TippingPoint IPS Signature Evasion through Packet Fragmentation

Author:
Chaitanya Sharma
chaitanya.sharma@gmail.com

TippingPoint IPS Signature Evasion through Packet Fragmentation

I was recently testing a website which had and IPS running on it. The IPS was from TippingPoint and my task was to execute XSS & Sql Injection attacks on the site - after bypassing the IPS. Now bypassing the IPs was something I had only read about and had never done it first hand. SO this seemed to be a challenge.

The vulnerability details can be found here:

http://www.3com.com/securityalert/alerts/3COM-07-002.html
http://www.securityfocus.com/bid/24861/info

This vulnerability can be exploited by sending fragmented packets so that the IPS would not detect the traffic. This vulnerability exists only in TippingPoint TOS versions 2.1.x, 2.2.x prior to 2.2.5, and 2.5.x.

I used a tool called 'fragroute' which comes preinstalled in BackTrack3.

fragroute creates a route to the server you traget and all your traffic passes through fragroute - no need to configure proxy in web browsers. The configuration that worked for me was -

```
tcp_seg 24
ip_frag 64
tcp_chaff paws
print
```

This configuration goes in the conf file /pentest/scanners/fragroute-1.2/fragroute.conf and the command would be -

```
bt ~ # fragroute -f /pentest/scanners/fragroute-1.2/fragroute.conf
```
xxx.xxx.xxx.xxx

After the command is executed, just browse to the site and your traffic will be fragged!

This thing worked for me. Another idea as suggested by BSDaemon (Rodrigo) would be to use gzip encoding. i.e. to send your traffic by encoding it using gzip and then send the traffic by fragging it. fragroute can be used to fragment the traffic. You will need to create a PHP script to send requests for you and use the function gzinflate to encode the traffic.

I have not tried this technique so I do not know the details of the working but this idea should give headway to anyone looking for help.

Any inputs / comments / feedback will be welcome :-)

Special thanks to Nightrover (Pallav Khandhar) and BSDaemon (Rodrigo Rubira Branco)

Peace out

- Chaitanya Sharma