Log Analysis for VPN Authentication Events

Project Overview

This project involves analyzing log files to extract specific information related to successful VPN authentication events. The task is to review two log files, 'practice.log.1' and 'practice.log.2', and address the following objectives:

- Objective A: Identify any user accounts with the keyword 'test' that have successfully authenticated via VPN.
- Objective B: Determine the source IP address for each 'test' account that authenticated successfully.
- Objective C: Identify any other user accounts that used the same source IP address as the 'test' accounts for VPN authentication.

Analysis Process

Step 1: Initial Inspection of Log Files

The analysis began by inspecting the contents of both 'practice.log.1' and 'practice.log.2' using the head command to display the first 10 lines.

```
cybrary@soc:~/Documents/Practice$ head practice.log.1
[    0.000000] kernel: Linux version 5.15.0-1031-aws (buildd@lcy02-amd64-016) (gcc (Ubuntu 11.3.0-1ubu
ntu1~22.04) 11.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #35-Ubuntu SMP Fri Feb 10 02:07:18 UTC 2023
 (Ubuntu 5.15.0-1031.35-aws 5.15.85)
[    0.000000] kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-1031-aws root=PARTUUID=f307bf97-4
8ad-40a2-adfd-4711e7382cf9 ro console=tty1 console=ttyS0 nvme_core.io_timeout=4294967295 panic=-1
[    0.000000] kernel: KERNEL supported cpus:
[    0.000000] kernel:   Intel GenuineIntel
[    0.000000] kernel:   AMD AuthenticAMD
[    0.000000] kernel:   Hygon HygonGenuine
[    0.000000] kernel:   Centaur CentaurHauls
[    0.000000] kernel:   zhaoxin   Shanghai
[    0.000000] kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
```

```
cybrary@soc:~/Documents/Practice$ head practice.log.2
Timestamp,Username,Source IP,Status
2023-08-04 12:01:34,john_doe,203.45.67.89,Failed
2023-08-04 12:01:35,john_doe,203.45.67.89,Failed
2023-08-04 12:02:10,jane_smith,104.32.11.78,Failed
2023-08-04 12:02:11,jane_smith,104.32.11.78,Failed
2023-08-04 12:03:20,vpn_user123,192.168.1.100,Success
2023-08-04 12:04:05,admin,54.23.87.112,Failed
2023-08-04 12:04:06,admin,54.23.87.112,Failed
2023-08-04 12:04:35,susan.johnson,88.76.54.32,Failed
2023-08-04 12:04:36,susan.johnson,88.76.54.32,Failed
```

Based on the initial inspection, it was evident that the VPN authentication events were recorded in 'practice.log.2'.

Step 2: Time Coverage of the Logs

To ensure comprehensive coverage, the log file's time range was examined:

```
cybrary@soc:~/Documents/Practice$ head -n 2 practice.log.2
Timestamp,Username,Source IP,Status
2023-08-04 12:01:34,john_doe,203.45.67.89,Failed
```

```
cybrary@soc:~/Documents/Practice$ tail practice.log.2
2023-08-04 12:15:15,robert_johnson,200.12.33.47,Failed
2023-08-04 12:15:16,robert_johnson,200.12.33.47,Failed
2023-08-04 12:15:45,anna.brown,88.76.54.34,Failed
2023-08-04 12:15:46,anna.brown,88.76.54.34,Failed
2023-08-04 12:16:30,vpn_user789,104.32.11.80,Success
2023-08-04 12:16:31,vpn_user789,104.32.11.80,Success
2023-08-04 12:17:15,michael.davis,88.76.54.33,Failed
2023-08-04 12:17:16,michael.davis,88.76.54.33,Success
2023-08-04 12:17:45,vpn_1234,88.76.54.35,Success
```

- Start Time: August 4, 2023, 12:01:34
- End Time: August 4, 2023, 12:17:45

The log file spanned a period of approximately 16 minutes.

Step 3: File Size and Content

```
cybrary@soc:~/Documents/Practice$ ls -lah practice.log.2
-rw-rw-r-- 1 cybrary cybrary 2.7K Sep  7  2023 practice.log.2
```

- File Size: The size of 'practice.log.2' was approximately 2.7 KB.

```
cybrary@soc:~/Documents/Practice$ wc -l practice.log.2
53 practice.log.2
```

- Total Lines: The file contained 53 lines, including header rows and blank lines.

Step 4: Searching for "Test" User Accounts (Objective A)

To identify any 'test' user accounts, ‘egrep’ command along with -i option which is used to make it a case-insensitive search. This allowed the extraction of relevant VPN authentication events associated with user accounts containing the keyword 'test'.

```
cybrary@soc:~/Documents/Practice$ egrep -i "test" practice.log.2
2023-08-04 12:11:45,vpn_tester,88.76.54.33,Success
```

Step 5: Identifying the Source IP Address (Objective B)

After identifying the 'test' accounts, the source IP addresses used for VPN connections were extracted from the logs. Each 'test' account's connection was traced to its respective source IP address.

```
cybrary@soc:~/Documents/Practice$ egrep "88.76.54.33" practice.log.2
2023-08-04 12:11:45,vpn_tester,88.76.54.33,Success
2023-08-04 12:17:15,michael.davis,88.76.54.33,Failed
2023-08-04 12:17:16,michael.davis,88.76.54.33,Success
```

Step 6: Identifying Other User Accounts with the Same IP Address (Objective C)

Finally, the logs were further examined to identify any other user accounts that utilized the same source IP address as the 'test' accounts. In this analysis, it was found that a user named 'micheal.davis' used the same IP address as one of the 'test' accounts.

Conclusion

The log analysis successfully met all three objectives:
- 'Test' user accounts were identified as having successfully authenticated via VPN.
- The corresponding source IP addresses for these accounts were extracted.
- Other user accounts, specifically 'micheal.davis', were found to have used the same IP address for VPN authentication.

This detailed analysis can be used to further investigate potential security incidents or unauthorized VPN access.

Commands used:

`head` command:

- This command displays the first 10 lines of a file by default. It's useful to quickly check the beginning content of the log files.
- Example: `head practice.log.1` shows the first 10 lines of `practice.log.1`.

`egrep -i` command:

- `egrep` is used to search for patterns or keywords in a file. The `-i` option makes the search case-insensitive, meaning it will match "Test", "test", or any other variation.
- Example: `egrep -i 'test' practice.log.2` searches for any occurrences of the word "test" in `practice.log.2` regardless of capitalization.

`wc` command:

- `wc` stands for "word count," but it also counts lines and file sizes. It's used here to find out the total number of lines in the log files.

- Example: `wc -l practice.log.2` counts the number of lines in `practice.log.2`

`tail` command: This shows the last 10 lines of the specified file.

- Example: `tail practice.log.2` will display the last 10 lines of `practice.log.2`.