WHITEHATS

Home | Security Forums | Free Tools | arachNIDS

[Wednesday, July 18]

- 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

IDS175/MISC_SOCKS-PROBE

Platform(s):	unix windows
Category:	misc
Classification:	Relay Attempt
CVE	nomatch
Bugtraq	nomatch
advICE	2003017

Summary

This event indicates that someone is scanning your system to see if it is running SOCKS. This may be a hacker that desires to "bounce" traffic through your system or a chat server (trying to determine if someone is bouncing through your system to chat anonymously).

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.

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. 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.

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:
IRC chat servers will often scan clients for open WinGate SOCKS servers. They will kick off such people with a message indicating how to fix the problem. If you receive such message, then you can /who the client to see if is a WinGate bot performing such a check.

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)*
