😂😂😂

Warm Up:

What is the name of the Ransomware Worm that disabled hospitals worldwide in May of 2017?

CYBER
TROY HIGH
Est 2010
DEFENSE

Forensix

Basic Linux

Better Google, Better Results

- Search for the right things
  - Terms like “hardening”, “security practices”
- Search conventions
  - “something“
    - Exact match
  - -something
    - Exclude
  - Site:something.com
    - Specific site
  - Type:pdf
    - Search by filetype

Bad thing?

- dpkg -l
  - Shows packages and what they do
  - dpkg -l | grep “<package name>” | less
- If you don’t know what something means google it
  - “Sniffers”, “crackers”, “brute force”, are generally bad
  - Even if something may be useful, consider what a hacker could do with it if they enter your system
  - Read the ReadMe

How to bad thing go away?

- sudo apt-get
  - remove
    - Gets rid of package
  - purge
    - Gets rid of package and configs
  - autoremove
    - Gets rid of package and dependencies
  - purge --autoremove
    -

> *“What the **** does the asterisk mean???” - Anya*

What are forensics?

- You will get several forensics questions on every competition image
  - Start with 2 and get more
- These are generally questions about your system but may include simple CTF materials (mostly crypto)
  - Includes but isn’t limited to file hunting, file properties (size, ownership, perms, etc.), log analysis, system info

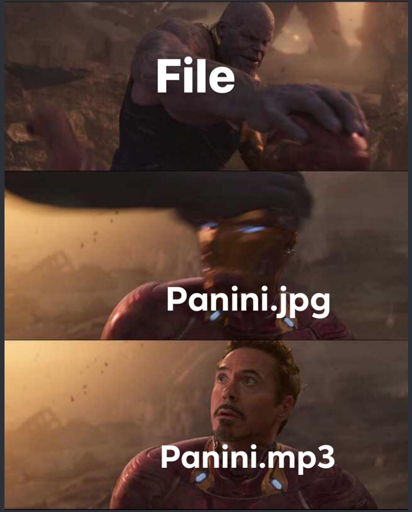
“

CP likes to keep things spicy; we will give you some starting tips but there will probably be something new to google almost every round

> “Why can’t I open this jpg?!?! REEEEEE!!!”
>
> - y’all

File

- file <filename/path>
  - Will show what the file’s real file type is
  - Forensics questions will sometime ask for a file’s type, or it may ask you to open or manipulate a file with the wrong extension
  - Just change the thing



How file hunt?

- Two (2) tools we commonly use
  - find
  - grep
- Each works differently, use depends on situation or personal preference

Find

- General syntax
  - find <filename/path>
- To find a certain filetype
  - find <directory> -name *.<file extension>
    - Use / for directory to search entire filesystem
    - EX: find /home -name *.<file extension> if file is known to be in a user directory
- Other options exist, look in the man page and play around in your spare time if you want

Grep

- General syntax
  - grep <pattern> <file>
- To find certain filetype
  - find <directory> | grep [.]<file extension>
  - Uses find to get all files in the directory, then uses grep to search for the file extension
  - Same rules as before for find
- Grep has MANY fun options to use, it is strongly recommended to play with it some time

Find vs Grep

- Can be used together
- find looks for file names and can be used for directories
- grep looks for strings/patterns and can only be used on text
  - Note that grep can look inside files^^
- Both use regex (regular expressions) to search for things
  - Advanced topic
  - If you want to, you can how to use regex to do all kinds of crazy things with grep
    - can make searching for certains strings (EX: IP Addresses) within files very easy
  - https://regexone.com/ is a useful training if you have spare time

> *“What?! This isn’t Caesar Cipher!!” *suffers mental breakdown**
>
> *- no0bs who did two (2) PicoCTF problems in middle school*

Crypto

- *CTF Crpyto problems get much harder than what is covered here very fast*
- More often than not, Crypto problems will be a simple base conversion or shift cipher
- Base Conversions
  - Binary, Octal, Hex, Base64
  - Find translators online
- Other simple things
  - http://rumkin.com/tools/cipher/
- Try googling ciphertext traits if these don’t work
  - EX: “=” signs at the end, only numbers, 3 keys, R-value provided

File properties

- Lots of info can provided by ls
- Man ls and play around with the options
  - Most commonly used are ls -a and ls -l
  - Shorthand for ls -a is la
    - Hidden files
  - Shorthand for ls -l is ll
    - Long list format, provides most of the useful file properties for forensics (perms, ownership)
  - *note, lla and lal don't exist, if you want to see hidden files with long list properties you'll have to use ls -la to stack the effects*

Godspeed and good hunting