D.F

OPERATION CHIMERA

DIGITAL FORENSICS MODULE // SECURITY BLUE TEAM

CONTENTS

[1] What is Digital Forensics?
[3] Why is it Useful?
[2] What skills Are Required?
[4] A day in The Life
[5] Associated Roles
[2] Steganography
[2] Tools for the Challenge
[5] Module Challenge

This information has been gathered from public sources and combined with my own knowledge and experiences for the purpose of Operation Chimera, an online, live blue-team training operation conducted by myself under the alias Known Divide, for the SecurityBlueTeam community.

Useful Links:

[1]
https://www.csoonline.com/article/3334396/what-is-digital-forensics-and-how-to-land-a-job-in-this-hot-field.html
[2]
https://en.wikipedia.org/wiki/Steganography
[3]
https://www.nccgroup.trust/uk/our-services/cyber-security/managed-detection-and-response/digital-forensics/

Sources:

[1]
https://en.wikipedia.org/wiki/Digital_forensics
[2]
https://www.lifewire.com/strings-linux-command-4093452

OPERATION CHIMERA – DIGITAL FORENSICS

This document is not 100% finished and will be updated within the next 24 hours. Thank you for your patience.

This module is designed to give a look into the world of Digital Forensics. It is aimed at individuals who are moving in to Cyber, so the material is aimed at an entry-level student. We strongly encourage further reading using the provided sources and any that you find yourself. Want to talk to other hackers about this specific module? Join the discussion in the "forensics-module" channel within the "Operation Chimera" category in the SBT Discord server. There is also a Chimera mega-thread on Reddit. Please make use of this to ask questions and talk to other participants!

WHAT IS DIGITAL FORENSICS?

"Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime." [1] So Forensics is the technical process of recovering or collecting evidence which will be used in an investigation. In regards to Security Operations, this discipline is associated with the monitoring of employees to maintain a high security posture, aiding with incident response to reveal details of how a compromise occurred and any post-actions, as well as other tasks which require a 'deep-dive' into technical aspects.

WHY IS IT USEFUL?

Recovering information can be crucial to security investigations, preventing individuals from hiding or deleting evidence. Digital Forensics skills can be used in many different ways, making it important for Security Operations work. From malware analysis to monitoring insider threats, investigating compromises to policy breachers, DF helps security teams respond to threats.

D.F

OPERATION CHIMERA

DIGITAL FORENSICS MODULE // SECURITY BLUE TEAM

If you've enjoyed this event, please consider donating whatever you can spare to buy me pizza, coffee, and help fund future events! (even £5/$5 will make a huge difference, and it only takes a few seconds).

PayPal.Me

https://paypal.me/KDMentoring

WHAT SKILLS ARE REQUIRED?

Organized: In order for evidence to remain valid, it must be recorded and managed under strict conditions. By following the Chain of Command, everything is documented, ensuring the integrity of the evidence is maintained.

Highly Technical: To work on Forensics tasks, you will need to have a high degree of technical ability, due to the complicated tasks that will be conducted. A comprehensive understand of operating systems, servers, clients, networking, log analysis, behavioral analysis, and more will help you during this discipline.

Analytical: Forensics is often time-consuming and tedious. You need to be able to work on repetitive, but important, tasks. Every piece of information is important and can't be overlooked or missed out.

A DAY IN THE LIFE:

The work can vary from day-to-day, but here are some scenarios where a Digital Forensics Analyst (or someone with forensics skills) would help within a Security Operations environment:

- Assisting Tier One/Tier Two Analysts by providing malware analysis for their investigations (usually as a result of a phishing email attachment, or URL with a drive-by download).
- Aiding Incident Responders with investigation on systems after a suspected or confirmed compromise (log analysis to identify any further actions conducted by the attackers).
- Analyzing hard-drive images to aid investigations into intentional or accidental malicious activity, or compromise.
- Investigating and monitoring activity from specific individuals for different reasons (insider threat, policy breaches, unusual activity).

