



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

NETWORK FLIGHT RECORDER - A NEW TOOL FOR THE WAR

Anthony Kelley

Nov 2000

NFR (Network Flight Recorder available at <http://www.nfr.net>) is an IDS (Intrusion Detection System) that gives the users a powerful tool for the war against illegal access to your network. With the flexibility of this tool, network managers can feel a little better about who is accessing their network and where their employees are going.

HOW DOES NFR WORK? FEATURES OF NFR

The NFR Intrusion Detection Appliance (IDA) is a flexible, extensible, general-purpose tool that addresses both security and network management. NFR uses N-Code that was released to allow the users the flexibility to configure the IDA for their configuration. NFR is a programmable traffic analysis/intrusion detection engine that can be instantly updated when a new attack is discovered. Most IDS like ISS RealSecure or Axent's Intruder Alert/NetProwler require that the vendor send out either an executable from ISS or a signature from Axent. With NFR a user can write their own request order and install it. NFR gives the users a chance to customize the IDA to their needs.

The architecture of NFR was designed as a set of components, each tailored to a specific activity. Data is gathered by one or more packet suckers, forwarded to the decision engine for filtering and reassembly, and possibly recorded to a backend for storage or statistical processing. The query interface is kept completely separate from the input data flow to minimize the performance impact

Of a users querying the system while it is collecting data. The N programming language is a derivation of an interpreted language designed years ago for use in a computer game. The interpreter operates on a byte-code instruction set that implements a simple stack machine. One advantage of this approach is that NFR filters occupy very little memory, yet are quite fast to evaluate. N is a complete programming language including flow control, procedures, variables with scoping rules, and list data types. Unlike many programming languages, however, N has primary data types such as "IP address." Since NFR's may be used on large networks, we chose to implement counter data types as 64-bit integers, to reduce the chance of overflow

CONFIGURATIONS :

NFR can be configured in both distributed and stand-alone configurations. In the stand-alone configuration, a single NFR station gathers and stores information. The distributed configuration places multiple remote stations on the network, and each rolls their data to a central station. Manage, query, and view alerts through the central station and as you network grows, you add a new remote for that segment. You can manage your IDA from any Windows machine on your network. Change system settings, run queries, or view and receive alerts from the location the convenient for you.

HOW CAN YOU MONITOR YOUR SYSTEM?

NFR has alerts that can be configured to popup on the NFR Console. The alerts popup and make a beep on the console which require immediate attention. The alerts are sent to the NFR console and the NFR IDA Recorder. If you are not running the console, you can use the alert viewer to view the alerts at a later time.

Triggers within N-code occur upon receipt or detection of an event that the code is attached to. Events can be triggered with limitations on source, destination, ports, client or server side (if known), or patterns within the TCP stream. The syntax looks like:

```
filter mailtrack tcp (client, dport: 25 ) {
```

The filter above is a simple TCP stream trigger that will monitor the client side of SMTP connections. The "client" and "server" notion is based on the reassembly engines recollection of which system initiated the connection that is being observed.

Keywords that can be placed within an event are:

```
client - from the caller
server - from the called
start: "string" - begin matching
stop: "string" - end matching
opensesion - on start of connection
closesession - on end of connection
port - IP port number (source or dest)
sport - source port
```

dport - destination port
host - source or destination address
net - source or destination network
dst - destination address
src - source address

A typical use is to configure an event to call N code for as small a subset of received data as is practical, then implement any further filtering in N code. To detect spam, for example, you might select TCP traffic for port 25/SMTP.

COMPONENTS :

NFR uses an IDA engine to sniff packets from one or more interfaces on the NFR IDA. Unlike a firewall, NFR IDA engine does not actually touch the packet. It only observes them to be recorded. Events tell the NFR IDA engine to take some sort of action. Events can be a command and control message, passage of time, and an arrival of a packet. Backends is one of the components of the IDA. Within Backends, you will have Filters, which list the event that caused the NFR IDA engine to begin gathering data. Configuration Files provide information about the title of the backend and other information displayed via the NFR console. Recorders write the information gathered by the backends to files. List Recorders collects, records, and maintain a log of activity. Histogram Recorders collects statistical information in many dimensions, rather than the one dimension typically used when gathering statistics. Packages group related types of Backends together. Shared N-Code filters that perform some of the processing for the backends in the package. Configuration files provide information about the title of the package and other information displayed via the NFR console.

1. Marcus J. Ranum, Kent Landfield, Mike Stolarchuk, Mark Sienkiewicz, Andrew Lambeth, and Eric Wall "Implementing A Generalized Tool For Network Monitoring" (31 October 1997)
URL: <http://www.nfr.net/forum/publications/LISA-97.htm>
2. Ken Phillips Eweek "One if by net, Two if by OS" (14 February 1999)
URL:
[wysiwyg://285/http://www.zdnet.com/products/stories/revie](http://www.zdnet.com/products/stories/revie)

ws/0,4161,389071,00.html

3. Deborah Kerr, "New Wave of Intrusion Detection" (20 April 1998)
URL: <http://www.zdnet.com/products/stories/reviews/0.4161.389071.00.html>
4. NFR INTRUSION DETECTION APPLICANCE ver 4.1.1 (1999)
URL: <http://www.nfr.com/products/ida-facts.html>
5. SANS, "How do we compare Intrusion Detection Systems?" (2000)
URL: http://www.sans.org/newlook/resources/IDFAQ/evaluating_IDS.htm
6. Stephanie Steenbergen, "Network flight Recorder releases new network monitoring software", 1 February 1998)
URL: <http://www.sunworld.com/swol-02-1998/swol-02-nfr.html>
7. Barnaby Page, "Network Flight Recorder Demonstrates Leading Intrusion Detection Capability, (16 September 1998)
URL: <http://www.nfr.com/news/press/199809-16-infowarcon.html>

© SANS Institute 2000 - 2005, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event