

## Re: Switch Security

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-10/9689.html>

---

**From:** Oliver ([oliver@greyhat.de](mailto:oliver@greyhat.de))

**Date:** 10/19/02

From: [oliver@greyhat.de](mailto:oliver@greyhat.de) (Oliver)

Date: 19 Oct 2002 12:08:07 -0700

Hi,

ethernet based networks have the problem that a packet sent from one system to another system in the same subnet, will arrive at each network-card in the same "broadcast-domain". The IP-Stack of each system is looking into the packet. If the packet is addressed to the system, the packet will be delivered to the next layer of the ip-stack. If the packet is not determined for the system, it will be discarded.

This causes a lot of network traffic. The solution is a switch (or multiport-bridge). The switch remembers the MAC-Adress of each network card which is connected and has an internal table about ports/mac-addresses.

If a packet arrives at the switch, the switch can determine the target of the packet by reading the mac-address. Furthermore the switch sends the packet ONLY to the target port and NOT to all systems like a "stupid" HUB would do.

By doing this, the switch automaticly enhances the security of your network, because "putting your NIC into promisc. mode" won't enable you to sniff all the network traffic.

So far so good. There are several technics to bypass this. Some buzzwords are: Mac-Duplicating, Mac/Arp-Spoofing, ARP-Flooding and Re-Routing-Attacks (f.e. ICMP-redirect, RIP....)

If the switch does not support features like "port-security", "enabling/disabling of unused ports", layer3-Filtering, a hacker can bypass the "security" of a switch with tools like "Parasite" (<http://www.thehackerschoice.com/download.php?t=r&d=parasite-1.2.tar.gz> - There is a readme file included which tells a lot about switch/arp security)

If you are a attacker in a switched environment, you have to start parasite to route all the network-traffic through your PC and to start

microsoft.public.win2000.security: Re: Switch Security

a Sniffer like DSNIFF or L0pht, and you are still able to sniff passwords!

Ok,

hope this helps you a little bit to understand the security which will be given by a switch!

Bye,

Oliver Karow  
www.greyhat.de

"Altan" <[s@s.com](mailto:s@s.com)> wrote in message news:<69b001c276d3\$45db4450\$2ae2c90a@phx.gbl>...  
> *My network*