

## SNMP False Positives

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-04/0020.html>

---

**From:** Cox, Michael ([mcox@ti.com](mailto:mcox@ti.com))

**Date:** 04/11/02

From: "Cox, Michael" <[mcox@ti.com](mailto:mcox@ti.com)>  
To: [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)  
Date: Thu, 11 Apr 2002 14:26:13 -0500

I'm getting a lot of "default community string enabled" false positives from Nessus, Retina, and verified with SNMPing.

On certain boxes, Nessus and Retina report that every string they check is enabled. When running SNMPing and "pinging" a Solaris 8 box I am told the service is enabled and available. I get this response no matter what community string I use. The output from tcpdump is below which seems to say that the requested object doesn't exist. Can anyone help me out here and explain this? I've seen this 20-30 times (and I think they are all Solaris boxes, but I need to double-check). I'm guessing that they (Sun) don't implement the standard MIB II variables, or something, since the request is just asking for the system name. The tools must have been written to look for any GetResponse, even if it is an error. Of course, that raises the question of why Solaris is sending anything, even errors, to invalid communities; any request from an invalid community should be dropped. Or, maybe I'm barking up the wrong tree entirely, and someone will have a better answer.

Many thanks in advance!

Mike

```
windump: listening on \Device\NPF_{BFF5A60B-F6E6-42FC-B01E-6C4CBD86B5FC}
15:20:46.996306 arp who-has hogan.itg.ti.com tell cna9815016
15:20:46.996718 arp reply hogan.itg.ti.com is-at 0:3:ba:8:50:3c
15:20:46.996731 cna9815016.1734 > hogan.itg.ti.com.161: |30|26|02|01|SNMPv1
|04|
06C=abc123 |a0|19GetRequest(25)|02|01|02|01|02|01|30|0e
|30|0c|06|08system.sysName
me.0|05|00 (ttl 128, id 5981, bad cksum 0!)
15:20:46.997434 hogan.itg.ti.com.161 > cna9815016.1734: |30|26|02|01|SNMPv1
|04|
06C=abc123 |a2|19GetResponse(25)|02|01|02|01 noSuchName|02|01|@1|30|0e
|30|0c|06|
08system.sysName.0=|05|00 (DF) (ttl 255, id 25971)
```

## SecurityFocus Penetration: SNMP False Positives

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

- **Previous message:** Alfred Huger: "Commercial Pen-testing tool"
- **Next in thread:** Ben Klang: "Re: SNMP False Positives"
- **Reply:** Ben Klang: "Re: SNMP False Positives"
- **Reply:** Leif Sawyer: "RE: SNMP False Positives"
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]