Executive Summary:

My name is Robert Ajegbo and I am an Access Log Analyst at a medium-sized organization called 'Turn a New Leaf.' My manager instructed me to monitor the logs for the Apache web server and send an alert if there is an unusual number of failed logins.

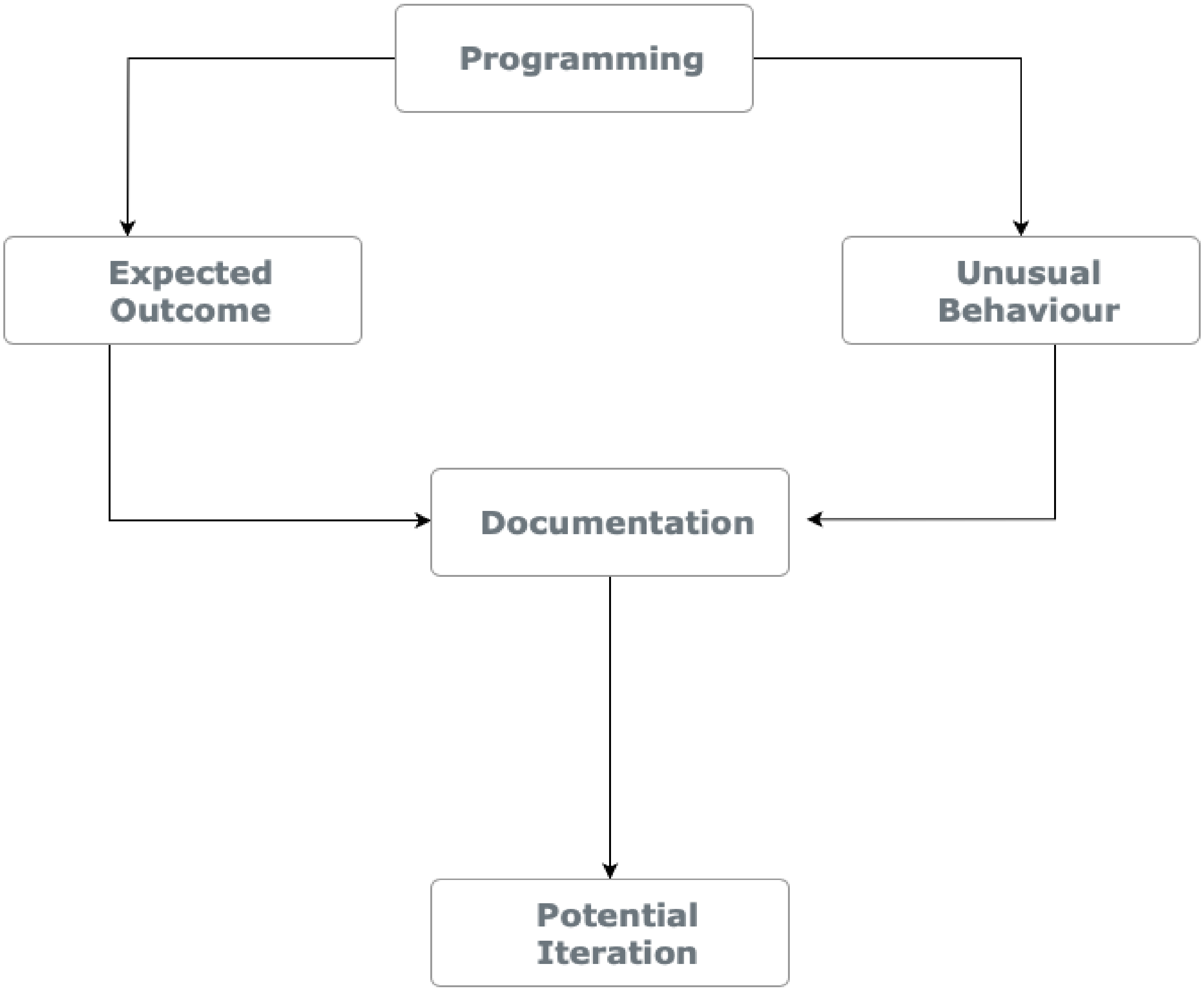
After setting up the log monitoring, I will be collecting data from the Apache logs and filtering them for information such as IP addresses, time stamps, login errors and other details helpful to the process.

