NCL FALL 2025 PRACTICE GAMES

▼ OSINT

▼ WHOIS (easy)

▼ Notes

- https://lookup.icann.org/en/lookup
- google search for last one

▼ Challenge

Q1 - 10 points
Who is the registrar of this domain?

- Dynadot Inc

Q2 - 10 points
On what day was this domain first registered?

- 2016-02-16

Q3 - 10 points
What is this domain's registry domain id?

- D15CD1AC4DEB54207A5048A69B9FC0558-ARI

Q4 - 10 points
What is the TLD of this domain?

- .cloud

Q5 - 10 points
What organization manages the TLD used by cityinthe.cloud?

- Aruba PEC SpA

▼ Vehicle (easy)

▼ Notes

- google images

▼ Challenge

- CHRYSLER 300M

▼ Geo Data (medium)

▼ Notes

- https://www.gps-coordinates.net/
- and chat

▼ Challenge

Q1 - 10 points
What is the street address of the building?

- 300 E Street SW, Washington, DC 20546

Q2 - 10 points
What is the name of the organization that occupies the building?

- NASA

Q3 - 30 points
What is the name of the organization that owns the building?

- Hana Alternative Asset Management

▼ Colonial Crypto (medium)

▼ Notes

- first one https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/did-the-fbi-hack-bitcoin-deconstructing-the-colonial-pipeline-ransom
- all of them https://x.com/andrew___morris/status/1402346861500026886

▼ Challenge

Q1 - 20 points What's the full address of the wallet ending in `eqwg45`?	bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45
Q2 - 20 points What's the full address of the wallet ending in `KcdNxB`?	3EYkxQSUv2KcuRTnHQA8tNuG7S2pKcdNxB
Q3 - 20 points What's the full address of the wallet ending in `cfsegq`?	bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq

▼ Base of Operations

▼ Notes

-

▼ Challenge

-

▼ Cryptography

▼ Decoding 1(easy)

▼ 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

▼ Decoding 2 (easy)

▼ Notes

- https://www.dcode.fr/caesar-cipher
- https://www.boxentriq.com/code-breaking/cipher-identifier
- regular Caesar cipher

▼ Challenge

Gurer jrer guerr ubfgf hc va gur cbeg fpna	There were three hosts up in the port scan
Q2 - 30 points Y vekdt vylu TDI husehti veh jxqj tecqyd	I found five DNS records for that domain

▼ Decoding 3 (easy)

▼ Notes

- Use https://www.boxentriq.com/code-breaking/cipher-identifier and https://www.prepostseo.com/tool/decimal-to-ascii

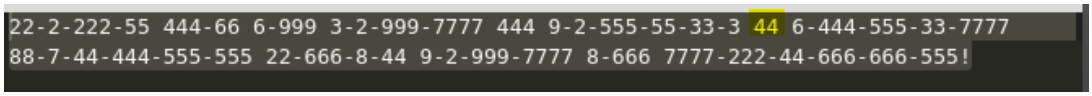
▼ Challenge

- Do you think they will be able to decrypt this - SKY-ASCI-4493

▼ Decoding 4 (medium)

▼ Notes

- asked chat what kind of cypher
- https://www.dcode.fr/multitap-abc-cipher
- Counted out the words to get the number of miles



▼ Challenge

back in my days i walked 44 miles uphill both ways to school!

▼ Decoding 5 (hard)

▼ Notes

- n=1079= 13 × 83
- used chat to do all the math

▼ Challenge

What is the value of p (the smaller prime)? (10 pts)

- 13

What is the value of q (the larger prime)? (10 pts)

- 83

What is the plaintext of the encrypted message? (30 pts)

- SKY-KRYG-5530

▼ Unknown (hard)

▼ Notes

-

▼ Challenge

▼ Password Cracking

▼ Hashing (easy)