ASSOCIATED ROLES:

The below roles generally contain work that includes certain aspects of Digital Forensics:

- Tier One SOC Analyst (Junior Security Analyst)
- Tier Two SOC Analyst (Security Analyst)

OPERATION CHIMERA

DIGITAL FORENSICS MODULE // SECURITY BLUE TEAM

- Tier Three SOC Analyst (Senior Security Analyst)
- Malware Analyst
- Digital Forensics Analyst
- Incident Responder/Security Incident Response Team

STEGANOGRAPHY

"*The practice of concealing messages or information within other non-secret text or data.*" An example of this would be having a text file that contains secret information, which is hidden inside an innocent image file. If this image file was sent as an email attachment, the recipient would receive a normal image file. However, using the right tools, you can recover the hidden file. You can also insert hidden messages in the form of text strings within a file's metadata. We suggest you read the following short article that explains what steganography is, written by TechTarget. The module Challenge is based around finding hidden information, so it's important you understand how to analyze files to see if they contain anything they shouldn't.

CHAIN OF CUSTODY

This is a very important aspect of Digital Forensics to learn. As previously mentioned, it's important that any evidence is valid in court, so it must be held to strict regulations and controls. Using a form, you need to keep track of any individuals that have touched the media, for activities such as collection, imaging, and return. Every time the media is removed from secure storage, it must be signed out by someone who is authorized to do so. If there were any gaps in the timeline between collection and submission in court, the evidence may become

TOOLS FOR THE CHALLENGE:

These tools and commands, although very simple, will help you gain a foundational understanding of Digital Forensics. Below are the techniques you are going to need to use:

1. **Command-line commands** (strings, cat, hexdump)
2. **ZIP password cracking**
3. **Identifying incorrect file extensions**
4. **Finding hidden files**
5. **File carving**

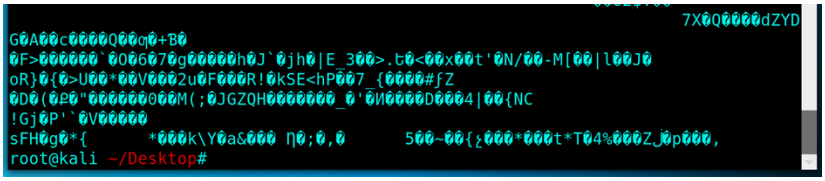
Strings, Cat, and Hexdump

"The Linux "strings" command makes it possible to view the human-readable characters within any file. The main purpose of using the "strings" command is to work out what type of file it is you are looking at, but you can also use it to extract text." [Lifewire]

This command is very similar to *cat*, which allows us to read the contents of a file in Linux. However, *strings* can give us some more information, such as the true file type. So, if a file has been assigned a new extension, we can recover the actual file type, and alter the file so we can open it. This will be covered in more detail during the "Identifying incorrect file extensions" section.

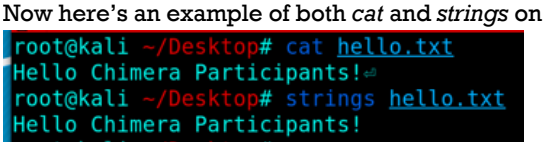
Here's an example of both *cat* and *strings* on the same file image file, meow.jpg:

Cat:



Strings:

Now here's an example of both *cat* and *strings* on the same text file, hello.txt:



More info coming soon.