Workflow:

The aim of this workflow intends to demonstrate a breakdown of my monitoring process, and how the data helps to investigate unusual behaviour on the web server.

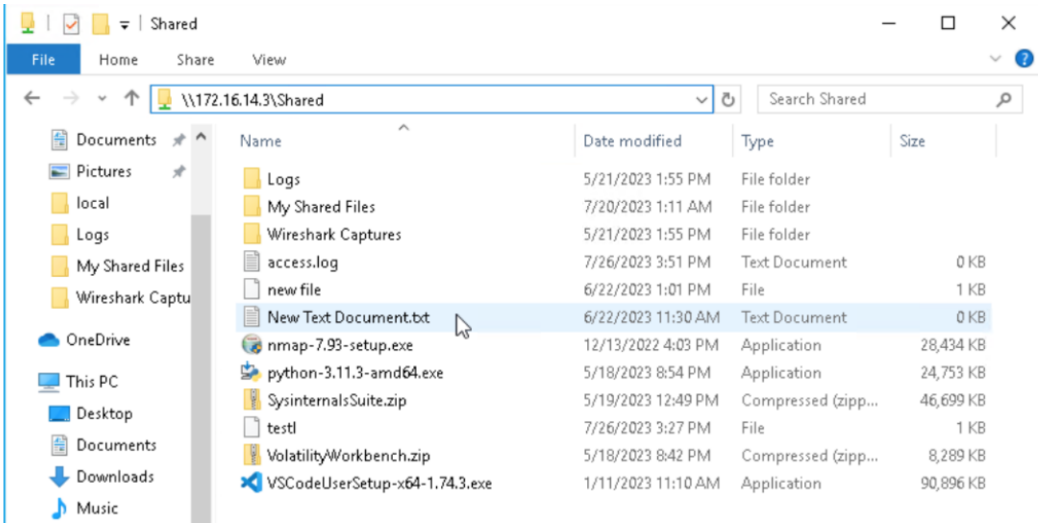
The log can also be accessed through any of the machines on the network through a Shared directory.

Workflow Diagram



Programming:
To set up your Shared Directory in, you must first verify your computer's name. (My PC name is VD-EVEP-POD1186. To access the Shared folder in the Windows 1 machine, navigate to the File Explorer and search for \\172.16.14.3\Shared. Once prompted, use the username: Student and Password: STest123.

