

Re: Firewalls and PCI

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-01/msg00207.html>

- *From:* "Jon R. Kibler" <Jon.Kibler@xxxxxxxx>
 - *Date:* Wed, 16 Jan 2008 18:31:14 +0000
-

Brian Johnson wrote:

How does a lack of DHCP let you KNOW who is on your network? Absent DHCP all an attacker with zero knowledge of the network configuration needs to do is sniff the ARP and other broadcast traffic to determine the addressing of the network and find themselves an open address or takeover a used address. Now if you have 802.1x or use IPSEC to limit communications that is another story entirely and can still function with DHCP.

A number of clients I visit say that lack of DHCP is a security measure. If they push back on my claim it would only slow an attacker down I demonstrate just how easy it is to find an open address, I end up able to talk to their network inside of 5 minutes.

I agree completely that a lack of DHCP does not mean security. However, anything DHCP I automatically presume is untrustworthy. With static IPs, I lock down switches, associating a MAC with a port or use 802.1x.

Since you mentioned it, a comment about IPSec: You not believe the number of sites that think they have IPSec enabled, but don't really. They take the average windows defaults in IPSec setup (no AH, no ESP) and think they now have IPSec security. Like everything else, unless configured correctly, and TESTED, IPSec is not going to provide any additional security. When a site enables IPSec, you would think they would at least sniff the network to see if the traffic is REALLY encrypted, but I have yet to see any site have actually tested their IPSec configuration.

Jon

—

Jon R. Kibler
Chief Technical Officer
Advanced Systems Engineering Technology, Inc.
Charleston, SC USA
(843) 849-8214

Re: Firewalls and PCI

=====

Filtered by: TRUSTEM.COM's Email Filtering Service

<http://www.trustem.com/>

No Spam. No Viruses. Just Good Clean Email.