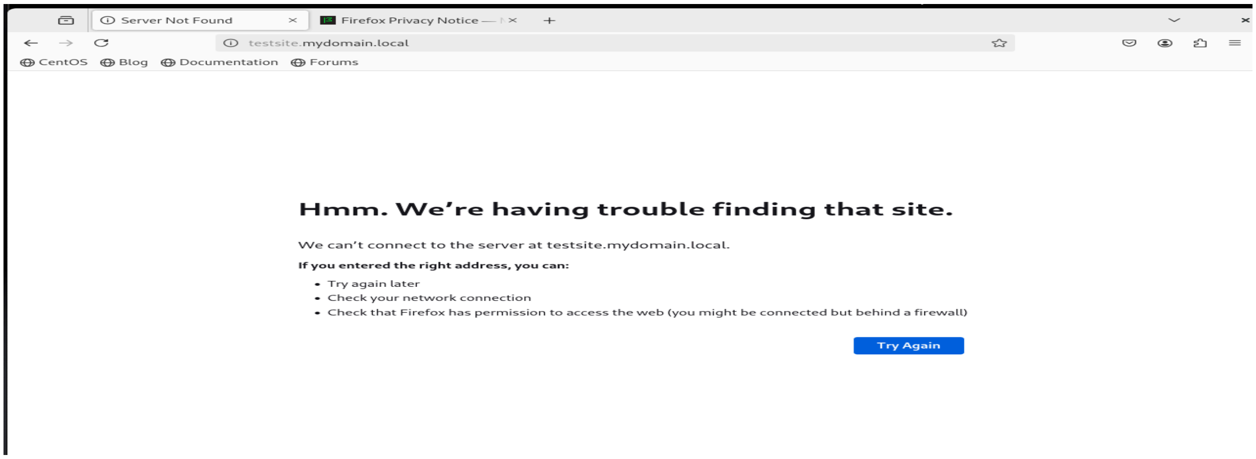
Troubleshooting and Setting Permissions

Resolving Hostname Error [Server Not Found Error]

The above gave an error that “server is not found”. So lets find a way out of this error. Why this happens

- DNS/hosts file does not map testsite.mydomain.local to your server’s IP
    - By default, testsite.mydomain.local is not a real, globally-known domain.
    - Your browser needs to know which IP address this name points to.
- Apache is running, but the browser can't find the virtual host
- If you use a custom domain, the browser must resolve it to the local server’s IP; otherwise, it cannot connect—even if Apache is working.



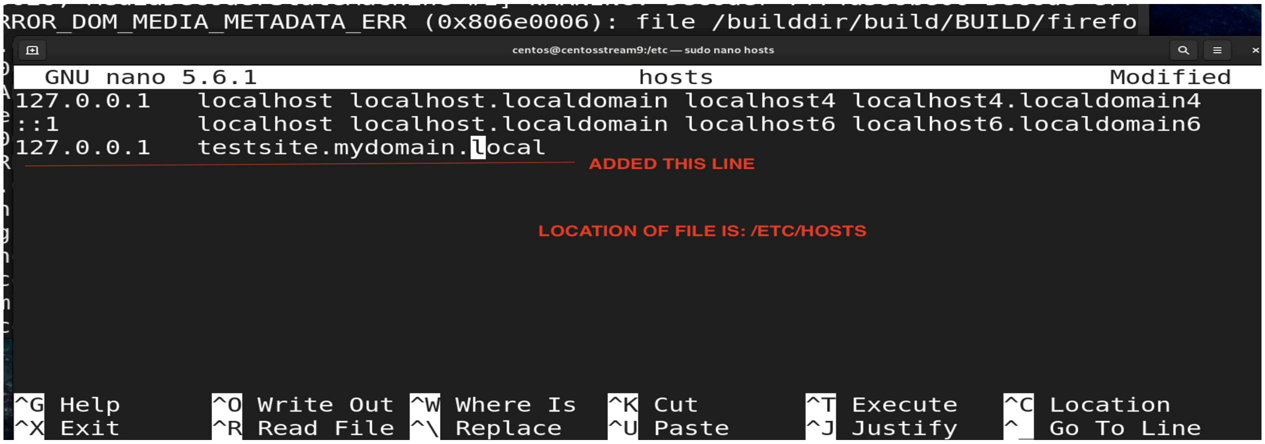
Hmm. We’re having trouble finding that site.

