



Network IPS Testing Requirements

Although network-based Intrusion Prevention Systems (NIPS) have recently entered the commercial marketplace as an important defense component security strategy, methodologies for evaluating these systems are still quite primitive. Few commercial tools are available for evaluating the security functionality of NIPS. The tools for testing NIPS have been expensive and limited in functionality, typically designed for testing other products, such as switches (e.g., SmartBits/ IXIA), server infrastructure (e.g., WebAvalanche), or Firewalls and Intrusion Detection Systems (Firewall Informer or IDS Informer). None of these tools simulate the harsh environment of real networks under attacks.

Introducing the Tomahawk Testing Tool

TippingPoint believes that current commercial tools for testing the network performance of NIPS do not effectively test and report a network's protection. As part of its internal testing and quality assurance programs, TippingPoint has developed a suite of tools for testing our NIPS over the past three years. The Tomahawk Test Suite is the result of this effort and provides a powerful tool for evaluating the network and security performance of NIPS. Tomahawk can be used to evaluate two aspects of NIPS: Network Performance and Security Performance.

Network Testing. Tomahawk can test the throughput of a NIPS using the most realistic mix of protocols possible: one obtained by taking a sample of traffic from the network and replaying it. A single Tomahawk server can generate 200-450 Mbps of traffic. By using multiple servers and aggregating the traffic through a switch, 1 Gbps or more of traffic can be replayed through the NIPS. Tomahawk can also test the connections/second rating of a NIPS. By capturing a packet trace that contains a simple connection setup and teardown (6 packets: SYN, SYN_ACK, ACK, FIN_ACK, FIN_ACK, ACK) and replaying the traffic, a single PC can generate 25-50 thousand connections/second of network traffic. With 3 inexpensive PCs, about 90K connections/sec can be generated, enough to test the limits of any NIPS.

Security Testing. Tomahawk can test the blocking capabilities of a NIPS by replaying attacks embedded in packet traces. Tomahawk reports if an attack completes or is blocked, allowing independent verification of the attack blocking capabilities in a NIPS. By replaying the same attack hundreds of times, Tomahawk can also test how reliably a NIPS blocks an attack. A NIPS that blocks an attack only 9 in 10 times is not worth much in a worm outbreak.

Open-Sourced for Extended Support

TippingPoint provides the Tomahawk testing tool as an open-source package hosted on Sourceforge. Through this open community of developers and network security engineers, the Tomahawk testing tool can translate to new platforms, receive extended testing and development, and reach a broader audience for testing their own network security.

Network Testing:

Background traffic

- ◆ Collect trace from target network, replay with Tomahawk
- ◆ Bottlenecks will show up as performance problem

Connections/sec testing

- ◆ Trace with 1000 full TCP connection setup and teardown
- ◆ Six (6) 64 byte packet connections
- ◆ Trace has 6000 packets
- ◆ Replay 250 copies of trace in parallel
- ◆ 31,000 connections/sec test capability

Security Testing: Blocking

- ◆ Collect trace with attack traffic, replay with Tomahawk
- ◆ If trace completes, attack was not blocked

Repeatability

- ◆ Replay attacks simultaneously: such as 20 PCAPs replayed 10x each for a total of 200 attacks
- ◆ IPS should consistently block or miss all of them

<http://www.tomahawktesttool.org>