

Re: Program to sniff out packets.. Virus HELP plz

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-10/msg00639.html>

- *From:* "PeOpLeS" <PeOpLeS@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 8 Oct 2005 15:02:01 -0700
-

Thanks for all the info. I will try ethereal on the network next week...

What size packets should i be looking out for?
or should i be just looking out for a high number of broadcasts, associated to a particular IP?

Oh . and do all the machines need to be logon or just switchd on?

"SuperGumby [SBS MVP]" wrote:

- > BINGO!!!
- >
- > shutdown all workstations.
- > Ensure AV on the server is functional and uptodate. IF IT AIN'T you have a
- > major problem.
- > Fire up a smallish group of workstations. Does anything peculiar happen? Do
- > they update their AV and is it fully functional?
- > Fire up another group.
- > Fire up another group.
- > Fire up another group.
- > Fire up another group.
- > Fire up another group.
- > Fire up another group.
- >
- > "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@xxxxxxxxxxxx>
- > wrote in message <news:O3VH%230EzFHA.904@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
- >> Unplug the cables if need be. Figure out when your network 'responds'
- >> again when you find the machine firing off the tcp/ip connections.
- >>
- >> PeOpLeS wrote:
- >>
- >>>Quite right, it a 2K box with 80 2k and XP nodes. I posted here, as it was
- >>>a fairly general question applicable to either OS. Plus i know folk here,
- >>>know their stuff :)
- >>>
- >>>As for Sophos, i think the virus on the network, is making it flaky by
- >>>uninstalling from various nodes and eating up the bandwidth preventing

Re: Program to sniff out packets.. Virus HELP plz

>>>internet access and thus updates :(
>>>
>>>"Marina Roos [SBS-MVP]" wrote:
>>>
>>>
>>>Hi,
>>>
>>>This can't be an SBS server with 80 nodes.
>>>And why is your Sophos enterprise out of date? It is far from flaky.
>>>
>>>--
>>>Regards,
>>>
>>>Marina Roos
>>>Microsoft SBS-MVP
>>>One of the Magical M&M's
>>>www.smallbizserver.net
>>>Take part in SBS forum:
>>><http://www.smallbizserver.net/Default.aspx?tabid=53>
>>>
>>>"PeOpLeS" <PeOpLeS@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> schreef in bericht
>>>news:A8D06559-0851-48F1-9610-7545115E6F7C@xxxxxxxxxxxxxxxxxxxx
>>>
>>>>Does anyone know of a program that scan detect which computer is trying
>>>>to
>>>>flood my network with packets.
>>>>
>>>>I have a server and 80 nodes. I have been informed by the person that
>>>>controls the firewall that there are viruses on my network. They believe
>>>>
>>>>that
>>>>
>>>>one machine in particular is trying to flood the network with packets
>>>>and
>>>>
>>>>is
>>>>
>>>>crashing the firewall.
>>>>
>>>>I run Sophos enterprise, but this version is a bit flaky and out of
>>>>date.
>>>>
>>>>Because of the high volume of packets being transmitted, many of the
>>>>computers can't connect to the network.
>>>>
>>>>So
>>>>
>>>>Can anyone suggest a good program that can tell me which machine is
>>>>
>>>>sending
>>>>