We can’t connect to the server at testsite.mydomain.local.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

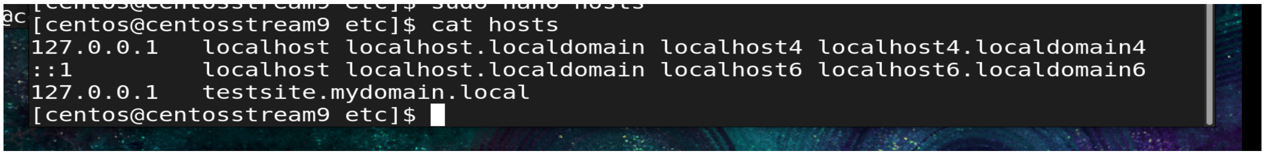
- Resolving: “Server Not Found”
- Edit your /etc/hosts file
- Add a line to /etc/hosts on your CentOS machine (and on your client if you’re browsing from another computer): `127.0.0.1 testsite.mydomain.local`



```
RROR_DOM_MEDIA_METADATA_ERR (0x806e0006): file /builddir/build/BUILD/firefo
centos@centosstream9:/etc — sudo nano hosts
  GNU nano 5.6.1                        hosts                        Modified
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1   testsite.mydomain.local

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

ADDED THIS LINE

LOCATION OF FILE IS: /ETC/HOSTS



```
[centos@centosstream9 etc]$ sudo nano hosts
[centos@centosstream9 etc]$ cat hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1   testsite.mydomain.local
[centos@centosstream9 etc]$ 
```

- Now check again, yes changes are saved in the etc/hosts/

SELinux Configuration [Forbidden error]

`chcon unconfined_u:object_r:httpd_sys_content_t:s0 /reports/`
is to set the SELinux context on the /reports/ directory, so the Apache HTTP server (httpd) can access and serve its contents.

Why the Forbidden (403) error happens

- On CentOS, SELinux is enabled by default and restricts web server access to directories that do not have the correct security context.
- When /reports/ or its contents have a context that httpd is not allowed to read (e.g., default context after a new directory is created or a symlink is made), you will get a 403 Forbidden error—even if UNIX permissions are correct.

What does the command do?

- `chcon` = change SELinux context
- `unconfined_u:object_r:httpd_sys_content_t:s0` = assigns an SELinux context specifically allowing Apache to read and serve files under /reports/
- This context makes SELinux treat /reports/ as web-accessible content, just like the usual /var/www/html.

How to use it and fix the error

- Run the command (with sudo):
  `sudo chcon -R unconfined_u:object_r:httpd_sys_content_t:s0 /reports/`
- (-R applies context recursively to all files within /reports/)
- Try reloading your URL (testsite.mydomain.local/reports/) again.
- The page should now be accessible unless there are other permission issues.

Configuring Fail2Ban Verifying Jail.local status

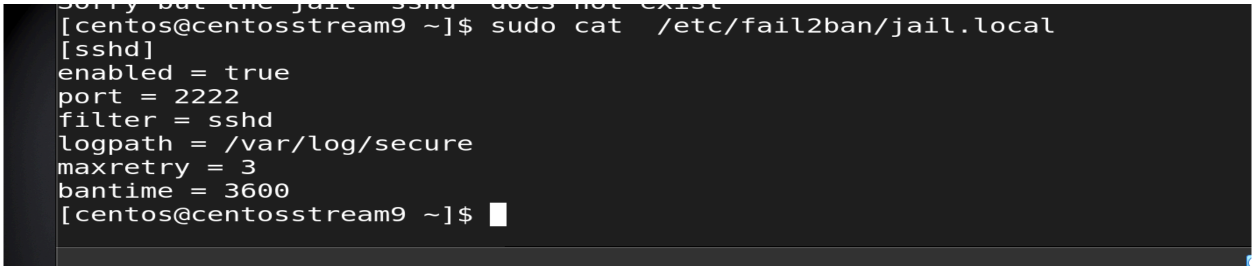
```
sudo fail2ban-client status sshd
```

The error "Sorry but the jail 'sshd' does not exist" means that Fail2ban has not been configured to protect your SSH service yet.

Step 1: Edit the jail configuration file

Open the main or local jail configuration file:

