

Re: Scanning Class A network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-10/0190.html>

From: Satanic.Brain (Satanic.brain_at_gmail.com)

Date: 10/24/05

Date: Mon, 24 Oct 2005 16:37:31 -0300

To: pen-test@securityfocus.com

Well, if ICMP isn't allowed in the network your best choice will be a "TCP Ping" (-PT nmap argument. Send TCP ACK, and wait for RST).

About point 2, i recommend you Nmap... you can save the output and then, with a little perl script, compare the results with a "diff" sentence...

I'm suposing that you are working in a Linux environment, cause Nmap in windows will be very slow (for that type of scans)

Sorry my poor english, but isn't my first language..

Cheers

tarunthenut@gmail.com wrote:

>Hello All,
> Recently I was given a task to carry out a port scan of an entire valid
>Class A range (Dont ask me what the huge pool of valid IP's was for :)).
>The scan needed to be carried out externally, and not from within the
>network to identify hosts and ports exposed to the Internet.
> The problem compounded cause of the following limitations :
>1. ICMP was not allowed in the network
>2. The IP range was to be scanned every month for the entire port range fro=
>m
>1-65535 for TCP & UDP
> After searching for a suitable scanner which could scan such a large range
>in reasonable time, I could think of only nmap, nessus, superscan and ISS.
> But because of the limitations stated above,all the tools took a huge
>amount of time (ran into month).
> I have struggled with options within the tools, tried configurable
>parameters (host time out, parallelism, RTT etc) and divided into smaller
>class C networks and scanned.but still the scan seems to take ages even if
>it is
> Any advise would be welcome :)
>
>Cheers
> tarunthenut

SecurityFocus Penetration: Re: Scanning Class A network

>

>

>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
