

## Re: [fw-wiz] New Script Kiddie tool ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-08/0467.html>

---

**From:** Jim MacLeod ([jmacleod@hotpop.com](mailto:jmacleod@hotpop.com))

**Date:** 08/23/02

To: Peter Robinson <[peter@securegateway.org](mailto:peter@securegateway.org)>

From: Jim MacLeod <[jmacleod@hotpop.com](mailto:jmacleod@hotpop.com)>

Date: Fri Aug 23 12:40:18 2002

Hello Peter,

ICMP type 8 is ping.  
UDP 53 is DNS.

If it is a tool, there's nothing very exciting about it. 3 pings followed by 2 DNS, repeat.

It'd be interesting to get a capture of the traffic to see whether it's queries or replies.

If the 61 addresses are all the same, this is most likely someone trying to DoS that device, possibly doing a modified smurf/DDoS to try to suck up your bandwidth. There's a detailed write-up of this sort of attack at <http://www.grc.com> under "Direct Reflected DoS".

Are you sure it's not more frequent, and your log source (firewall?) is only reporting it every 10 seconds?

Regards,  
-Jim MacLeod

At 04:00 PM 8/22/2002, Peter Robinson wrote:

>G/Day all

>

>Has any one seem this sort of probe ??

>

>It appears from all over the place and it seems to be spaced exactly 10  
>seconds appart.

>

>I am assuming this is a tool of sorts..

>

>

>Source Address=208.184.139.82

> Aug 22 14:04:21 Firewall 208.184.139.82 61.x.x.x----ICMP TYPE=8

Firewall-Wizards: Re: [fw-wiz] New Script Kiddie tool ?

> Aug 22 14:04:31 Firewall 208.184.139.82 61.x.x.x----ICMP TYPE=8  
> Aug 22 14:04:41 Firewall 208.184.139.82 61.x.x.x----ICMP TYPE=8  
> Aug 22 14:04:51 Firewall 208.184.139.82 61.x.x.x----UDP 53  
> Aug 22 14:05:01 Firewall 208.184.139.82 61.x.x.x----UDP 53  
> Aug 22 17:00:03 Firewall 208.184.139.82 61.x.x.x----ICMP TYPE=8  
> Aug 22 17:00:13 Firewall 208.184.139.82 61.x.x.x----ICMP TYPE=8  
> Aug 22 17:00:23 Firewall 208.184.139.82 61.x.x.x----ICMP TYPE=8  
> Aug 22 17:00:33 Firewall 208.184.139.82 61.x.x.x----UDP 53  
> Aug 22 17:00:43 Firewall 208.184.139.82 61.x.x.x----UDP 53

>

>Source Address=208.185.54.14

> Aug 22 14:04:21 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 14:04:32 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 14:04:42 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 14:04:52 Firewall 208.185.54.14 61.x.x.x----UDP 53  
> Aug 22 14:05:02 Firewall 208.185.54.14 61.x.x.x----UDP 53  
> Aug 22 15:53:32 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:42 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:52 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:54:02 Firewall 208.185.54.14 61.x.x.x----UDP 53  
> Aug 22 15:54:12 Firewall 208.185.54.14 61.x.x.x----UDP 53  
> Aug 22 17:00:02 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 17:00:12 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 17:00:22 Firewall 208.185.54.14 61.x.x.x----ICMP TYPE=8  
> Aug 22 17:00:32 Firewall 208.185.54.14 61.x.x.x----UDP 53  
> Aug 22 17:00:42 Firewall 208.185.54.14 61.x.x.x----UDP 53

>

>Source Address=208.225.197.194

> Aug 22 15:53:35 Firewall 208.225.197.194 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:45 Firewall 208.225.197.194 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:55 Firewall 208.225.197.194 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:54:05 Firewall 208.225.197.194 61.x.x.x----UDP 53  
> Aug 22 15:54:15 Firewall 208.225.197.194 61.x.x.x----UDP 53

>

>Source Address=208.254.18.130

> Aug 22 15:53:31 Firewall 208.254.18.130 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:41 Firewall 208.254.18.130 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:51 Firewall 208.254.18.130 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:54:02 Firewall 208.254.18.130 61.x.x.x----UDP 53  
> Aug 22 15:54:11 Firewall 208.254.18.130 61.x.x.x----UDP 53

>

>Source Address=208.254.75.130

> Aug 22 15:53:32 Firewall 208.254.75.130 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:42 Firewall 208.254.75.130 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:53:52 Firewall 208.254.75.130 61.x.x.x----ICMP TYPE=8  
> Aug 22 15:54:02 Firewall 208.254.75.130 61.x.x.x----UDP 53  
> Aug 22 15:54:12 Firewall 208.254.75.130 61.x.x.x----UDP

>

>Peter Robinson

>Senior Security Engineer – Sydney

>DeMorgan Information Security Specialists

Re: [fw-wiz] New Script Kiddie tool ?

Firewall-Wizards: Re: [fw-wiz] New Script Kiddie tool ?

>[robinson\\_p@demorgan.com.au](mailto:robinson_p@demorgan.com.au), [www.demorgan.com.au](http://www.demorgan.com.au),  
>Tel. 1800 336 674  
>Tel. +61 2 9929-0377  
>Fax +61 2 9499 4885  
>  
>  
>\_\_\_\_\_

---

>*firewall-wizards mailing list*  
>[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)  
><http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>