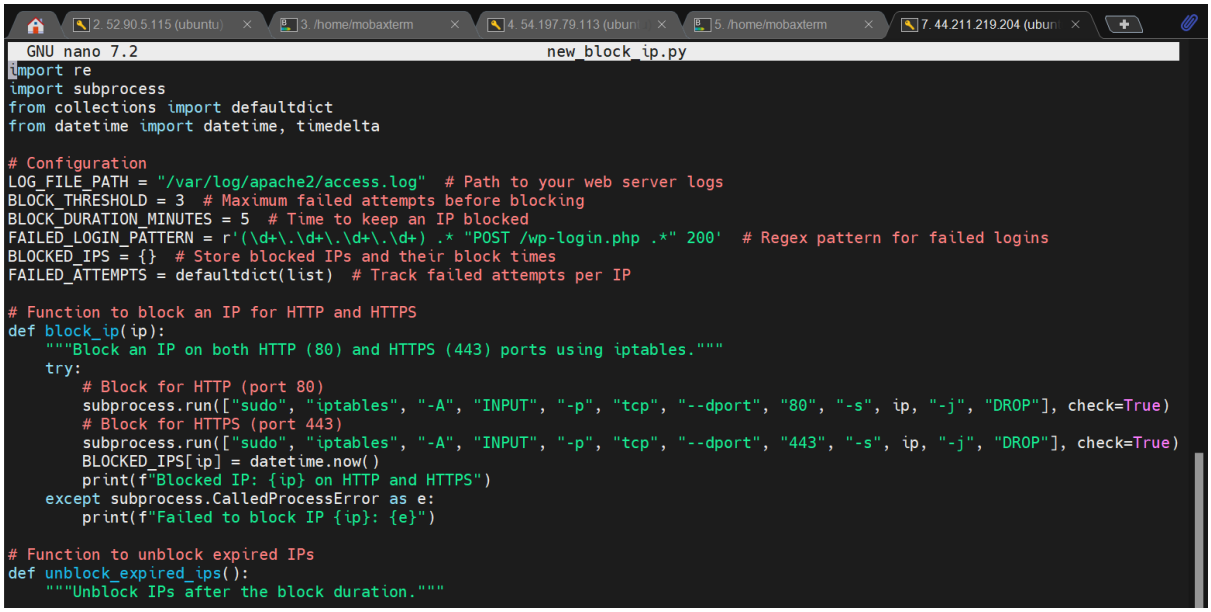
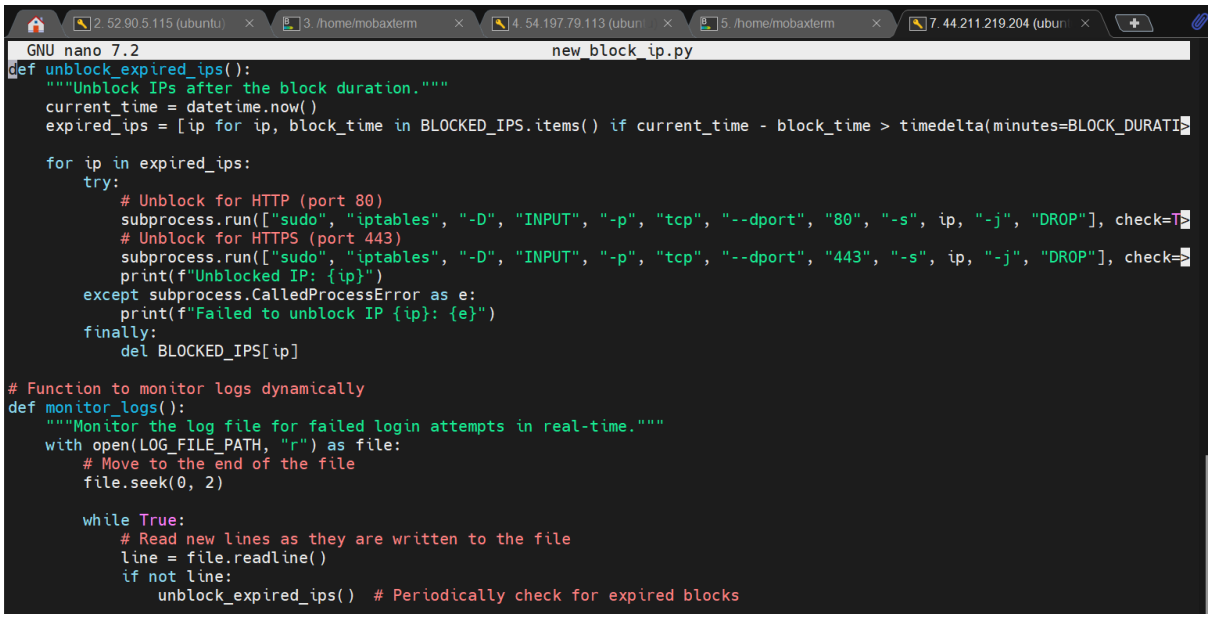
Create a Python script

