

Re: Mail Server in the DMZ question

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-05/0085.html>

From: Kevin Stevens (freebsd_at_pursued-with.net)

Date: 05/19/04

Date: Tue, 18 May 2004 17:07:23 -0700 (PDT)

To: Michael Collette <metrol@metrol.net>

> *Nothing specifically. Just the notion of allowing any kind of request
> to come from the DMZ into the secure network didn't seem right. In an
> ideal setup nothing should be allowed to make a request to the internal
> network. At least that's been my thinking on the matter.*
>
> > *If you're
> > protecting against mail being sent in, well clearly that will happen
> > either way. If you're protecting against an attacker that would hijack
> > the DMZ host and try to attack your internal machine via port 25, well
> > yes it will stop that, but if the attacker manages to hijack the machine
> > they're going to be able to do a lot worse things (snoop on all your
> > mail, possibly capture passwords, etc).*
> >
> > *Really, the possibility that an attack would be able to make a
> > successful attack using only port 25 of your internal host is very
> > remote, and the possibility that they couldn't do anything else
> > malicious even though they had hijacked a host is even more remote.
> > Make sure you're not over architecting your environment and introducing
> > unnecessary complications for very minimal potential benefit.*
>
> *I can fully appreciate your concern about over architecting this thing. As I
> began researching this and kept seeing UUCP getting mentioned my arms went up
> in the air. I hadn't imagined it was going to get this "clever" to spool up
> mail in the DMZ then request it down into the secure network. Yet another
> protocol was not the solution I was hoping for.*

All UUCP offers is that it's a "pull" technology, so you don't have to permit a session to be initiated from your DMZ to get the mail in. SMTP is "push", so you have to open the firewall enough to allow the bastion mailhost in to deliver.

The downside is that it's a pull technology – anyone who can hack your uucp account on the bastion can get all your mail. Plus I'm not sure how thoroughly inspected the UUCP code is; all my experience is with using it over dialup or frame serial circuits, not over IP.

FreeBSD-Security: Re: Mail Server in the DMZ question

KeS

freebsd-security@freebsd.org mailing list

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

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"