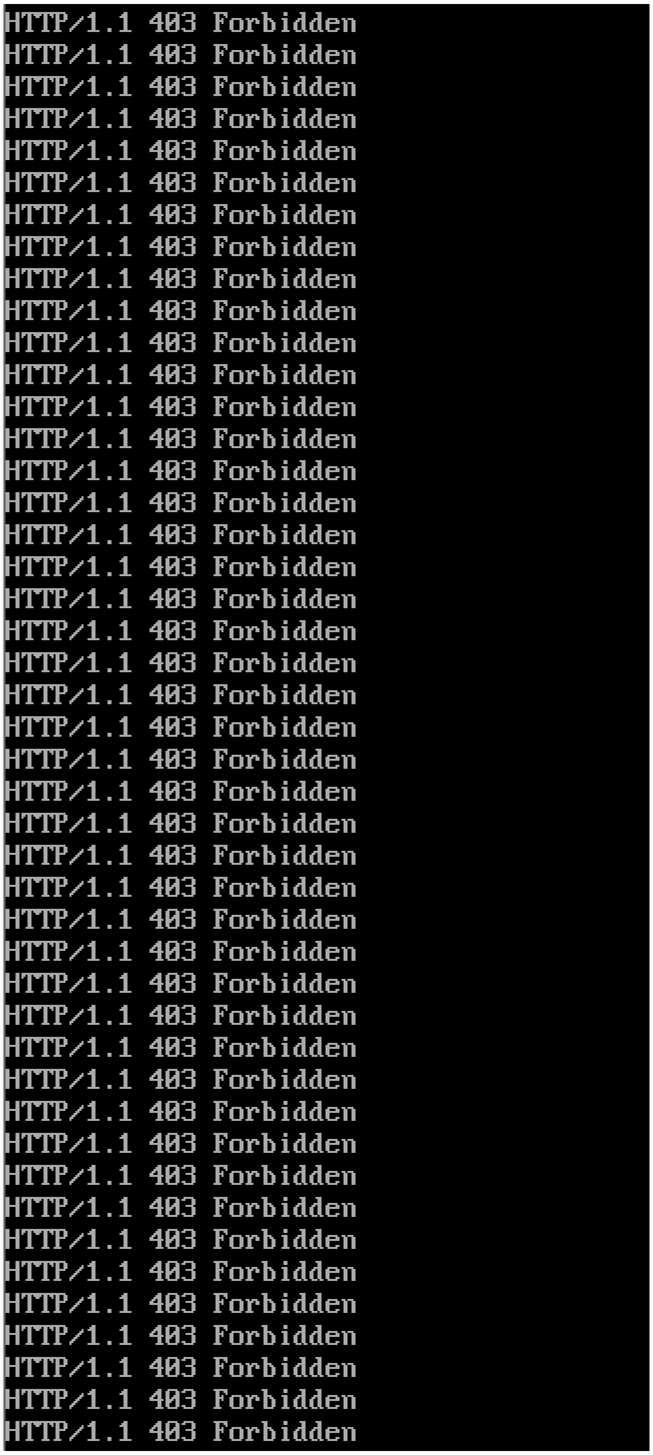
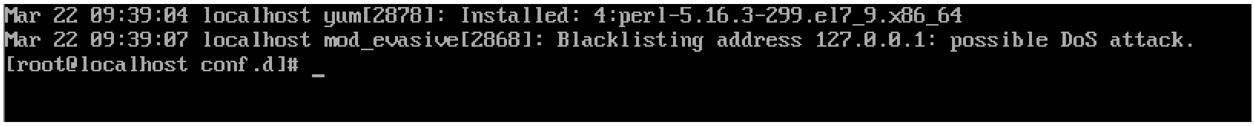
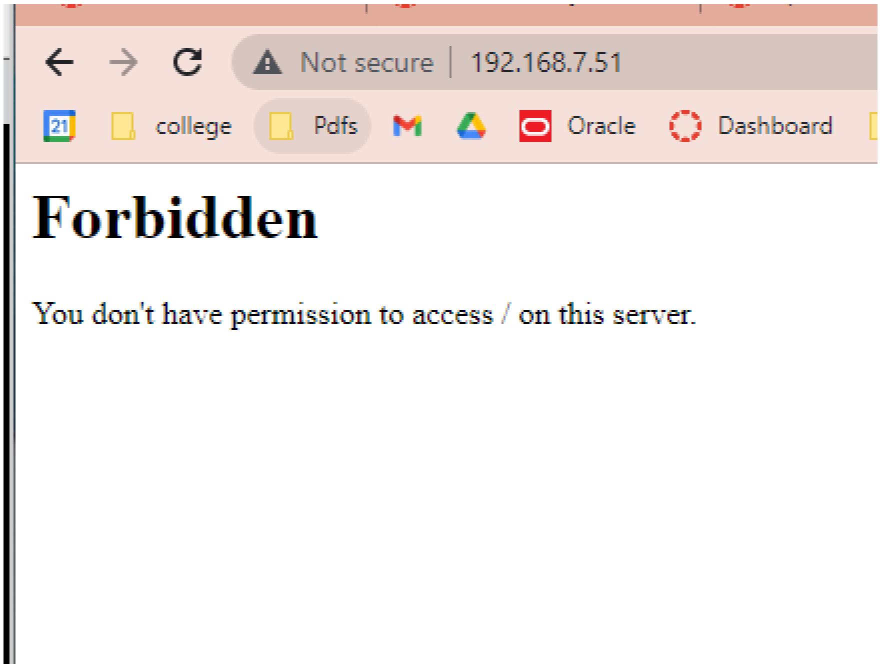
David Thomsen
SEC-260



```
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
```