- Parse logs from a web server.
- Identify IPs causing the most failed login attempts.
- Block those IPs by dynamically updating firewall rules

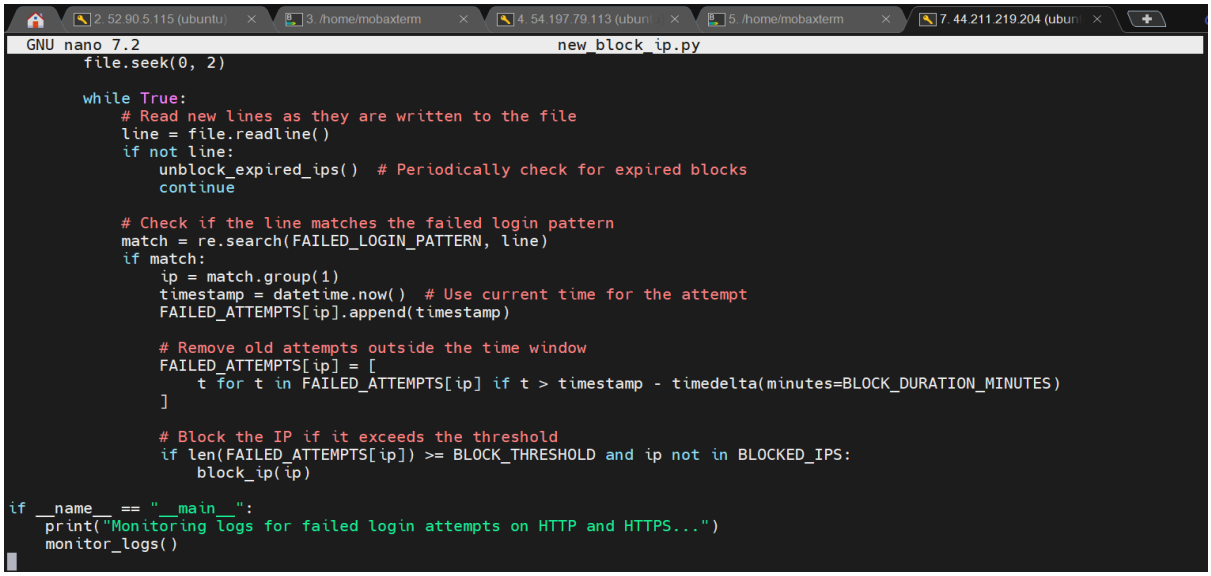
The script continuously watches the web server log file, detects failed login attempts, and blocks IPs exceeding the threshold instantly.



