WHITEHATS




- What's New
- About Whitehats
- Infosec Library
- Contact Us
- Terms Of Use
- Privacy Policy

- Intrusion Detection
  - . arachNIDS Center
  - . Mailing List *
  - . Submit Signatures
  - . Forum: General NIDS
  - . Forum: arachNIDS
  - . Forum: Signatures
  - . Forum: Snort IDS
  - . IDS Tools
- Penetration Testing
  - . Forum: Penetration
  - . Forum: Nessus
  - . Assessment Tools
- Network Defense
  - . Forum: DDOS Attacks
  - . Forum: Internet Law
  - . Forum: Incidents
  - . Defense Tools

Search arachNIDS

Search Tools

Search Forums


arachNIDS - The Intrusion Event Database

browse by grouping, classification, target affected

Event | Protocol | Research | Signatures

# IDS7/MISC_SOURCEPORTTRAFFIC-53-TCP

**Summary**

AThis event indicates that an ttacker is making a connection to a privileged port using the source port 53 (dns). This should not normally occur. Old or misconfigured packetfilters may allow the connection if they allow all dns traffic.

**Platform(s)**: unix windows device
**Category**: misc
**Classification**: Suspicious

**How Specific**

This event is specific to a vulnerability, but may have been caused by any of several possible exploits. Packet payload is not considered in the signatures used to detect this attack.

**CVE** nomatch
**Bugtraq** nomatch
**advICE** nomatch

**Trusting The Source IP Address**

Although this event was caused by a TCP packet, the packet is not thought to be a part of an existing TCP session. Therefor the source IP address could be easily forged.

**False Positives**

There are reported incidents where legitimate traffic may cause an intrusion detection system to raise "false positive" alerts for this event. The following details have been reported:
Some combinations of windows may cause dns service requests to occur to local priveleged port 137, thus triggering this rule innocently.

Protocol details... *(ip header, tcp/udp/icmp header, payload data)*
Research details... *(packet captures, background, credits)*
IDS Signatures... *(dynamically generated signatures for free and commercial IDS)*