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

IDS277/DNS_NAMED-PROBE-IQUERY

Summary

This event indicates that a remote user attempted to determine if a nameserver supports IQUERY. This often indicates a pre-attack probe used to locate vulnerable servers running the named service.

Platform(s):	unix windows
Category:	dns
Classification:	Information Gathering Attempt
CVE	CVE-1999-0009
Bugtraq	134
advICE	2000409

How Specific

This event is specific to a particular exploit and is detected based on a particular string of characters found in the packet payload. Signatures for this event are very specific.

Trusting The Source IP Address

Since this event was caused by a UDP packet, the source IP address could be easily forged. It has been noted that the intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed.

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)*