```
sudo cat /etc/fail2ban/jail.local
```



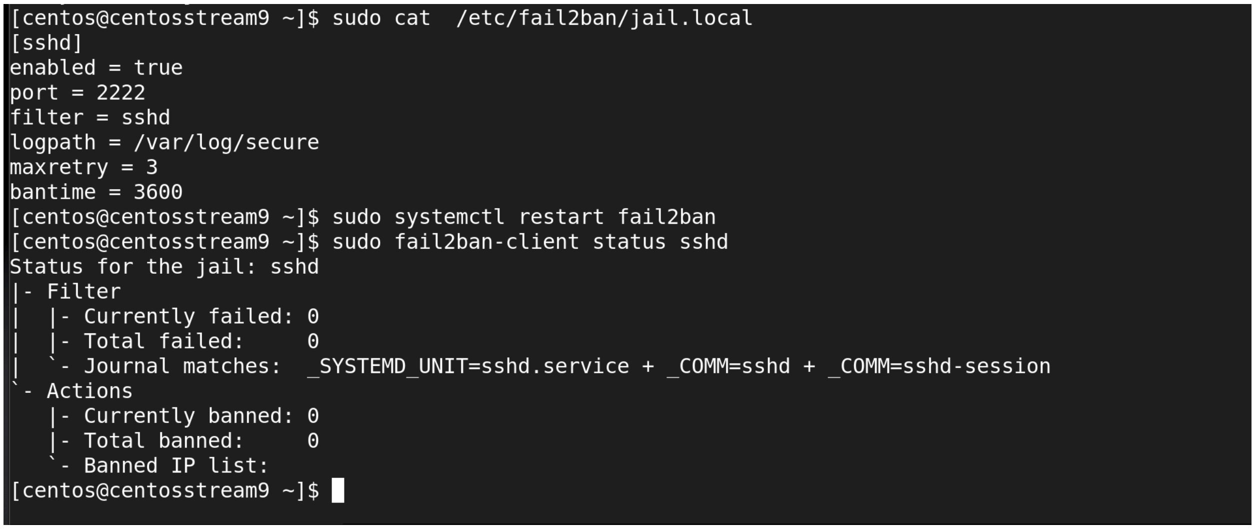
```
Sorry but the jail 'sshd' does not exist
[centos@centosstream9 ~]$ sudo cat  /etc/fail2ban/jail.local
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/secure
maxretry = 3
bantime = 3600
[centos@centosstream9 ~]$ 
```

Step 2: Save and restart Fail2ban