▼ Notes

- used chat

▼ Challenge

Q1 - 5 points What is the MD5 hash of "LXBWUBEU"	f1e0e04ba5834bf737cc10acb262048b
Q2 - 5 points What is the SHA1 hash of "AJCRVRZE"	1a622a01ea36687c9bef8d46b22bc3d3a0a372a1
Q3 - 5 points What is the SHA256 hash of "ANBZCNVM"	517a8d1c32eb1b423de55cf9bf07dafedd8d1060c8b5c6ff5021ec9f99f2f86b

▼ Cracking 1 (easy)

▼ Notes

- sudo nano cracking1.txt, copy and paste the passwords to be cracked
- look up rock you txt github, go to terminal
- git clone https://github.com/RykerWilder/rockyou.txt.git
- unzip rockyou.txt-main.zip
- mv folder to same directory
- hashcat -m 0 -a 0 cracking1.txt rockyou.txt-main

▼ Challenge

d9a336ea69220c9383bcf9ab0a86b13d

- 56gemma56

23438e607b757fd755a00f708cad9f24

- loquitakitana

12ec6692013de5cf87f55a4a24f9ee60

- monnaka55

▼ Cracking 2 (medium)

▼ Notes

- Download ophcrack on windows and the small table
- input each hash one by one

▼ Challenge

6AF7253D3F2E0BD51D71060D896B7A46:0FD4E353D19B1507E8421BFA119EA7DE

- ofarij22

75F319E42A9540CB1AA818381E4E281B:9D90CD8797F3BF9918B23AC096B8EE6F

- lutani83

25CB3174B9E50DBF1AA818381E4E281B:D8E8861BBD7DC37AFFB9EAC45075ACFB

- ocuvet73

▼ Cracking 3 (medium)

▼ Notes

- make a txt file with your hashes
- since we are given more than half of the flag we use hashcat -m 0 -a 3 cracking3.txt 'SKY-BMYS-?d?d?d?d'
- tries all combos 0000-9999

▼ Challenge

1650676a6409df93c005c6f040e29bd7

- SKY-BMYS-6991

---

ad12908ab4f2db14915b9a27def5c244

- SKY-BMYS-7279

---

d75c4976711bc318c33d2f5d770728f8

- SKY-BMYS-8426

▼ Cracking 4 (hard)

▼ Notes

- make a file with all the hashes
-

▼ Challenge

Q1 - 10 points1uxff$sOWmNmM0vFCumj19j0I981	
Q2 - 10 points1tnck$hhGUKgOmf.fRaG3ZFAMvx1	
Q3 - 15 points1dgsn$2ZgX3pvquWorGD2Lgjj3W1	
Q4 - 35 points1vgah$VnxHyh1o3FwMZAvKA5AQo0	
Q5 - 50 points1lkwc$iOXF5ekiNNyj1KByGFO8s/	

▼ PDF (medium)

▼ Zip (hard)

▼ Notes

-

▼ Challenge

▼ Log Analysis

▼ AWS Route 53 (easy)

▼ 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

▼ Devices (medium)

▼ Notes

- 1- awk '!/^\/\// { gsub(/\[|\]/,"",$2); print $2 }' devices.log | sort -u | wc -l
- 2- awk '!/^\/\// { gsub(/[{}]/,"",$3); print $3 }' devices.log | sort -u | wc -l
- 3- awk '!/^\/\// { gsub(/%/,"",$4); sum+=$4; n++ } END { printf("%.0f\n", sum/n) }' devices.log
- 4- awk '!/^\/\// && $3=="{POWER_METER}" { total+=$5 } END { print total }' devices.log
- 5- awk '!/^\/\// && $3=="{POWER_METER}" { day=substr($1,1,10); usage[day]+=$5 }
  END { for (d in usage) print d, usage[d] }' devices.log \
  | sort -k2,2nr | head -1
- 6- awk '!/^\/\// && $3=="{POWER_METER}" { day=substr($1,1,10); usage[day]+=$5 }
  END { for (d in usage) print d, usage[d] }' devices.log \
  | sort -k2,2nr | head -1 | awk '{print $2}'

