MEGA REVIEW

What do you want to review?

Linux/Command Line

Python Basics

Conditionals

Functions

Binary/Hex Conversions

Loops

Cryptography (Caesar, Vigenere, One Time Pad, RSA)

Hashing (MD5, SHA-1, SHA-2)

Password Cracking (John the Ripper, Hashcat)

CS4CS Story (Pelon Husk, Geoff Pesos, Rich Brandad)

Linux Basics/Command Line Matching

1. cd
2. ls
3. touch
4. cat
5. mv
6. mkdir
7. sudo apt-get install
8. sl

“Create a file”

“Make a new directory”

“Move a file/directory”

“Install a program”

“Change the directory”

“TRAIN!!”

“Lists directory contents such as files/directories”

“Displays contents of a file and can create multiple files”

Back

Python Basics - What does this syntax do?

1. 20 % 4
2. sentence = “Python is cool”; my_age = 17
3. len(sentence)
4. 7 // 2
5. print(my_age)
6. str(my_age)
7. sentence[4]
8. name = input(“What’s your name?”)
9. fave_num = int(input(“What’s your favorite number?”))

Back

Conditionals!

- ★ Perform an action depending on whether a condition is TRUE or FALSE
- ★ if, elif, else
  - if - only runs when the condition is true
  - elif - used when there are multiple conditions and will only run when its condition is true
  - else - runs when the condition doesn't run true
- ★ >
- ★ <
- ★ >=
- ★ <=
- ★ ==
- ★ AND / OR

Back

Define the parts of this Function!

```
def greatest_Num(num1, num2):
      if num1 == num2:
            print(“Nope!”)
      return(num1 + num2)
```

Def - defines the function and creates it

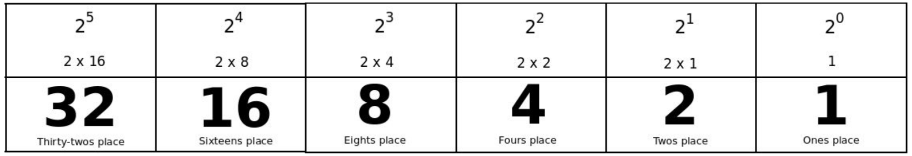
Red - the parameters of the function; what gets passed in and returned

Return - if function runs smoothly it will return certain values through this statement

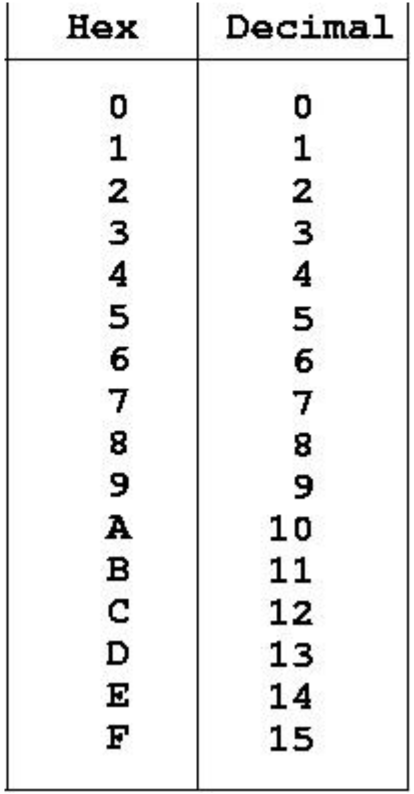
Back

Binary and Hex Conversions

1. Decimal → Binary
    a. 42
    b. 245
    c. 67
2. Binary → Decimal
    a. 111000
    b. 1111010
    c. 1100001
3. Decimal → Hex
    a. 77
    b. 335
    c. 410
4. Hex → Decimal
    a. 3A
    b. 13B
    c. D4



2^5 2 x 16	2^4 2 x 8	2^3 2 x 4	2^2 2 x 2	2^1 2 x 1	2^0 1
32 Thirty-twos place	**16** Sixteens place	**8** Eights place	**4** Fours place	**2** Twos place	**1** Ones place



Hex	Decimal
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
A	10
B	11
C	12
D	13
E	14
F	15

Solutions

ANSWERS!