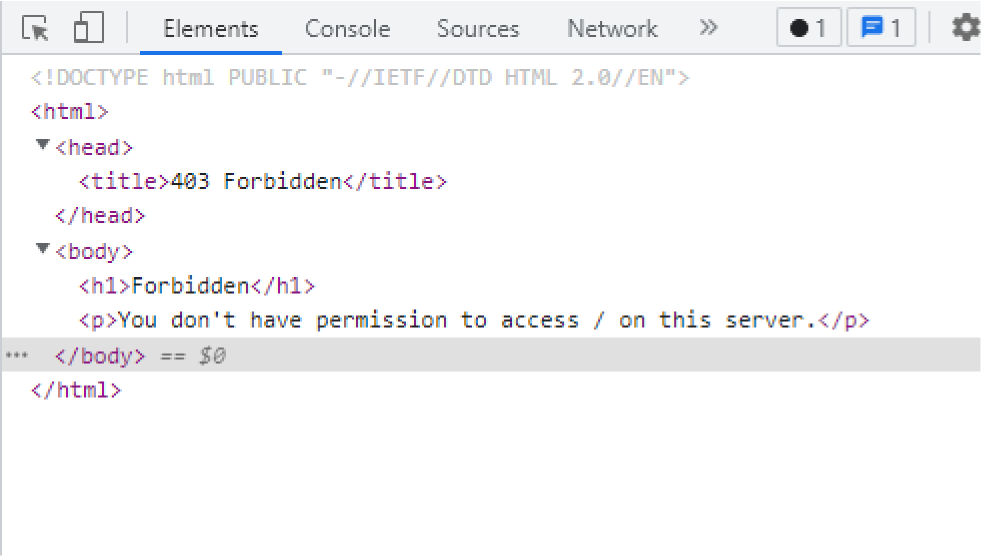


```
Mar 22 09:39:04 localhost yum[2878]: Installed: 4:perl-5.16.3-299.el7_9.x86_64
Mar 22 09:39:07 localhost mod_evasive[2868]: Blacklisting address 127.0.0.1: possible DoS attack.
[root@localhost conf.d]# _
```