▼ Challenges

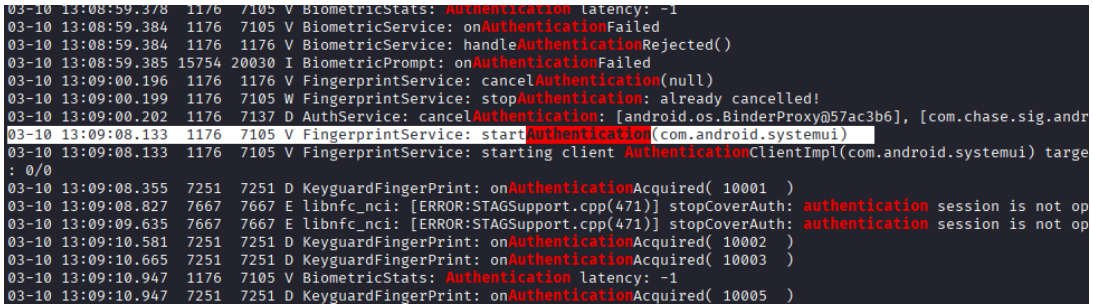
Q1 - 10 points How many different devices are present in the log?	7
Q2 - 10 points How many different device types are present in the log?	4

Q3 - 20 points What is the average battery life of all the devices throughout the duration of the log? (Round to the nearest whole percent)	58
Q4 - 15 points What is the total power usages reported from the power meters?	142970
Q5 - 25 points On what day was the most power used?	2022-03-24
Q6 - 30 points How much power was consumed that day?	26380

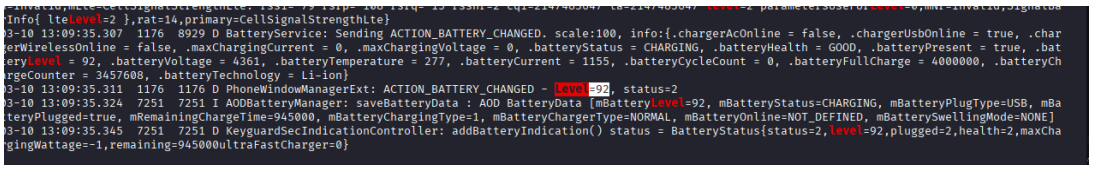
▼ mobile (hard)

▼ Notes

- 1- awk 'NF>4 && $5=="D"' system.log | wc -l
- 2- grep -iE 'build fingerprint|ro\.build\.version|Android [0-9]|OS version' system.log | head -20 → look at the first line
- 3- `grep -i 'onAuthenticationSucceeded' system.log | wc -l`
- 4-`grep -c -F 'FingerprintService: handleAuthenticated: false' system.log`
- 5- grep -i 'Authentication' system.log

