NCIRC Security Tools NIAPC Submission Summary

Sniffer Pro

Document Reference: Security Tools Internal NIAPC Submission
NIAPC Category: Network Security Management and Forensics
Date Approved for Submission: 24-04-2007
Evaluation/Submission Agency: NCIRC
Issue Number: Draft 0.01
TABLE of CONTENTS

1  Product ......................................................................................................................................3
2  Category ....................................................................................................................................3
3  Role ............................................................................................................................................3
4  Certification ..............................................................................................................................3
5  Company ....................................................................................................................................3
6  Country of Origin .....................................................................................................................3
7  Web Link ...................................................................................................................................3
8  Overview ....................................................................................................................................3
9  Product Description ..................................................................................................................3
10 Technical Requirements ..........................................................................................................4
11 Limitations ..............................................................................................................................4
12 Evaluation/Review Conclusions/Comments: ......................................................................4
1 Product
Sniffer Pro, versions 4.5.

2 Category

3 Role
Monitoring of network traffic in real-time.

4 Certification
This product has not undergone certification.

5 Company
Mcafee Inc (formerly Network Associates)

6 Country of Origin
USA.

7 Web Link
http://www.networkgeneral.com/
Note that this product has reached end-of-life.

8 Overview
Briefly describe the usage context/s for the use of this tool.

9 Product Description
Sniffer Pro High-Speed is a portable fault and performance management tool from Mcafee specifically designed for troubleshooting and optimizing high speed corporate networks, including client/server applications over cell-based networks. Its monitoring and advanced diagnostic capabilities observe your high-speed network, confirming connection setups and automatically decoding ATM transport and LAN protocols - helping avoid downtime and maximizing network efficiency. With the most complete collection protocol decodes and innovative capturing techniques, Sniffer Pro High-Speed helps uncover high-speed network problems - fast. The Sniffer Pro Portable Analysis Suite is a portable fault and performance management solution that enables network professionals to proactively maintain multi-topology and multi-protocol networks and significantly reduce their network operating costs. Sniffer Pro incorporates Expert Analysis and advanced protocol decodes that automatically zero in on and troubleshoot performance problems on virtually any network. It even recommends intelligent corrective action. Sniffer Pro gives you
more flexibility, more in-depth analysis, and solid market leadership experience. Identifying and resolving network performance problems has never been easier.

Sniffer Pro is a powerful network visibility tool that enables you to:

- Monitor network activity in real time
- Collect detailed utilization and error statistics for individual stations, conversations, or any portion of your network
- Save historical utilization and error information for baseline analysis
- Generate visible and audible real-time alarms
- Notify network administrators when troubles are detected
- Capture network traffic for detailed packet analysis
- Receive Expert analysis of network traffic
- Probe the network with active tools to simulate traffic, measure response times, count hops, and troubleshoot problems

Sniffer Pro is designed to take full advantage of Windows 32-bit multitasking features. You can run multiple instances of the program and its individual tools, and it can run concurrently with other Windows applications. The intuitive Windows user interface makes Sniffer Pro easy to learn and simple to use.

You can use Sniffer Pro on network segments running:

- Ethernet
- Gigabit Ethernet
- Fast Ethernet (100BASE-T)
- Token Ring
- ATM
- WAN/Synchronous
  - RS/V interfaces using the LM2000 adapter.
  - HSSI interfaces using the HSSI adapter
  - RS/V, T1, E1, and ISDN (BRI and PRI) interfaces using the SnifferBook Ultra and a corresponding interface module.
  - RS/V, T1, E1, and ISDN (BRI and PRI) interfaces using the WANBook and a corresponding interface module.

10 Technical Requirements
Runs on MS Windows based machines (NT and above).

11 Limitations
Due to end-of-life product availability is limited.

NITC approval must be sought for use of as this application as inappropriate and misconfigured software can cause severe network infrastructure degradation and data loss.

12 Evaluation/Review Conclusions/Comments: