A pixel art of a christmas wreath

Description automatically generated

# Bournemouth 2600 Xmas Challenge Questions

**Note:**

* An Answers Doc shall be provided at the end of the challenge.
* There is an MD5 hash of all answers in this document, which you can use to check if you are correct before the Answers Doc is provided.
* Please use GCHQ’s [CyberChef](https://gchq.github.io/CyberChef/#recipe=MD5()) to check your answers in the Input box.

## Challenge 1 – Posh Christmas Tree

Qr code on a chalkboard surrounded by presents and ornaments

Description automatically generated

MD5 of the Answer: c9f1ffad2e6bb76185a7c13b85e73033

## Challenge 2 – Packets for Presents

Download the PCAPs from the B2600 GitHub and open them in Wireshark (free to download as well from wireshark.org)

<https://github.com/Bournemouth2600/XmasChallenge>

1. Find the Exfil domain in PCAP ccda62b0-4607-4670-bd19-9823687bdf25
2. Find the Exfil Server’s Password in PCAP cbfd7146-bf87-4356-9551-9ecbcdf28344

MD5 of the answer for A: 1b86f1407d3db723d47354eba6f03594

MD5 of the answer for B: a5c4da6fadeb5290c986fadfb6139921

## Challenge 3 – Ransomware for Christmas

Q1. Using OSINT, which Japanese company was a victim to ransomware in August 2023?

MD5 of the answer (all caps): f05bc92a3226029b50ed9eb83f21c6b4

Q2. Using OSINT, which ransomware group attacked that company?

MD5 of the answer (all caps): 247c8c480e9aa03e3679dc10252f2254

Q3. Using OSINT, which initial access broker offered access to the victim company?

MD5 of the answer (same as the forum profile): 6af99b338644a106a9337c33bfcc86cf

Q4. Using OSINT, which Forum did the initial access broker make post on?

MD5 of the answer (use the domain): 993816f95f2cda3daa9c20906fbb50bc

## Challenge 4 – Scrooge’s Bitcoin

Q1. How much Bitcoin did Akira receive in total from the six addresses associated with them?

Find the BTC addresses (bc1q): <https://www.ransomware.live/group/akira#btc>

Check them on: <https://blockchain.com>

MD5 of the answer (just the digits, e.g., 1.11111111): b4af2534d75c4dee6937773562e53e0e

## Challenge 5 – IOCs for Pudding

Download the list of indicators of compromise (IOCs) from the GitHub

<https://github.com/Bournemouth2600/XmasChallenge>

Q1. Which IP address is attributed to FANCY BEAR (aka APT28)?

Q2. Which IP address is attributed to WICKED PANDA (aka APT41) ?

Q3. Which Domain is attributed to CHARMING KITTEN (aka APT35) ?

Q4. Which Domain is attributed to VELVET CHOLLIMA (aka APT43 or Kimsuky) ?

Q5. Which Hash is attributed to PUNK SPIDER (aka Akira) ?

Q6. Which Hash is attributed to SCATTERED SPIDER (aka 0ktapus) ?

**Hint:** You could use sites like VirusTotal, MalwareBazaar, and LevelBlue (formerly OTX Alienvault) to help you figure these out.