

LIS 385T.6 – 2.07.00

Information and Network Security

Issues & Questions

- Hands on demos
- Final Project

Networking Basics - Hardware

- LAN specifications
- CSMA/CD
- Utilization and Design (another 80/20 example)
- NIC Cards
- Cables
- Hubs
- Switches
- Routers

Networking Basics - Software

- Clients and Servers
- Remote Access
- File Transfer
- Email
- Web Browsers
- Sniffers
- Scanners
- Back-doors, Trojans, and rootkits

Supplemental Reading

- www.symantec.com and www.nai.com (virus databases)
- www.cert.org (The Computer Emergency Response Team)
- www.securityfocus.com (bugtraq vuln archive)
- www.cerias.purdue.edu/coast/coast.html (COAST @ Purdue)

Preparation for Next Week

Readings for the week:

- *Maximum Security*: Chapters 5,6

Topic Paper 2 - Guidance

- Topic – Network Vulnerabilities
- 5-7 page research paper equivalent
- Research one of the following network/host vulnerabilities
 - Viruses - Nimda (any variant), Melissa (any variant), SirCam (any variant)
 - Backdoors – BO2K, Sub7, NetBus
 - Specific service or app vulnerability (use bugtraq – more research)
 - Buffer Overflow vulnerabilities (more technical)
 - Distributed Denial of Service (DDoS) – General concepts (more technical)
- Give me the basics – what it is, how it works, what it does, how to fix...
- DUE – February 21, 2002