Comandos útiles para análisis de logs del sistema

Monitorear en tiempo real	tail -f <ruta>	
Buscar aparición exacta	grep -e "<patrón>" <ruta>	*-e = regular expresion*
Buscar un texto	grep -i <cadena> <ruta>	*-i = case insensitive*

Capturar búsquedas en tiempo real: <tail> | <grep>

Ruta de los logs principales

/var/log/

auth.log - Registros de autentificación

Intentos fallido de convertirse en root	grep -e "FAILED su for root"
Autentificaciones fallidas en general	grep -i failure

fail2ban.log - Logs del programa Fail2Ban

syslog.log - Mensajes del Sistema

Bloqueos de iptables	grep -e "SRC=<ip>" [-c]	*-c = count*

apt/history.log - Historial de cambios efectuados por apt

Laboratorio 75-A

Elaborar un informe forense con la siguiente información:

- Cantidad de veces que se intentó acceder a la web katmandu<N>.laeci.org con la palabra admin como parte de la URI
- Lista de Ips que a simple vista, han realizado uno o más intentos de conexión fallida al sistema. La lista deberá ser una lista de filas por IP, con dos columnas:
  <ip> <número de conexiones fallidas detectadas>

Bibliografía adicional:

Análisis de los logs de acceso de Apache, E. Bahit, 2013

Para control del alumno:

```
FECHA TEÓRICO:                  _____/_____/_________
FECHA ENTREGA LABORATORIO:      _____/_____/_________
FECHA RECUPERATORIO:            _____/_____/_________
LABORATORIO EXAMINATORIO:       [ ] SI    [ ] NO
APROBADO:                       [ ] SI    [ ] NO
```