WHITEHATS

Home | **Security Forums** | **Free Tools** | **arachNIDS**

[Friday, July 20]

- **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

IDS152/ICMP_PING BSDTYPE

Platform(s):	unix windows device
Category:	icmp
Classification:	Information Gathering Attempt

CVE	CAN-1999-0523
Bugtraq	nomatch
advICE	nomatch

Summary

This event indicates that a ping request was sent to your network. Ping requests are usually used to determine whether a host is reponsive, but can be misused to map your network. This particular ping was probably generated by BSD/OS, FreeBSD, NetBSD, OpenBSD 2.5, Linux, or Solaris 2.5-2.7.

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 ICMP 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.

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:

This is only the default ping setting. Other ping software can emulate this signature. --start from dr_skipper-- Update - A company named Speedera has a new technology that uses rougly 90 machines distributed around the world to detect the closest web server to you for large corporate sites. They seem to test internet latency using BSD type pings. Each time someone connectes to a Speedera hosted site, you will see roughly 90 hosts ping you with a BSD type payload. I've recommeded they change the pings payload to include a URL with an explanation of their technology. See www.speedera.com for more info. I've contacted Speedera and they have confirmed the following list of IP's belong to their servers: 209.155.224.130, 216.117.57.66, 203.89.210.82, 38.144.51.2, 64.27.29.2, 211.169.245.98, 64.78.174.34, 213.61.6.2, 209.10.58.124, 207.230.26.34, 204.71.35.136, 207.136.170.10, 208.225.197.194, 64.41.192.103, 64.14.117.10, 209.92.236.2, 206.190.24.162, 209.83.178.130, 209.240.77.130, 64.37.246.2, 146.101.78.130, 64.78.156.2, 216.6.49.9, 193.214.57.194, 216.6.49.143, 193.45.3.130, 202.130.158.130, 216.148.216.2, 216.219.241.162, 216.28.22.130, 202.54.111.72, 64.245.120.2, 64.28.86.226, 204.176.88.5, 198.5.148.6, 38.144.121.2, 212.62.17.145, 212.0.126.130, 64.70.61.2, 202.160.241.130, 212.73.220.2, 211.2.249.194, 216.74.133.194, 203.197.173.129, 63.236.103.130, 203.166.49.226, 202.144.78.2, 208.151.247.34, 208.187.29.66, 64.67.26.194, 212.31.251.66, 200.194.68.4, 210.192.104.66, 63.251.167.2, 63.236.82.135, 213.41.76.66, 203.197.88.130, 206.63.151.4, 63.209.37.11, 208.185.109.130, 208.185.54.14, 207.235.98.194, 209.68.217.194, 209.219.187.34, 64.37.65.194, 202.132.53.2, 63.251.235.226, 205.158.108.194, 64.0.96.12, 216.52.110.66, 63.140.72.3, 213.174.196.130, 64.94.163.226, 64.105.14.218, 64.94.206.66, 216.52.172.130, 63.251.143.2, 216.52.153.130, 216.52.125.38, 216.52.85.194, 216.52.195.230, 216.52.44.194, 216.52.189.26, 200.53.184.66 --end from dr_skipper--

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)*