## TASK 4: LOG ANALYSIS TOOLS USING LINUX COMMAND LINE

## TASK 5: LOG ANALYSIS USING REGULAR EXPRESSIONS

## TASK 6: LOG ANALYSIS USING CYBERCHEF

## TASK 7: LOG ANALYSIS TOOLS: YARA AND SIGMA

Answer the questions below

What's the term for a consolidated chronological view of logged events from diverse sources, often used in log analysis and digital forensics?

Super Timeline — ✓ Correct Answer

Which threat intelligence indicator would `5b31f93c09ad1d065c0491b764d04933` and `763f8bdbc98d105a8e82f36157e98bbe` be classified as?

File Hashes — ✓ Correct Answer

What is the default file path to view logs regarding HTTP requests on an Nginx server?

/var/log/nginx/access.log — ✓ Correct Answer

A log entry containing `%2E%2E%2F%2E%2E%2Fproc%2Fself%2Fenviron` was identified. What kind of attack might this infer?

Path Traversal — ✓ Correct Answer

A log file is processed by a tool which returns an output. What form of analysis is this?

Automated — ✓ Correct Answer

An analyst opens a log file and searches for events. What form of analysis is this?

Manual — ✓ Correct Answer

Use `cut` on the `apache.log` file to return only the URLs. What is the flag that is returned in one of the unique entries?

c701d43cc5a3acb9b5b04db7f1be94f6 — ✓ Correct Answer — Hint

In the `apache.log` file, how many total HTTP 200 responses were logged?

52 — ✓ Correct Answer — Hint

In the `apache.log` file, which IP address generated the most traffic?

145.76.33.201 — ✓ Correct Answer — Hint

What is the complete timestamp of the entry where `110.122.65.76` accessed `/login.php`?

31/Jul/2023:12:34:40 +0000 — ✓ Correct Answer — Hint

How would you modify the original `grep` pattern above to match blog posts with an ID between 20-29?

post=2[0-9] — ✓ Correct Answer — Hint

What is the name of the filter plugin used in Logstash to parse unstructured log data?

Grok — ✓ Correct Answer

Locate the "loganalysis.zip" file under `/root/Rooms/introloganalysis/task8` and extract the contents.

No answer needed — ✓ Correct Answer

Upload the log file named "access.log" to CyberChef. Use regex to list all of the IP addresses. What is the full IP address beginning in 212?

212.14.17.145 — ✓ Correct Answer

Using the same log file from Question #2, a request was made that is encoded in base64. What is the decoded value?

THM{CYBERCHEF_WIZARD} — ✓ Correct Answer

Using CyberChef, decode the file named "encodedflag.txt" and use regex to extract by MAC address. What is the extracted value?

08-2E-9A-4B-7F-61 — ✓ Correct Answer

What languages does Sigma use?

YAML — ✓ Correct Answer

What keyword is used to denote the "title" of a Sigma rule?

title — ✓ Correct Answer

What keyword is used to denote the "name" of a rule in YARA?

rule — ✓ Correct Answer

**RESULT:**

After completing this, got a solid foundation in log analysis, a critical skill in cybersecurity for identifying, investigating, and responding to security threats efficiently.

# PROCESS CODE INJECTION

**EXP.NO: 10** **DATE:01-04-2025**

## AIM:

To do process code injection on Firefox using ptrace system call

## ALGORITHM:

1. Find out the pid of the running Firefox program.
2. Create the code injection file.
3. Get the pid of the Firefox from the command line arguments.
4. Allocate memory buffers for the shellcode.
5. Attach to the victim process with PTRACE_ATTACH.
6. Get the register values of the attached process.
7. Use PTRACE_POKETEXT to insert the shellcode.
8. Detach from the victim process using PTRACE_DETACH

## PROGRAM CODE:

### INJECTOR PROGRAM

```
# include <stdio.h>//C standard input output
# include <stdlib.h>//C Standard General Utilities Library
# include <string.h>//C string lib header
# include <unistd.h>//standard symbolic constants and types
# include <sys/wait.h>//declarations for waiting
# include <sys/ptrace.h>//gives access to ptrace functionality
# include <sys/user.h>//gives ref to regs
```