

RE: Fingerprinting Firewall

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-04/0058.html>

From: Clement Dupuis (cdupuis_at_cccure.org)

Date: 04/14/05

To: <pen-test@securityfocus.com>

Date: Wed, 13 Apr 2005 23:11:49 -0400

Take a look at the ISSAF, it has a nice section on common ways to test firewall and a lot of those identification items mentioned below.

You can find it at:

<http://www.professionalsecuritytesters.org/modules.php?name=News&file=article&sid=287>

Enjoy

Clement

Clement Dupuis, CD
CCCure Enterprise Security & Training Inc.
CISSP, GCFW, GCIA, Security+, CEH, CCSA, CCSE, ACE
President/Chief Learning Officer (CLO)
Tel: 954 364 8410 (Florida)
Tel: 819 340 0138 (Quebec)
Fax: 636 773 6328

Maintainer of :

The CISSP and SSCP Open Study Guides Web Site
<http://www.cccure.org>

The Professional Security Testers Warehouse
<http://www.professionalsecuritytesters.org>

-----Original Message-----

From: Fatih OZAVCI [<mailto:fatih.ozavci@infosecurenet.com>]

Sent: Wednesday, April 13, 2005 3:18 AM

To: Prashant Gawade

Cc: pen-test@securityfocus.com

Subject: Re: Fingerprinting Firewall

hi,

RE: Fingerprinting Firewall

SecurityFocus Penetration: RE: Fingerprinting Firewall

some firewalls (like checkpoint fw-1) have by-default open services, you can detect firewall if this services or ports are open.

for example 256/18264/264 ports are open, this firewall is checkpoint fw-1.

also you can analyze tcp/ip fingerprints for firewall operation system (*bsd, linux, solaris etc.)

good luck.

Fatih Ozavci
IT Security Consultant

Prashant Gawade wrote:

>
> *hi*
>
> *We all know that, we can identify firewall using various methods and tools like "firewalk".*
> *Is there any method or tool available which will remotely fingerprint and enumerate rule base configured on the firewall?*
>
>
> *Prashant Vijayanand Gawade*
> *Paladion Networks*
> *Security Engineer*
> *Navi- Mumbai*
>