Capture of Shared Folder in Windows 1

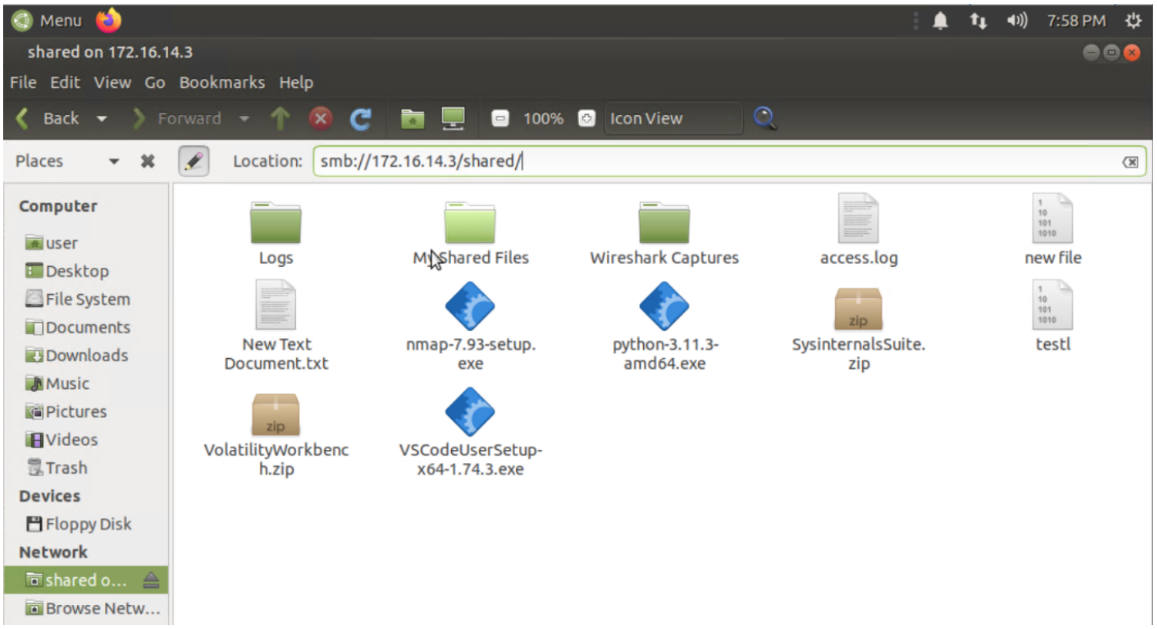


\\172.16.14.3\Shared

Name	Date modified	Type	Size
Logs	5/21/2023 1:55 PM	File folder	
My Shared Files	7/20/2023 1:11 AM	File folder	
Wireshark Captures	5/21/2023 1:55 PM	File folder	
access.log	7/26/2023 3:51 PM	Text Document	0 KB
new file	6/22/2023 1:01 PM	File	1 KB
New Text Document.txt	6/22/2023 11:30 AM	Text Document	0 KB
nmap-7.93-setup.exe	12/13/2022 4:03 PM	Application	28,434 KB
python-3.11.3-amd64.exe	5/18/2023 8:54 PM	Application	24,753 KB
SysinternalsSuite.zip	5/19/2023 12:49 PM	Compressed (zipp...	46,699 KB
testl	7/26/2023 3:27 PM	File	1 KB
VolatilityWorkbench.zip	5/18/2023 8:42 PM	Compressed (zipp...	8,289 KB
VSCodeUserSetup-x64-1.74.3.exe	1/11/2023 11:10 AM	Application	90,896 KB

To access the Shared Folder in Linux. Navigate to the home file system and search for smb://172.16.14.3/Shared. Enter the same username and password used for Windows when prompted.

