

Engineering Issues for an Adaptive Defensive Network

AI Piszcz

703-983-7124 • apiszcz@mitre.org

Army-Contract MOIE

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

MITRE
Technology
Program

Problem

- **CERT and NIPC warn of an increasing number of network attacks from newer and more widespread tools**
- **Distributed Denial of Service**
 - **A multi-source attack whose fundamental objective is to use up resources so that few or none are available**
 - **Current Defenses**
 - **Point firewalls block intrusion**
 - **Sufficient and secure bandwidth must be preserved to support a response**

Background

- **How is the task performed today?**
 - Most organizations are relying on a network single entry point and sensors including monitoring and alarms focused into a network operations center. Working across organizations is a manual process where NOC operators consider options.
- **What are the limitations of current methods or tools?**
 - Response time, human required to initiate action.
- **What is the operational impact of the deficiency?**
 - Coordinated early warning events could mitigate downtime and give the NOC a few more minutes/hours of decision time.

Objective

■ Hypothesis

- A collection of WAN distributed firewalls can cooperate to autonomously interact in the trusted member's VPN/network to provide instantaneous response to DDoS attacks.

■ Experiment goal

- Provide a defense for the first 30-60 minutes of a DDoS attack which will provide continuous service to support the mission

■ Technical Issues

- Cooperating distributed and trusted firewall network will provide adaptive behavior based on anomaly detection and other triggers. Second adaptive response will interact with quality of service parameters to maintain network availability.

Activities

■ Tool Development

- **NETRECON: Captured and Visualized Standard Traffic Patterns**
- **Developed Automated Attack Tool and Analysis Suites**

■ Technique Testing

- **Examined Out of Band Control and Failover**

■ Product Evaluations

- **Created a compendium of DDoS mitigation/prevention products**
- **Evaluated Click Router, MULTOPS, TopLayer, PeakFlow, 3Com Adaptive Firewall Cards and a Product X Integrated DDoS Appliance/Firewall**

Highlight

■ Hypothesis and Goal

- collaborate with G2x sensors and deliver TCP/IP and other session information to other projects, tools including DDoS sensor techniques
- evaluate of potential DDoS tools to detect signature traffic (theoretical plan) ADN attack lab -> DMZ -> formal adoption as a MITRE tool
- gain experience with live network traffic volumes and monitor a realistic network for DDoS events

■ Status

- Configured firewall rules
- Delivered NETRECON and platform to G2x
- Collecting data, developing visualization tools

Highlight/Demonstration

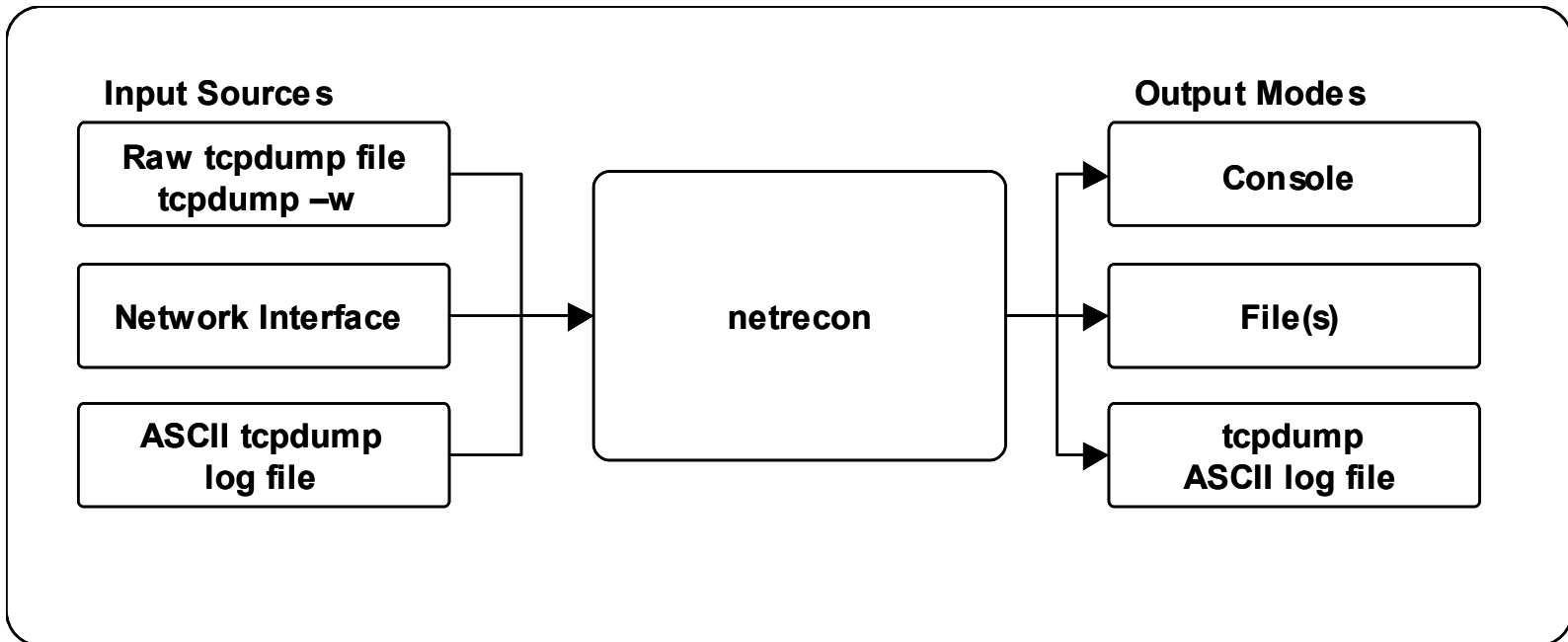
- Perl ~ 2000 lines

- Time::HiRes
- IO::File
- AppConfig

- Input provided as command-line pipe from tcpdump

- Output

- Connection summary information
- tcpdump pos-processed logfile (ASCII human readable)
- TCP connection state



Impacts

■ Analysis Performed

- Initial characterization of network traffic
 - Interest in NETRECON, both internal and external to MITRE
- Evaluated tools and provided feedback to vendors/developers who have incorporated our suggestions

■ Deliverables

- NETRECON to ISIS
- White Papers on each of the products analyzed and tools developed

Future Plans

- **Continued study of network traffic patterns**
 - **Use this in development of anomaly detection and other intrusion detection tools**
 - **Enhancement of visualization tools**
- **Further research into related areas**
 - **Border Gateway Protocols**
 - **Gigabit LANs**
 - **MPLS**