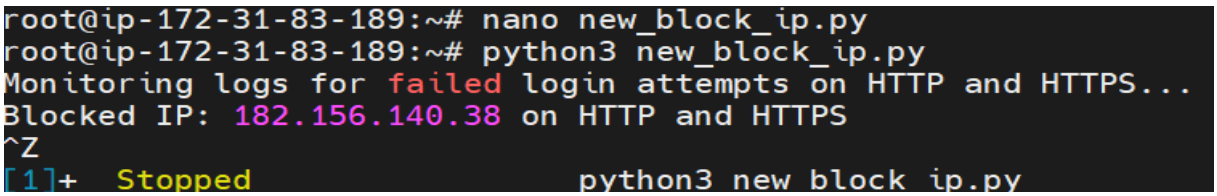
```
  GNU nano 7.2                                    new_block_ip.py
import re
import subprocess
from collections import defaultdict
from datetime import datetime, timedelta

# Configuration
LOG_FILE_PATH = "/var/log/apache2/access.log"  # Path to your web server logs
BLOCK_THRESHOLD = 3  # Maximum failed attempts before blocking
BLOCK_DURATION_MINUTES = 5  # Time to keep an IP blocked
FAILED_LOGIN_PATTERN = r'(\d+\.\d+\.\d+\.\d+) .* "POST /wp-login.php .*" 200'  # Regex pattern for failed logins
BLOCKED_IPS = {}  # Store blocked IPs and their block times
FAILED_ATTEMPTS = defaultdict(list)  # Track failed attempts per IP

# Function to block an IP for HTTP and HTTPS
def block_ip(ip):
    """Block an IP on both HTTP (80) and HTTPS (443) ports using iptables."""
    try:
        # Block for HTTP (port 80)
        subprocess.run(["sudo", "iptables", "-A", "INPUT", "-p", "tcp", "--dport", "80", "-s", ip, "-j", "DROP"], check=True)
        # Block for HTTPS (port 443)
        subprocess.run(["sudo", "iptables", "-A", "INPUT", "-p", "tcp", "--dport", "443", "-s", ip, "-j", "DROP"], check=True)
        BLOCKED_IPS[ip] = datetime.now()
        print(f"Blocked IP: {ip} on HTTP and HTTPS")
    except subprocess.CalledProcessError as e:
        print(f"Failed to block IP {ip}: {e}")

# Function to unblock expired IPs
def unblock_expired_ips():
    """Unblock IPs after the block duration."""
```



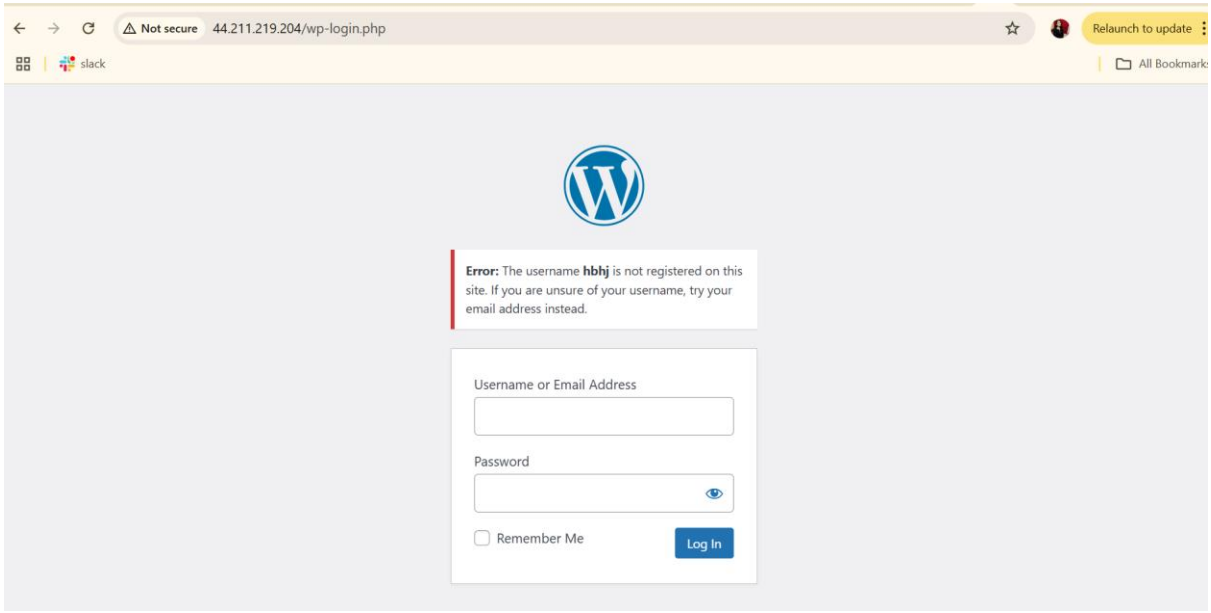
```
  GNU nano 7.2                                    new_block_ip.py
def unblock_expired_ips():
    """Unblock IPs after the block duration."""
    current_time = datetime.now()
    expired_ips = [ip for ip, block_time in BLOCKED_IPS.items() if current_time - block_time > timedelta(minutes=BLOCK_DURATI>

    for ip in expired_ips:
        try:
            # Unblock for HTTP (port 80)
            subprocess.run(["sudo", "iptables", "-D", "INPUT", "-p", "tcp", "--dport", "80", "-s", ip, "-j", "DROP"], check=T>
            # Unblock for HTTPS (port 443)
            subprocess.run(["sudo", "iptables", "-D", "INPUT", "-p", "tcp", "--dport", "443", "-s", ip, "-j", "DROP"], check=>
            print(f"Unblocked IP: {ip}")
        except subprocess.CalledProcessError as e:
            print(f"Failed to unblock IP {ip}: {e}")
        finally:
            del BLOCKED_IPS[ip]

# Function to monitor logs dynamically
def monitor_logs():
    """Monitor the log file for failed login attempts in real-time."""
    with open(LOG_FILE_PATH, "r") as file:
        # Move to the end of the file
        file.seek(0, 2)

        while True:
            # Read new lines as they are written to the file
            line = file.readline()
            if not line:
                unblock_expired_ips()  # Periodically check for expired blocks
```