Capture of Shared Folder in Linux

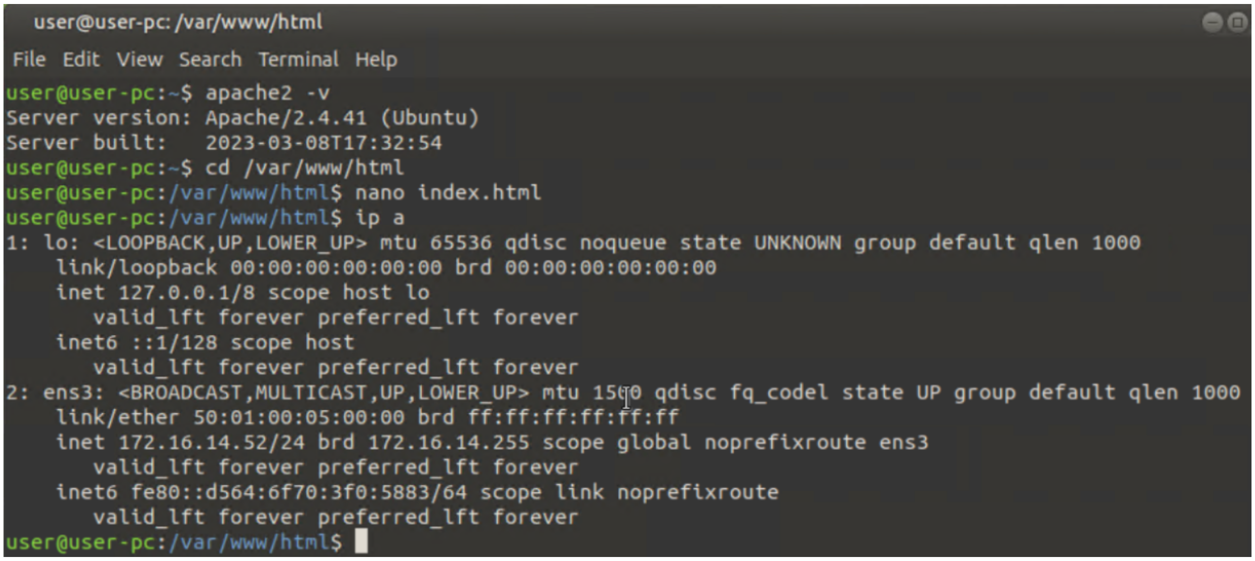


Location: smb://172.16.14.3/shared/

Logs
My Shared Files
Wireshark Captures
access.log
new file
New Text Document.txt
nmap-7.93-setup.exe
python-3.11.3-amd64.exe
SysinternalsSuite.zip
testl
VolatilityWorkbench.zip
VSCodeUserSetup-x64-1.74.3.exe

I also filtered the logs to give me better results that relate to my investigation. This included filters for IPs, login errors, time stamps and more. I also used commands like ip a and awk.
$ ip a is used to find IP addresses
$ awk is used to filter for one or more pieces of individual text

