NCL INDIVIDUAL

- OSINT
  - recipe
    - Notes
      - chat
    - Challenge
      - **Chef**
      - SKY-WAFF-1355
  - NotPeyta
    -
  - (hard)
    -
    - Cryptography
- Cryptography
  - Notes
    - https://www.boxentriq.com/code-breaking/cipher-identifier + https://gchq.github.io/CyberChef/
    - 1 is binary. from binary in cyber chef.
    - 2 is from hex
    - 3 is from base64
  - Challenge

    00110011 01110011 01101001 01101100 00111000 00110100 00111001

- 3sil849

616e746a75616e31343339

- antjuan1439

OWtsbXBkbzA3

- 9klmpdo07

▼ Password Cracking

▼ Redacted (medium)

▼ Notes

- pdf2john conflict.pdf > pdf.txt
- john --wordlist=rockyou.txt pdf.txt

▼ Challenge

▼ Log Analysis

▼

▼ Notes

- 1- scrolled to the bottom to see last number
- 2 - FILE=route53.log , `awk '{print $(NF-1)}' route53.log | sort | uniq -c | sort -nr | awk 'NR==1{print $2}'`
- 3- `awk '$4!="-"{print tolower($4)}' route53.log | sort | uniq -c | sort -n | awk 'NR==1{print $2}'`
- 4- awk '$NF != "-" && $NF ~ /\/[0-9]+$/ {print $NF}' route53.log \ | sort | uniq -c | sort -nr | awk 'NR==1{print $2}'
- 5- `awk '{print substr($2,1,16)}' route53.log | sort | uniq -c | sort -nr | awk 'NR==1{print $2}'`
- 6- `awk '{print $(NF-2)}' route53.log | sort | uniq -c | sort -nr | awk 'NR==10{print $2}'`
- 7- awk '{ # find the token that looks like an AWS resolver location, e.g. IAD89-C3, DFW55-C1 for(i=1;i<=NF;i++){ if ($i ~ /^[A-Z]{3}

[0-9]+-C[0-9]+$/) { city = substr($i,1,3) # keep only the first 3 letters ⇒ city code count[city]++ break } } } END{ for (c in count) print count[c], c }' route53.log | sort -nr | awk 'NR==10{print $2}’

- 8- grep -i 'cityinthe.cloud' route53.log \| awk '{print $(NF-2)}' \| sed -E 's/^([A-Z]{3}).*/\1/' \| sort | uniq -c | sort -nr | awk 'NR==1{print $2}' \| awk 'BEGIN{r["IAD"]="us-east-1"; r["JFK"]="us-east-1"; r["EWR"]="us-east-1"; r["BOS"]="us-east-1";r["ATL"]="us-east-1"; r["MIA"]="us-east-1"; r["DFW"]="us-east-1";r["CMH"]="us-east-2"; r["ORD"]="us-east-2";r["SFO"]="us-west-1"; r["LAX"]="us-west-1";r["SEA"]="us-west-2"; r["PDX"]="us-west-2"; r["PHX"]="us-west-2"; r["DEN"]="us-west-2"} {print (r[$0]?r[$0]:"unknown("$0")")}’

▼ Challenge

Q1 - 5 points How many total requests are recorded in this log?	4519
Q2 - 15 points What is the IP address of the resolver that made the largest number of requests?	155.225.66.25
Q3 - 15 points What is the least requested domain name?	backup.cityinthe.cloud
Q4 - 15 points What is the client subnet (in CIDR notation) that made the largest number of requests?	192.154.46.0/24
Q5 - 15 points Which minute of the day had the largest number of requests?	19:35
Q6 - 25 points Which city received the 10th largest number of requests?	Miami
Q7 - 10 points What AWS region does cityinthe.cloud use for its Virtual Private Cloud?	us-east-1

▼ Network Traffic Analysis

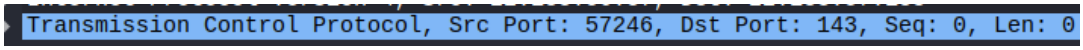
▼

▼ Notes

1. 1st packet → internet protocol → src

2. 1st packet → internet protocol → dst

3.



4. follow TCP steam
5. follow TCP steam
6. follow TCP steam
7. follow TCP steam

▼ Challenge

Q1 - 10 points What is the client's IP address?	22.183.56.37
Q2 - 10 points What is the server's IP address?	22.183.57.188
Q3 - 10 points What TCP port are they communicating over?	143
Q4 - 10 points What is the name of the server software?	Dovecot
Q5 - 15 points What is Tom's password?	mashandgravy
Q6 - 15 points What is the email address of the malicious actor?	b33b0p@wonkey.leaks
Q7- 20 points Where does the actor want to meet Tom?	Paris

▼ Forensics

▼ four & six (easy)

▼ Notes

- ls --quoting-style=literal ~/Downloads - gets rid of quotes

▼ Challenge

-

Q1 - 10 pointsWhat is the name of the storage volume?	
Q2 - 10 pointsWhat specific variant of file system is used to store the data?	
Q3 - 10 pointsHow many files are deleted files?	
Q4 - 10 pointsHow many files are present on the volume? (excluding deleted or system volume files)	
Q5 - 10 pointsWhat is the total number of bytes for the deleted files in unallocated space?	
Q6 - 15 pointsDon't sweat this. The photo says the flag is valid so try it here →	
Q7 - 15 pointsWhat is the flag hidden in the binary data of one of the files?	
Q8 - 20 pointsThere is a flag that appears after viewing a file for at least 8 seconds. What is the flag?	

▼

▼ Web App

1. delete debug button in source code, flag will flash

- check chat log for answer to number two

2.

try using use burp

either in inspect console or storage

robots.txt

3. could not figure out hard

▼ Enumeration