California State University
Northridge

University Procedure for Excessive Flows

Purpose

The purpose of this procedure is to define what the campus considers Excessive Flows and the actions taken to protect the campus network from such an offense.

Procedure

As an adjunct to the “University Policy for Use of Computing Resources”, the campus is proposing a procedure for excessive flows.

The number of simultaneous flows considered excessive is approximately 200 for any computer not identified as a campus server.

Examples of the excessive flow activity include Denial of Service (DOS) attacks targeted at the campus network and servers initiated from off campus networks. There are also DOS attacks to off-campus networks and servers initiated from our campus network.

Tools used to identify any of the above stated attacks are Bandwidth Management, Firewalls, and Intrusion Detection Systems (IDS).

Once identified, the computer is quarantined. In the case of a total subnet used for an attack, the data virtual local area network (VLAN) interface is administratively shutdown. Notification of the offense and action taken will be reported to the University Helpdesk and/or Operations. The University Helpdesk will attempt to notify the appropriate local IT staff.

To reconnect a quarantined computer to the CSUN network, the IT staff must submit a Technology Service Request (TSR), with appropriate billing information and approvals, stating the steps taken to resolve the problem. If a reconnected computer continues to present a

problem and is re-quarantined, a technician from the Technical Equipment Services (TES) branch of Information Technology Resources (ITR) will assist the local IT staff to address the problem. Relevant service charges will be applied to the submitted TSR.

For further information, contact:

Chief Technology Officer
Information Technology Resources
cto@csun.edu

Reference

Section 502 of the California Penal Code entitled "A Comprehensive Computer Data Access and Fraud Act".

University Policy for Use of Computing Resources

Security Attack