

Re: Attacking our pc router at work

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2006-04/msg00444.html>

- *From:* Michal Mertl <michal.mertl@xxxx>
 - *Date:* Wed, 05 Apr 2006 15:19:06 +0200
-

Mark Jayson Alvarez wrote:

Hi,

I have one question. What if I change my ip and mac address at the same time to that of our pcrouter's ip and mac... Will this going to kick out that router in our network, causing the rest of the entire lan to be out of service?? No one's gonna caught me right?? Arpwatch can only watch if an ip address has moved to another mac address but not when both ip and mac has moved to another ip and mac... Do you know any possible solution to this??

Your question is off topic for this list.

Use intelligent switches (not hubs) and port security (you can allow only a specific MAC address behind a switch port). You could also use static entries on the switch for some MAC addresses (entry on a switch is a MAC address + port behind which the address can be found) but that isn't as safe. An attacker can generate traffic with lots of source MAC addresses. Every switch has limited memory to store the MAC addresses and usually when the table is full it starts working as a hub. A sophisticate attacker may still be able to contaminate end stations – if he sends a gratuitous ARP reply to a station where he pretends he is the router (changes the MAC address), he will receive the traffic for the router and can also then make man-in-the-middle attacks (insert himself into forwarding chain of the station).

More sophisticated solution is using 802.1x – port-based authentication – a switch will only start forwarding traffic to you once you authenticate and you of course shouldn't be able to authenticate as the server.

On FreeBSD you can disable ARP and/or create static ARP entries and it will protect you a little but you also need to configure some protection on the network infrastructure.

Re: Attacking our pc router at work

It's quite a complex issue to protect against this type of attack and I am no real guru so please take what I said with a grain of salt.

HTH

Michal

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"