Scenario

One of our web servers recently got compromised and was hit with ransomware. Luckily, we had a restore point just before the files were encrypted and managed to recover a suspicious script file that didn't appear to have been run yet.

What is the malicious IP address referenced multiple times in the script?

- *Format:* `IP Address`

The script uses apt-get to retrieve two tools, and uses yum to install them. What is the command line to remove the yum logs afterwards?

- *Format:* `Command Line`

A message is created in the file /etc/motd. What are the three first words?

- *Format:* `Message Text`

This message also contains a contact email address to have the system fixed. What is it?

- *Format:* `Mailbox@domain.tld`

When files are encrypted, an unusual file extension is used. What is it?

- *Format:* `.X`

There are 5 functions associated with the encryption process that start with ‘encrypt’. What are they, in the order they’re actually executed in the script? (do not include "()")

- *Format:* `function1, function2, ...`

The script will check a text file hosted on the C2 server. What is the full URL of this file?

- *Format:* `https://IPAddress/something/file.txt`