

Re: Finding multi-homed, internet connected, systems as potential point-of-entry.

Re: Finding multi-homed, internet connected, systems as potential point-of-entry.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-12/msg00076.html>

- *From:* MadHat <madhat@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 6 Dec 2005 11:39:27 -0600
-

<http://www.unspecific.com/.go/routedetector/>

It uses ICMP and may or may not work depending on how the local network is set up. It worked well at my last job.

On Dec 5, 2005, at 7:41 AM, Bongers, Coen wrote:

Hello,

Im asked to assess the existence of so-called multi-homed systems on the network of a customer, that are able to directly connect to the internet (and thus circumventing the proxy services), in order to reduce the risk of network compromise through this 'illegal' internet-access.

Any tips and/or help on how to approach this would be appreciated.

The following approach is my present idea;

- Send a spoofed (spoofer an internet address under our control) message (IP/ICMP/UDP,etc) to the target(s) from the internal network.
- Detect for the response of this message on the spoofed address at the internet.
- Log some identifying information in the initial message, that will end up on the response so that the response can be correlated with

Re: Finding multi-homed, internet connected, systems as potential point-of-entry.

the
internal address of the system.

Questions for me now are;

- What are the risks of false negatives and false positives using this methode?
- What prerequisites are ther for thes methode to be succesfull?
- Are there any other ways of identifieing these 'illegal' internet connections?
- Are there any freeware/commercial tools that allready do the job?
- If so, how good of a job are they doing?

p.s.> there is no administrative access to the target systems, so it has to be a black-box-approach.

Thank you.

Met vriendelijke groet / with kind regards,

Coen Bongers

Security Consultant

Re: Finding multi-homed, internet connected, systems as potential point-of-entry.

The information contained in this email and its attachments (if any) is confidential and may be legally privileged. It is intended solely for the use of the individual or entity to whom it is addressed and others authorised to receive it. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or action in reliance of the contents of this information is strictly prohibited and may be unlawful. LogicaCMG is neither liable for the proper and complete transmission of the information contained in this email nor for any delay in its receipt. If received in error, please contact LogicaCMG on +31 (0)40 295 77 77 quoting the name of the sender and the addressee and then delete it from your system. LogicaCMG does not accept any responsibility for viruses and it is your responsibility to scan the email and attachments.

Re: Finding multi-homed, internet connected, systems as potential point-of-entry.

This e-mail and any attachment is for authorised use by the intended recipient(s) only. It may contain proprietary material, confidential information and/or be subject to legal privilege. It should not be copied, disclosed to, retained or used by, any other party. If you are not an intended recipient then please promptly delete this e-mail and any attachment and all copies and inform the sender. Thank you.

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

--
MadHat (at) Unspecific.com, C²ISSP
E786 7B30 7534 DCC2 94D5 91DE E922 0B21 9DDC 3E98
gpg --keyserver wwwkeys.us.pgp.net --recv-keys 9DDC3E98

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:

Re: Finding multi-homed, internet connected, systems as potential point-of-entry.

Re: Finding multi-homed, internet connected, systems as potential point-of-entry.

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