

# [UNIX] Honeyd Remote Detection Via Simple Probe Packet

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0072.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 01/22/04

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

Date: 22 Jan 2004 17:26:25 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Honeyd Remote Detection Via Simple Probe Packet

---

## SUMMARY

<<http://www.honeyd.org/>> Honeyd is a virtual honey pot daemon that can simulate virtual hosts on unallocated IP addresses.

A bug in the way honeyd handles NMAP fingerprints makes it possible to detect IP addresses simulated by honeyd.

## DETAILS

Vulnerable Systems:

- \* Honeyd versions prior to 0.8

Immune Systems:

- \* Honeyd version 0.8

A bug in handling NMAP fingerprints caused Honeyd to reply to TCP packets with both the SYN and RST flags set. Watching for replies, it is possible to detect IP addresses simulated by Honeyd. Although there are no public exploits known for Honeyd, the detection of Honeyd IP addresses may in some cases be undesirable.

## Securiteam: [UNIX] Honeyd Remote Detection Via Simple Probe Packet

### Patch Availability:

A new version of Honeyd has been released in order to address this issue.  
It can be downloaded from <http://www.citi.umich.edu/u/provos/honeyd/>  
here

### ADDITIONAL INFORMATION

The information has been provided by <mailto:provos@citi.umich.edu> Niels  
Provos

=====

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.