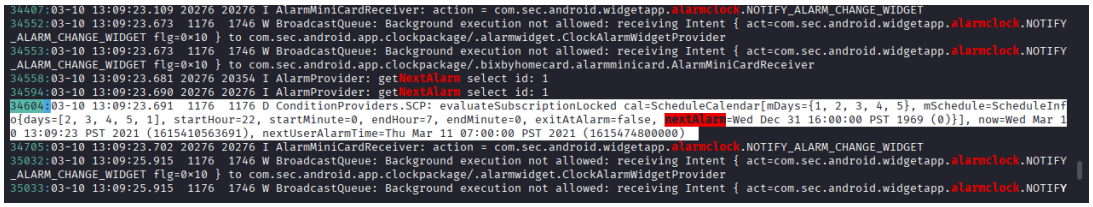


- 6- grep -i 'ssid' system.log
- 7- grep -i 'level' system.log



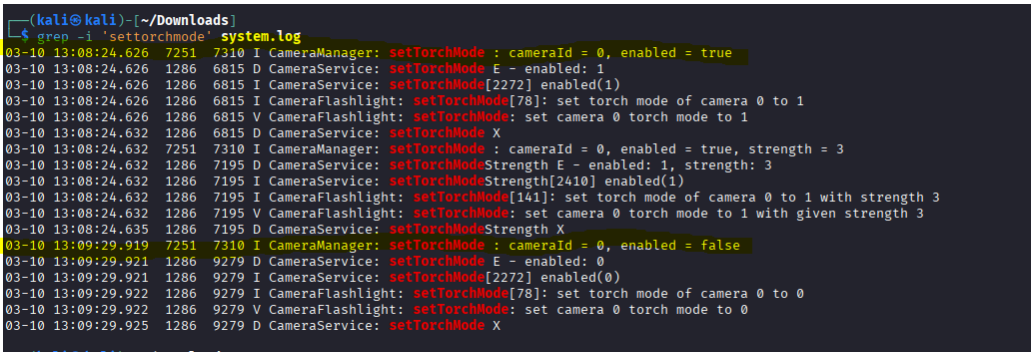
▼ Notes P2

- 8- grep -niE 'AlarmClock|nextAlarm|DeskClock|com\.android\.deskclock' system.log



- 9- grep -i 'flashlight' system.log

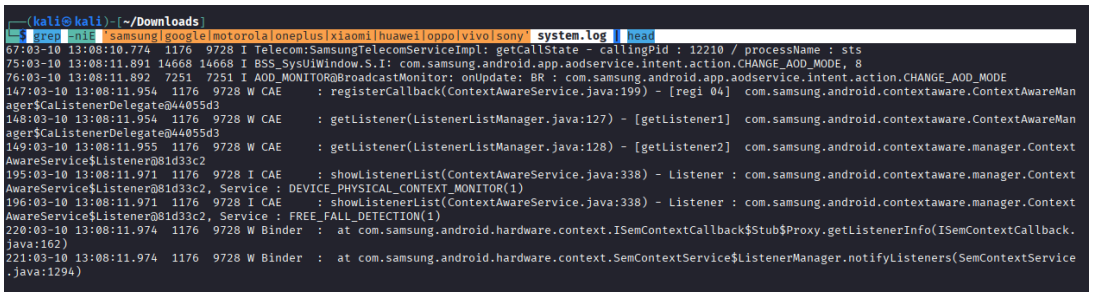
  - grep -i 'settorchmode' system.log



- ON = **13:08:24.623** → ((13×3600 + 8×60 + 24)×1000 + 623) = **47,304,623 ms**
- OFF = **13:09:29.919** → ((13×3600 + 9×60 + 29)×1000 + 919) = **47,369,919 ms**

  OFF – ON = 47,369,919 – 47,304,623 = 65,296 ms

- 10- grep -niE 'samsung|google|motorola|oneplus|xiaomi|huawei|oppo|vivo|sony' system.log | head



- 11-grep -niE '\bSM-[A-Z0-9]+' system.log

```
┌──(kali㉿kali)-[~/Downloads]
└─$ grep -niE '\bSM-[A-Z0-9]+' system.log
13126:03-10 13:08:40.147 15902 15902 I FeatureManager: FeatureManager() : product is o1quew, model is SM-G991U1
14118:03-10 13:08:40.506 13041 15979 I eggInc  : Device Platform: samsung SM-G991U1
14351:03-10 13:08:40.655 15902 15902 I ModelUtil: isHighEndModel() : this model is SM-G991U1
14497:03-10 13:08:40.762 13041 15972 D AppLovinSdk: Model: SM-G991U1
15857:03-10 13:08:41.693 13041 16449 I UnityAds: com.unity3d.services.core.api.Sdk.logInfo() (line:84) :: Requesting configuration from https://publisher-config.unityads.unity3d.com/games/1079239/configuration?deviceMake=samsung&screenDensity=480&screenSize=2684358106idfi=d7892a5b-e1c8-4b98-a7e9-1b99047e8d15&advertisingTrackingId=60b069fd-5c03-48c8-81d4-d036ee26df1c&limitAdTracking=false&connectionType=wifi&screenHeight=2275&screenWidth=1080&bundleId=com.auxbrain.eggInc&encrypted=true&rooted=false&platform=android&sdkVersion=3600&osVersion=11&deviceModel=SM-G991U1&language=en_US&test=false&first=false&c.ads=true&c.external=true&c.gameExp=true
16866:03-10 13:08:42.023 13041 16449 I UnityAds: com.unity3d.services.core.api.Sdk.logInfo() (line:84) :: Requesting ad plan from https://auction.unityads.unity3d.com/v6/games/1079239/requests?idfi=d7892a5b-e1c8-4b98-a7e9-1b99047e8d15&advertisingTrackingId=60b069fd-5c03-48c8-81d4-d036ee26df1c&limitAdTracking=false&deviceModel=SM-G991U1&platform=android&sdkVersion=3600&stores=google&deviceMake=samsung&screenSize=268435810&screenDensity=480&apiLevel=30&screenWidth=1080&screenHeight=2275&connectionType=wifi&networkType=0
17024:03-10 13:08:43.661 15902 15902 I ModelUtil: isHighEndModel() : this model is SM-G991U1
17327:03-10 13:08:46.665 15902 15902 I ModelUtil: isHighEndModel() : this model is SM-G991U1
```