Part 1-	a) 101010	b) 11110101	c) 1000011
Part 2-	a) 56	b) 122	c) 97
Part 3-	a) 4D	b) 14F	c) 19A
Part 4-	a) 58	b) 315	c) 212

Loops on Loops

1. What kind of loop requires a condition being met?
2. What kind of loop runs a certain number of time?
3. Create the basic syntax of a For Loop
4. Create the basic syntax for a While Loop
5. Create the basic syntax for a loop that finds all the even numbers from 1 to 20, inclusive.

Back

Cryptography: a Quick Review

- One Time Pad
  - -Completely RANDOM key - same length as message
  - The Perfect Cypher
- RSA
  - Public and Private Keys
- Vigenere
  - Plaintext: A T T A C K A T D A W N
    Key: L E M O N L E M O N L E Your shift changes with the word LEMON
    Ciphertext: L X F O P V E F R N H R
- Caesar Cipher
  - Substitution of letters with a single shift
  - Bad because it's very easy to decrypt

Back

Hashing: a Quick Review

What is Hashing?

★ Encode through a one way function digital signatures

Why use it?

★ Hide file names → use hashes instead!

Common and Easy to Crack Hashing Methods

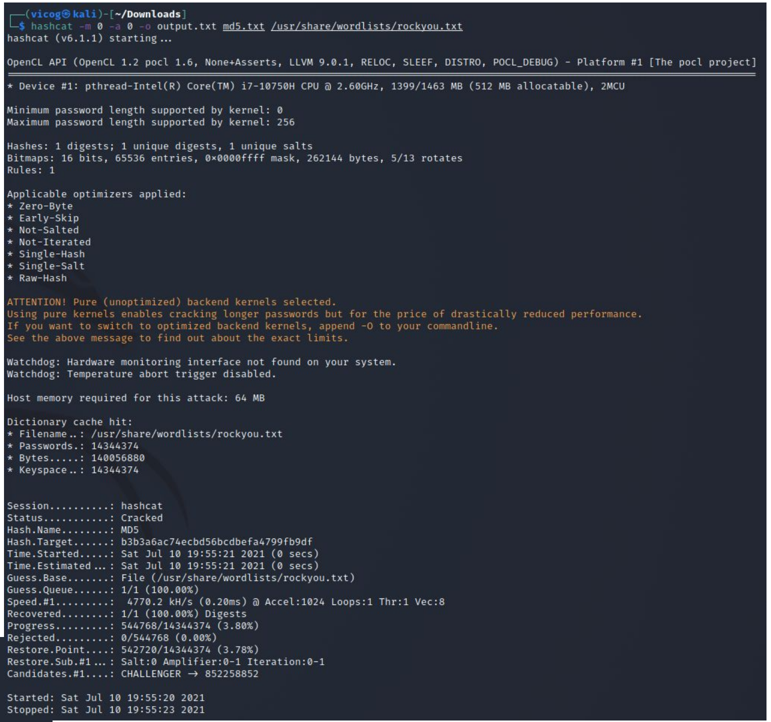
★ **MD5**: 128 bit hash, can have many vulnerabilities
★ **SHA1**: 160 bit hash, much more secure than MD5

