File Ext, File Category, Signature, Description, Protected, Is Deleted, Last Accessed, File Created, Last Written, Entry Modified, and File Deleted. The selected entry is \$MFT:\$0, which is a File, Invalid Cluster, Hidd... with a size of 57,344 bytes. The bottom pane shows the file's metadata, including Name, Tag, File Ext, File Type, File Category, Signature, Description, Protected, Is Deleted, Last Accessed, File Created, Last Written, Entry Modified, and File Deleted.

Name	Tag	File Type	File Ext	File Category	Signature	Description	Protected	Is Deleted	Last Accessed	File Created	Last Written	Entry Modified	File Deleted
\$MFT:\$0		File		Invalid Cluster, Hidd...				N	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)	04/25/11 22:23:16 (-4:00 Eastern Daylight Time)	

# Anti-Forensic techniques

- **Hiding Data** : cryptography or steganography
  - Cryptographic File Systems (EFS, TrueCrypt)
  - Encrypted Network Protocols (SSL, SSH, Onion Routing)
  - Program Packers (PECompact, Burney) & Rootkits
  - Steganography



# Anti-Forensic techniques

- **Slacker**: Hides data in slack space
- **FragFS**: Hides in NTFS Master File Table
- **RuneFS**: Stores data in “bad blocks”
- **KY FS**: Stores data in directories
- **Data Mule FS**: Stores in inode reserved space

```
C:\>slacker.exe

Hiding a file in slack space:
-----
slacker.exe -s <file> <path> <levels> <metadata> [password] [-dxi] [-n|-k|-f <xorfile>]
-s          store a file in slack space
<file>      file to be hidden
<path>      root directory in which to search for slack space
<levels>    depth of subdirectories to search for slack space
<metadata>  file containing slack space tracking information
[password]  passphrase used to encrypt the metadata file
-dxi       dumb, random, or intelligent slack space selection
-nkf       none, random key, or file based data obfuscation
<xorfile>   the file whose contents will be used as the xor key

Restoring a file from slack space:
-----
slacker.exe -r <metadata> [password] [-o outfile]

-r          restore a file from slack space
<metadata>  file containing slack space tracking information
[password]  passphrase used to decrypt the metadata file
[-o outfile] output file, else original location is used, no clobber
```

# Anti-Forensic techniques

**Memory Injection and Userland Execve:** Running a program without Os intervention for loading the code.

- Buffer overflow

## **Userland Execve:**

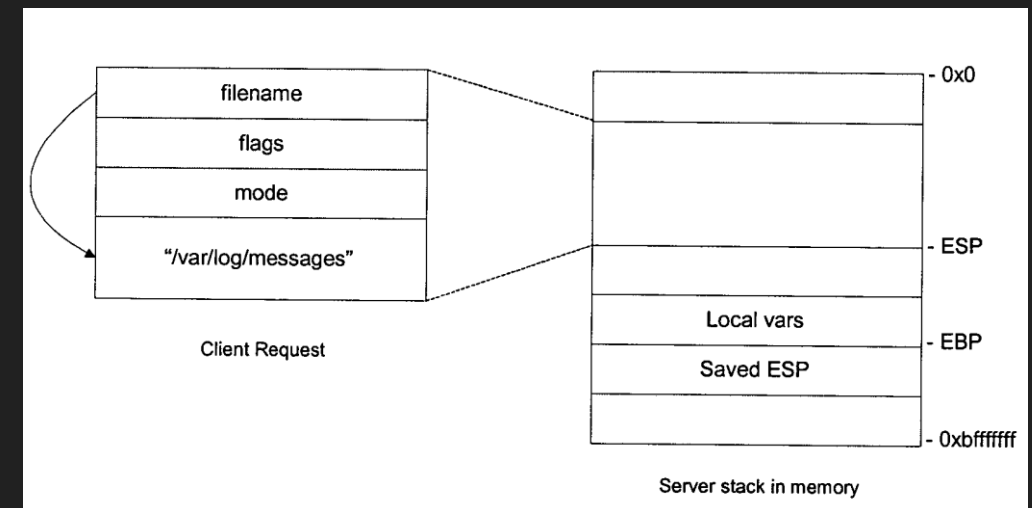
- Runs program without using execve()
- Bypasses logging and access control
- Works with code from disk or read from network



# Anti-Forensic techniques

## Syscall Proxying: (RMI)

- Program runs on one computer, syscalls executed on another.
- Program not available for analysis
- May generate a lot of network traffic
- Developed by Core Security; used in Impact





# Anti-Forensic techniques

Attackers have long made use of anonymous e-mail accounts.

Today these accounts are far more powerful.

- Yahoo and Gmail both have 2GB of storage
- APIs allow this storage to be used as if it were a file system.

Amazon's Elastic Compute Cloud (EC2) and Simple Storage Service (S3) provide high-capability, little-patrolled services to anyone with a credit card

- EC2: 10 ¢/CPU hour (Xen-based virtual machines)
- S3: 10 ¢/GB-Month

# Anti-Forensic techniques

- Attacking the Investigator
  - Ability to run code on the forensic appliance
  - Erase collected evidence
  - Break the investigative software
  - Leak information about the analyst or the investigation
  - Implicate the investigator



Thank you...