```
sudo systemctl restart fail2ban
```

Step 3: Check jail status again

```
sudo fail2ban-client status sshd
```



```
[centos@centosstream9 ~]$ sudo cat  /etc/fail2ban/jail.local
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/secure
maxretry = 3
bantime = 3600
[centos@centosstream9 ~]$ sudo systemctl restart fail2ban
[centos@centosstream9 ~]$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[centos@centosstream9 ~]$ 
```

Now, SSH jail is active.

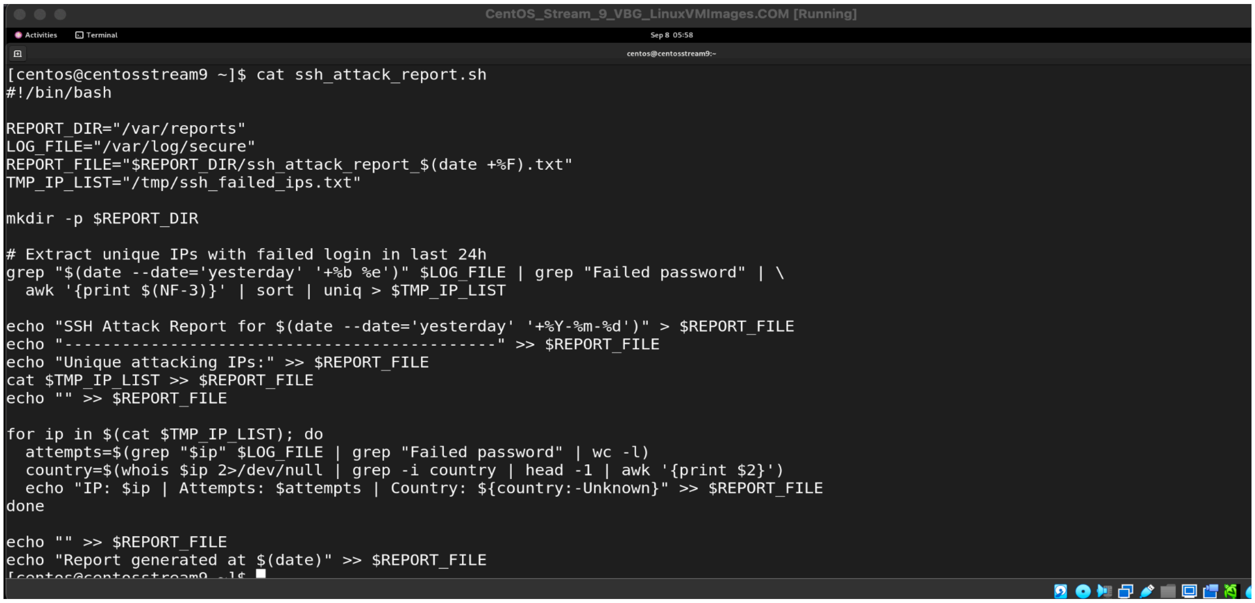
Automating Log Analysis and Reporting

Test the Script

`sudo ~/ssh_attack_report.sh`

Since we were not getting output of our script as expected we will remove code and start creating a simpler script with no date formatting.

Current state

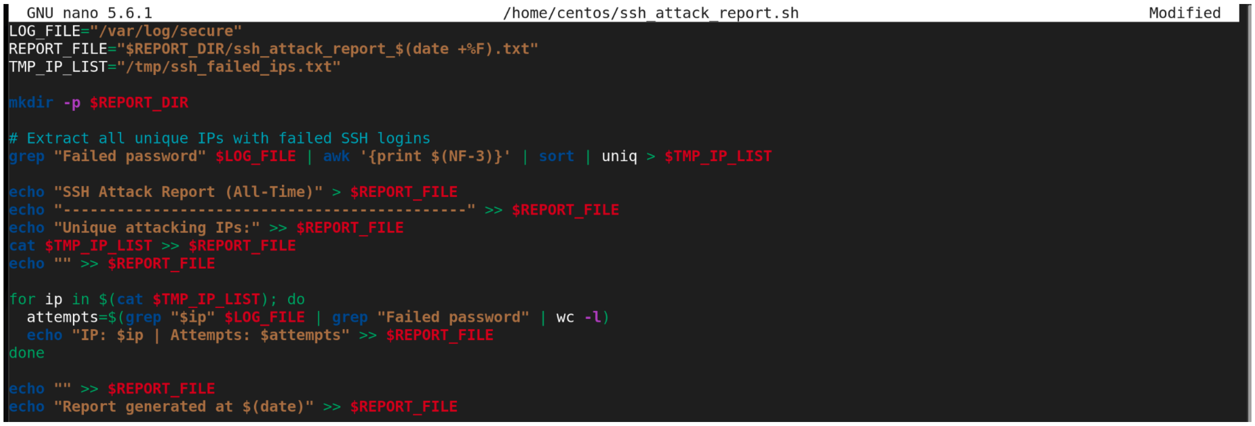


