Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > Debian / Ubuntu

Linux Null route an attackers ip

Posted by Vivek Gite <vivek@nixcraft.com>

Q. How do I null route an attakers IP under Red Hat Enterprise Linux? I would like to block unwanted traffic from a particular source.

A. A null route is a network route that goes nowhere. When a network packet is received by Linux (or UNIX or any other network device) operating system, it needs to route that packet somewhere. It uses the routing table to decide where to send the packet. To kill the packet, in essence dropping the packet and forbidding the packet from travelling further, a nullroute could be put in place.

There are two ways to achieve the same.
First find out attacker IP address from system log files such as
=> /var/log/messages
=> /var/log/secure
=> /var/log/auth

Use tail -f command to view incoming messages

```
# tail -f /var/log/messages
```

You can also use faillog [1] command or combination of grep and awk [2] to find out list of failed ssh login attempt.

Option #1: Using Iptables

Use following iptables rules:

```
# iptables --append INPUT --source IP-ADDRESS -j DROP
```

Add above rules to your iptables shell script. To drop bunch of IPs use something as follows in your shell script:

```
BADIPS="64.56.1.2 69.51.11.21 1.2.3.4"
for i in $BADIPS
do
iptables --append INPUT --source $i -j DROP
done
```

Option # 2: Using route command

See previous article [3] for more information.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/howto-null-route-an-attackers-ip/**

URLs in this post:

[1] faillog: **http://www.cyberciti.biz/tips/linux-how-do-i-display-failed-login-attempt.html**
[2] grep and awk: **http://www.cyberciti.biz/tips/linux-how-to-find-all-failed-login-attempts.html**
[3] previous article: **http://www.cyberciti.biz/tips/how-do-i-drop-or-block-attackers-ip-with-null-routes.html**