

Confirmation on Loadbalancing

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-10/0163.html>

From: BSK (*bishan4u_at_yahoo.co.uk*)

Date: 10/22/05

Date: Sat, 22 Oct 2005 13:03:42 +0100 (BST)

To: pen-test@securityfocus.com

Dear All,

I'm doing a Firewall Assessment (fingerprinted as a Cisco PIX box) and this is the response for IPID using Hping from the firewall.

```
HPING x.x.x.x (eth0 x.x.x.x): icmp mode set, 28
headers + 0 data bytes
len=46 ip=x.x.x.x ttl=237 id=48312 icmp_seq=0
rtt=344.9 ms
len=46 ip=x.x.x.x ttl=237 id=41778 icmp_seq=1
rtt=339.0 ms
len=46 ip=x.x.x.x ttl=237 id=21596 icmp_seq=2
rtt=358.7 ms
len=46 ip=x.x.x.x ttl=237 id=2524 icmp_seq=3 rtt=347.1
ms
len=46 ip=x.x.x.x ttl=237 id=17443 icmp_seq=4
rtt=347.2 ms
len=46 ip=x.x.x.x ttl=237 id=43891 icmp_seq=5
rtt=354.7 ms
len=46 ip=x.x.x.x ttl=237 id=27058 icmp_seq=6
rtt=348.7 ms
len=46 ip=x.x.x.x ttl=237 id=54317 icmp_seq=7
rtt=345.1 ms
len=46 ip=x.x.x.x ttl=237 id=30840 icmp_seq=8
rtt=353.3 ms
len=46 ip=x.x.x.x ttl=237 id=43748 icmp_seq=9
rtt=338.9 ms
len=46 ip=x.x.x.x ttl=237 id=60042 icmp_seq=10
rtt=339.2 ms
len=46 ip=x.x.x.x ttl=237 id=4548 icmp_seq=11
rtt=348.9 ms
len=46 ip=x.x.x.x ttl=237 id=62406 icmp_seq=12
rtt=343.1 ms
len=46 ip=x.x.x.x ttl=237 id=58227 icmp_seq=13
rtt=350.0 ms
len=46 ip=x.x.x.x ttl=237 id=8455 icmp_seq=14
```

SecurityFocus Penetration: Confirmation on Loadbalancing

rtt=341.5 ms
len=46 ip=x.x.x.x ttl=237 id=24647 icmp_seq=15
rtt=356.6 ms
len=46 ip=x.x.x.x ttl=237 id=41050 icmp_seq=16
rtt=341.1 ms
len=46 ip=x.x.x.x ttl=237 id=17346 icmp_seq=17
rtt=340.6 ms
len=46 ip=x.x.x.x ttl=237 id=11365 icmp_seq=18
rtt=343.0 ms
len=46 ip=x.x.x.x ttl=237 id=39006 icmp_seq=19
rtt=340.5 ms
len=46 ip=x.x.x.x ttl=237 id=61653 icmp_seq=20
rtt=345.2 ms
len=46 ip=x.x.x.x ttl=237 id=51762 icmp_seq=21
rtt=357.0 ms
len=46 ip=x.x.x.x ttl=237 id=50924 icmp_seq=22
rtt=356.0 ms
len=46 ip=x.x.x.x ttl=237 id=53055 icmp_seq=23
rtt=357.2 ms
len=46 ip=x.x.x.x ttl=237 id=58137 icmp_seq=24
rtt=356.9 ms
len=46 ip=x.x.x.x ttl=237 id=60414 icmp_seq=25
rtt=341.9 ms
len=46 ip=x.x.x.x ttl=237 id=26515 icmp_seq=26
rtt=339.2 ms
len=46 ip=x.x.x.x ttl=237 id=3580 icmp_seq=27
rtt=350.5 ms
len=46 ip=x.x.x.x ttl=237 id=24117 icmp_seq=28
rtt=355.8 ms
len=46 ip=x.x.x.x ttl=237 id=34794 icmp_seq=29
rtt=341.3 ms

Is it a load balancing firewall / firewall in failover mode or Cisco PIX is generating a random IPID?

Await your thoughts.

Thanks bshan

To help you stay safe and secure online, we've developed the all new Yahoo! Security Centre.
<http://uk.security.yahoo.com>

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

SecurityFocus Penetration: Confirmation on Loadbalancing

to SQL injection, Cross site scripting and other web attacks before hackers do!
Download Trial at:

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