

1 Incoming Attacks

The University of Maryland network receives on a daily basis **17 millions** TCP connections directed to non-existent hosts.

The goal of this research is to study network threats by replying to these connections with unused computer resources (**honeypots**)



3 Data Analysis

Attacks are analyzed at several levels:

- **Reconnaissance**: when attackers try to discover vulnerable systems
- **Exploit**: when attackers try to compromise targeted systems
- **Usage**: when attackers control compromised systems

Top Attacked Ports and Services	
TCP/22	SSH Server
TCP/2967	Symantec Antivirus
TCP/1433	Microsoft SQL Server
TCP/80	Web Server (IIS, Apache)
UDP/1026	Microsoft Messenger Spam
TCP/5900	VNC Server

2 Honeypot Architecture