```
[centos@centosstream9 ~]$ cat ssh_attack_report.sh
#!/bin/bash

REPORT_DIR="/var/reports"
LOG_FILE="/var/log/secure"
REPORT_FILE="$REPORT_DIR/ssh_attack_report_$(date +%F).txt"
TMP_IP_LIST="/tmp/ssh_failed_ips.txt"

mkdir -p $REPORT_DIR

# Extract unique IPs with failed login in last 24h
grep "$(date --date='yesterday' '+%b %e')" $LOG_FILE | grep "Failed password" | \
  awk '{print $(NF-3)}' | sort | uniq > $TMP_IP_LIST

echo "SSH Attack Report for $(date --date='yesterday' '+%Y-%m-%d')" > $REPORT_FILE
echo "---------------------------------------------" >> $REPORT_FILE
echo "Unique attacking IPs:" >> $REPORT_FILE
cat $TMP_IP_LIST >> $REPORT_FILE
echo "" >> $REPORT_FILE

for ip in $(cat $TMP_IP_LIST); do
  attempts=$(grep "$ip" $LOG_FILE | grep "Failed password" | wc -l)
  country=$(whois $ip 2>/dev/null | grep -i country | head -1 | awk '{print $2}')
  echo "IP: $ip | Attempts: $attempts | Country: ${country:-Unknown}" >> $REPORT_FILE
done

echo "" >> $REPORT_FILE
echo "Report generated at $(date)" >> $REPORT_FILE
[centos@centosstream9 ~]$
```

Lets limit lines and try to get the minimum result first and then expand.

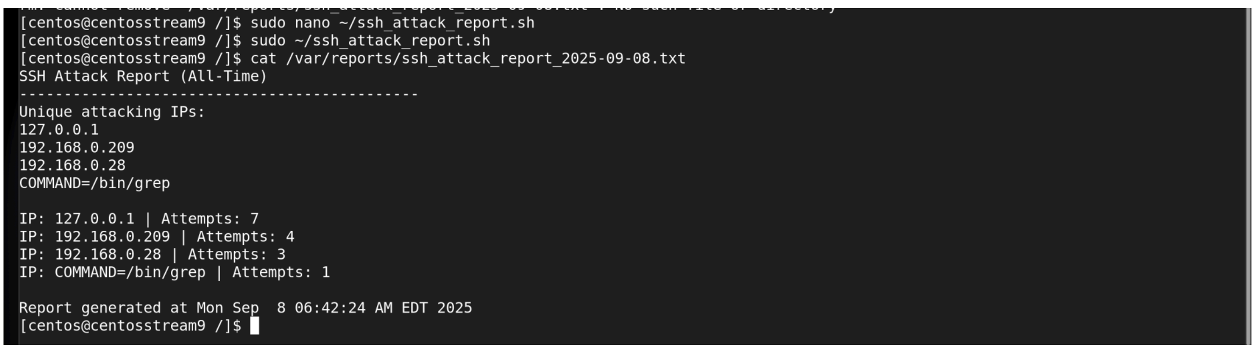
This script must return

- List unique attacking IPs.