Cracking .ZIP files

In this section, I'll teach you how to crack a password-protected ZIP file. The tool we're going to use is fcrackzip, which comes installed with the Offensive Security Kali Linux disk image. Type "fcrackzip –help" to see more information about the tool.

```
root@kali ~# fcrackzip --help

fcrackzip version 1.0, a fast/free zip password cracker
written by Marc Lehmann <pcg@goof.com> You can find more info on
http://www.goof.com/pcg/marc/

USAGE: fcrackzip
         [-b|--brute-force]            use brute force algorithm
         [-D|--dictionary]             use a dictionary
         [-B|--benchmark]              execute a small benchmark
         [-c|--charset characterset]   use characters from charset
         [-h|--help]                   show this message
         [--version]                   show the version of this program
         [-V|--validate]               sanity-check the algortihm
         [-v|--verbose]                be more verbose
         [-p|--init-password string]   use string as initial password/file
         [-l|--length min-max]         check password with length min to max
         [-u|--use-unzip]              use unzip to weed out wrong passwords
         [-m|--method num]             use method number "num" (see below)
         [-2|--modulo r/m]             only calculcate 1/m of the password
         file...                    the zipfiles to crack
```

In this example, the target ZIP is called 'MEOW.ZIP', with the password '1234'. We will use the following command to launch a Dictionary attack, using a password wordlist. In this attack, the tool will attempt thousands of different password strings, in the hope of finding the correct one. This works well with low-medium strength passwords, and requires the password to be in the list, otherwise it won't work. If you don't know the location of your wordlists (which come default with the Offensive Security Kali image), use "locate wordlists" or "locate rockyou.txt".

Fcrackzip -D -u -p /usr/share/wordlists/rockyou.txt MEOW.ZIP

(Tool) (Dictionary Attack) (Weed out wrong passwords) (use string as password) (Wordlist file path) (target ZIP)

```
root@kali ~/Desktop# fcrackzip -D -u -p /usr/share/wordlists/rockyou.txt MEOW.ZIP


PASSWORD FOUND!!!!: pw == 1234
root@kali ~/Desktop# unzip MEOW.ZIP
Archive:  MEOW.ZIP
[MEOW.ZIP] meow.jpg password:
replace meow.jpg? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: meow.jpg
```

Obviously this was a very simple password, so it was cracked in under a second. If a password was very complex, such as "AM4nBr0WnaPP73w1n!", this is very unlikely going to be in a password wordlist, so this would need to be cracked used a Bruteforce Attack. This is where the tool will use every possible character combination until the password is found. This can be very time consuming, depending on the resources your system has. Using this type of attack is out-of-scope for this Challenge, so you will not need to do it.

In the Challenge, look out for passworded .Zip files. There may be something important inside.

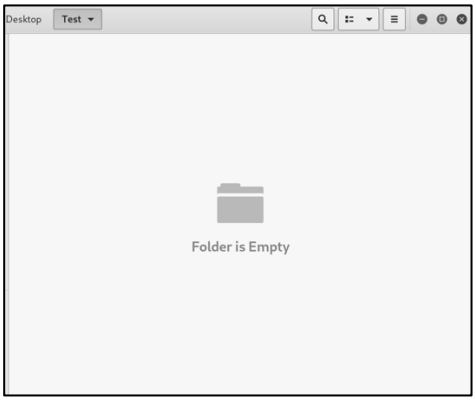
Identifying Incorrect File Extensions

Section Coming Soon.

Hidden Files

In Linux systems, if a file or directory name begins with a period (.) then it is hidden from view both in command-line, and GUI. In this example, we have a hidden text file in a directory named "Test".

When looking at the directory in the GUI, we can't see any files:



And trying to list any files in the directory using "ls" shows nothing:

```
root@kali ~/Desktop# cd Test
root@kali ~/D/Test# ls
root@kali ~/D/Test#
```

However, if we use "ls -a", which lists all possible files, we can now see the text file which begins with ".":

```
root@kali ~/D/Test# ls -a
 ./   ../  '.Secret Message'
```

