

RE: Topology discover

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-09/0426.html>

From: Steve McLaughlin (*Steve.McLaughlin_at_aggreko.co.uk*)

Date: 09/28/05

Date: Wed, 28 Sep 2005 16:24:42 +0100

To: "RSMC" <smcsoc@yahoo.es>, <pen-test@securityfocus.com>

Try cheops-ng

<http://cheops-ng.sourceforge.net/>

It's like a pen-testers network neighbourhood.

Discovers, Draws the Maps, and Scans.

Steve McLaughlin

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

From: RSMC [mailto:smcsoc@yahoo.es]

Sent: 21 September 2005 21:57

To: pen-test@securityfocus.com

Subject: Topology discover

Hi there,

I am currently performing a pen-test in the internal network of a company.

I am used to pen-testing systems and the set of applications they support, looking for vulnerabilities in software version, logic or misconfiguration.

I have also considered routing and protocol attacks as ARP spoofing and RIP packet injection.

But I think I am missing some techniques to find out what the topology is. I know about traceroute, firewall and CDP, but I would like to know if there is a whitepaper or documentation that explains how to find out as much as possible about the environment I am in. Help about discovering VLANs is also welcomed.

Thanks in advance.

Audit your website security with Acunetix Web Vulnerability Scanner:

SecurityFocus Penetration: RE: Topology discover

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

This email has been scanned by the MessageLabs Email Security System.

Visit us at <http://www.aggreko.com>

Confidentiality Notice: This communication and any accompanying attachments contain confidential information intended for a specific individual and purpose. This communication is private and protected by law. If you are not the intended recipient, you are hereby respectfully notified that any disclosures, copying, forwarding or distribution, or the taking of any action based on the contents of this communication is strictly prohibited.

This email has been scanned by the MessageLabs Email Security System.
For more information please visit <http://www.messagelabs.com/email>

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
