

Re: Pen testing Fiber Channel

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-01/msg00215.html>

- *From:* Bob Beringer <bob.beringer@xxxxxxx>
 - *Date:* Thu, 19 Jan 2006 01:13:45 -0500
-

Bojan,

Thanks for the helpful email, the information below might also be of value...

World-Wide names are sometimes spoofable.
Softzone's are often easy targets for compromise.
The "fibre channel" protocol looks very similar to that of TCP/IP and can on occasion be used to carry information other than data.

You started to hit the nail on the head with your questions below, however, other questions should be asked about the protocol(s) that the target network is running on.

Also a little known fact is that many of the Fibre Channel switches have undisclosed backup accounts with default passwords that will allow for easy access and management of the security zones.

If direct access to the network is available, a top notch protocol analyzer will come in handy and show which protocols can exist for exploitation.

Some other solutions out there also work as fibre channel variants and allow for C&C to occur over their devices, as an example, all kinds of hacks and applications are available for Myricom gear...

Hope this helps,
Bob Beringer

----- Original Message -----
Received: Thu, 19 Jan 2006 12:56:09 AM EST
From: Bojan Zdrnja <bojan.zdrnja@xxxxxxx>
To: "pentesticle@xxxxxxx" <pentesticle@xxxxxxx>Cc:
pen-test@xxxxxxxxxxxxxxxxxxxx
Subject: Re: Pen testing Fiber Channel

On 17 Jan 2006 20:06:45 -0000, pentesticle@xxxxxxx
<pentesticle@xxxxxxx> wrote:
> Hello list...
>

Re: Pen testing Fiber Channel

> I'm performing my first pen-test on a network that uses fiber channel for their backup network. The network diagrams show fiber channel switches on the backside and nothing else to prevent access from one
> server to another on a different higher security network. Can anyone tell me if it is possible once I compromise one of the servers on the lower security network can I hop across the fiber channel to a server on the
> higher security network? If so how would I go about hopping over via the fiber?

Are you sure you are not talking about SAN here? If it's SAN then you can't use it to do anything else but transfer data on it. You could check one of the machines to see which LUNs (logical disks) are mapped – there can be problems here if a SAN admin allowed access to more LUNs than needed.

Other than that, SAN servers (backend servers) are usually on isolated or private network, so you can check if you can reach them somehow (you shouldn't be able to). They basically hold the "keys to kingdom" as they can allow you to map LUNs to anything and then access the disk from other servers, completely compromising the security.

Cheers,

Bojan

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities

to SQL injection, Cross site scripting and other web attacks before hackers do!

Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are

Re: Pen testing Fiber Channel

futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!
Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831

- Prev by Date: [*Re: Pen testing Fiber Channel*](#)
- Next by Date: [*New Unix security article on SecurityFocus*](#)
- Previous by thread: [*Re: Pen testing Fiber Channel*](#)
- Next by thread: [*Reason 0.1.0 \(New Nessus Client\)*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)