Run the Script: Start the script and watch it block the IP after 5 attempts:



Test the system by intentionally attempting multiple failed logins



Verify Blocking: Check if the IP is blocked using iptables:

```
root@ip-172-31-83-189:~# sudo iptables -L -v
Chain INPUT (policy ACCEPT 658 packets, 73191 bytes)
 pkts bytes target     prot opt in     out     source               destination
   28  1184 DROP       tcp  --  any    any     mail.tataidc.com     anywhere             tcp dpt:http
    0     0 DROP       tcp  --  any    any     mail.tataidc.com     anywhere             tcp dpt:https

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ip-172-31-83-189:~#
```

To monitor the log file in real-time, use:

```
root@ip-172-31-83-189:~# tail -f /var/log/apache2/access.log
182.156.140.38 - - [30/Dec/2024:08:42:04 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://44.211.219.204/wp-login.php" "M
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
182.156.140.38 - - [30/Dec/2024:08:42:12 +0000] "POST /wp-login.php HTTP/1.1" 200 2390 "http://44.211.219.204/wp-login.php" "M
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
182.156.140.38 - - [30/Dec/2024:08:42:20 +0000] "POST /wp-login.php HTTP/1.1" 200 2389 "http://44.211.219.204/wp-login.php" "M
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
182.156.140.38 - - [30/Dec/2024:08:42:28 +0000] "POST /wp-login.php HTTP/1.1" 200 2389 "http://44.211.219.204/wp-login.php" "M
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
182.156.140.38 - - [30/Dec/2024:08:51:56 +0000] "GET /wp-login.php HTTP/1.1" 200 2235 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
182.156.140.38 - - [30/Dec/2024:08:52:47 +0000] "-" 408 0 "-" "-"
182.156.140.38 - - [30/Dec/2024:08:52:48 +0000] "-" 408 0 "-" "-"
182.156.140.38 - - [30/Dec/2024:09:07:49 +0000] "POST /wp-login.php HTTP/1.1" 200 2389 "http://44.211.219.204/wp-login.php" "M
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
182.156.140.38 - - [30/Dec/2024:09:07:58 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://44.211.219.204/wp-login.php" "M
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
182.156.140.38 - - [30/Dec/2024:09:08:06 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://44.211.219.204/wp-login.php" "M
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
```