Capture of Apache server command line analysis

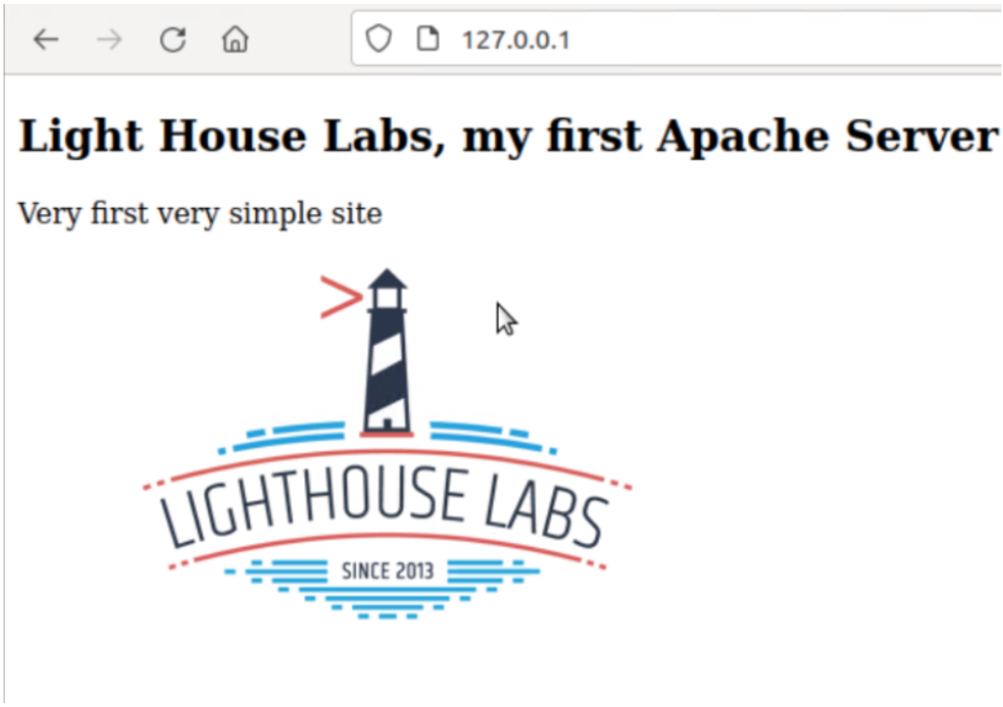


user@user-pc: /var/www/html
File Edit View Search Terminal Help

```
user@user-pc:~$ apache2 -v
Server version: Apache/2.4.41 (Ubuntu)
Server built:   2023-03-08T17:32:54
user@user-pc:~$ cd /var/www/html
user@user-pc:/var/www/html$ nano index.html
user@user-pc:/var/www/html$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:01:00:05:00:00 brd ff:ff:ff:ff:ff:ff
    inet 172.16.14.52/24 brd 172.16.14.255 scope global noprefixroute ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::d564:6f70:3f0:5883/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
user@user-pc:/var/www/html$
```

Expected Output:

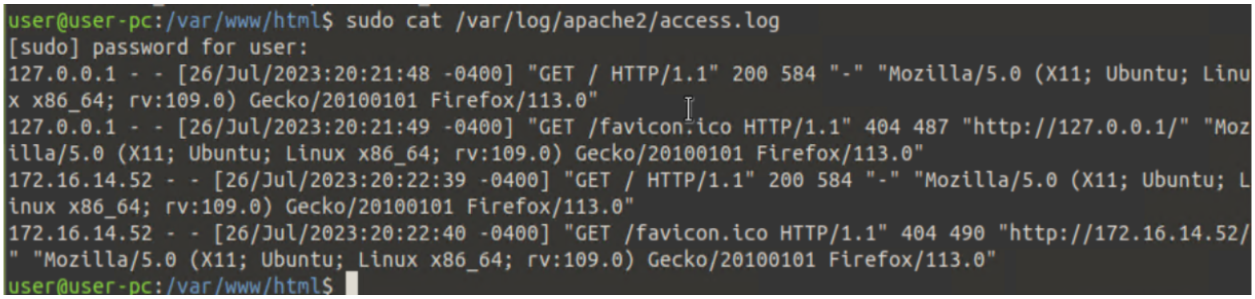
Capture of Turning a New Leaf Apache Web Server



Light House Labs, my first Apache Server

Very first very simple site

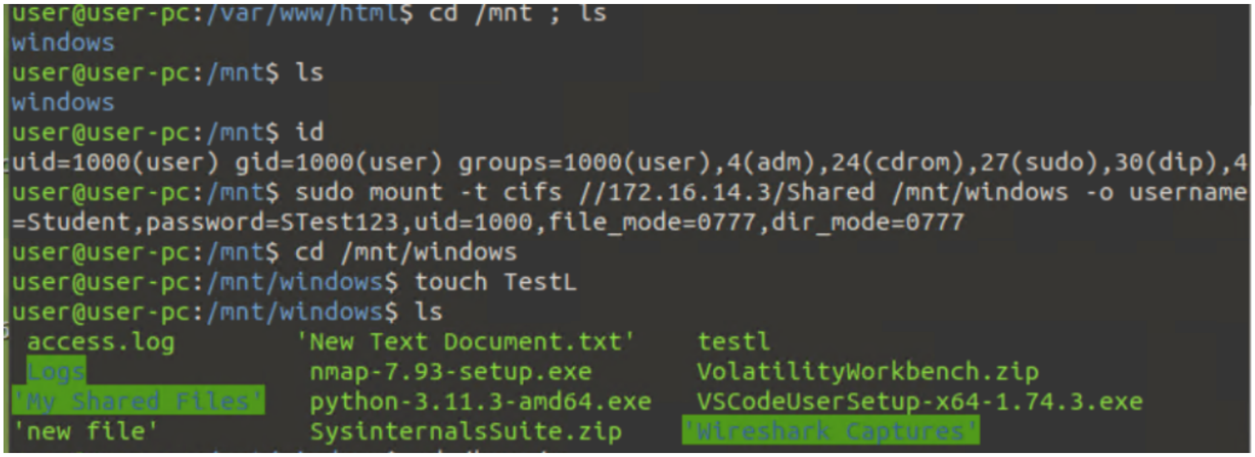
Capture showing Apache Access log



```
user@user-pc:/var/www/html$ sudo cat /var/log/apache2/access.log
[sudo] password for user:
127.0.0.1 - - [26/Jul/2023:20:21:48 -0400] "GET / HTTP/1.1" 200 584 "-" "Mozilla/5.0 (X11; Ubuntu; Linu
x x86_64; rv:109.0) Gecko/20100101 Firefox/113.0"
127.0.0.1 - - [26/Jul/2023:20:21:49 -0400] "GET /favicon.ico HTTP/1.1" 404 487 "http://127.0.0.1/" "Moz
illa/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0"
172.16.14.52 - - [26/Jul/2023:20:22:39 -0400] "GET / HTTP/1.1" 200 584 "-" "Mozilla/5.0 (X11; Ubuntu; L
inux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0"
172.16.14.52 - - [26/Jul/2023:20:22:40 -0400] "GET /favicon.ico HTTP/1.1" 404 490 "http://172.16.14.52/
" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0"
user@user-pc:/var/www/html$
```

