

RE: sniffer in promiscuous mode

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-02/0182.html>

From: Smith, Chris (csmith@Calence.com)

Date: 02/06/02

From: "Smith, Chris" <csmith@Calence.com>
To: 'Siddharta Govindaraj' <govind@iiitb.ac.in>
Date: Wed, 6 Feb 2002 13:14:28 -0700

Are you in a switched environment? If so you will need to span ports (copy traffic from one port to another) so the port with the sniffer gets copies of the frames and can read the traffic. Normally switches utilize "microsegmentation" – only copying frames to the port owning the destination MAC address(es). You will see ARP and other broadcast traffic as broadcasts (mac = FF:FF:FF:FF:FF:FF) are copied to each port.

-----Original Message-----

From: Siddharta Govindaraj [<mailto:govind@iiitb.ac.in>]
Sent: Tuesday, February 05, 2002 8:04 AM
To: security-basics@securityfocus.com
Subject: sniffer in promiscuous mode

Hi,

I have a funny problem with the ethereal packet sniffer. It correctly captures all packets entering or leaving my interface, but in promiscuous mode, it only seems to capture ARP, NETBIOS, IPX, RIP and such protocols, and never seems to get any UDP or TCP packets ! I have tried other sniffers, and they all exhibit the same behaviour, so I dont think its a sniffer problem. Is there something else I have to do to capture TCP packets ? Or could it be something to do with Wincap ?

Thanks
Siddharta

- **Previous message:** [Red Wolf: "Re: Help with Win2000 Server."](#)
- **Maybe in reply to:** [Siddharta Govindaraj: "sniffer in promiscuous mode"](#)
- **Next in thread:** [Damon Sisola: "RE: sniffer in promiscuous mode"](#)
- **Next in thread:** [brien mac: "Re: sniffer in promiscuous mode"](#)
- **Reply:** [Damon Sisola: "RE: sniffer in promiscuous mode"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)