

Trouble programming network access filter gateway

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-04/0419.html>

From: Sachs (*sushah23_at_yahoo.com*)

Date: 04/28/04

Date: 28 Apr 2004 14:58:54 -0700

Hi,

I am programming a real-time network access filter gateway as a requirement of my course. The main purpose of the gateway is to block access to some black-listed websites (i.e. block some HTTP requests).

I am using WinPCap 3.0 library and using VC++ 6.0 for development. WinPCap is good for developing network analysis tools, but there is one feature of the library which allows one to send raw packets to the network adapter (http://winpcap.polito.it/docs/man/html/group_wpcap_tut8.html).

Now my pseudo code for capturing request packets goes like this

```
request_capture_thread()
start
open network adapter connected to internal network (e.g. LAN);
capture all request packets;
if tcp request
  if http request
    parse http header and get domain name;
    lookup the domain name in the blocked list;
    if blocked
      drop the request packet(s);
      send customized response back;
    else allow the request;
send captured request packets to the network adapter connected to
the external network (e.g. Internet);
end
=====
response_capture_thread()
start
open network adapter connected to external network;
capture all response packets;
send captured responses to the adapter connected to the internal
network;
end
```

Now I am trying to capture packets from the internal network adapter using a filter expression (http://winpcap.polito.it/docs/man/html/group_language.html) in a promiscuous mode. The expression looks like "eth src xx:xx:xx:xx:xx:xx and eth dst yy:yy:yy:yy:yy:yy", where "xx:xx:....:xx" is MAC address of the adapter where the requests are coming from (e.g. router) and "yy:yy:....:yy" is MAC address of the adapter on the gateway connected to internal network. similarly I follow the similar filter expression for the response packet capturing.

Now the main issue is I don't see any response coming from the external network even if I transfer all the captured packets from internal network adapter to the external network adapter. Do I have to change the MAC layer addresses when I transfer all the packets from internal network to the external network ?

I will appreciate any guidelines or references to the similar implementation.

Thank you.

Wishes
Sachin Shah