▼ Challenge

Q1 - 5 points How many debug messages are present in the log?	10699
Q2 - 5 points What OS is this device running?	android
Q3 - 10 points How many times was finger print authentication accepted?	3
Q4 - 10 points How many times was finger print authentication denied?	7
Q5 - 15 points What is the application ID (other than the lock-screen) that successfully used finger print authentication?	com.x8bit.bitwarden
Q6 - 15 points What is the name of the WiFi network the phone is connected to?	BBNET5
Q7 - 20 points What is the battery percentage at the end of the log? NOTE: This question only allows maximum of 5 attempts, you have 5 attempts remaining.	92
Q8 - 20 points What date and time is the alarm set for? (in UTC)	2021-03-11 15:00
Q9 - 20 points How long (in milliseconds) was the flashlight on?	65,296
Q10 - 5 points What company is the manufacturer of the phone?	samsung
Q11 - 25 points What is the full model number of the phone?	SM-G991U1

▼ Network Traffic Analysis

▼ Retriever (easy)

▼ Notes

1. 1st packet → internet protocol → src
2. 1st packet → internet protocol → dst

```
Internet Protocol Version 4, Src: 22.183.56.37, Dst: 22.183.57.188
```

3.

```
Transmission Control Protocol, Src Port: 57246, Dst Port: 143, Seq: 0, Len: 0
```

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

▼ Cracking (medium)

▼ Notes

1.

▼ Challenge

Q1 - 10 points What channel was the victim network operating on?	Channel 4
Q2 - 10 points What is the ESSID of the wifi network that was hacked?	
Q3 - 10 points What is the MAC address of the device generating traffic that makes cracking the password on the wifi network possible?	
Q4 - 10 points What company is assigned the OUI of the access point?	
Q5 - 30 points What is the wireless password (in hex)?	

▼ TV (medium)

u can use pcap analyzer → a packets.com

▼ Secret (hard)

▼ Forensics

▼ Archive (easy)

▼ Notes

- To get the first question
  - file corrupted.rar

        - unrar l corrupted.rar
    - To get the flag
        - unrar l corrupted.rar
        - unrar p -inul corrupted.rar not_a_flag.jpg > recovered.jpg
        - open recovered.jpg
  - ▼ Challenge

    What is the full name of the file inside the archive? (20 pts)

    - not_a_flag.jpg
    - SKY-RARA-7458
- ▼ Puzzle (medium)
  - ▼ Notes
  - ▼ Challenge

Q1 - 50 points What is the SHA256 checksum (in hexadecimal representation) of the reassembled file?	
Q2 - 50 points What is the flag?	

  - ▼

- ▼ Web App a

  use burp

  either in inspect console or storage

  robots.txt

- ▼ Enumeration