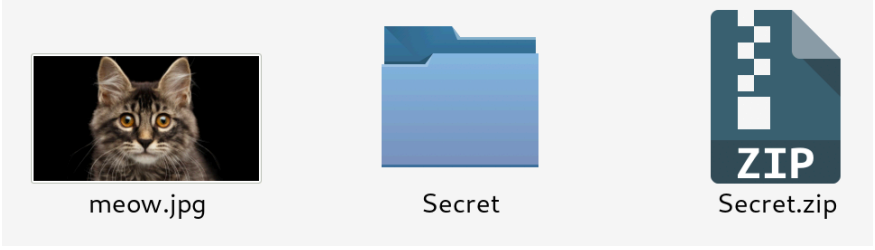
And we can read it using "cat" to reveal the message "Secret Message":

```
root@kali ~/D/Test# cat .Secret\ Message
Secret Message
root@kali ~/D/Test#
```

During the module Challenge, keep an eye out for files and directories hidden using this technique!

File Carving

In this example, I'll show you how it's possible to hide files inside of another file, and how to retrieve them. To start, we have a Directory ('Secret') which includes any files we want to hide, and an innocent image file (meow.jpg), that we will hide our files inside. Once your Directory is ready to go, right-click and Compress it, to send it to a .zip file.



Now we need to hide the Secret.zip inside of meow.jpg. We can do that using the following command:

cat meow.jpg Secret.zip > Cat.jpg

(image file) (zip file) (output to new file Cat.jpg)

```
meow.jpg  Secret/  Secret.zip
root@kali ~/D/Test# cat meow.jpg Secret.zip > Cat.jpg
```

Now we have a new image file, called Cat.jpg. There is no way to tell by looking at it, that there is a .zip file hidden inside. The image will open and function as expected, however, we are still able to retrieve the hidden information, using unzip:

```
root@kali ~/D/Test# ls
Cat.jpg
root@kali ~/D/Test# unzip Cat.jpg
Archive:  Cat.jpg
warning [Cat.jpg]:  59968 extra bytes at beginning or within zipfile
  (attempting to process anyway)
   creating: Secret/
  inflating: Secret/SecretMessage
root@kali ~/D/Test# cd Secret
root@kali ~/D/T/Secret# ls
SecretMessage
root@kali ~/D/T/Secret# cat SecretMessage
This is a Secret message!
root@kali ~/D/T/Secret#
```

A quick and easy way to see if a file may contain hidden files, instead of using unzip on everything, is to use the 'strings' command. Here's the output from using strings on Cat.jpg:

```
dZYD
|E_3
JGZQH
0?3O
Secret/UT
0?3O
Secret/SecretMessageUT
0?3O
Secret/UT
0?3O
Secret/SecretMessageUT
```

During the Challenge, keep an eye out for images that contain hidden files!

MODULE CHALLENGE

If you feel you're familiar with what Digital Forensics is, and how to conduct a simple investigation, then you may be ready for the Challenge! We suggest you still do some of your own research using the 'Useful Links' on the first page before attempting the Challenge.

What will I need for this Challenge?

- Recommend using Virtualbox (https://www.virtualbox.org/wiki/Downloads)
- Offensive Security Kali Linux image (https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/)
- Here's a YouTube guide to help you set up a Kali VM: https://www.youtube.com/watch?v=FVmWMogGX4Q

D.F

OPERATION CHIMERA

DIGITAL FORENSICS MODULE // SECURITY BLUE TEAM

Challenge Brief:
The SOC has received an anonymous report that a user is potentially exfiltrating data from the company. An image of the user's hard drive has been taken, and you are responsible for analyzing the contents to find any evidence of malicious activity. Using your newly developed skills, search through the folders and files using techniques to uncover hidden information. Keep a record of all information you find that may be relevant to the investigation and write a short report on what you believe is going on. The report should include the following information (link here):

- **Hidden information you have found**
- **Methods used to retrieve information**
- **The locations/files of the information**
- **A conclusion on the activity you have discovered**

Some useful commands include the following:
(Remember you can view the manual page for tools by using "man <command>" to get VERY useful information!)

- **Strings <file>**
- **Hexdump -c <file>**
- **Cat <file>**
- **Fcrackzip**
-