

Re: Blocking Port scans

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-10/0185.html>

From: Justin (justinvinn_at_gmail.com)

Date: 10/24/05

Date: Mon, 24 Oct 2005 14:10:42 -0400

To: BSK <bishan4u@yahoo.co.uk>

BSK,

Its kind of hard to block SYN scans as to maintain functionality, the server has to respond to a SYN with a SYN/ACK. Of course, if there is no server behind the router, you could just have it drop the SYNs (in nmap terms filter the ports).

There are several other approaches to this problem (such as John Ericson's shroud2.sh script), that take different views. You could also jack the scan rate limiting way up, so the scan would take forever and a day to complete. While this wouldn't stop a dedicated attacker, it could discourage a script kiddie who'd get bored of watching nmap shoot new ETC values to STDOUT.

Course, I'm not an admin and have never had hands on expirience with building a Cisco PIX firewall. So, my advice may be dead wrong...

peace,
--Justin

On 10/24/05, BSK <bishan4u@yahoo.co.uk> wrote:

> *Hello Everyone,*
>
> *Just wanted some feedback from you people. I'm doing a*
> *Firewall Assessment for a CISCO PIX firewall. The*
> *firewall allows SYN, FIN, NULL and XMAS scans but*
> *blocks ACK scans (largely means its a stateful*
> *firewall).*
>
> *Now what do we do to block the scans that are allowed.*
> *I think it should be easy to block FIN, NULL and XMAS*
> *scans but how do we block or limit or workaroud a SYN*
> *scan. I way that I think is probably blocking or*
> *limiting the packets from the source (using IDS/IPS)*
>
> *Looking ahead to some ideas, thoughts, hints.*
>

SecurityFocus Penetration: Re: Blocking Port scans

> thns bshan

>

>

>

>

>

> *To help you stay safe and secure online, we've developed the all new Yahoo! Security Centre.*

> <http://uk.security.yahoo.com>

>

>

> *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 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
