

RE: Routers, Switches, and Firewall testing

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-01/0014.html>

From: rzaluski (*rzaluski_at_ivolution.ca*)

Date: 01/03/05

To: "'Greg Dreelin'" <gdreelin@edsicorp.com>, <pen-test@lists.securityfocus.com>

Date: Mon, 3 Jan 2005 13:15:37 -0500

Hello...

We have been using the ISIC tool suite. Basically it is a suite of tools that test the TCP/IP Stack and ruins under Linux. Its also free and you can download it from: <http://www.packetfactory.net/projects/ISIC/>

As per the website :

"ISIC is a suite of utilities to exercise the stability of an IP Stack and its component stacks (TCP, UDP, ICMP et. al.) It generates piles of pseudo random packets of the target protocol. The packets be given tendancies to conform to. Ie 50% of the packets generated can have IP Options. 25% of the packets can be IP fragments... But the percentages are arbitrary and most of the packet fields have a configurable tendency."

It basically comes with 5 tools under the ISIC suite. Which are : isic, tpsic, udpsic, icmpsic and esic. All have variouis functions and there is some overlap in what the tools do but they do a great job in testing.

isic – handles IP level tests and covers the source and destination number and header length. When you run it it dumps IP packets onto the network as quickly as possible. Some packets are intentionally malformed. This allows you to test general networking protocols as well as more specific ones

tpsic – is a utility for geterating random TCP packets and data. It works at layer 4. You have to supply information such as the source and destination ports. This enables you to test ports such as 80, 25 or VPNs etc. example tpsic -s 172.31.20.5,1200 -d 172.32.15.1,80
(if you omit a number tpsic uses a random port)

udpsic works much like tpsic but with udp (obviously!) Allows you to specify the source and destination port along with the IP.

Icmpsic – basically it's a tool that allows you to test how your security device handles icmp traffic that does not fall use only icmp echo.

Esic – is a tool that transmits pacets packets with random port numbers. The

SecurityFocus Penetration: RE: Routers, Switches, and Firewall testing

E in esic stands for Ethernet. This tool works below the network layer.

As you can see the suite works in various layers and tests them all.

For instance you could test your firewall ruleset and performance under pressure. Firewalls operate most efficiently when they receive normal traffic. But what happens when it received abnormal traffic under heavy load? You can use a command such as the one below. The P, V, F -80 switches indicate that 75% of traffic will be malformed.

```
isic -s 192.168.1.5 -d 10.21.1.5 -P80 -V80 I-80
```

You could also run tcpsic in conjunction with the command above to see how the firewall performance is affected when receiving data to an internal web server.

```
Tcpsic -s 192.168.1.4,2020 -d 10.21.1.6,80
```

While the test above is not "realistic" as firewalls generally do not receive 80% of traffic malformed it will stress test the system and give you good snapshot at what you need to look at to improve performance.

It is a good tool suite that has a lot to offer if you learn how to use it properly. The nice thing about it is that it can be used in shell scripts.

As a previous poster commented, there is no "one mega tool" but a collection of tools and techniques.....

Good luck!

Richard Zaluski, CCNA, CRCP
CISO, Security and Infrastructure Services
iVolution Technologies Incorporated
905.309.1911
866.601.4678
905.524.8450 (Pager)
www.ivololution.ca
rzaluski@ivololution.ca

Key fingerprint = DB39 7FC3 1F5D AD94 85DD 78B0 774D

=====
CONFIDENTIALITY NOTICE: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, please contact the sender. Any unauthorized review, use, disclosure, or distribution is prohibited.
=====

-----Original Message-----
From: Greg Dreelin [mailto:gdreelin@edsicorp.com]

RE: Routers, Switches, and Firewall testing

SecurityFocus Penetration: RE: Routers, Switches, and Firewall testing

Sent: Monday, January 03, 2005 9:59 AM
To: pen-test@lists.securityfocus.com
Subject: Routers, Switches, and Firewall testing

Pen-Test Group,

I have a question to present that is in need of a good answer. The question I have is "Is there any good programs for VAP testing routers, switches, and firewalls?" I know there is the Router Assessment Tool (RAT) for Cisco router and there is FTEST for firewalls, but are there any other programs that can be loaded on to a Laptop Toolkit that can do the testing? Looking for a all in one program if there is such a thing. If anyone has any good ideas please let me know. Thanks ahead.

v/r

Gregory (Greg) S. Dreelin
Senior Systems Analyst
Marine Corp Information Assurance Assessment Team (MCIAAT)
gdreelin@edsicorp.com
540-720-0841/0843/2093 /2106
Cell 703-843-1962

‘Information is Knowledge, Knowledge is Power, and Power is Dangerous’