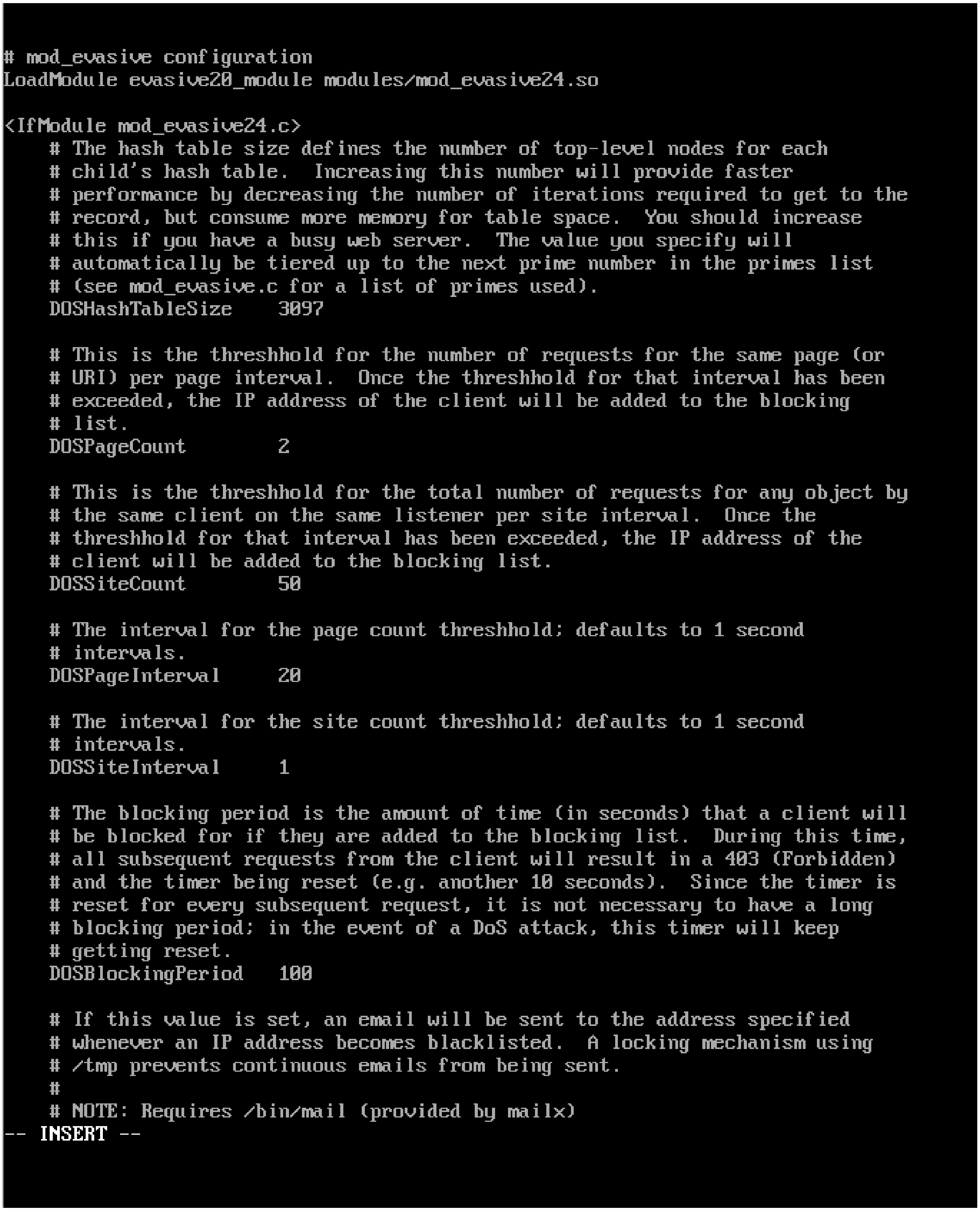


Forbidden

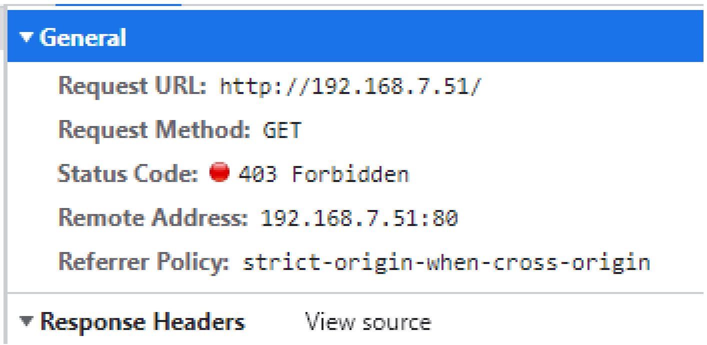
You don't have permission to access / on this server.



```
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
▼<head>
    <title>403 Forbidden</title>
  </head>
▼<body>
    <h1>Forbidden</h1>
    <p>You don't have permission to access / on this server.</p>
…  </body> == $0
</html>
```



```
# mod_evasive configuration
LoadModule evasive20_module modules/mod_evasive24.so

<IfModule mod_evasive24.c>
    # The hash table size defines the number of top-level nodes for each
    # child's hash table.  Increasing this number will provide faster
    # performance by decreasing the number of iterations required to get to the
    # record, but consume more memory for table space.  You should increase
    # this if you have a busy web server.  The value you specify will
    # automatically be tiered up to the next prime number in the primes list
    # (see mod_evasive.c for a list of primes used).
    DOSHashTableSize    3097

    # This is the threshhold for the number of requests for the same page (or
    # URI) per page interval.  Once the threshhold for that interval has been
    # exceeded, the IP address of the client will be added to the blocking
    # list.
    DOSPageCount        2

    # This is the threshhold for the total number of requests for any object by
    # the same client on the same listener per site interval.  Once the
    # threshhold for that interval has been exceeded, the IP address of the
    # client will be added to the blocking list.
