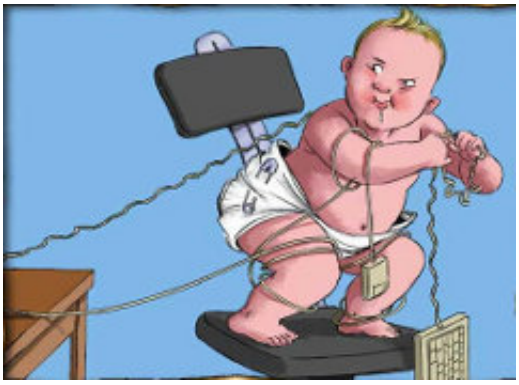
w00tw00t.at.ISC.SANS.DFind in apache error.log - Filtering script kiddie port scanner on GNU / Linux

Author : admin



If you get thousand of messages:

[Wed Nov 21 16:28:49 2012] [error] [client 89.136.100.192] client sent HTTP/1.1 request without hostname (see RFC2616 section 14.23): /w00tw00t.at.ISC.SANS.DFind:)

in **/var/log/apache2/error.log** It is due to a script kiddie port scanner, usually such requests originate from Turkia, Romania ,Russia.. Usually, for servers getting in Apache error.log **GET/w00tw00t.at.ISC.SANS.DFind:)** once in a while, it is not an issue however if you get too many of this messages it is sometimes useful to filter them with a simple iptables rule

debian:~# /sbin/iptables -A INPUT -p tcp -m tcp --dport 80 -m string --string "GET /w00tw00t.at.ISC.SANS." --algo bm --to 70 -j DROP

What above command does is it greps the 1st 70 bytes and checks, whether it contains string '/w00tw00t.at.ISC.SANS.DFind:)' , whether string is matched it jumps to DROP rule filtering the IP. Of course on busy servers checking each incoming IP client TCP/IP request for a certain string might not be very efficient and even can be a possible bottleneck. So I don't know whether filtering **/w00tw00t.at.ISC.SANS.DFind:)** is good or bad practice. Anyways generally it is wise to filter IPs doing the request anyways since, they could try a various script kiddie cracking tools, port scanners and even some of them might be hosts attempting ***DoS*** or ***DDoS***.

Also it is useful to store for later the rule with:

debian:~# /sbin/iptables-save > /root/iptables_rules.txt

Then you can load up /root/iptables_rules.txt with**:**

debian:~# /sbin/iptables-restore

Some common way to keep the iptables rule loaded on system boot is by adding */iptables-restore* to **/etc/rc.local**

Some alternative methods to filter IPs issuing GET **/w00tw00t.at.ISC.SANS.DFind:)** to Apache is through fail2ban, denyhosts or blockhosts or Apache mod security filters.
You can read further Information on what DFind hacktool does here

To keep an eye on all DROPped and REJECT-ed traffic (in bytes) it is useful to use:

```
 debian:~# /sbin/iptables -L INPUT -nvx|grep -i -E 'drop|reject'
      0        0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3306 reject-with icmp-
port-unreachable
      0        0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 17
      0        0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 13
      0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
      0        0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
   1526    77004 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp reject-with icmp-host-
prohibited
```

For filtering