NAME

sc_tbitblind — scamper driver to test systems for resilience to blind TCP attacks.

SYNOPSIS

sc_tbitblind [**-r**] [**-a** *addressfile*] [**-A** *application*] [**-c** *completed-file*]
[**-l** *limit-per-file*] [**-o** *output-file*] [**-O** *options*]
[**-p** *scamper-port*] [**-t** *log-file*] [**-T** *ttl*] [**-w** *wait-between*]

DESCRIPTION

The **sc_tbitblind** utility provides the ability to connect to a running scamper(1) instance and use that instance to test systems for resilience to blind TCP attacks, with the output written to a file in warts format. The utility tests a given system for regular TCP behavior, and then tests the system for response to reset, SYN, and data packets that could have come from a blind attacker because the sequence number is not the next sequence number value expected by the receiver (the reset and SYN cases) or the acknowledgment value covers data ahead or behind the receiver's point in their sequence number space (the data cases). The utility also tests the system's response to a connection that advertises support for window scaling, TCP timestamps, and Selective Acknowledgments (SACK).

The options are as follows:

-? prints a list of command line options and a synopsis of each.

-a *addressfile*
specifies the name of the input file which constists of a sequence of systems to test, one system per line.

-A *application*
specifies the type of application to simulate while testing the system. Options are HTTP and BGP.

-c *completed-file*
specifies the name of a file to record IP addresses that have been tested.

-l *limit-per-file*
specifies the number of tbit objects to record per warts file, before opening a new file and placing new objects.

-o *output-file*
specifies the name of the file to be written. The output file will use the warts format.

-O *options*
allows the behavior of **sc_tbitblind** to be further tailored. The current choices for this option are:

- **noshuffle:** do not shuffle the order of the input list or the order of the tests.
- **gz:** compress the warts output using gzip compression.
- **warts.gz:** compress the warts output using gzip compression.
- **bz2:** compress the warts output using bzip2 compression.
- **warts.bz2:** compress the warts output using bzip2 compression.
- **xz:** compress the warts output using xz compression.
- **warts.xz:** compress the warts output using xz compression.

-p *scamper-port*
specifies the port on the local host where scamper(1) is accepting control socket connections.

-r causes the random number generator used to shuffle tests be seeded.

-t *log-file*
specifies the name of a file to log progress output from **sc_tbitblind** generated at run time.

-T *ttl*
specifies the IP-TTL to use with the blind TCP tests.

-w *wait-between*
specifies the length of time to wait between any two TCP tests to one system.

EXAMPLES

Use of this driver requires a scamper instance listening on a port for commands, which has been configured to use the IPFW firewall rules 1 to 100, as follows:

```
scamper -P 31337 -F ipfw:1-100
```

To test a set of web servers specified in a file named webservers.txt and formatted as follows:

```
1,example.com 1263 192.0.2.1 http://www.example.com/
1,example.com 1263 2001:DB8::1 http://www.example.com/
1,example.com 1263 2001:DB8::2 https://www.example.com/
```

the following command will test all servers for resilience to blind TCP attacks and record raw data into webservers_00.warts, webservers_01.warts, etc:

```
sc_tbitblind -a webservers.txt -p 31337 -o webservers
```

The webservers.txt file is required to be formatted as above. The format is: numeric ID to pass to tbit, a label for the webserver, the size of the object to be fetched, the IP address to contact, and the URL to use.

To test a set of BGP routers specified in bgprouters.txt and formatted as follows:

```
192.0.2.2 65000
192.0.2.2 65001
```

the following command will test all BGP routers for resilience to blind TCP attacks, without shuffling the test order, waiting 180 seconds between tests, and record raw data into bgprouters_00.warts, bgprouters_01.warts, etc:

```
sc_tbitblind -a bgprouters.txt -p 31337 -o bgprouters -A bgp -O
noshuffle -w 180
```

The bgprouters.txt file is required to be formatted as above. The format of that file is: IP address to establish a BGP session with, and the ASN to use.

SEE ALSO

M. Luckie, R. Beverly, T. Wu, M. Allman, and k. claffy, *Resilience of Deployed TCP to Blind Attacks*, Proc. ACM/SIGCOMM Internet Measurement Conference 2015. scamper(1), sc_wartsdump(1), sc_warts2json(1), warts(5)

AUTHORS

sc_tbitblind was written by Matthew Luckie <mjl@luckie.org.nz>. Tiange Wu contributed an initial implementation of the blind in-window TBIT test to scamper, and Robert Beverly contributed support for testing BGP routers.