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

IDS362/SHELLCODE_SHELLCODE-X86-NOPS-UDP

Summary

This event may indicate that a string of the character 0x90 was detected. Depending on the context, this usually indicates the NOP operation in x86 machine code. Many remote buffer overflow exploits send a series of NOP (no-operation) bytes to pad their chances of successful exploitation.

Platform(s): windows solaris linux bsd sco
Category: shellcode
Classification: System Integrity Attempt

CVE nomatch
Bugtraq nomatch
advICE nomatch

How Specific

This event is specific to a vulnerability, but may have been caused by any of several possible exploits. Signatures used to detect this event are specific and consider the packet payload.

Trusting The Source IP Address

Since this event was caused by a UDP packet, 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:
Since all network traffic is watched, it is possible this sequence may occur in any binary file transmission, and not be a part of an overflow attempt. Confirm by looking at the packet trace generated by this alert.

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)*