Back

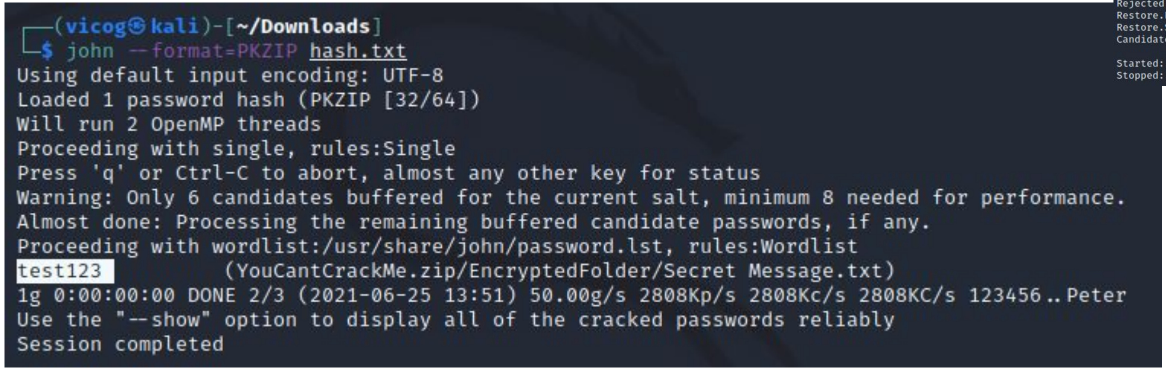
Password Cracking

Cracking MD5/SHA1 hashes using Hashcat

Cracking Zip File Password using John the Ripper

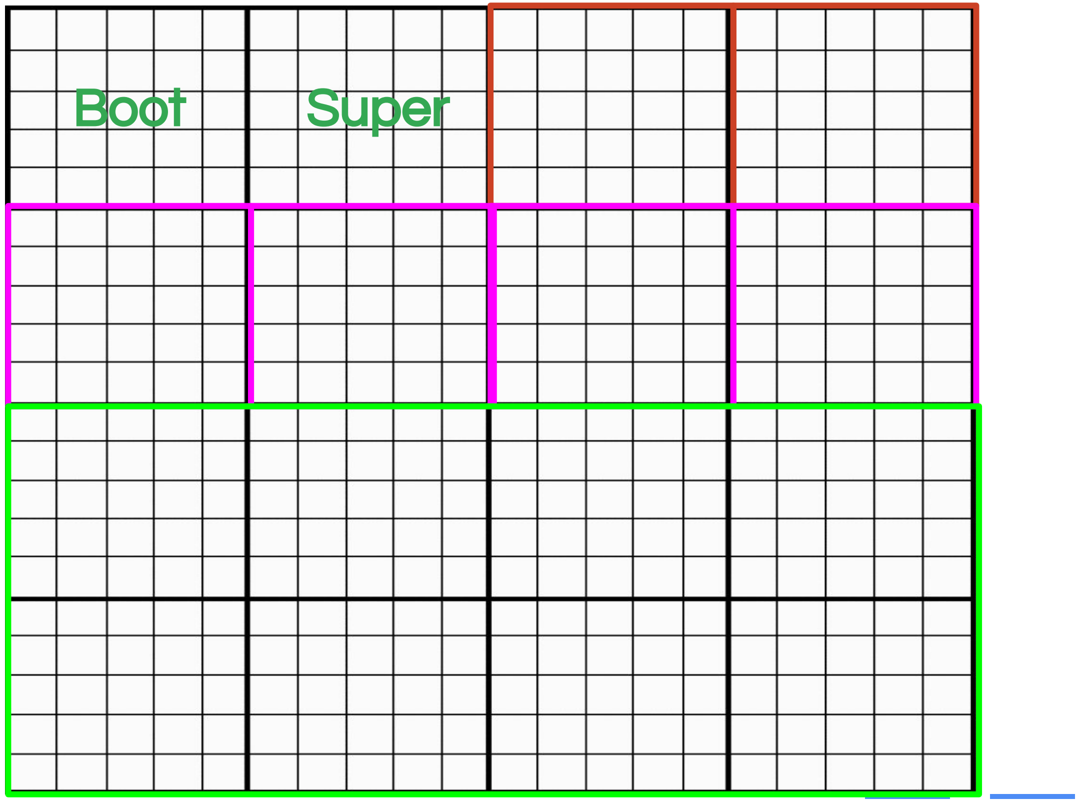


```
┌──(vicog㉿kali)-[~/Downloads]
└─$ hashcat -m 0 -a 0 -o output.txt md5.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=============================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1399/1463 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344374
* Bytes.....: 140056880
* Keyspace..: 14344374


Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: b3b3a6ac74ecbd56bcdbefa4799fb9df
Time.Started.....: Sat Jul 10 19:55:21 2021 (0 secs)
Time.Estimated...: Sat Jul 10 19:55:21 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  4770.2 kH/s (0.20ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 544768/14344374 (3.80%)
Rejected.........: 0/544768 (0.00%)
Restore.Point....: 542720/14344374 (3.78%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: CHALLENGER → 852258852

Started: Sat Jul 10 19:55:20 2021
Stopped: Sat Jul 10 19:55:23 2021
```



```
┌──(vicog㉿kali)-[~/Downloads]
└─$ john --format=PKZIP hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
test123          (YouCantCrackMe.zip/EncryptedFolder/Secret Message.txt)
1g 0:00:00:00 DONE 2/3 (2021-06-25 13:51) 50.00g/s 2808Kp/s 2808Kc/s 2808KC/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

File Systems



CS4CS Story