

[TOOL] iptraffic – A Perl Based Sniffer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0065.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/15/05

To: list@securiteam.com

Date: 15 Mar 2005 16:11:31 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

iptraffic – A Perl Based Sniffer

SUMMARY

DETAILS

iptraffic is an attempt to learn more about network protocols, PERL, and MySQL database by integrating the three components into a useful tool. The goal is to develop a sniffer written entirely in PERL and capture the network traffic into a MySQL database. This will be used to develop network statistics such as protocol distributions and bandwidth utilization. Once that goal has been realized, this tool will be used as a foundation for a statistical anomaly detection engine. The project contains a phased approach:

Phase 1:

Write a PERL sniffer that can identify and decode as many network protocols as the developer can put together. PERL has packages to decode Ethernet, IP, TCP, UDP, ARP, and STP. Phase I will incorporate those protocols.

Phase 2:

Take resulting traffic as its sniffed and parse it into a normalized database schema. The developer have come up with a schema based on the field information provided for each protocol. This is being enhanced as

Securiteam: [TOOL] iptraffic – A Perl Based Sniffer

the developer write more decodes and figure out how to link the various tables together for tracking purposes. Options will exist to send output to Screen, File, and Database.

Phase 3:

Perform analysis of traffic to produce a table of hosts with their provided services. As the table is developed, hosts would be manually verified, and the host/service pairs would then be flagged as "validated". This is a precursor step to developing an Anomaly Detection database. New host/service pairs would be flagged as "anomalies" to be validated. This could provide some level of protection against 0-day exploits.

Phase 4:

Perform analysis of traffic to determine traffic flow across subnets. The goal is to be able to get a high level understanding of traffic patterns to aid the development of network ACLs.

ADDITIONAL INFORMATION

The information has been provided by <mailto:randy.nash@gmail.com> Randy Nash.

To keep updated with the tool visit the project's homepage at:

<<http://www.atriskonline.com/projects/iptraffic.html>>

<http://www.atriskonline.com/projects/iptraffic.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.