In the above logs, you can see the log shows lots of details but we will focus on the status codes. The HTTP 200 status code represents a successful login while unsuccessful logins are represented by 400 and 500. The 400 status codes are for bad requests while 500 codes are for internal server errors. These status codes are essential for us to quickly see what is happening on the server and to recognize a potential threat from an attacker.

Capture showing log mounted between both machines in Shared folder



```
user@user-pc:/var/www/html$ cd /mnt ; ls
windows
user@user-pc:/mnt$ ls
windows
user@user-pc:/mnt$ id
uid=1000(user) gid=1000(user) groups=1000(user),4(adm),24(cdrom),27(sudo),30(dip),4
user@user-pc:/mnt$ sudo mount -t cifs //172.16.14.3/Shared /mnt/windows -o username
=Student,password=STest123,uid=1000,file_mode=0777,dir_mode=0777
user@user-pc:/mnt$ cd /mnt/windows
user@user-pc:/mnt/windows$ touch TestL
user@user-pc:/mnt/windows$ ls
 access.log          'New Text Document.txt'    testl
 Logs                 nmap-7.93-setup.exe       VolatilityWorkbench.zip
'My Shared Files'     python-3.11.3-amd64.exe   VSCodeUserSetup-x64-1.74.3.exe
'new file'            SysinternalsSuite.zip    'Wireshark Captures'
```

Unusual Behaviour:

As stated above, it is equally or even more important to view unusual behaviour within the logs. I noticed some 400 status code errors when accessing the web server through the Linux IP address. This is an example of what could be flagged and sent to the manager if there are an unusual amount of repeat errors.

Potential Iteration:

While there is not anything to worry about on the server currently, we should always look to improve security. This could be done by installing a proxy server on the Apache web server to act as a firewall and filter for web requests.

References

Benjamin, A. (2023, January 16). *:)*. Retrieved July 26, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w01d2/activities/2712

HTTP response status codes - HTTP | MDN. (2023, April 10). MDN Web Docs. Retrieved July 26, 2023, from https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

Lemonaki, D. (2021, October 12). *The Linux AWK Command – Linux and Unix Usage Syntax Examples*. freeCodeCamp. Retrieved July 26, 2023, from https://www.freecodecamp.org/news/the-linux-awk-command-linux-and-unix-usage-syntax-examples/

Security considerations for your website (ITSM.60.005). (2022, February 11). Canadian Centre for Cyber Security. Retrieved July 26, 2023, from https://www.cyber.gc.ca/en/guidance/security-considerations-your-website-itsm60005