

Intrusion Detection: Principles and Practice – Vern Paxson

Why Network Intrusion Detection?

Why Not?

Styles of Approaches

An Example of a Network Intrusion Detection: Bro

Detecting activity: sniffers, stepping stones and backdoors

Network Equipment Tracking System (NETS) – James Rothfuss

Protection Concepts

NETS Vision

Current Implementation

Future Development and Integration

Components of good protection – Bill Kramer

Policy and Procedures

Good Systems Protection

Response teams

Other “best practices”

Deployment in an Open HPC Environment – Stephen Lau

Deploying security in an HPC environment

Defense in Depth

Tools for deployment

Firewalls, scanning, virus protection, etc.

Limitations / benefits

Incident Response

Bro at SC2003

Bro as SCinet’s IDS

Demonstration of statistics collected by Bro at SC2003