```
  GNU nano 5.6.1                    /home/centos/ssh_attack_report.sh                    Modified
LOG_FILE="/var/log/secure"
REPORT_FILE="$REPORT_DIR/ssh_attack_report_$(date +%F).txt"
TMP_IP_LIST="/tmp/ssh_failed_ips.txt"

mkdir -p $REPORT_DIR

# Extract all unique IPs with failed SSH logins
grep "Failed password" $LOG_FILE | awk '{print $(NF-3)}' | sort | uniq > $TMP_IP_LIST

echo "SSH Attack Report (All-Time)" > $REPORT_FILE
echo "---------------------------------------------" >> $REPORT_FILE
echo "Unique attacking IPs:" >> $REPORT_FILE
cat $TMP_IP_LIST >> $REPORT_FILE
echo "" >> $REPORT_FILE

for ip in $(cat $TMP_IP_LIST); do
  attempts=$(grep "$ip" $LOG_FILE | grep "Failed password" | wc -l)
  echo "IP: $ip | Attempts: $attempts" >> $REPORT_FILE
done

echo "" >> $REPORT_FILE
echo "Report generated at $(date)" >> $REPORT_FILE
```

- Count the number of failed attempts for each IP.
- Output a simple, readable report



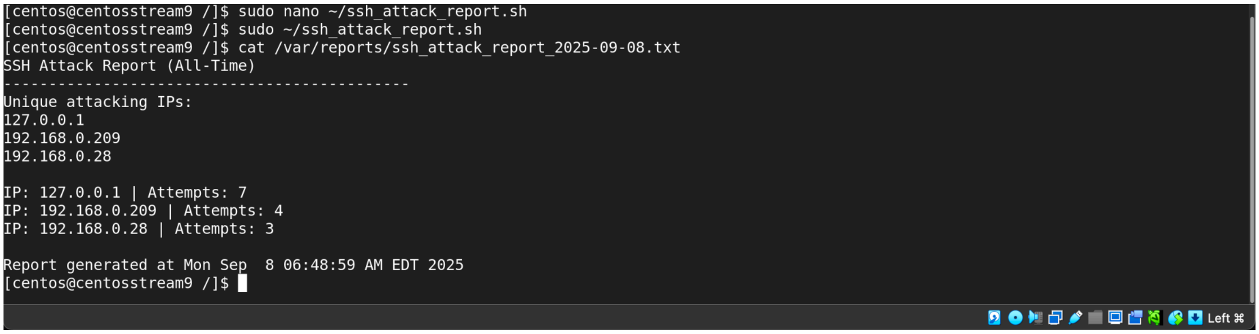
```
[centos@centosstream9 /]$ sudo nano ~/ssh_attack_report.sh
[centos@centosstream9 /]$ sudo ~/ssh_attack_report.sh
[centos@centosstream9 /]$ cat /var/reports/ssh_attack_report_2025-09-08.txt
SSH Attack Report (All-Time)
---------------------------------------------
Unique attacking IPs:
127.0.0.1
192.168.0.209
192.168.0.28
COMMAND=/bin/grep

IP: 127.0.0.1 | Attempts: 7
IP: 192.168.0.209 | Attempts: 4
IP: 192.168.0.28 | Attempts: 3
IP: COMMAND=/bin/grep | Attempts: 1

Report generated at Mon Sep  8 06:42:24 AM EDT 2025
[centos@centosstream9 /]$ 
```

Now we get the above output from the script into this file.
But there is some unwanted `command=/bin/grep` entry which can be fixed by replacing

grep command in the line 6 with

```
grep "Failed password" $LOG_FILE | awk '{print $(NF-3)}' | egrep '([0-9]{1,3}\.){3}[0-9]{1,3}' | sort | uniq > $TMP_IP_LIST
```

And now our output is in the screenshot



```
[centos@centosstream9 /]$ sudo nano ~/ssh_attack_report.sh
[centos@centosstream9 /]$ sudo ~/ssh_attack_report.sh
[centos@centosstream9 /]$ cat /var/reports/ssh_attack_report_2025-09-08.txt
SSH Attack Report (All-Time)
---------------------------------------------
Unique attacking IPs:
127.0.0.1
192.168.0.209
192.168.0.28

IP: 127.0.0.1 | Attempts: 7
IP: 192.168.0.209 | Attempts: 4
IP: 192.168.0.28 | Attempts: 3

Report generated at Mon Sep  8 06:48:59 AM EDT 2025
[centos@centosstream9 /]$ 
```