    DOSSiteCount        50

    # The interval for the page count threshhold; defaults to 1 second
    # intervals.
    DOSPageInterval     20

    # The interval for the site count threshhold; defaults to 1 second
    # intervals.
    DOSSiteInterval     1

    # The blocking period is the amount of time (in seconds) that a client will
    # be blocked for if they are added to the blocking list.  During this time,
    # all subsequent requests from the client will result in a 403 (Forbidden)
    # and the timer being reset (e.g. another 10 seconds).  Since the timer is
    # reset for every subsequent request, it is not necessary to have a long
    # blocking period; in the event of a DoS attack, this timer will keep
    # getting reset.
    DOSBlockingPeriod   100

    # If this value is set, an email will be sent to the address specified
    # whenever an IP address becomes blacklisted.  A locking mechanism using
    # /tmp prevents continuous emails from being sent.
    #
    # NOTE: Requires /bin/mail (provided by mailx)
-- INSERT --
```



▾ General

Request URL: http://192.168.7.51/

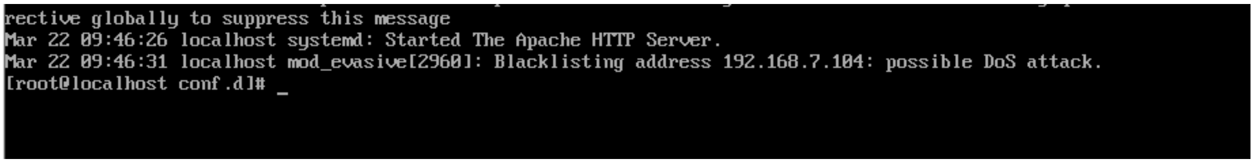
Request Method: GET

Status Code: ● 403 Forbidden

Remote Address: 192.168.7.51:80

Referrer Policy: strict-origin-when-cross-origin

▾ Response Headers   View source



```
rective globally to suppress this message
Mar 22 09:46:26 localhost systemd: Started The Apache HTTP Server.
Mar 22 09:46:31 localhost mod_evasive[2960]: Blacklisting address 192.168.7.104: possible DoS attack.
[root@localhost conf.d]# _
```